

APPENDIX B: SCHEDULE OF TRANSCRIPT REFERENCES

TABLE OF CONTENTS

DAY 2.....	3
CROSS-EXAMINATION OF DR CRAIG WRIGHT BY JONATHAN HOUGH KC	3
DAY 3.....	36
CROSS-EXAMINATION OF DR CRAIG WRIGHT BY JONATHAN HOUGH KC	36
DAY 4.....	68
CROSS-EXAMINATION OF DR CRAIG WRIGHT BY JONATHAN HOUGH KC	68
DAY 5.....	116
CROSS-EXAMINATION OF DR CRAIG WRIGHT BY JONATHAN HOUGH KC	116
DAY 6.....	156
CROSS - EXAMINATION OF DR CRAIG WRIGHT BY JONATHAN HOUGH KC	156
DAY 7.....	199
CROSS - EXAMINATION OF DR CRAIG WRIGHT BY JONATHAN HOUGH KC	199
DAY 8.....	251
CROSS - EXAMINATION OF DR CRAIG WRIGHT BY JONATHAN HOUGH KC	251
DAY 9.....	321
CROSS - EXAMINATION OF DR IGNATIUS PANG BY JONATHAN HOUGH KC.....	321
CROSS - EXAMINATION OF MR ROBERT JENKINS BY JONATHAN MOSS.....	327
RE - EXAMINATION OF MR ROBERT JENKINS BY LORD GRABINER KC	338
CROSS - EXAMINATION OF MR ROBERT JENKINS BY JONATHAN MOSS.....	339
CROSS - EXAMINATION OF MR SHOAIB YOUSUF BY JONATHAN MOSS	342
DAY 10.....	349
CROSS - EXAMINATION OF DANIELLE DEMORGAN.....	349
CROSS EXAMINATION OF MARK ARCHBOLD	349
CROSS - EXAMINATION OF CERIAN JONES	351
DAY 11.....	361
CROSS-EXAMINATION OF DAVID BRIDGES BY JONATHAN HOUGH KC	361
CROSS-EXAMINATION OF MAXWELL LYNAM BY JONATHAN HOUGH KC.....	366
CROSS-EXAMINATION OF STEFAN MATTHEWS BY JONATHAN HOUGH KC.....	374
DAY 12.....	417
CROSS - EXAMINATION OF STEFAN MATTHEWS BY JONATHAN HOUGH KC.....	417
MR JUSTICE MELLOR QUESTIONS FOR MR STEFAN MATTHEWS	449
RE-EXAMINATION OF MR STEFAN MATTHEWS BY LORD GRABINER KC.....	451
CROSS - EXAMINATION OF MR STEVE LEE BY LORD GRABINER KC	452

Appendix B: Schedule of Transcript References

DAY 13.....	454
CROSS-EXAMINATION OF MR MARTTI MALMI BY CRAIG ORR KC	454
QUESTION FROM MR JUSTICE MELLOR TO MR MARTTI MALMI.....	457
CROSS-EXAMINATION OF DR ADAM BACK BY CRAIG ORR KC	458
DAY 14.....	468
CROSS-EXAMINATION OF MICHAEL CHRISTOPHER HEARN BY LORD GRABINER KC	468
CROSS-EXAMINATION OF DR HOWARD HINNANT BY CRAIG ORR KC.....	472
RE-EXAMINATION OF DR HINNANT - JONATHAN HOUGH KC.....	473
CROSS-EXAMINATION OF ZOOKO WILCOX-O’HEARN	475
DAY 15.....	479
CROSS-EXAMINATION OF DR WRIGHT BY JONATHAN HOUGH KC	479
CROSS-EXAMINATION OF DR WRIGHT BY MR GUNNING KC	499
DAY 18.....	528
CROSS-EXAMINATION OF MR ZEMING GAO BY MR HOUGH.....	528
DAY 19.....	545
CROSS-EXAMINATION OF DR CRAIG STEVEN WRIGHT BY MR HOUGH KC.....	545
RE-EXAMINATION OF DR WRIGHT BY MR ORR KC IN RELATION TO THE DRAFT TRANSCRIPT AT {Day19/18:17}.....	559
QUESTIONS FROM MR JUSTICE MELLOR IN RELATION TO THE DRAFT TRANSCRIPT AT {Day19/30:18}.....	559
FURTHER CROSS-EXAMINATION OF DR WRIGHT BY MR HOUGH KC.....	561

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
DAY 2		
CROSS-EXAMINATION OF DR CRAIG WRIGHT BY JONATHAN HOUGH KC		
Dr Wright’s position on COPA’s forgery allegations		
{Day2/14:8-15}	<p>MR HOUGH: Dr Wright, have you ever forged or falsified a document in support of your claim to be Satoshi Nakamoto?</p> <p>A. No.</p> <p>Q. Have you ever knowingly presented a forged or falsified document in support of your claim to be Satoshi Nakamoto?</p> <p>A. I have not.</p>	<p>Dr Wright states, on oath, that he has never forged or falsified a document in support of his claim.</p>
{L2/245} Mr Madden’s Appendix PM6 - JSTOR Article		
{Day2/16:10-22}	<p>Q. Is it right that you were holding up this article to demonstrate your interest in Nakamoto dating from that time?</p> <p>A. I was holding up the article to basically reference Nakamoto’s origin and the I guess name origin.</p> <p>Q. You were doing so to show you’d had that interest in Nakamoto as the basis for the Satoshi Nakamoto pseudonym?</p> <p>A. I was saying that’s why it was chosen, yes.</p> <p>Q. Now, can you see and accept just from the image here that in the date, 05/01/2008, the numerals 08 are slightly smaller than the numerals 20?</p> <p>A. I can.</p>	<p>Dr Wright admits that the JSTOR article numbers look different.</p>
{Day2/17:10-13}	<p>Q. But you’ve always maintained that this is, to your knowledge, an authentic document, not one that’s ever been tampered with?</p> <p>A. I have no knowledge of it being tampered with.</p>	<p>Dr Wright confirms that he has no knowledge of the JSTOR article being tampered with.</p>
{Day2/18:10} - {Day2/19:18}	<p>Q. May we now go to {H/40/1}. Now, this is an appendix to Mr Madden’s first report where he addresses this document. I’m going to put some of his findings to you for you to comment on. Page 3, please {H/40/3}. He makes some observations about the document. We can</p>	<p>Dr Wright accepts Mr Madden’s findings in respect of ID_004019 {L2/245}.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>see that he’s referring to it. It’s a document numbered ID_004019. What I want to put to you is on {H/40/4}. If you show the whole page on screen. He identifies irregularities in the numerals in the accessed date and time with the numerals “08” not being aligned or the same size as the “20” figure. Again, would you accept that as a matter of visual impression?</p> <p>A. Yes.</p> <p>Q. And if we go over the page {H/40/5}, he also identifies irregularities in the ”11:17” with the ”11” and the ”17” being visibly different. Again, would you accept that as a matter of visual impression?</p> <p>A. I would.</p> <p>Q. Mr Madden also analysed a publicly available version of the document which he found on the Wayback Machine, and we can see that at {H/44/1}. Now, this is a document Mr Madden says was captured on the Wayback Machine in 2016. Do we see that that has a date on the front, “Accessed: 05/01/2015”?</p> <p>A. I see what it says, yes.</p> <p>Q. And then may we go back to his report at his appendix PM6 at {H/40/22}, and in the upper half of the page, he compares the figures on this version with the figures on the version you held up. Would you accept, again, just as a matter of visual impression, that the figures in the date from the 2015 version are aligned by contrast with those on your document?</p> <p>A. Yes, I see they’re aligned.</p>	
<p>{Day2/20:11} - {Day2/21:6}</p>	<p>Q. He's comparing footers from documents downloaded from the JSTOR database, isn't he?</p> <p>A. There's not a - - sorry, there's not a JSTOR database. There are multiple repositories. Each of these, including the Nipponica, are held separately and update separately, so you cannot take one from one era and compare it. So, no, I don't agree.</p> <p>Q. Have you or your expert identified any JSTOR documents from any repository with a footer matching yours in form which is dated to the 2008 era?</p> <p>A. I don't know what Mr Placks has done, but other documents had ones like mine, yes.</p> <p>Q. I'm going to suggest to you - - and no doubt I can be corrected on this if I'm wrong - - that no document from the JSTOR database with a footer matching yours authentically from the 2008 era has been provided. Are you able to agree or disagree with that?</p>	<p>When asked about whether any JSTOR documents have a footer matching that produced by Dr Wright from 2008, Dr Wright produces a new excuse and seeks to rely on privilege where it is not applicable.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. I disagree.</p> <p>Q. But you're not able to identify the document?</p> <p>A. No. I can't really discuss what has been done in privilege with lawyers.</p>	
<p>{Day2/21:7} - {Day2/23:8}</p>	<p>Q. Now, Mr Madden's conclusion is that the document which he found captured in 2016 was a likely source of your document, that's to say a publicly available document with the access date and time matching those of your document other than the irregular figures. Do you agree or disagree with that conclusion?</p> <p>A. I completely disagree. The document that he has sourced is from Gwern. Gwern was an individual who worked with Ira Kleiman to out me in 2015. Ira Kleiman had been shown that document in 2014. Gwern produced it with helping people as part of the 2015 doxing, where he provided information to WIRED and Gizmodo. So that document was provided to Ira Kleiman in 2014.</p> <p>Q. So this document, dated 2015, was provided to Ira Kleiman in 2014?</p> <p>A. No, my document was provided to Ira Kleiman. Gwern, who basically put things out to WIRED, provided that and put it up there afterwards.</p> <p>Q. So your document from 2008, which nobody's found directly on the internet, was put out to - - from Gwern to Ira Kleiman; correct? Is that what you're saying?</p> <p>A. I'm saying that Gwern loaded it, and you shouldn't find it on the internet because that's actually a breach of copyright. It's a document owned by JSTOR, and loading it and publishing it that way is actually a breach of the intellectual property associated with that document.</p> <p>Q. Your account then is that the document which was captured in 2016 bearing a date of 2015 was a manipulated document; is that right? Is that what you're saying?</p> <p>A. I'm saying it was loaded on that date by Gwern, who put these things up.</p> <p>Q. And why are you saying that was done?</p> <p>A. Part of all of this with Mr Kleiman was to try and discredit me. Other people involved in COPA were also part of this, including Mr Maxwell.</p> <p>Q. But it wouldn't be a very effective way of discrediting you to do this before you had made the public commitment, in December 2019, that this document which you were holding up was the source of the Satoshi pseudonym, would it?</p>	<p>Dr Wright produces a new excuse, attributing the irregularities in ID_004019 to an individual named Gwern, and Ira Kleiman.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. It would, actually, because I'd already spoken to Ira Kleiman in 2014 and Ira Kleiman had already started planning his case against me. On top of that, the idea was to try and discredit me by putting me out into the media and then having people immediately, within 3 minutes, try and discredit things saying that some of my - - my papers were false, etc. As an example, Mr Maxwell, minutes after WIRED produced things, had a double digit length paper discrediting falsely my PGP keys that were done seconds after the articles went up, something that would take days to write.</p>	
<p>{Day2/23:9} - {Day2/24:3}</p>	<p>Q. Well, we're not going to address that latter point now, but what I am going to address with you is this. Your account is that your document with the 2008 date numbers misaligned is the authentic document, whereas the document with the numerals properly aligned is a document that's been planted for use against you; correct?</p> <p>A. What you're arguing is a printout on a cheap printer has misalignment, which is correct. Printers do that. If you edit a PDF, you don't change fonts. So what Mr Madden has failed to note is, if I went in with, say, Soda or Adobe and I edited, my Lord, a document, there is no way that you will naturally change the font. The font only will change if you do something like printing it. So, the argument not being presented by Mr Madden is very simple. He has failed to note that a printout that has been scanned isn't a native PDF.</p> <p>Q. That's not a point made by your expert, is it, in relation to this document?</p> <p>A. I don't know what my expert's done.</p>	<p>Dr Wright blames the misalignment on a "cheap printer". Dr Wright also states that he does not know what his own expert has done in relation to this document.</p>
<p>{Day2/24:4} - {Day2/25:8}</p>	<p>Q. The reality is that this is a document which you edited, as Mr Madden established, from a publicly available version to suggest an interest in Tominaga Nakamoto from 2008?</p> <p>A. I also presented this to people at the Australian Stock Exchange in 2013 when I was talking to them. I mentioned it to Ira Kleiman, so I can tell you the exact source of why that's out there is Mr Ira Kleiman and Gwern.</p> <p>Q. You've never - again, you can tell me if I'm wrong and then this can be checked, but you've never provided any evidence in support of any of those propositions that you provided this document to the Australian Stock Exchange or that Ira Kleiman received it, have you?</p> <p>A. I have no evidence that I've shown it to someone at the - - at there, but I have noted this for the Kleiman case that I showed a variety of documents, including this one. So</p>	<p>Dr Wright states that ID_004019 was received by Ira Kleiman; he has presented no documentary evidence to support this claim.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>in the Kleiman case, where I was talking about this as my evidence, that is because 'd given it to Ira Kleiman.</p> <p>Q. But there's no evidence, is there, that you - - for example, an email, that you provided this specific document to Ira Kleiman, is there?</p> <p>A. I don't know if there's something in relativity or not. I don't have any of my earlier emails. A lot of my data's been lost, a lot of i's been deleted, and finding things in relativity is very difficult. So my answer is very simple: this came from Gwern. Gwern is part of the outing in 2015 that doxed me.</p>	
{Day2/25:9-17}	<p>Q. The answer is much simpler: this is a document forged by you as part of the origin myth, isn't it?</p> <p>A. If I'd forged that document then it would be perfect. It's very simple. If you go into Adobe, my Lord, and I change everything, there's not going to be a font error. The curve that you note, or don't note, where things aren't printed correctly because there's a curve doesn't happen apart from print errors. So I'm sorry again, that's false.</p>	<p>Dr Wright states that if he had forged a document, it would be perfect, and then proceeds to explain to the Court how he would hypothetically forge a document.</p>
<p>{L14/451} Evidence and Law by Craig Wright (Bitcoin SV is Bitcoin.)</p>		
{Day2/26:16} - {Day2/27:25}	<p>Q. Page 3 {L14/451/3}: "I used AnonymousSpeech.com for many years, and held copies of the SecureAnonymousSurfing software. I started using it when I was investigating malware breaches and peer - to - peer copyright violations. It enabled me to track and analyse people breaching software licenses and media licenses and such people who were attacking my clients, that is, cyber criminals. I used the service as it stopped the cyber criminals from being able to find out who I really was. "This is the source of Vistomail and registration of the domain bitcoin.org." Then over the page {L14/451/4}: "What you don't realise yet is that I used my credit card. Yes, as crazy as it might seem to you, I used my credit card to purchase anonymous services. I even claimed it on my tax." And so on. You wrote that, did you?</p> <p>A. I did.</p> <p>Q. Now over the page to {L14/451/5}, please, middle of the page: "Argue all you want about the nature of evidence, but there is one simple point I can categorically prove: "The source of the funds that went to pay for the bitcoin.org domain registration on AnonymousSpeech... derived from my credit card. More importantly, the same</p>	<p>Dr Wright corroborates statements made in his blog post, {L14/451}, stating that he has credit card payment records for the purchase of the Vistomail address and bitcoin.org domain registration from Anonymous Speech {L14/451}.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>records remain current and valid." You wrote that, did you?</p> <p>A. Yes, I did.</p> <p>Q. So you were saying that you'd obtained the Vistomail address and the bitcoin.org domain registration from Anonymous Speech with a credit card payment for which you had records?</p> <p>A. I did.</p>	
<p>{O4/25/35} Fred Schebesta interview with Craig Wright (Who created Bitcoin? Craig Wright reveals alleged contributors for the first time)</p>		
<p>{Day2/28:6-20}</p>	<p>Q. If we go down to {O4/25/34}, please. Go down to letter F. Do we see that, after a discussion of cryptographic proof, you're recorded as saying: "Proof is something simple, like a credit card statement saying that you actually bought the Bitcoin.com - - sorry, Bitcoin.org domain, but not Bitcoin.com, and paid for the Satoshi email account ..." Do you recall that is something you said?</p> <p>A. No, this was transcribed incorrectly.</p> <p>Q. Okay, well, we can bring up the video after a break, but what do you say was said wrong - -</p> <p>A. It's close, but it's not quite right.</p> <p>Q. What do you say is wrong?</p> <p>A. Just the way that it's written. Some of the things are wrong. But it's close enough.</p>	<p>Dr Wright is evasive, he initially claims that the transcript is incorrect, then concedes that it is 'close enough' when COPA's counsel offers to produce the video.</p>
<p>{H/78/1} Appendix PM17 to Mr Madden's First Report</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day2/30:10} - {Day2/31:11}</p>	<p>Q. The number at the top of the email, the number consisting of four sets of four digits, is that a credit card number?</p> <p>A. I don't know. It's not mine. I mean, what I'm saying, "my old credit card", this isn't actually a credit card, it was a debit, so where this is linked is - - is wrong. What I was sending to Jimmy is what I got from Amanda, basically it was a summary of information.</p> <p>Q. We'll come to that in a moment, but you're saying it's a debit card number, are you?</p> <p>A. I had a debit card number, but this was put down in the message to Amanda as my old credit card.</p> <p>Q. We see that the email says: "Anonymous Speech is vistomail." Then that number which is at the top of the screen: "... is my old credit card." Was that the number for your old credit card?</p> <p>A. No, I had a debit card, and that was actually cancelled in 2005. So this was part of why I was pointing out the problem.</p> <p>Q. So you were writing, "This number is my old credit card", to say that that was a number that wasn't associated with any credit card you'd ever held?</p> <p>A. I was doing a point form of what Amanda had received, which basically said, from an anonymous Reddit person, that this was my old credit card buying the Bitcoin domain.</p>	<p>Dr Wright is presented with an email from himself (craig@rcjbr.org) to Jimmy Nguyen from 10 June 2019 in which he purports to provide his old credit card information. Dr Wright is evasive, he states that the number in the email is not that of his old credit card.</p> <p>Later, at {Day2/81:20} - {Day2/82:12} Dr Wright is presented with evidence that directly refutes his assertion that he cancelled his credit card in 2005.</p>
<p>{Day2/32:10} - {Day2/33:2}</p>	<p>Q. Just to be clear with the answer you have just given, you say that you did purchase the Satoshi Vistomail email and bitcoin.org with your Westpac credit card?</p> <p>A. No, I said I purchased the Anonymous Surfer VPN software and I applied payments to that site until 2006 using Westpac. After 2006, I used my WebMoney New Zealand account.</p> <p>Q. So you're saying you used your WebMoney New Zealand account to purchase the Vistomail domain and the bitcoin.org domain?</p> <p>A. Yes. The New Zealand company ran a credit/debit card system linked to Liberty Reserve. In some of my communications with Martti Malmi, which is in his emails as well, I explained Liberty Reserve, I explained WebMoney and I helped him set up an exchange where he actually linked that the same way I'd been doing this. This isn't the first time I've said it. In my 2020 blog, I explained Liberty Reserve and WebMoney.</p>	<p>Dr Wright changes his story in relation to the purchase of the Satoshi Vistomail email and bitcoin.org, stating that he purchased them using his WebMoney New Zealand account linked to Liberty Reserve.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{H/78/2} Appendix PM17 to Mr Madden’s First Report - NAB Screenshots</p>		
<p>{Day2/33:3} - {Day2/35:20}</p>	<p>Q. Next page, please {H/78/2}. You see that you had included in that email a screenshot which appears to show a credit card transaction from the number in the email to Anonymous Speech of \$687.</p> <p>A. I do.</p> <p>Q. And I suggest to you the natural meaning of this email in the context of your article and your interview is that you're putting forward those documents as the banking records showing your purchase of the Satoshi Vistomail account.</p> <p>A. No, I was pointing out the falsity of it because Amanda had received these and we needed to answer that question, because any even adverse documents need to go into court.</p> <p>Q. Let's go through your story. You claim that these screenshots were sent to you by your US law firm, specifically by Amanda McGovern, in the context of the Kleiman litigation?</p> <p>A. Yes.</p> <p>Q. You first made this claim after Ms McGovern had died, didn't you?</p> <p>A. I didn't plan her dying, and I didn't have any other - - there was nothing to respond to. So, no, I didn't make this claim first. This was part of the Kleiman litigation. In privileged communications with Jimmy, which, if you look at the other emails in this thread, basically support that, saying to take this offline to communicate.</p> <p>Q. You first gave this account which you're now giving in any sort of public forum after Ms McGovern had died, didn't you?</p> <p>A. I don't discuss my legally privileged communications in public forums. This only came out because Ontier accidentally released privileged documents.</p> <p>Q. Is the answer to my question "yes"?</p> <p>A. It depends on what you consider a public forum. It was mentioned in the Kleiman litigation. Some of that was in a closed court, but that is still public.</p> <p>Q. So you're saying that the story of these screenshots being sent to you was mentioned in the Kleiman litigation in court?</p>	<p>Dr Wright claims that he first received the NAB screenshots from his lawyer Amanda McGovern who has since died, and that he told various solicitors that these screenshots were false.</p> <p>Dr Wright has not provided any proof that he gave this account prior to Ms McGovern’s death. He then states that the documents were accidentally disclosed in these proceedings by Ontier.</p> <p>Dr Wright goes on to claim that he has been told not to name the solicitors/attorneys to whom he told that the NAB screenshots were false. Mellor J requests that he should identify them, but Dr Wright cannot recall other than “Jonny”, who is a Sikh corporate lawyer.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. I don't know if it was in public. Some of the things we had in Kleiman were closed.</p> <p>Q. Are you saying that the account you have given of these screenshots being dumped on you was something said in the Kleiman litigation in court, bearing in mind that this can be checked, even if it was in a closed session?</p> <p>A. I told my various solicitors, including other ones, both in Rivero and otherwise, this was false.</p> <p>Q. Who do you say you told that this was false? Just Ms McGovern or other individual lawyers?</p> <p>A. I told other individual lawyers, but I've been told not to name solicitors or attorneys, so I don't know ... Do I or don't I, my Lord?</p> <p>MR JUSTICE MELLOR: You should identify them. If they told you not to reveal something, you should identify them.</p> <p>A. Johnny - - I probably don't remember Johnny's name, I haven't dealt with him in a while - - he's a Sikh Jonny has not got back to us. Can I get back to you on his last name?</p> <p>MR JUSTICE MELLOR: Which firm was he from?</p> <p>A. He's an American firm that was basically dealing with one of the American entity companies. He's a corporate lawyer. But I can get his name next break very quickly, I just can't remember it off the top of my head. Jimmy Nguyen, Amanda McGovern and one of her juniors, but I can't - - if I can get back to you on the name of the junior as well.</p>	
<p>{Day2/35:21} - {Day2/36:12}</p>	<p>Q: And you say, don't you, that they were sent to you by WhatsApp?</p> <p>A. I said that they were sent to me, I believe, by WhatsApp, yes. I can't recall exactly, but I don't have any other applications any more, I don't have Facebook, I don't have anything else, so it would be WhatsApp.</p> <p>Q. And you don't have the WhatsApp message captured anywhere?</p> <p>A. No, I don't.</p> <p>Q. You say that the screenshots had been sent to Ms McGovern using a direct message from a pseudonymous Reddit user whose identity remains undisclosed; is that right?</p> <p>A. That's what she told me, yes.</p> <p>Q. You've never provided, have you, a copy of the Reddit message?</p>	<p>Dr Wright alludes to the existence of a Reddit message via which Ms McGovern received the NAB screenshots, notably he has not produced any documentary evidence of this hearsay evidence (although he claims that he has it, but has chosen not to disclose it).</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. There was no reason to.</p>	
<p>{Day2/39:7-18}</p>	<p>Q. When your lawyers in these proceedings disclosed this document, this email, they didn't mention, did they, that it was a set of false documents which had been planted on you?</p> <p>A. They didn't mention that it was a privileged communication either.</p> <p>Q. Well, answer the question that I'm asking, please. When your lawyers disclosed these documents in these proceedings, they didn't mention that they were false documents which had been planted on you, did they?</p> <p>A. I have no idea what Ontier did. I do know that they didn't tell you that they were privileged.</p>	<p>Despite signing a disclosure certificate in which he relied on privilege as a basis for withholding production of documents {K/4/7}, Dr Wright states that the NAB screenshots were in fact privileged and therefore wrongfully disclosed by Ontier.</p>
<p>{Day2/40:12} - {Day2/41:13}</p>	<p>Q. When did you first - - well, do you say that you told Ontier materially, before September 2023, that these documents were fakes?</p> <p>A. Yes.</p> <p>Q. And Ontier then sat on that information and didn't tell the other parties; is that what you're saying?</p> <p>A. I have no idea what Ontier did.</p> <p>Q. But if the other parties weren't told by Ontier, they were sitting on that information and allowing the other parties to be misled; that's right, isn't it?</p> <p>A. I have no idea what Ontier did.</p> <p>Q. Now, you're aware, aren't you, that Mr Madden's first report established that these screenshots had to be inauthentic, including because the NAB records couldn't have been accessed after more than ten years? You're aware of that, aren't you?</p> <p>A. That's actually not correct. In Australian law you can actually access records because they're connected to a home loan. So, my Lord, what he's doing is reporting under the credit history, but in Australia, when it is associated - - and these were connected directly to the home loan, it's 25 years. So the records were legally required to be kept 25 years, not because they're a credit card, but the other. But despite that, I agree, they are not real, but it's not real for the wrong reason.</p>	<p>Dr Wright blames his previous law firm Ontier for allowing fake documents into the proceedings and allowing the parties to be misled. Notably this is not the first time Dr Wright has blamed Ontier. Ontier have previously denied allegations of advice Dr Wright has purported to have received from Ontier, see for example {M/2/691}.</p>
<p>{Day2/42:1-14}</p>	<p>Q. What happened is that you forged or had someone forge these screenshots to provide proof of your purchase of the Vistomail domain, didn't you?</p>	<p>Dr Wright produces a new excuse that cannot be verified, as he blames a</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. No. As I stated, the purchase of the Anonymous Speech software was done, my Lord, by Westpac. Those are in evidence. That shows me buying from that company for several years. What I don't have, that I wanted to get, is the WebMoney New Zealand account, because unfortunately that company has gone into liquidation.</p> <p>Q. You claimed, in April 2019, that you had credit card records to demonstrate your purchase of these domains didn't you?</p> <p>A. Yes, at that stage, the New Zealand company was still active and had not liquidated.</p>	<p>company that has since gone into liquidation.</p> <p>The WebMoney New Zealand account was not mentioned in the Disclosure Review Document as an inaccessible source. The company was active for years after Dr Wright's doxing, however he did not attempt to capture accurate credit card records despite the evidentiary value these would have had.</p>
<p>{E/4/10} - Fourth Witness Statement of Dr Wright</p>		
<p>{Day2/45:15} - {Day2/47:11}</p>	<p>Q. May we have {E/4/10} on screen, please. So this is the tenth page of your fourth witness statement. Paragraph 16, you say: "Returning to creating the Bitcoin.org Website, I do not recall how I purchased the domain name. I had various payment methods available to me then, including accounts with Liberty Reserve and overseas credit cards from companies I formerly operated. If I were to have used by Liberty Reserve account, I may have used LRD ..." And so on. So when you wrote that witness statement in October last year, you couldn't remember the payment method, could you?</p> <p>A. Like I said, I used the other. But WebMoney, natively, LRD are two different things. So when I'm saying I used one of the cards, I didn't say I used a particular card. I don't recall which one. I know that it was a WebMoney account; that could be WebMoney directly, it could be Liberty Reserve tied to it, or it could be one of a number of Visa and Mastercards that were tied by that company.</p> <p>Q. You said in your fourth statement that you couldn't remember the payment means and you've now remembered it by the time of your evidence, haven't you?</p> <p>A. No, that's exactly the same. I just said I don't remember which particular card I used, so that's still ...</p> <p>Q. No, you're saying here that you couldn't remember, from a whole range of payment methods, rather than you can remember the level of detail which you've told the court today.</p>	<p>Dr Wright is evasive, failing to directly answer to the discrepancies between his evidence in his Fourth Witness Statement and before the Court on Day 2.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Let me give you an analogy. I have a Wise account now. In Wise, I have a euro, a US dollar and a GBT - - B - - sort of account. If I use Wise, that doesn't mean I'd know which - - a year later, which particular payment account I used.</p> <p>Q. And the reason that you have come up with this recollection in court today is to make sense of what you had said in April 2019, that you had the records to prove it, which conveniently then fell out of your access?</p> <p>A. No, the company closed. As I noted in one of my other witness statements, the company closed, so I cannot now grab which particular account I used, or exactly where the funds came, whether it was WebMoney or Liberty Reserve direct.</p>	
<p>{Day2/47:12} – {Day2/48:14}</p>	<p>Q. Carrying on in this statement, may we look at paragraph 19, towards the bottom of the page. You say here: “With regard to Vistomail, Simon Cohen, then a Managing Associate at Ontier LLP, accessed my Vistomail before it was discontinued. When he did, I understand that he saw records and communications pertaining to the purchase and operation of the bitcoin .org domain and site. For the avoidance of doubt, my solicitors have asked me to emphasise that this is not a waiver of privilege. Mr Cohen has never provided written confirmation of that story by a statement or any other means, has he?</p> <p>A. No.</p> <p>Q. If the story had been true, it would have been straightforward to have your former solicitor confirm it, wouldn't it?</p> <p>A. No, it wouldn't, because I fired that - - those - - Ontier, and everyone keeps telling me not to waive privilege.</p> <p>Q. This wouldn't be a waiver of privilege. If your solicitor had accessed this material, he could have confirmed what he had done without going into any matters of legal advice, couldn't he?</p> <p>A. That's not what I've been advised.</p> <p>Q. That's just another fiction told at the expense of Ontier, isn't it?</p> <p>A. No, it isn't.</p>	<p>Dr Wright refuses to face an obvious truth; that if the story had been true, it would have been straightforward to have his former solicitor confirm it.</p>
<p>{H/241/12} Mr Madden’s Second Report and the video at {F/155/1}, Exhibit CSW12 to Dr Wright’s Fourth Witness Statement</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day2/49:17} - {Day2/51:2}</p>	<p>Q. Play to the end, please.</p> <p>(Video footage played)</p> <p>Pause there, please. Can we get it so that we can see the passport clearly. You should see your passport held up with the passport number of N2511450 and an issue date of 23 June 2010?</p> <p>A. I did.</p> <p>Q. May we now go to {H/241/1}. This is appendix PM45 to 49. Mr Madden’s second report, and at paragraph 22 on {H/241/12}, he explains that from his researches, the copyright statement on Anonymous Speech, on the website, was updated in the footer each year, and this form of footer wouldn’t have been in use after 2009; he identifies several differences from the former footer in the video and those in use after 2009. Are you aware of those findings he made?</p> <p>A. I’m aware of them.</p> <p>Q. It’s right, isn’t it, that if you’d been accessing the account live in June 2019, it wouldn’t have displayed this footer, would it?</p> <p>A. No, actually it would have. Mr Madden has taken the main site without logging in, and Vistomail was not the most highly advanced site, and many of the aspects didn’t update.</p> <p>Q. You’re aware, aren’t you, that your expert agreed with Mr Madden about the inauthenticity of the original set of NAB records, aren’t you?</p> <p>A. Yes.</p> <p>Q. And you’re aware, aren’t you, that there is no evidence put in before the court that Anonymous Speech retained old copyright notices in later years? No evidence of what you’ve just said, is there?</p> <p>A. Because they closed down, so you can’t log into the site. After giving access to my solicitors, the server closed.</p>	<p>Dr Wright acknowledges that his expert has agreed with Mr Madden about the inauthenticity of the original set of NAB records; when faced with the fact that there is no evidence to support his assertion that Anonymous Speech retained old copyright notices in later years, Dr Wright claims that this is because the server closed down once he gave access to his solicitors.</p>
<p>{Day2/51:24} - {Day2/52:17}</p>	<p>Q. I’m going to put this to you. They don’t show the address bar. They don’t show any live navigation from any — from one page to another.</p> <p>A. If you’re trying to argue accessing the Wayback Machine and altering that, first of all, there’s no Wayback Machine capture of internal data. Then, next, the argument would be altering that, and if there was a capture on the machine, then that would still be a log-in, and at that point I could get a log-in to that site, so I’m not sure what your point is.</p>	<p>When asked why he did not capture any live navigation between the websites, Dr Wright blames his previous lawyers in the US.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. I'm putting to you that you recorded separate videos, each showing separate pages, rather than a single video showing navigation from page to page because you weren't accessing a live site.</p> <p>A. No, I'm telling you I was.</p> <p>Q. Why do you say that you recorded a separate video for each web page then?</p> <p>A. Because I was asked by my attorneys in the US case to capture the site.</p>	
<p>{Day2/52:25} - {Day2/53:9}</p>	<p>Q. As a forensic documents expert, would you accept that this is all exactly what someone would do if they were presenting fake videos?</p> <p>A. No, actually, if you were going to do it as a fake video, my Lord, what you would do, as someone skilled as I am, is you would go to the sort of developer bar and access and change online live. Now, what he wants to say is, then that will have the header bar, etc, but you could actually do that. That's why I gave the access and log - in to solicitors from Ontier, who did log in.</p>	<p>Dr Wright suggests that he is a skilled forger.</p>
<p>{L16/272/1} Transcript of Dr Wright's deposition in Kleiman on 18 March 2020</p>		
<p>{Day2/53:21} - {Day2/55:10}</p>	<p>Q. Then over the page, please, {L16/272/193}, you say you didn't. Question: "Why not?" Answer: Because I have not logged into there for ages and Vistomail requires payment. Without payment the account goes into lockdown and basically you end up not being able to log in. "Question: Can you pay and log back in?" Answer: No. Vistomail is not a standard open thing where you can communicate with anyone properly. It is run by a bunch of anarchists who - - yes, well, they are anarchists. On top of that the site was taken over in 2013. A new company bought the site and re - enabled a new version, so the disabled accounts no longer exist ." You were saying there, weren't you, that the site was no longer accessible, you hadn't accessed it in ages and in fact it hadn't been accessible since 2013?</p> <p>A. No, what I was saying there is that the Satoshi emails were no longer accessible. So there are separate parts to the site. One is domain management, one is purchase of VPS services. Both of those were still showing, but they couldn't be changed. The other was the Satoshi email system. So, what I couldn't get - - gain access to any more was the original emails that I would have had as Satoshi.</p> <p>Q. You didn't draw that distinction in that - - when you were giving evidence in that case, did you?</p>	<p>At this part in the transcript, Dr Wright is asked whether he tried to log in to the Satoshi Vistomail account to collect documents for the case.</p> <p>Dr Wright relies on a new reason as to why he did not produce the Satoshi emails in the Kleiman case.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. No. I was very hostile, I was very upset, I felt betrayed by Ira Kleiman and I reacted badly in the court, so I admit that.</p> <p>Q. And in fact, in the next question and answer, you were asked whether you tried logging in to the Anonymous Speech account to provide documents for this case, and, drawing no distinction at all, you said: "Anonymous Speech and Vistomail are the same server. If you have Satoshi@vistomail.com anything and Satoshi@anonymousspeech.com, anything, they are the same account."</p> <p>A. Yes, I did say that.</p>	
<p>{Day2/56:6-21}</p>	<p>Q. So, your position throughout the Kleiman litigation was that the Vistomail account was something you didn't have access to and you didn't draw a distinction between having access to certain parts of it, did you?</p> <p>A. As I noted, the Sakura account was the main account that linked into the email. I no longer had access to the Satoshi emails, and I was being particularly difficult. I'm not doing that for this court, your Honour - - my Lord. I did get really annoyed with that case and I didn't lie, but I didn't give information about the site. So you're correct.</p> <p>Q. So you may have told the truth and nothing but the truth, you say, but not the whole truth?</p> <p>A. I wasn't asked the rest of the question, and I'm doing beyond what I need to now. I should have actually said I how it worked. I didn't.</p>	<p>Dr Wright concedes that he did not provide the full truth whilst under oath in the Kleiman trial.</p>
<p>{L1/79} and {L1/80} - ITOL Application Project BlackNet</p>		
<p>{Day2/69:13-22}</p>	<p>Q. Then the document we were just looking at {L1/80/2}. The "Version control" indicates that it's the same document, doesn't it?</p> <p>A. No, it just means we haven't updated it. Version control on our documents wasn't terribly good.</p> <p>Q. So you're saying the version control may be wrong?</p> <p>A. It definitely is wrong. If you have a look there it says "Version: 1.0", and it says "Version 1.2" at the bottom. So, just on the page you're showing shows that the version control is screwed.</p>	<p>Dr Wright produces a new excuse in relation to version control.</p>
<p>{Day2/72:22} - {Day2/73:1}</p>	<p>Q. The document to which - - in which Stage 4 did appear, when was that first filed with AusIndustry?</p>	<p>Dr Wright states that the ITOL application in 2002 did have Stage 4 included.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. That would have been filed in 2002 and then in 2003. In neither instance did we get any feedback from them -- positive feedback.</p>	
<p>{Day2/76:10-15}</p>	<p>Q. And page 6 {L7/211/6}, you see the project is divided into four subprojects: "Spyder", "Redback", "TripleS" and "BlackNet"?</p> <p>A. Yes, and I forgot to update the dates.</p> <p>Q. BlackNet finish date, 30 June 2004, yes?</p> <p>A. Like I said, I didn't update the date. It's 2009.</p>	<p>Dr Wright accepts that he has put forward documents with false dates (because he forgot to update the dates).</p>
<p>{Day2/81:20} - {Day2/83:12}</p>	<p>Q. And do you see that the card number has the first four digits and last four digits from the account we were just looking at 4557 and 1583?</p> <p>A. It has account details, yes.</p> <p>Q. And do you see, at the bottom, that the payment out is dated 3 May 2009 at 12.47?</p> <p>A. I do.</p> <p>Q. And it's described as an NAB visa credit card?</p> <p>A. Yes.</p> <p>Q. So you're wrong, aren't you, to deny that that was a number for a visa credit card which you were actively using well after 2005?</p> <p>A. No. My wife did obviously use it. It wasn't meant to be used. We had been told by the bank we weren't meant to use it.</p> <p>Q. You said it had been cancelled in 2005. How was your wife using it in 2009?</p> <p>A. We still had the home loan.</p>	<p>Dr Wright fails to accept the obvious truth, that he cannot have cancelled the NAB visa credit card in 2005 as he previously states.</p>
<p>Video at {L19/271/1}</p>		
<p>{Day2/83:11} - {Day2/85:1}</p>	<p>Now, this is one of your videos, isn't it?</p> <p>A. It is.</p> <p>Q. And it's supposedly showing the Satoshi email part of the Vistomail site, isn't it?</p> <p>A. No, it's not. This is not showing any of the emails, this is just where you actually have the email account. So that it's separate things again. What you're confusing is the options that were there with the storage of email. As I said, the email was not there at that stage.</p>	<p>Dr Wright is questioned about whether the video is showing the Satoshi email part of the Vistomail site. Dr Wright denies this and provides an evasive response, claiming there was no storage of email. Mellor J queries whether Dr Wright was logged into the email account. Dr</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Well, I have to suggest to you that this is just more fiction to explain this morning's fiction.</p> <p>A. You can make up whatever answer you want.</p> <p>Q. If we play on to the end, we'll see how it's used. (Video footage played) The inbox folder, spam box, sent folder and so on, you were presenting this as an accessible email page, weren't you?</p> <p>A. No, I was saying that was a page. None of the other things had any email in them. As I said, no storage was there.</p> <p>MR JUSTICE MELLOR: But you were logged into the email account, weren't you?</p> <p>A. I was logged into the secure account that linked to the email, but because I hadn't paid and it had changed, all of the storage had gone. So, any of the 2009 or '10 emails that I had sent had expired and gone. So what I'm explaining is, while I had the ability to send a new email, I couldn't access any of the old ones, hence why I didn't give anything in court, because there was nothing to give.</p> <p>MR HOUGH: So when you said earlier that the Satoshi email system was no longer accessible on the site, you're qualifying that now?</p> <p>A. No, I mean the Satoshi emails. You were talking about why I didn't give these into court, because I didn't have anything to give. There was nothing in the Florida case for me to send a new email. It wasn't about whether I was Satoshi in Florida. The issue wasn't whether I could send an email in Florida. The issue: did I have any 2009 emails. I did not.</p>	<p>Wright accepts that he was, but that he could not access any of the 2009/10 emails.</p>
<p>Video at {L19/269/1}, Exhibit CSW11 to Dr Wright's Fourth Witness Statement</p>		
<p>{Day2/85:8-21}</p>	<p>A. That's why I ended up getting my other thing. It wasn't - - I used my ELMO and ... yeah. I don't like doing it. The fact that I can try and do it doesn't mean I like doing it.</p> <p>Q. I am just going to ask for it to be played again, and I'm going to suggest to you that it carefully avoids showing the address bar. So play on. It goes almost up to the address bar, but not quite during the course of this video.</p> <p>(Video footage played)</p> <p>Like all the other - - as in all the other videos, you were careful not to show the address bar, weren't you, Dr Wright?</p> <p>A. No, I was not.</p>	<p>Dr Wright fails to accept the obvious truth, that he was careful in the videos not to show the address bar.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{L14/294/1} Twitter post by Dr Wright {A/3/16} Dr Wright's Defence</p>		
<p>{Day2/89:23} - {Day2/91:8}</p>	<p>Q. May we go to your defence {A/3/16}, paragraphs 45 and onwards. Now, at paragraph 45, we see how you explained this difference, this oddity of BlackNet - - the BlackNet paper which you tweeted containing language which is in the March 2009 version of the White Paper but not the August 2008 and October 2008 ones. You say: "Dr Wright first submitted his Project BlackNet research paper to AUSIndustry in 2001 as part of an application for a research grant and R&D tax rebate. He obtained R&D tax rebates from AUSIndustry (but not research grant funding) for Project BlackNet during the period 2001 to 2009. He subsequently and unsuccessfully sought research grant funding and R&D tax rebates in 2009 and 2010. Dr Wright updated his Project BlackNet research paper each year that he submitted it to AUSIndustry. Early applications did not contain the abstract of the White Paper but later unsuccessful applications did. The image of the research paper published on Twitter is that used for a later application containing an abstract from the White Paper." Is that paragraph of your defence correct?</p> <p>A. Completely. What I put in the Twitter was a mash up of 2001 to 2010, when everything was working, basically showing this is where I started, this is where I ended up. And the problem you seem to be having is, you have this assumption that I write something and then don't reuse it. That's completely wrong. You'll find in even the posts I've done to your witnesses that I have block quoted to Gavin, to Martti and to other people information. So I just cut and paste my own writing. That includes the abstract. So sometimes - - I don't know how you write, but sometimes I write something and I rewrite it and I rewrite it and I go back to the original.</p>	<p>Dr Wright explains his tweet regarding the BlackNet paper.</p>
<p>{Day2/92:2} - {Day2/92:16}</p>	<p>Q. The natural meaning of this tweet is: I filed what I'm showing here with the Australian government in 2001, isn't it? That's the natural meaning of what you've written?</p> <p>A. I'm better at code than words. So if you think that, that's the problem.</p> <p>Q. "My stupidest mistake was going to the Australian government in 2001 and filing this shit." And then a whole series of images. The meaning was perfectly clear: I filed this, that you see below you, in 2001, wasn't it?</p> <p>A. I don't see any emphasis on this. I didn't put it in italics, there are no parenthesis, there's no asterisk, it's not bold.</p>	<p>Dr Wright blames the discrepancies between his tweet and evidence on the fact that he is better at code than words.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	So no, it isn't "this", as you just emphasised. That's a completely different meaning.	
{Day2/93:9-22}	<p>Q. Pause there. Would you accept now, looking at this document, that if you're right and some of what appears did not exist in 2001, then this was a positively misleading tweet?</p> <p>A. No, not at all. I have stated that I have been working on this over a decade. Misleading would be trying to tell someone, I just did this now, or I did it in the past, or something else. My saying I have spent well over 15 years of my life working, fighting, struggling, doing 30 degrees nearly, doing multiple doctorates, filing papers, spending every cent I've had, sometimes at the expense of my family - - love them, because they actually put up with me - - no, that's not misleading.</p>	Dr Wright refuses to accept the obvious truth that his tweet was misleading.
BlackNet abstract {L1/79/4} versus abstract extract in tweet at {L14/294/2}		
{Day2/94:14} - {Day2/95:2}	<p>Q. "Early applications did not contain the abstract of the White Paper but later unsuccessful applications did."</p> <p>A. That doesn't contain the abstract of the White Paper. What you have on screen is not the abstract of the White Paper.</p> <p>Q. Dr Wright, in your defence you said: "Early applications ..." Meaning your applications to AusIndustry: "... did not contain the abstract of the White Paper but later unsuccessful applications did."</p> <p>A. Yes, verbatim. That isn't the application - - that isn't the abstract from the White Paper, so I'm sorry, you're mistaken</p>	Dr Wright refuses to accept an obvious truth and is overly pedantic.
{A/3/16} Dr Wright's Re - Re - Amended Defence		
{Day2/97:7-24}	<p>A. One of the versions of what I filed with the tax office included the Timecoin paper.</p> <p>Q. The project paper was also wrong in citing Lynn Wright as an author, wasn't it?</p> <p>A. Well, she wasn't an author, but she was one of the executives in the firm.</p> <p>Q. She had no idea what BlackNet was, did she?</p> <p>A. She did.</p>	Dr Wright blames Lynn Wright's testimony in Kleiman on her illness (cancer) and taking medication for this. See {Day2/118:3-13} where Dr Wright is shown the video at {L16/116/8}, where Lynn Wright directly refutes this.

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. So when, in her deposition within the Kleiman litigation, she said she had no idea what BlackNet was, she was lying, was she?</p> <p>A. No. Lynn Wright had just suffered a - - cancer and had a double mastectomy. When you had that, what you're taking, she was on a lot of medication, she was in chemotherapy, radiotherapy, her breasts were still being rebuilt, she was heavily sedated, she was on opioids, so - - and she wasn't terribly happy about being pulled in to be interviewed.</p>	
<p>{L1/91} Project Spyder version 1.2 {L1/99/1} Project Spyder version 1.2</p>		
<p>{Day2/98:23} – {Day2/99:5}</p>	<p>Q. Dr Wright, this is a document which is - - which has internal metadata dating it to November 2002. Will you take that from me?</p> <p>A. I'll take that from you.</p> <p>Q. If it were authentic to that date, it would support your claim to be Satoshi, wouldn't it?</p> <p>A. It would support my BlackNet claim, but other things, such as AusIndustry, do.</p>	<p>Dr Wright is evasive in response to the proposition that {L1/91} would support his claim to be Satoshi if it were authentic.</p>
<p>{Day2/100:10-15}</p>	<p>Q. This document was created in or after 2016 and backdated, wasn't it?</p> <p>A. No, it wasn't.</p> <p>Q. Each of those is a clear indication of a document which has been backdated?</p> <p>A. Actually, it's not.</p>	<p>Dr Wright fails to accept the obvious truth that this document contains indications of backdating.</p>
<p>{Day2/105:23} - {Day2/106:6}</p>	<p>Q. Would you accept that all these signs on this email are that it's a late creation, forged and backdated email?</p> <p>A. I wouldn't say that from that. I don't know what I'd say without more analysis. What I would say is I don't use Outlook.</p> <p>Q. All these signs indicate that this is an email which you produced to give legitimacy to the document?</p> <p>A. I produced every file that I had, effectively, so I didn't produce anything for any legitimacy.</p>	<p>Dr Wright fails to accept an obvious truth and blames Ontier for producing his reliance documents.</p>
<p>{L2/148/1} - “Bond Percolation in timecoin”</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day2/106:18} - {Day2/108:9}</p>	<p>Q. It's one of the documents you've nominated as one on which you primarily rely for your claim to be Satoshi?</p> <p>A. It's a reliance document.</p> <p>Q. Well, the order asked you to nominate documents on which you primarily relied for your claim to be Satoshi, and this was one of those you nominated; correct?</p> <p>A. Well, I didn't nominate it, but my lawyers went through lists and pulled out ones, but ...</p> <p>Q. They nominated these documents on your instructions, didn't they?</p> <p>A. They gave me a list and I signed off.</p> <p>Q. That's a list you still subscribe to, though, isn't it? A. This is a document that I wrote, if that's what you're saying, yes.</p> <p>Q. I didn't ask that question. I said: do you still subscribe to the list of documents your solicitors have nominated as those you primarily rely upon for your claim to be Satoshi, a list they endorsed just a few weeks ago?</p> <p>A. I'm sorry, I'm not sure what you mean, the way you're putting that.</p> <p>MR JUSTICE MELLOR: It's a simple question, Dr Wright.</p> <p>A. Do I rely on these documents? Yes.</p> <p>MR JUSTICE MELLOR: That wasn't quite the question. Please listen to the question and answer it. Counsel, try again.</p> <p>MR HOUGH: Your solicitors - - you were ordered to provide a list of those documents on which you primarily relied for your claim to be Satoshi; do you understand?</p> <p>A. Yes.</p> <p>Q. Your solicitors produced such a list on your behalf; do you understand?</p> <p>A. Yes.</p> <p>Q. They endorsed that list and added to it just a few weeks ago; do you understand?</p> <p>A. I do.</p> <p>Q. Is that a list you yourself still subscribe to as documents on which you primarily rely for your claim to be Satoshi?</p> <p>A. If you mean do I still stand by these documents, yes.</p> <p>MR HOUGH: Well, my Lord, I'm not sure I can ask -</p>	<p>When asked whether he accepts {L2/148} is one of his primary reliance documents, Dr Wright is evasive, refusing to answer the question asked and instead reframes the question as it being a document on which he relies.</p> <p>Mellor J interjects and requests Dr Wright to answer the question asked. Dr Wright still does not answer the question.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. "Subscribe" has a different meaning.</p>	
<p>{Day2/108:22} - {Day2/110:12}</p>	<p>Q. So if the metadata were correct and this document was authentic, it would support your claim to be Satoshi, wouldn't it?</p> <p>A. Not necessarily. Metadata isn't going to stay the same over time. Your presumption is that over 15 to 20 years of use and access by multiple people that files are exactly the same. Having forensic experience, I would say the anomaly would be ever finding a file that hasn't changed.</p> <p>Q. If this document had been authentic to its stated metadata as something created in July 2007 and in your hands, it would support your claim to be Satoshi, wouldn't it?</p> <p>A. No. The material and the knowledge supports my claim to be Satoshi. The fact that I wrote this, did this research, was researching this area, is what I'm stating to be my claim.</p> <p>Q. Mr Madden has found that this document has a Grammarly encoded timestamp of 16 January 2020, and on that basis he concludes that this has been backdated. Dr Placks agrees it's a backdated document. Do you agree with that?</p> <p>A. No. As I've noted in other things, that is only a Grammarly timestamp that comes from certain versions of Grammarly opened in certain ways. If you normally run Grammarly on a machine, it won't be embedded. The - - that just means somebody has opened or looked at the document, without saving it, on a machine that has the Enterprise version of Grammarly.</p> <p>Q. Well, I have to put to you that you're wrong in point of fact, as the experts have found that a Grammarly tag is not attached simply by opening a document and not interacting with it or saving it.</p> <p>A. I'll put it to you that neither expert looked at any Enterprise version of Grammarly, or even the business version, and neither of them showed how Grammarly tags get embedded. When you even save a document running Grammarly, that tag is never embedded. Neither of the experts decided to open a document, run Grammarly, save it. If they did, as I showed in my own witness statement, that doesn't happen.</p>	<p>Dr Wright's comments on changes to metadata appears to amount to a disavowal of any documentary proof. Dr Wright is evasive when asked if he accepts this document would support his claim to be Satoshi, if it were authentic to July 2007.</p> <p>Dr Wright does not agree with his own forensic expert's conclusion in relation to this document (Dr Placks).</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day2/115:18} - {Day2/116:3}</p>	<p>Q. So he had found that this was likely created from a .DOCX file and then he subsequently finds that just such a document is attached to your Slack post of January 2020, the time of the changes. Is that an extraordinary coincidence?</p> <p>A. No, it's extraordinarily bad analysis. The reason being that if you were to actually cut and paste from a DOC file into OpenOffice and save as ODT, none of that would happen. If he had done a good forensic job, he would have tested that, but he has a biased sort of outlook.</p>	<p>Dr Wright accuses COPA's forensic expert, Mr Madden, of bias.</p>
<p>{L16/116/8} - Deposition of Lynn Wright (Kleiman Proceedings)</p>		
<p>{Day2/118:3-24}</p>	<p>Q. This is the deposition of Lynn Wright. Do you remember you saying that when Lynn Wright gave evidence in this deposition, she was basically unfit to give proper evidence?</p> <p>A. I do.</p> <p>Q. Do you see that she was asked at line 6: "Do you have any medical conditions that affect your ability to provide truthful and accurate testimony today?"</p> <p>A. I do.</p> <p>Q. You see she said, "No"?</p> <p>A. Yes, I think it's a silly question to ask someone who has just gone through a double mastectomy who happens to be on opioids.</p> <p>Q. It wasn't suggested by her or anyone for that she was unable to give truthful and complete evidence, and in fact she said the opposite, didn't she?</p> <p>A. Like I said, if you'd just gone through a double mastectomy that you were on opioids because of, it's unlikely that you're going to be thinking straight enough to basically argue with the people who want to grab you into giving testimony you don't want to give.</p>	<p>Dr Wright is presented with evidence that directly contradicts his evidence that Lynn Wright was not fit to give evidence in Kleiman at {Day2/97:7-24}.</p>
<p>{L3/200} Phase transitions in block propagation networks</p>		
<p>{Day2/121:5-9}</p>	<p>Q. So on its face, that document would appear to give support to your evidence, wouldn't it?</p> <p>A. I would still link it to other people, including Ignatius Pang, and go into the research I was doing with others.</p>	<p>Dr Wright is evasive, refusing to directly answer the question being put to him.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{Day2/128:4-24}	<p>Q. But all your non - specific hearsay is up against two independent experts in this case, isn't it, Dr Wright?</p> <p>A. No, it's against the people who are the experts in this case.</p> <p>Q. Are you suggesting they're not independent, Mr Madden and Dr Placks?</p> <p>A. I don't see them as terribly independent, but anyway.</p> <p>Q. Why do you say that Dr Placks, your own expert, isn't independent?</p> <p>A. I didn't choose Dr Placks. I didn't want Dr Placks.</p> <p>Q. Do you consider that Dr Placks is incompetent?</p> <p>A. I consider Dr Placks is a psychologist. He has a degree in psychology, he has no qualifications in information security. He has not done SANS, neither has Mr Madden. Neither of them have done a single IT security, IT forensics or other certification, course or training.</p> <p>Q. So is it your position that your expert, the expert that's being called on your side, Dr Placks, is not a suitably qualified expert to give evidence on what he covers in his reports?</p> <p>A. If you're asking that - - that directly, yes.</p>	<p>Dr Wright asserts that his own forensic expert, Dr Placks, (i) is not independent and (ii) is not suitably qualified, thereby disclaiming his own expert.</p> <p>Dr Wright also asserts that Mr Madden is not independent.</p>
{H/137/5} Mr Madden's PM32		
{Day2/130:13-24}	<p>Q. Page 5 then {H/137/5}, paragraphs 15 to 16, Mr Madden made findings that the equations that we saw on the page had underlying dated structured in XML formats, which isn't typical of documents in .DOC format and it's not how such images are stored from the version of MS Word recorded for this document. We see that finding at paragraph 17. Do you see that?</p> <p>A. Yes. Unfortunately, again, the tools that I say that I use, he hasn't actually looked at, and those tools that I did mention save in this format. Those tools have been doing that since actually the '90s, before any of these other formats existed.</p>	<p>Dr Wright did not produce this information on the format/tools that he claims to have used until after Mr Madden's expert report was served.</p>
{L2/149/1} Defining the possible Graph Structures - ID_000462		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day2/130:25} - {Day2/132:19}</p>	<p>Q. The reality is that, as he finds, these equations were created in .DOCX format in a later version of MS Word than the dates suggest and then imported into this document, weren't they?</p> <p>A. No, that's incorrect.</p> <p>Q. That's because the .DOC format, which this document appears primarily created in, structures data as appears primarily created in, structures data as OLE linked objects, not in the XML format found here, unlike .DOCX format documents?</p> <p>A. No, the statement that I made earlier and that I've got in my witness statement is that the software that I have with Word, which has been around since at least 1998, saves in XML and XBRL format. The reason I used XML and XBRL format was I would actually import audit data as well so I could work on it. While I was an auditor, XML and XBRL allowed me to capture information and have it automatically update in some of the things I did in other documents for reports. So, you're saying this is unusual. Well, all of my tools are basically unusual.</p> <p>Q. If Mr Madden's right, then writing a document in one format and waiting years and importing equations from another document would be bizarre to the point of absurdity, wouldn't it?</p> <p>A. No. If Madden was actually doing his job, he would run up what I said and check. He would analyse a Citrix machine and see what happens even after two weeks of running. Now - - which I have done. So if you do have a document and you do leave it, even when it's not in the forefront, because of the way Citrix works, the application keeps the edit time running.</p> <p>Q. Dr Wright, I'm not going to address your comments about your private tests, because those have been ruled inadmissible by the court. What I'm going to address with you is the expert evidence that has been put in, and I suggest to you that that suggests clearly, as Mr Madden found, that the computer clock was manipulated in the production of this document?</p> <p>A. Actually, no. As I just said, I've personally seen it, I know how it works, I've been running Citrix servers and been certified in the past, though didn't keep it, since '97 or so, back when it was a different product. So, I totally disagree. And if I had edited the clock, there are other markers in Word that would have been there.</p>	<p>Dr Wright is presented with Mr Madden's findings that the equations in this document were created in a later version of MS Word and then imported into the document.</p> <p>In response, Dr Wright seeks to rely on experiments which have been ruled as inadmissible.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{L3/237} - Statistics studies.doc - ID_00550		
{Day2/135:1-20}	<p>Q. Now, Mr Madden’s conclusion is that somebody has changed a document written years after the release of Bitcoin to suggest its creation shortly before that release. You’re aware of that finding, aren’t you?</p> <p>A. I ’m aware of it, yes.</p> <p>Q. And that’s correct, isn’t it?</p> <p>A. No, it’s not correct. What you have here is a shared environment where a completely different file , the file that you have there is unrelated to the earlier research, has been merged. The particular note that was later was to do with a a sort of explanation that was given to the Australian Tax Office that has nothing to do with any of the SAIRC(?) information; it’s to do with the legal aspects of Bitcoin. If someone was to completely fabricate a document, then they wouldn’t have merged documents. For instance, if I setback a computer, ran an old version of software, cut and paste from text, formatted, did this , then it would be perfect. So the irony is , if I was to manipulate and fabricate documents, they would be perfect.</p>	<p>Dr Wright suggests that he is skilled at manipulating and fabricating documents.</p>
{Day2/135:21} - {Day2/136:9}	<p>Q. Well, you keep saying that, Dr Wright, but I'm putting to you that the findings of so many of your documents bearing signs of inauthenticity and manipulation, which you have to explain in many different ways, suggests that you're not quite as good at forgery as you're postulating you might be?</p> <p>A. No, because I didn't forge anything.</p> <p>Q. Now - -</p> <p>A. As I suggested and as I've stated, I have had multiple companies over the years, I have had several hundred staff, files are shared, because we do research, and that research has led to what has now been over 4,000, approaching 5,000 patents being filed, none of which could be done just by cutting and pasting.</p>	<p>Dr Wright denies forging any documents, and refers to his many patent filings, which is irrelevant to the question asked.</p>
{Day2/136:10} - {Day2/136:14}	<p>Q. Your excuse for this document is that it's become corrupted by a process of two documents merging?</p> <p>A. Someone probably had two different documents open simultaneously. When you have Citrix and other such environments, this is uncommon, but it does occur.</p>	<p>Dr Wright refuses to accept an obvious truth that this document is manipulated, instead proposing a far less likely explanation that the documents spontaneously merged due to his Citrix environment.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day2/136:21} - {Day2/137:7}</p>	<p>Q. Just setting aside the technology for a moment. If you had a process of accidental corruption, it would be an extraordinary coincidence for it just to happen to create a document which looked as though it was the same thing but looking ahead at Bitcoin rather than looking at it in the past. That would be a remarkable coincidence, wouldn't it, Dr Wright?</p> <p>A. No, it wouldn't. It meant -- I would say that someone's updated or not saved the document the same way and that the server has had a partial image at the same time. It would be an immense anomaly to find a group of 15 - year old files with no anomalies. I've never seen it before</p>	<p>Note that Dr Wright has produced a number of documents dated to 2002, which Mr Madden has found authentic.</p>
<p>{Day2/137:8} - {Day2/138:3}</p>	<p>Q. Let's put it simply. If you mashed two documents together completely randomly, even speaking without any technical expertise, you wouldn't produce something that just happened to read as perfect English but looking at Bitcoin as an established fact, rather than something in the future.</p> <p>A. There are different parts of what you're saying. One, there's an edit on this document, and two, there is a completely separate document. The completely separate document that is a legal document on Bitcoin is tacked on at the end. The other document is an edit that hasn't saved properly.</p> <p>Q. The only explanation you gave for these anomalies in your appendix B to your 11th statement is that there was a simple corruption between two documents; that's right, isn't it?</p> <p>A. That is a corruption between two documents. There's an edit that hasn't happened correctly on one of them, and there's a merge of another document, which has also led to other corruptions at the end, where you have the references then followed up by other terms.</p>	<p>Dr Wright produces a new excuse that has not been supported by expert evidence and is not discussed in his evidence.</p>
<p>{Day2/139:3} - {Day2/140:6} {H/14/1} Exhibit PM1.13 to Appendix PM1</p>	<p>Q. The 2013 report was removed because it would be an anachronistic to a document of 2008. That's the reason, isn't it?</p> <p>A. No, if you look just above it, "... following 'phases' ...", so it's talking about something different. So, the controls, the rate, etc, it's actually different. So the "mining" in its other sort of "Senate" thing is a different area in a different document talking about a different thing. It's part of a submission that was given to the Australian tax authorities.</p> <p>Q. There's a difference, because it's under a different heading, "Mining". But in other respects, this document, all the changes that we see are changes to remove references to Bitcoin already existing and to events postdating 2008. So we see: "To date, over 17 million</p>	<p>Dr Wright is presented with Exhibit PM1.13, which is a comparison document of the original text (PM1.3) and ID_000550 - a reliance document.</p> <p>Dr Wright blames the changes to the document on a third party (possibly staff at one of his companies).</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Bitcoin are estimated to be in circulation. However, a Bitcoin ..." And then that's edited to: "This will force low power nodes out of the system ..." To remove a reference to something that's - - that dates it to much after 2008. That's not an accidental change, is it, Dr Wright?</p> <p>A. Again, I don't know how the change happened. This is two different documents. How the parts are merged into one, I can't answer. These documents are given to different staff at all of my companies so that we can actually create and file the research that we do.</p>	
<p>{Day2/140:7-19} {H/16/1} - SSRN Article / Exhibit PM1.15</p>	<p>Q. May we then go to {H/16/1}. We see that's a web page from the SSRN website describing an article with the same title as this one written by you in March 2017?</p> <p>A. No, that was posted at that date.</p> <p>Q. It says, "Posted: ... April 2018. "Date written: March 28, 2017." Is that wrong?</p> <p>A. That just means when it started being loaded and it doesn't go into when it's initially there. So, I'm not sure who loaded things in - - I don't actually manage SSRN, but I don't know who did at the time. I can't recall.</p>	<p>Dr Wright is shown a web page from the SSRN website describing an article with the same title as those examined by Mr Madden above - PM1.3, ID_000550, which was written in 2017. Dr Wright is evasive in response, stating that he does not manage his own SSRN page.</p>
<p>{Day2/142:14} - {Day2/142:25} {H/1} Mr Madden's Appendix PM1, ID_000550</p>	<p>Q. These are classic signs of a conversion error, not using a different and carefully chosen tool to input the equations, aren't they?</p> <p>A. I disagree on that one, once again.</p> <p>Q. So you say that you chose a tool specifically in order to put the equations in and they came out as this - - well, with respect, junk in the left - hand column?</p> <p>A. No, but if you've got something that isn't loaded correctly, it can. It's not conversion. What I do know is obviously someone has added something I don't want because of the cryptocurrency bit in my document that I need to take down.</p>	<p>Dr Wright is presented with Mr Madden's table comparing ID_000550 and the SSRN version (Exhibit PM1.4). The table shows that the equations in his reliance document have been corrupted, likely due to a conversion error.</p> <p>Dr Wright is evasive in response and blames an unspecified third party, who has "added something I don't want".</p>
<p>{Day2/143:1-9}</p>	<p>Q. And then, in addition, as a further finding , Mr Madden found, at page 22 {H/1/22}, that the metadata of the document contained references to Microsoft schemas dating from 2010 and later and references to Grammarly, which was released in 2009. Do you see those findings?</p> <p>A. I do.</p> <p>Q. So it happens, along with all these other findings , to have those signs of alteration as well , doesn't it ?</p> <p>A. It does. Like I said, shared environment.</p>	<p>Dr Wright accepts that his reliance document ID_000550 {L3/237} has signs of alteration.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{L3/185} - Block diffusion within bitcoin.doc		
<p>{Day2/147:14} - {Day2/148:22} {H/130/1} Exhibit PM30.1</p>	<p>Q. May we now go to {H/130/1}. This is a document Mr Madden found online, a ResearchGate article which, we see from the header, was received, revised and accepted in April 2012; do you see that?</p> <p>A. I do.</p> <p>Q. Thank you.</p> <p>A. It was published in the Huawei network, submitted in 2011 from earlier publications given in China in 2009.</p> <p>Q. This is an article on small - world analysis to address epidemic diffusion problems, isn't it?</p> <p>A. It is.</p> <p>Q. It doesn't say anything about Bitcoin or the blockchain?</p> <p>A. No.</p> <p>Q. May we look under the introduction and at the second paragraph and the second sentence: "Actually, many recent research efforts have been devoted to understanding the prevention and control of epidemics, such as those of Wein et al, Wein et al, Craft et al, Kaplan et al, and Matsuura et al." Would you accept there's a clear parallel with the passage we reviewed in your paper?</p> <p>A. Yes, I used their work when I was studying at Newcastle. The university is in medical epidemiology and medical statistics, so when I was doing my statistics degrees, I engaged with a lot of researchers. I get pre - done papers and I don't publish them as my own, I used my research, basically. And do you see that the Shi and Dong article has a reference number in this one? That's a difference. It's got a reference number 7.</p> <p>A. Yes, it was released at this point.</p> <p>Q. And then at page {H/130/13}, please, we can see that number [7] is an article published in 2012?</p> <p>A. That version. There's an earlier one as well.</p>	<p>Dr Wright suggests that there is an earlier publication of the article at {H/130/1}, but has not put forward any evidence to support this.</p>
<p>{Day2/149:9} - {Day2/150:15}</p>	<p>Q. {H/129/9}, please. What Mr Madden has done, in the lower part of this page and over the page, is to compare sections of your paper against the equivalent sections of the ResearchGate paper. May we go to, please {H/129/10}, the section beginning just over halfway down: "Hsu and Shih "The section from your paper is</p>	<p>Dr Wright refuses to accept the obvious truth that sections of his paper and the paper at {H/129/10} are virtually identical. When pressed he concedes they are "very close", but struggles to</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>virtually identical to the section in the published article, isn't it?</p> <p>A. No. The paragraph is in about the same place.</p> <p>Q. I can read out these two paragraphs, the one in black and the one in red, but I'm putting to you that they are virtually identical to each other. Are you accepting that?</p> <p>A. What I'm saying is I took work from these authors in my research. I didn't publish it, because I didn't finish it. When I make my notes, I do use other people's work.</p> <p>Q. I appreciate you're trying to give your excuse and make your argument, but the question at the moment is a simple one: those two passages are virtually identical, aren't they?</p> <p>A. They're very close. They're not quite exactly the same.</p> <p>Q. They're almost word - for - word identical.</p> <p>A. Almost isn't.</p> <p>Q. Point out a difference.</p> <p>A. "Ref". A different reference number. A couple of other bits like that.</p> <p>Q. Anything else, other than the two reference numbers being changed?</p> <p>A. They're the main bits, but, yes.</p> <p>Q. It's a word - for - word copy, isn't it, Dr Wright?</p> <p>A. Yes. I took other people's work in my notes.</p>	<p>identify any actual differences.</p> <p>Dr Wright admits that he takes other people's work when making his notes.</p>
<p>{Day2/150:24} - {Day2/151:13}</p>	<p>Q. But he found that although these weren't explicitly referenced, the text contained references to four of the five works which postdated 2008.</p> <p>A. Other people were also working and collaborating.</p> <p>Q. So you say that you just happened to have pre - publication versions of four of those five papers?</p> <p>A. I was studying as a postgraduate in a medical research university doing a masters in statistics in a university that specialises in epidemiology and medical research. So, yes, researchers share.</p> <p>Q. This paper doesn't just replicate ideas, does it, it replicates whole sections?</p> <p>A. Because I used other people's papers, and pre - release. People ask me for papers, I send them my pre - release work, all the time.</p>	<p>Dr Wright refuses to accept the obvious truth that he was unlikely to possess pre-publication versions of 4 of the 5 references that postdate 2008.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day2/151:21} - {Day2/152:5}</p>	<p>Q. So you had a pre - publication paper from several years beforehand which contained these passages which are so similar to your document and in the same font?</p> <p>A. When you write a document and you publish it, you don't just publish it in a large - scale publication first, this was published first in China. So, yes, two years later it got published there. Earlier, it was published in China.</p> <p>Q. Was it published in English or Chinese?</p> <p>A. English.</p>	<p>Dr Wright produces a highly unlikely explanation that a paper by Chinese researchers would be published in China, in English.</p>
<p>{Day2/152:12} - {Day2/153:7}</p>	<p>Q. So the explanation for this remarkable similarity is that you happened to have pre - publication copies of not just the ResearchGate article but four of the five papers cited in it which were produced after 2009? That's what you're telling the court?</p> <p>A. What I'm telling the court is, as a medical researcher doing statistics in a medical research university, I engaged with a lot of people and took lots of papers. It can be years between writing and publication, and then rewriting and publication in a better journal can be years later again.</p> <p>Q. I have to pin you down on this so that we can cite it, in due course, in closing argument. Your evidence to the court is that you happened to have a pre - publication version of not just the ResearchGate article, when you produced your document in 2008, but four of the five papers cited in it which postdate - -</p> <p>A. They were cited in another paper. You're asking me do I have the cited papers from someone else's cited paper. I have the paper where they cited that. Other Chinese people - - academics, also share.</p>	<p>Dr Wright continues to be evasive when pressed about his alleged possession of pre-publication copies of 4 of the 5 papers postdating 2008.</p>
<p>{L1/323/2} University of Newcastle Assignment - ID_000073 {H/145/11} Appendix PM38</p>		
<p>{Day2/155:2-15}</p>	<p>Q. Next page, please {L1/323/2}. The contents page has one substantive item, "Poisson competing process"; do you see that?</p> <p>A. I do.</p> <p>Q. Then page 3 {L1/323/3} begins the substantive content. You see that it reads: "We consider the scenario of an attacker trying to generate an alternate chain of time rounds faster than the honest TSA chain." That, and subsequent parts of the text, have clear features in common with concepts of the blockchain and the way of avoiding an attacker subverting the chain, don't they?</p> <p>A. They do.</p>	<p>Dr Wright accepts that this document would be evidence of his precursor work.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day2/157:20} - {Day2/158:15}</p>	<p>Q. What you've said in your appendix B to your 11th witness statement is that there was a precursor document, other than the Bitcoin White Paper, from which you pasted these sections. Am I getting that right?</p> <p>A. That's correct.</p> <p>Q. You haven't ever disclosed that precursor document, have you?</p> <p>A. As I've noted before, this is many years later and the majority of documents don't exist any more.</p> <p>Q. May we go back to the previous page where we see the comparison {H/145/12}. Now, there are obviously differences between the Bitcoin White Paper and this document, but if that's right, then before 2005 you had a working document which contained a number of passages which found their way word - for - word into the Bitcoin White Paper; would you accept that?</p> <p>A. Yes, I would.</p> <p>Q. And you'd have had that document on your systems in late 2005?</p> <p>A. I'm not sure of the exact date of that course, but '5 or '6, whatever it is.</p>	<p>Dr Wright admits that he has not disclosed the precursor document from which he pasted the sections that Mr Madden found had been inserted from the Bitcoin Paper.</p>
<p>{L1/337/27} - University of Newcastle Statistics Assignment {H/145/8} Appendix PM38</p>		
<p>{Day2/160:13-15}</p>	<p>Q. Is it an actual statistics assignment you completed in 2005?</p> <p>A. Yes.</p>	<p>Dr Wright accepts that {L1/337} was an actual assignment that he completed in 2005.</p>
<p>{Day2/160:23} - {Day2/161:3}</p>	<p>Q. And page 9 {H/145/9}, if we look at the last boxes on the text, we can see that he - that various of the standard university student questions appear in embedded form within the document you've got, talking about a precursor to Bitcoin?</p> <p>A. Yes, this is the undergraduate level questions.</p>	<p>Dr Wright accepts that the hidden passages are present in ID_000073.</p>
<p>{Day2/161:15-22}</p>	<p>Q. Now, again, I'm going to put to you what I understand to be your excuse based on appendix B to Wright 11. As I understand it, you say that there was a precursor document, different from both of these, which you edited to produce both of them.</p> <p>A. Hence why the date is before the course here, so, yes.</p> <p>Q. You've never provided that precursor document, have you?</p> <p>A. I don't have it.</p>	<p>Dr Wright admits that he has not disclosed the precursor document that he edited to produce these assignments.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day2/162:17} - {Day2/163:5}</p>	<p>Q. And then the other document that we were looking at earlier, {L1/323/1}, is a very odd document, isn't it, it's not a complete assignment?</p> <p>A. There are two questions there. No, it's not an odd document, it's a working document. And it's not an assignment in the same way. The courses, 22 - whatever, is an undergraduate course, taken at a postgraduate level, which Dr Gerlach ran. 6640 is the postgraduate phase. What you have are two separate things. For a masters student, you sit in on the undergraduate course, you complete all of that at 3 a higher level, and then you also do project work. So, apart from the normal everyday undergraduate assignments, you complete a project.</p>	<p>Dr Wright asserts that whilst he is in possession of a working document from 2005, he does not possess the alleged precursor document.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
DAY 3		
CROSS-EXAMINATION OF DR CRAIG WRIGHT BY JONATHAN HOUGH KC		
{I/1/5} First Expert Report of Simon Placks on Digital Forensics		
{Day3/3:10} - {Day3/4:12}	<p>A. No, I'm not. CCE, while an introductory certification, doesn't go into any of the issues. The certified examiner - the CNCE - is a tool certification. It just means you can run the tool and take an image. His PhD is not in any related topic, it is in the analysis of analysing communications to detect lying on chats, of which he determined that it isn't - he couldn't do it. In the two tests, he failed both times, and he said you can't detect - his method didn't detect any lying or deception. Now, on top of that, to be an expert doesn't necessarily require forensic certification. What it would require is Vmware, Vmsphere, someone with that qualification, Citrix, metadata, analysing a Citrix server. He has no experience or qualifications in Citrix or virtualised environments. He has no certifications in ROX or CentOS. He has no experience using virtualised machines running Linux. He has no experience and has never touched a metadata, Metaframe system. He has never touched a SAN, a NAS, or a corporate environment. So my answer is no.</p> <p>Q. Dr Wright, this is a man who has been a senior and experienced digital forensic practitioners for 20 years. Are you seriously suggesting that this man is not competent to express views on documents having regard to the possible use of virtualised systems?</p> <p>A. Yes.</p>	Dr Wright questions his own expert's competence.
{J/19/1} First Expert Report of Spencer Lynch - Exhibit 1		
{Day3/5:14-21}	<p>Q. Dr Wright, is Spencer Lynch an expert suitably qualified and experienced to give evidence on the matters he covers in his reports?</p> <p>A. No, he is not.</p> <p>Q. Well, I suggest to you again that he is a person, based on this CV, based on the contents of his reports, who is amply qualified and able to give evidence on digital</p>	Dr Wright questions his own expert's competence.

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	forensic investigations and digital forensic document examination.	
{Day3/6:5-16}	<p>MR JUSTICE MELLOR: Can I just ask a question. Dr Wright, presumably you would have been able to point your solicitors in the direction of people who were suitably qualified to undertake the forensic analysis in this case?</p> <p>A. Unfortunately, Ali Zafar and Christen Ager-Hanssen were signed up, without my permission, with Travers Smith, and everyone I mentioned with a SANS qualification, or other things, were summarily dismissed. So every single person I recommended was dismissed, without telling me, to my lawyers, which created a conflict, which is why I had to change from Travers.</p>	Dr Wright blames third parties (Ali Zafar KC, Christen Ager-Hanssen and Travers Smith) for failing to instruct a suitably competent expert (according to Dr Wright).
{L3/219/5} The Economics of central core BitCoin Nodes		
{Day3/10:25} - {Day3/11:10}	<p>Q. We're not talking about BTC Core, we're talking about the original design of Bitcoin.</p> <p>A. If I can finish. The original design of Bitcoin, and to give the analogy to explain the difference, I will need to do both. BTC Core has limited the transactions, having three to four transactions per second maximum. That cap limits the number of transactions that can be taken. That makes them more expensive. Whenever you have an economic scarcity, the price goes up, and we've seen that. In BTC Core, £45 to £60 transaction fees. That means no micropayments. That means a limit.</p>	Dr Wright is evasive, answering the question about the original design of Bitcoin with a speech on BSV.
{Day3/15:7-14}	<p>MR HOUGH: Just before we move on from this, would you at least accept this, Dr Wright, that the White Paper itself says nothing about large actors taking injunctions as a critical part of the protective elements of the system?</p> <p>A. No, it doesn't need to say that, because the system defines "honest" and "dishonest", and those terms are defined in British law.</p>	Dr Wright clearly shows his willingness to claim knowledge in a topic he has little actual knowledge of.
{H/121/4} Appendix PM26		
{Day3/16:1} - {Day3/17:5}	Q. Mr Madden concluded, and Dr Placks agreed on the basis of these findings, that the document was backdated. That's the case, isn't it?	Dr Wright blames third parties (indicating documents that appear to

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. No, it's not. What I need to clarify, though, is, you seem to be implying that my case is about proving metadata, or that these are reliance because of metadata. I'm going to very simply say, I put these in in support of what I do, the research I do. These documents are maintained on corporate servers. None of the ones you have have come from me directly; they've been taken from staff laptops and images, all of which were given over when I sold IP to nChain in 2015. So, while you're saying this, the thing to remember is, I never set up a time capsule, nor said that I did. What I said was I have files that I give to my staff members. I do that so that they can take my ideas. The way that I work is, I create the research, I have an idea. That idea is then fleshed out. Sometimes, when I say "I created a document", I, on a voice recorder, speak to it, sometimes I write handwritten notes, and then my staff do this for me. So, what I'm basically saying, these are the origins 21 of the 350 White Papers that I've completed. These are the origins of the 1,900 OI papers, which are original idea papers. These are the origins of the 1,040-something granted patents that I've created. These are the origins of the 4,000 plus filed patents that are now public and the other ones that are in the 18-month, as my Lord will know, secret period where we can change them.</p>	<p>be backdated were on staff servers).</p> <p>Dr Wright emphasises the number of patents he has connections to, here falling back on the concept of 'British law'.</p>
<p>{Day3/17:16} - {Day3/18:20}</p>	<p>Q. And you're aware that this, like many others in that list, contain metadata dating it to before the creation, or certainly the release of the Bitcoin System?</p> <p>A. Yes, I am.</p> <p>Q. And you're aware, aren't you, that your solicitors on your behalf said nothing to suggest that the metadata should be expected to be inaccurate, or that the documents had in fact been subject to alteration, deliberate and accidental, for many years since their creation?</p> <p>A. Well, actually, if you check Relativity and other platforms that you have access to, what you'll see is the majority of these come from either corporate servers or staff laptops; they don't come from me. There are very few documents, apart from the later ones, that came from me directly, so that was all in the chain of custody and it's in Relativity. So at no point have I ever said otherwise. In the Kleiman case, I explicitly said that all of these came from file servers. The QNAP server that was taken and not imaged well is -- was, when it was taken, a several hundred thousand pound rack system that was unfortunately taken with 250 terabytes worth of data that I can't access at the moment. So, what I'm telling you is, at no point did I say that this was a case about metadata from me. My case is different. My case is these are the origins of the ideas I've created, my Lord, these are the</p>	<p>Dr Wright blaming third parties (his solicitors) for the failure to notify COPA that documents he disclosed were supposedly unreliable.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	things that led to how I have those patents. We, last year, did 79 patents at nChain.	
{M/1/778} Letter from Ontier to Bird & Bird of 11 May 2023		
{Day3/19:25} - {Day3/20:10}	<p>Q. If we can go through this document, it refers to most of these documents simply as having been drafted by you, typed by Lynn Wright. There's no suggestion that these documents were likely altered by other people in the process of transmission, is there?</p> <p>A. The files naturally alter. This is the issue I've been saying. I've done, in my career, before I did Bitcoin, over a thousand engagements, and in a thousand engagements, I have never once seen a file that is more than five years old that is pristine. The only way for that to happen is an anomaly.</p>	This is contradicted by the large number of pristine documents in his disclosure.
{Day3/21:18-21}	When I gave these files over, I didn't think, in 2009, "Hey, I'm going to be in court 15 years later saying 'I'm Satoshi'". In fact, I never wanted to be known as Satoshi. I didn't want to come out at all.	Dr Wright recites his PR spin on this case and claims that he never wanted to be known as Satoshi.
{Day3/21:22}- {Day3/22:19}	<p>Q. We'll come to that later. You've made that point. But you did choose to identify these documents and you did choose to give chain of custody information which made no suggestion that they were altered by numerous members of staff, as you're now telling us.</p> <p>A. Again, "altered" is wrong. Used. And, yes, if you actually look in Relativity against those ID numbers, you will see laptops that aren't mine that they came from, you will see file servers that are corporate. So, I'm sorry if I -- I didn't explain that, but I didn't think that I would need to explain that when a third party document has been through multiple staff and employees, that I need to explain that it could be different.</p> <p>Q. Well, let me just put this point to you before we move back to the document and make some progress, and this is for the experts to address later. It's right, isn't it, there are many documents in this case which are pristine, like one of the BlackNet documents we looked at yesterday, and like the real White Papers?</p> <p>A. Yes. Out of the many documents, some have been untouched. I'm actually surprised. And I wouldn't call them pristine; they're not perfect, but they're close.</p>	<p>Compare what is said here to Dr Wright's DRD (K2/2):</p> <p>"The data sources set out in Annex 1 were collected from or on behalf of the Defendant in the period 2018 - 2020, and imaged, for the purposes of complying with the Defendant's disclosure/discovery obligations in separate US proceedings (which concluded in December 2021) and separate English proceedings. In the production orders issued in the US proceedings "Defendant" had a broader meaning than Dr Wright in his individual capacity and</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
		<p>was defined as the following:</p> <ul style="list-style-type: none"> - Craig Wright and any Person or Trust (as defined herein) of which (a) Craig Wright is an owner, shareholder, member, manager, director, officer, trustee, employee, or beneficiary of (“CSW Persons/ Trusts”), or that (b) is controlled by Craig Wright or any CSW Persons/Trusts; - “Person” or “Persons” shall mean each and every individual, corporation, partnership, joint venture, social or political organization, or any other entity, incorporated or unincorporated, or encompassed within the usual and customary meaning of “person” or “persons”; - “Trust” includes any arrangement, entity, vehicle, agreement, deed or relationship, in any jurisdiction, where the person with title or control over property has duties to deal with it for another’s benefit. Due to variances in various jurisdictions’ laws, this definition should not be given an overly formalistic construction, but a liberal one. It should include any arrangement bearing a similarity to a “trust”, and any such arrangement you (or others) have actually referred to as a “trust”; <p>(the “US Defendant”).”</p> <p>Dr Wright also undermines his previous assertion, by accepting</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
		that there are some pristine (or close) documents.
<p>{Day3/23:20} - {Day3/24:14}</p>	<p>Q. Again, I need to ask you to answer the question. If there is a disconnect between this article and the paragraph to which it was footnoted, that is equally consistent with being a clumsy edit, isn't it?</p> <p>A. No, not at all. It's equally consistent with someone opening up and not saving properly on Citrix Metaframe.</p> <p>Q. You also say, in appendix B to Wright 11, that what happened to this document was that copying of it in 2019 caused fragments of other documents to be merged into it. Have I got that right?</p> <p>A. Yes, you do.</p> <p>Q. Now what I have to put to you, based on Mr Madden's careful explanation in Madden 4, is that a process of merger, or the use of templates, would not cause text to be carried over to create a readable document, would it?</p> <p>A. That's actually incorrect, and I've tested this. When you actually use Citrix Metaframe, different versions of Word and .M files, the templates will result in changes, even when you don't save. This is especially prevalent when you have Linux as the back end rather than Windows.</p>	<p>Dr Wright refuses to accept that clumsy editing could be the cause.</p>
<p>{H/126/3} Appendix PM29</p>		
<p>{Day3/26:4-15}</p>	<p>Q. And Mr Madden concludes, page 3, please, {H/126/3}, that that indicates the use of computer clock manipulation as would be used in backdating a document, and Dr Placks agrees; that's right, isn't it?</p> <p>A. No, it's actually incorrect. The operation of Citrix leads to persistence, as I've stated, and the date on the file date when copying using Xcopy, as I showed in my witness statement, leads to these changes.</p> <p>Q. Are you aware that both of experts reject those explanations?</p> <p>A. The expert actually said that Xcopy can be used in manipulating timestamps.</p>	<p>Dr Wright's disagreement with both experts on computer clock manipulation.</p>
<p>{H/127/1} Exhibit PM29.1 Economic Security Blog Post</p>		
<p>{Day3/27:15} - {Day3/28:10}</p>	<p>Q. {H/127/1}, please. Mr Madden also found online an article by you headed, "Economic Security", on the</p>	<p>Dr Wright's discussion of how his blog operates and</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Medium website with a publication date of May 2009 [sic]; do you see that?</p> <p>A. I do.</p> <p>Q. Did you write that article?</p> <p>MR JUSTICE MELLOR: Sorry, 2019.</p> <p>MR HOUGH: Sorry, 2019. I'm sorry, I mis-spoke, my Lord.</p> <p>A. Yes, I wrote the paper and that goes to an article. To explain how this works, my Lord, I have -- I write papers and they go now to Sebastian, in the past to other people, including Alex, and they run my blog. I write the paper and they go into a list of what gets published and I send these documents. My backlog at the moment is four years, where they publish weekly or so. So basically, there are -- every time I -- I do a number -- I'm still in university, I'm an Aspie, so I haven't managed to get out of university yet, and I do a lot of courses and I write at least one paper every two days. They go into a backlog, like these other papers, and they select them and they publish them.</p>	<p>how he writes a paper every two days.</p>
<p>{H/128/1} Exhibit PM29.2</p>		
<p>{Day3/28:11-24}</p>	<p>Q. Can we move away from the fetching photograph of Al Yankovic in a tin foil hat to the comparison between this, your article, and the document, {H/128/1}. Now, this is a table in which Mr Madden's compared the face value of the document, the redundant draft and the medium hosted blog. Would you accept that the redundant draft of the document closely matches your article which was posted, at any rate, in 2019 and speaks of Bitcoin as a system already in operation?</p> <p>A. Yes. As I noted, my -- the employees at nChain who run this would have various versions of this document and they would have chose one to load and probably edited it.</p>	<p>Dr Wright shifting blame onto third parties - employees at nChain – for anomalies in the document.</p>
<p>{CSW/2/30} Appendix B to CSW 11</p>		
<p>{Day3/29:22} - {Day3/30:14}</p>	<p>Q. This presumes, doesn't it, that you write, first of all, a version with present tense references to Bitcoin and additional content, then Lynn Wright edits it to change to the future tense and removes some comments; correct?</p> <p>A. Not necessarily, no.</p>	<p>Dr Wright's comments on the change from present to future tense.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Well, the remnant text speaks in the present tense, the face value text speaks in the future tense, so if the face value document has been produced by editing the remnant text, then the present tense references have been changed to the future tense; correct?</p> <p>A. No, that's not what I said there. What I've said is those two documents are different. I didn't say that Lynn edited the first one to get the second one, I said she edited the face value document. After that, it's been edited again. I don't know which of my staff and when. It could have been right at the beginning. I had staff in 2009 and I've had staff now. So what I'm saying is there are different versions of documents.</p>	
<p>{Day3/30:20} - {Day3/31:13}</p>	<p>Q. And what you've done just now is to embellish the excuse by adding another layer of editing with other people, which you didn't even mention in your appendix B a couple of weeks ago?</p> <p>A. I said I had employees. And even what you're saying is wrong. As I say at 8.6. What you're saying is this is about the future, but it isn't. The attacks that I were [sic] getting happened before the launch the Bitcoin. My Lord, before I even launched Bitcoin, I was on the mailing list and people like James Donald came up and started explaining why my system was wrong. They talked about this idea it will -- I mean, I said it will end in server farms, and they said, "Oh, the government will take it over", and they had rants and I had rants, and my idea there was -- actually, I got quite annoyed, that's why I elided(?), and one of the few times a spelling mistake from Satoshi happened. And James Donald and others were basically saying how my system was wrong before I even launched it to try.</p>	<p>Dr Wright refers to people that he spoke to about Bitcoin (including James Donald) about his system. If this were true, there would be many people who knew he was Satoshi in 2009, and yet there are no such witnesses in these proceedings.</p>
<p>{H/142/1} Exhibit PM35.1 Random Graphs and Complex Networks</p>		
<p>{Day3/34:15} - {Day3/35:20}</p>	<p>Q. May we go to {H/142/1}, and at page 2 internally, please -- sorry, page 20, which is internal page 2 {H/142/20}. Page 20 of the PDF, which is internal page 2. Thank you very much. If we look at the second sentence, it reads: "A graph $G = (V, E)$ consists of a collection of vertices, called vertex set, V and a collection of edges, called edge set, E." Now, just this simple question, no need for any digression: is that the same sentence that we saw earlier?</p> <p>Q. This was obviously the source for the section of your document we looked at, isn't it?</p> <p>A. No, actually, van der Hofstad -- Professor -- started, around ten years before this, teaching this topic. Now, this</p>	<p>Dr Wright raises a new excuse, that he found external notes and copied them.</p> <p>Dr Wright admits the content matches.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>book is actually an amalgamation of all the lecture notes and it has grown. So the version here is actually an earlier version and there are now two versions. My Lord, the person has taken their course notes, which were available earlier, which I had access to, because as I said, I was a postgraduate statistics student, I was a researcher at a university, and I worked on these topics and, like most postgraduates, I grabbed every set of notes I could from every professor I could in my topic. That included ones in my university and others, because postgrad is different from undergrad. When you're a postgrad, you're doing research. So I found the lecture notes of this professor, which were turned into this book, and I used them.</p>	
<p>{H/141/8-10} Appendix PM35 “The study of Complex Networks”</p>		
<p>{Day3/36:10-14}</p>	<p>Q. Now, Mr Madden's researches told him that the first 48 version of the book, which happened to contain all the passages reflected in yours, was the fifth edition available online, produced in 2016, yes?</p> <p>A. That's what he said, yes.</p>	<p>Dr Wright claims he had notes of a 2016 book, when his notes are dated 2008.</p>
<p>{H/107/9} Appendix PM23</p>		
<p>{Day3/39:24} - {Day3/41:8}</p>	<p>Q. Now, Mr Madden made a number of findings that 53 the document wasn't authentic with which Dr Placks agreed. Let me put one of them to you, {H/107/9}. If we look at paragraph 24, he found that the metadata indicated that the document had been created using the version 2.4 of the OpenOffice.org software, which wasn't released until some weeks after the supposed creation date of the document. That dating was then confirmed by evidence from Joost Andrae, which Mr Madden received from Bird & Bird. Are you aware of those findings?</p> <p>A. I am.</p> <p>Q. It's right, isn't it, that it wouldn't have been possible to generate those metadata tags before the creation of OpenOffice in that version, would it?</p> <p>A. No, actually, it's very possible. I'm not saying that this happened in this case, but to do this, all you need to do is fill out a metadata tag. Now, when I used OpenOffice, I also stated that I used LaTeX plugins. Now, as I've demonstrated, the metadata in any document in a LaTeX area can be set. Using the HTML ref, you can put down any timeframe you want, any program, any operating</p>	<p>Dr Wright resorts to incoherent technical ranting to avoid providing a proper answer as to how it would be possible to generate anachronistic metadata tags.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>system. In my 2007 forensic book and also then in my later book on audit, one of the things I do note is changing versions of systems. The reason I say this, my Lord, is attackers, well, basically, attack based on known versions. So one of the things I would do back then would make funky versions. I used to teach this to my students as well. So, things would actually -- it's difficult on Windows, because it doesn't let you do it, but on Linux and applications that you build, for instance DNS software, if you change the version information, it makes it so that attackers use the wrong attacks. And the same happens with other applications.</p>	
<p>{CSW/2/33} CSW11 Appendix B</p>		
<p>{Day3/42:9-19}</p>	<p>Q. You say you deliberately altered the metadata of this document as a demonstration tool for students, right?</p> <p>A. I demonstrated many documents as demonstration tools to students.</p> <p>Q. Again, that wasn't the question. You're saying that you altered the metadata of this document as a demonstration tool for students?</p> <p>A. That is not what I said. I said I used to do it for that. I also did it when I was writing my book on the topic. So which particular time I did these things, I don't remember.</p>	<p>Dr Wright was evasive when answering a question regarding his manipulation of documents, which he says he used as a demonstration tool.</p>
<p>{Day3/43:5-18}</p>	<p>Q. But you don't say that in your appendix B, do you?</p> <p>A. I'm giving an example of one of the times. I did not say every time I've done it. At no point did I say it was every time that I've ever done this.</p> <p>Q. Let me put to you, the clear implication of your appendix B evidence is that your alteration of this document was as a demonstration tool for students.</p> <p>A. Again, it could have been. It could also be for the other purpose. On top of that, it could also be that I changed the -- re-did the document from LaTeX at a later date and it could have even been that version of OpenOffice, because if I was to use LaTeX and timestamps that are set and build it later, but I don't have the original LaTeX code, so I can't tell you.</p>	<p>Dr Wright backs away from his own sworn evidence.</p>
<p>{Day3/43:24} - {Day3/45:3}</p>	<p>A. No, actually, this is another area you don't understand, I'm sorry. Anonymous is not pseudonymous. So if we look at many authors through history who have been known pseudonymously, even recent ones like a certain author of Harry Potter, pseudonymous is not unknown. I was pseudonymous, private. The tax office in Australia knew who I was, government officials knew who I was,</p>	<p>Dr Wright claims that he, as Satoshi, was willing to reveal his identity to students and that this doesn't contradict</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>individuals at companies knew who I was; I just didn't want to be public. There's a big difference. So many people knew.</p> <p>Q. Pausing you there, and just to be clear that we dispute all of what you've just said, but it's right, isn't it, that if the real Satoshi had wanted to stay even pseudonymous, it would have been absurd to reveal the entire game for a bunch of random students?</p> <p>A. Not at all. They weren't random students. One of these people is Shoaib, who was my student, as well as being a student with him. Shoaib, for instance, ended up working in my companies and being a director of one of them and had a lot of interaction. So, my Lord, a lot of students ended up working with me. So, why would I think hiding from them? I actually want my students to know about my stuff. The fact is, then they trust me and they know me. And people like Shoaib knew what I was doing for years, but he didn't go out to the world and go, "Hey, Craig's Satoshi". He worked on systems, he sources them, he went and visited the companies. But that's different: people you can trust versus the world. I didn't care about being anonymous, I cared about being private.</p>	<p>Satoshi's clear intent to remain pseudonymous.</p>
{Day3/45:4-8}	<p>Q. Can you give us the name of all the other students, other than Shoaib, who knew that you were Satoshi and who will be giving evidence in this case?</p> <p>A. Who will be giving he was in this case, David Bridges was also a student.</p>	<p>Bridges does not say anywhere in his witness statement that he was a student of Dr Wright.</p>
{H/124/6} Appendix PM28 "Non-Sparse Random Graphs"		
{Day3/48:17-22}	<p>Q. As Mr Madden finds on this basis, and Dr Placks agreed, this is another backdated document, isn't it?</p> <p>A. No. Again, when using Metaframe and Citrix applications, you have shared access to files. Unfortunately, neither Mr Placks nor Mr Madden have ever taken even a basic Citrix course.</p>	<p>Dr Wright disagrees with both Mr Madden and Dr Placks, and uses Citrix as excuse for backdated documents, which is technically implausible.</p>
{L1/371/1} Document 1 - Non-Sparse Random Graphs.pdf		
{Day3/50:5-16}	<p>Q. What I put to you simply is that this document, which can't be analysed in the same way, is no more authentic than the electronic version, is it?</p> <p>A. It can actually be analysed, and it was. Ontier had done a handwriting and other paper analysis showing that it --</p>	<p>Dr Wright shifts the blame to Ontier.</p> <p>The ink analysis pinholes that we discovered in the hard copies Bird & Bird</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Just --</p> <p>A. -- several years old --</p> <p>Q. -- just be careful about relying upon things that are privileged and that haven't been disclosed, Dr Wright. I'm just going to stop you there to give you the opportunity not to go into privileged matters.</p>	<p>inspected are referred to in ISC {M/2/6}.</p>
<p>{L3/288/2} Maths.doc</p>		
<p>{Day3/53:14-22}</p>	<p>Q. Can you at least agree that this document in this form is not authentic to 2008?</p> <p>A. None of them are from 2008, if you're going to look at it that way, because they have all been accessed and all used.</p> <p>Q. So would you accept, on the basis of what you've just said, that none of your primary reliance documents are authentic to their stated dates where they're 2008?</p> <p>A. No, I would not. Again, you're --</p>	<p>Dr Wright was evasive when answering and initially undermined all of his reliance documents, before rowing back. It is not clear what his ultimate answer is.</p>
<p>{H/139/7} Appendix PM34 Maths.doc</p>		
<p>{Day3/54:24} - {Day3/55:5}</p>	<p>Q. The obvious inference is that this document has been edited in such a way as to include those dates, giving an impression that the document was drafted before the release of Bitcoin, isn't it?</p> <p>A. No, it's not. It's basically a document that has been used, and over time, researchers have accessed the documents. I've never denied that.</p>	<p>Dr Wright shifts the blame to third parties, researchers who accessed the document.</p>
<p>{H/118/10} Appendix PM25</p>		
<p>{Day3/59:11} - {Day3/60:4}</p>	<p>A. Not at all. As I've noted multiple times, when you use Metaframe, when people have access to documents, these things change. Now, this version of document was on employee machines and accessed, and the reason for that is that I allowed them to access these things. To understand the purpose I had for Bitcoin, these files were made available.</p> <p>Q. But you say not changed?</p> <p>A. A system changes something by itself. So, if you're talking about changing a document, then the system does</p>	<p>Dr Wright backs down from his previous decision to blame other people, taking an inconsistent stance.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>things like changing schemas, but that doesn't mean a user did it, so that's not manipulation.</p> <p>Q. Are you able to say that all these many people who had access to this document didn't make any changes to the text?</p> <p>A. Yes, this is the same. When you have a read only access but administrator access in Citrix, the document can update schemas and make changes in the background while not letting the user make changes.</p>	
<p>{Day3/60:5} - {Day3/61:18}</p>	<p>Q. In your appendix B, your excuse was that the references to the anachronistic fonts and schema appeared because of your businesses having group policies that implemented normal .M template files; that's right, isn't it?</p> <p>A. That is correct, and when they're implemented over the Citrix environment, this is how they react. So, the normal .M is run as a domain administrator. That is a macro enabled template, and all of the corporate updates happen. Now, that happens at the same time as the user accesses the file. But even if the user has only read-only access, there's a disparity between the system having access and the user having access. So the file won't be updated by the user, but it can be by the system.</p> <p>Q. I'm going to put these points to you in response to that based on Mr Madden's conclusions. It is simply wrong to say that making a change to a current template causes existing or past documents to be altered in the way you've suggested, isn't it?</p> <p>A. No, that's actually incorrect, and he's talking about a DOCX template. These, and, as you'll notice, other ones, have ".M". .M is a macro enabled template. My Lord, a macro enabled template, to explain, is a template with Visual Studio Code in it. So programming in there. So that enables the organisation to make updates and keep consistency across other documents. It's not designed for these documents, but mainly for marketing documents and other such things.</p> <p>Q. And it's also nonsense to suggest that Grammarly, the Grammarly timestamp, would alter other than through Grammarly interacting at a user's command, isn't it?</p> <p>A. No, that's, again, incorrect. The Grammarly system doesn't embed a timestamp of this type on the normal one. It's only done in the Enterprise version. The reason I would put is that Mr Madden couldn't replicate this himself is he didn't use the Enterprise version. The Enterprise version is a business version that runs for the organisation.</p>	<p>Dr Wright is not accepting the obvious truth of Mr Madden's finding regarding anomalies that Dr Wright says come from template changes, and the presence of Grammarly timestamps.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{H/236/6} Exhibit PM43.16		
{Day3/66:16-24}	<p>Q. Page 6, please, {H/236/6}, can we have the screenshot blown up. Do you see on this screenshot, the "Open Grammarly" button at the top left?</p> <p>A. I do.</p> <p>Q. And that was the same software which left the embedded timestamp in the backdated reliance document?</p> <p>A. No, actually, this is not the business version. The Enterprise version is used in the organisation, but I don't, at this point, have an nChain laptop.</p>	<p>Dr Wright accepts that he himself uses the standard version of Grammarly.</p>
{CSW/2/18} CSW11 Appendix B		
{Day3/69:4-25}	<p>MR JUSTICE MELLOR: Dr Wright, why would you post on SSRN your LLM proposal?</p> <p>A. Because I had been working on this topic, so I posted both my LLM and the proposal to show the differences. When I first started, my first thing was I put in "trusted third parties" which was rejected by the university, because "trusted third parties" is a term of art in computer science, but payment intermediaries is in law. So I had been using the wrong terms, but only because they mean the same thing. There are a few other differences as well that I had to remove. So, I put a full version of what I'd initially proposed as well as my thesis. Part of the reason for that is that that was the entirety of my marking. So, in British universities, for masters, that's quite common. I've just submitted a proposal at University of London for another masters, and that follows with the dissertation, which will be due in March, but both get marked. So, because one is 25% of the marks and the other's the rest of the marks, I considered that the proposal and the dissertation should both be put up.</p>	<p>Dr Wright only provides a vague, rambling response, with no good answer to Mellor J's question as to why he uploaded his LLM proposal.</p>
{A1/1/2} BTC Core Claim Form		
{Day3/72:9-22}	<p>MR HOUGH: Dr Wright, when you said you're not suing people for hundreds of billions of dollars, you're wrong, aren't you?</p>	<p>Dr Wright refuses to accept that he is suing the Developers for claims said to be worth billions.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. No, actually, if I'm correct -- which I am -- and all of the different aspects, including the patented material that is granted patents that are in BTC Core's products, aren't there, then this isn't I get that money, this is how the market reacts. Right now, if it is found out, as I'm saying, that nodes, aka pools, can be put under a legal constraint that the Sinaloa cartel can't pass money through them, that North Korea can't pass money through BCC, that it can be seized, that's worth hundreds of billions of dollars, not to me, to the industry.</p>	
<p>{Day3/73:1-25}</p>	<p>Q. Dr Wright, this is a statement of value in a court claim form in which a party who is bringing a claim says how much they want to recover. Did you not understand that that was the significance of the statement of value when you endorsed this and other similar claim forms?</p> <p>A. The value has that in what I will personally lose, not that I get from you. My Lord --</p> <p>MR JUSTICE MELLOR: Can you answer the question, Dr Wright.</p> <p>A. I'm trying to, my Lord. What I'm saying is, I will lose, potentially, hundreds of billions of dollars, because if I'm right and I didn't do everything the way that I'm doing and I did the BTC Core way of doing it and I was an anonymous Satoshi, I would be worth lots more money. The value is what diminishes.</p> <p>MR HOUGH: So is your position now, Dr Wright, that, the statements of value saying that your claims, including this one, are put at hundreds of billions of pounds do not mean that you are trying to recover sums of that amount, contrary to what anyone would understand the court statement of value to mean?</p> <p>A. No, I don't think I would recover hundreds of billions of dollars. I don't think that would be possible. In fact, the value would go down.</p>	<p>Dr Wright provides evasive responses, refusing to accept clear facts and providing false statements in response.</p>
<p>{H/118/11} Appendix PM25</p>		
<p>{Day3/75:17} – {Day3/76:4}</p>	<p>Mr Madden found, in relation to the editing times of these documents, that the editing times for both of the last documents we've looked at were unusually long, and the edit time for the last one was longer than the period between the creation and the last saved date, which Mr Madden finds is impossible. Again, I put it to you that that's another sign of manipulation of these documents.</p> <p>A. No, actually, it's not. As I have explained multiple times, the use of Citrix Metaframe, corporate</p>	<p>Dr Wright discusses the claimed impact of computing environment.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	environments and tools in PowerShell, such as Xcopy, produce these results. The analysis being provided is under a presumption of a home user laptop.	
{L18/373/27} Exhibit HP-[6] Wright LLM Thesis		
{Day3/80:20} – {Day3/82:5}	<p>Q. Can I stop you there and focus on the question I'm actually asking you. In your 11th witness statement, you spend six or seven pages setting out what you say are linguistic parallels between the proposal and the Bitcoin White Paper, but you don't draw any similar linguistic parallel between the Bitcoin White Paper and the actual dissertation, do you?</p> <p>A. No, not linguistic. What I note, as a whole. But I note that there was poker code and this exact area you have here talks about that.</p> <p>Q. So, Dr Wright, on your account, you included references to your innovative new system that you were working on in the proposal, but cut them all out when you came to the actual dissertation?</p> <p>A. Yes.</p> <p>My Lord, as a person who has studied engineering will know that when you have a system being mentioned, unless it's particularly the thing you're working on, when you're writing a paper, you have to take them out in academic terms. So when I first proposed this, the first comment is, "Well, you're not writing about a computer science project, you're doing an intermediary project, so please write it based on that". So, I restructured my proposal from Northumbria into what this ended up to be.</p> <p>Q. Pausing there, do you have any documents to evidence the university coming back to you and saying you needed to take this out?</p> <p>A. No, I don't have any of my Northumbria emails -- very few of them.</p> <p>Q. And presumably you don't have any person who can back you up on that?</p> <p>A. It has been quite a number of years. It was actually surprising that Northumbria still had a copy of my dissertation.</p>	<p>Dr Wright evades the question, refusing to accept a clear fact.</p> <p>The evidence of him being expected to remove the system in engineering papers is lacking.</p> <p>The Northumbria emails are further missing/lost documents.</p>
{Day3/83:18} – {Day3/84:6}	Q. The documents sent back by the university didn't include the proposal which you then go on to discuss at length in the statement, did they?	Dr Wright shifts the blame to third parties for failing

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. I don't know, I've got conflicting narratives on that one, but that proposal should have been with the marked copy.</p> <p>Q. Just to be clear, Dr Wright, in your 13th statement, I think it was, you made clear that you weren't saying that the proposal form came back in the letter from the university; that's right, isn't it?</p> <p>A. What I'm saying is, we cannot verify because no one checked. No one opened the document and put down what was actually there, so we don't know what is in the -- the contents of the envelope in that way.</p>	<p>to check documents from the University.</p>
<p>{CSW/23/1} Letter to Simon Cohen</p>		
<p>{Day3/84:20} – {Day3/86:7}</p>	<p>Q. And you cannot say, as you make very clear in your 13th witness statement, that it included the proposal? The first time I saw the document was when I opened the envelope at Shoosmiths. When I opened it, the thesis had that document, the proposal, inside when you open the front cover. The first time that I had accessed that was with people from Shoosmiths, so that I -- I didn't put anything in there. We opened the envelope, that envelope had the thesis, but the front cover had the proposal inside.</p> <p>Q. There's not a word of that story in your 11th or 13th witness statement, is there, Dr Wright? Not a word of it.</p> <p>A. The way that it worked was --</p> <p>Q. No, just an answer to that question before you digress, please. There's not a word of that explanation in either statement, is there?</p> <p>A. As stated, I can't say what happened before that happened.</p> <p>Q. Again, I really have to press for an answer to the question. The story you've just told about one document being inside another, there's not a word of it in your 11th or is 13th statement, is there?</p> <p>A. As far as I'm concerned, my thesis includes the proposal which I sent. So when I said "the proposal" -- I wouldn't have said "the proposal", I would have said "the thesis", and when I said "the thesis as published", that would include the proposal. That's why I loaded both on the website.</p> <p>Q. For the final time, your 11th and 13th witness statements did not include a word of the story you've just told me about one document being inside another, did they?</p>	<p>Dr Wright refuses to accept the changes in his story and the contradiction with the actual documents, about whether his LLM Proposal was included in a letter from the University.</p> <p>Ultimately, Dr Wright fails to answer the question.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. I did not say that my proposal was put inside my other document when it was marked. As far as I'm concerned, the two documents are part of the one. Just like my current one at University of London, they're part of the one.</p>	
<p>{H/132/14} Appendix PM31 “UCP500.doc” {CSW/3/16} CSW 11 Appendix C</p>		
<p>{Day3/90:18} – {Day3/91/19}</p>	<p>Q. I suggest to you that it wouldn't have been very sensible to do that if it was one that had simply been edited by someone else in 2015; it wouldn't prove anything.</p> <p>A. No, actually, it does. This was a university paper that I'd done that I then sent for publication at a -- a college here in the UK, so my argument is not that this has anything to do with metadata, and there are other things, including the email to Professor Bradney. So, my paper demonstrates that I was writing these topics contemporaneously and that there'd be no reason for me to edit metadata on my own document that is sent to other parties.</p> <p>Q. Well, Dr Wright, just focusing on the document that was analysed, which you've accepted was edited, it would be a bit bizarre, wouldn't it, for somebody at nChain, in 2015 or afterwards, to be editing your LLM homework?</p> <p>A. No, it actually wouldn't. The documentary credit here is still valid. So, one of the -- actually, an area that we've got probably 40 patents granted on is international trade and finance, and looking at this, this is a way of embedding into Bitcoin script, so we're talking about the basics. So, for -- my homework is not just my homework in university, it is a training session for staff; people read this. So why was that updated? Probably because the site wasn't available any more, so that they've gone back and added one.</p>	<p>Dr Wright gives an incoherent answer, citing a missing email to a previously unknown person (Professor Bradney).</p>
<p>{E/32/6} Thirteenth witness statement of Dr Wright</p>		
<p>{Day3/100:22} - {Day3/101:4}</p>	<p>Q. You were saying there, confidently and clearly, to the court and all of us, that the proposal was not attached to the University of Northumbria letter, not in that envelope, weren't you?</p> <p>A. No, I said it wasn't attached to the letter. “Attached to the letter” would mean something like stapled or something similar. Because it wasn't stapled, I can't say whether it is the same.</p>	<p>Dr Wright evades the question of whether the LLM proposal was attached to the letter from Northumbria.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day3/101:11} - {Day3/102:4}</p>	<p>Q. If you'd wanted to say that, "I think it was enclosed with the letter, although not physically attached with a stapler", that would have been the place to say it, wouldn't it?</p> <p>A. No, it wouldn't.</p> <p>Q. This statement is setting out a version which is flatly contrary to what you have said today and you are telling the court lie after lie, aren't you, Dr Wright?</p> <p>A. I have not lied at all. I apologise if I need to clarify, but where I said it's not attached to the letter, I mean the letter was standalone, it was a single piece of paper. I believe that the stapled document was inside that other document. Certainly when I opened the envelope, those were all together. The only things in that envelope were the letter, my printed thesis and the proposal, and I have no reason to believe that someone slipped it in there, and I certainly don't believe my solicitors would have done something like that.</p>	<p>Dr Wright flatly contradicts what he said in 20(d) of CSW13.</p>
<p>{Day3/102:10} - {Day3/102:20}</p>	<p>Q. I just ask you if you accept this basic proposition. If a -- with a .DOC file, if any change to the file at all occurs which is committed to the file, whether content, properties, internal tags, like Grammarly tags, the root entry timestamp changes, doesn't it?</p> <p>A. No, it doesn't need to. That's only when you're running on a laptop in a standard mode. The behaviour on Citrix virtualised environments and other similar areas where there's shared access is very different. In these, you have a, basically, template file and schema that can be loaded separately. When you open a file, the schema file can be accessed separately, and that can be updated without the document.</p>	<p>Dr Wright's response to Madden, in which he cites the use of his Citrix environment (implausibly) to explain the addition of Grammarly tags and other document anomalies.</p>
<p>{L2/159/1} BDO Minutes from August 2007</p>		
<p>{Day3/104:20} - {Day3/105:9}</p>	<p>Q. I'll deal later with your story that you sought to pitch Bitcoin in this way to BDO, but I'm just focusing on the document here. Do you recall, and I can show you the transcript if you'd like, that in the Granath trial, you said that the second entry was, "Finish POC", meaning proof of concept, an initial working version of the Bitcoin code?</p> <p>A. Well, technically, it's Timecoin code, but, yes.</p> <p>Q. And do you recall that in the Kleiman trial, you said that the second entry was, "Finish DOC", document, and that it was a reference to the Bitcoin White Paper? Would it help for me to show you that?</p>	<p>Dr Wright claims he made a mistake in the Kleiman trial when discerning the meaning of the minutes.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. No, I think I made a mistake in that one, but it's been many years, but I would say it's "POC". My own handwriting even escapes me sometimes.</p>	
<p>{L17/327/88} Kleiman Transcript Day 14</p>		
<p>{Day3/105:24} - {Day3/106:21}</p>	<p>Q. Then over the page, page 88 {L17/327/88}, and you said: "That's: 'Finish doc' ... When you said 'POC' ... This is: 'Finish doc', which would be the whitepaper." And you agreed it was DOC, not POC. So you were quite specific about that, weren't you?</p> <p>A. I was.</p> <p>Q. You can take that off screen. You're aware, aren't you, that we have evidence from Mr Stathakis and Ms Li, who are responsible for manufacturing this from of Quill notepad, that the first version ever produced of this pad was produced in March 2012?</p> <p>A. I'll have to answer that in two parts. First of all, I'm not aware that they were actually involved at all, rather Quill was purchased by Bantex. The person you're talking about had no interaction with Quill and was only there after five years later. The Chinese factory that Ms Li is from had nothing to do with the printing at that stage either, they were Bantex. They were merged into another Chinese factory. The other part is that the PDF, as Dr Placks showed, was not the first version, so there were earlier versions. So, no, I can answer, that's not correct.</p>	<p>Dr Wright claims greater knowledge of the origins of the Quill minute pad than the knowledge of individuals working for the company and its predecessor.</p>
<p>{C/17/1} Claimant's Amended First Hearsay (CEA) Notice</p>		
<p>{Day3/107:19} - {Day3/107:22}</p>	<p>A. I actually do. I used to work for Corporate Express, which is now Staples, and other family members still do. Quill and Bantex were both Australian companies. I have had dealings with both of them since the '90s.</p>	<p>Dr Wright provides entirely new information on his connection to Quill/Bantex.</p>
<p>{Day3/109:16} - {Day3/110:10}</p>	<p>Q. Dr Wright, you are making this up as you go along without any supportive evidence for a word of this, aren't you?</p> <p>A. Can we look at the first page?</p> <p>Q. Yes. {C/17/1}.</p> <p>A. Quill brands was not always owned by Hamelin Brands. Before 2015, Quill was an independent company. At that time Hamelin Brands was known as Bantex. Bantex basically purchased Quill. The person involved</p>	<p>Dr Wright evades the question, refusing to accept a clear fact.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>was a manager from the other company. He had nothing to do with Quill, they were competitors.</p> <p>Q. Dr Wright, we're going round in circles, but I'm just going to put to you again, this statement is perfectly clear that the Quill product had been manufactured by the factory in Shenzhen, and Ms Li, who confirmed this statement, was responsible for it.</p> <p>A. To be perfectly clear: "The person who managed our investigation from Australia ... [Mr] Stathakis, Sales Director, Hamelin Brands."</p>	
{CSW/2/67} CSW 11 Appendix B		
{Day3/110:25} - {Day3/111:6}	<p>A. No, it's a difference between size. One is slightly larger than the other. It's not about pixelation. That's a scan.</p> <p>Q. I'm going to suggest to you that, looking pretty clearly at the grid, it's a question of pixelation not size?</p> <p>A. No, very clearly, that's why I drew the two lines in there. It's a question of size.</p>	Dr Wright refuses to accept a clear fact that the differences between the print proof of the notes and his disclosure document are because one of them is a scan.
{H/31/7} Appendix PM5		
{Day3/113:2} - {Day3/113:10}	<p>Q. But you go further, don't you, Dr Wright? You say that Mr Stathakis and Ms Li are wrong in what they say in their confirmation about how, when and where this document was produced based on information you have, don't you? That's what you said before at the start of questions this afternoon?</p> <p>A. My CV, that is part of this, has that I worked at Corporate Express. Corporate Express/Staples are one of the global providers and suppliers of that brand.</p>	Dr Wright claims his CV shows that he worked in the stationery industry.
{K/11/1} Chain of Custody of Reliance Documents		
{Day3/116:21} - {Day3/117:8}	<p>Q. Column R states that for each document: "Ontier was provided with a login to the MYOB live system and were talked through how to take screenshots for evidence. "The Ontier account was used to login and download each of these and add them as evidence." Was that also information given on your instructions?</p> <p>A. I basically told the log-in to be given to several email addresses of solicitors. Those solicitors had then a log-in</p>	Dr Wright seeks to blame third parties (Ontier).

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	to MYOB. I told them that I could get it online. For some reason they downloaded it. Both are valid versions, I guess.	
<p>{Day3/118:6} - {Day3/118:13}</p>	<p>Q. And you give a fairly detailed explanation there, didn't you?</p> <p>A. I do, but I can't tell you, from looking at pictures, which one's which.</p> <p>Q. You had every opportunity in that part of the chain of custody schedule to provide further information if you wanted to, didn't you?</p> <p>A. Yes, I did.</p>	<p>Dr Wright admits he had an opportunity to set out in his Chain of Custody the fact that documents were different in some way, but did not take it.</p>
<p>{CSW/2/71} CSW 11 Appendix B</p>		
<p>{Day3/122:18} - {Day3/123:6}</p>	<p>Q. What you're saying is that in order to provide documents for, first of all, the Kleiman litigation and then for these proceedings, you laboriously took entries from a live version of MYOB and entered them in one by one into a non-live version of MYOB and then produced some versions of that?</p> <p>A. No, in multiple ways. Firstly, these were never used in this proceedings. The reason you're saying your needle in a haystack is that you had people go through every single email I have ever sent and looked for them. That was then part of the litigation in that case. Next, the log-in for the live version of MYOB was provided to Ontier and AlixPartners in 2019. 2019 precedes this.</p>	<p>Dr Wright evades the question about the creation of the MYOB records, providing a confusing reply.</p>
<p>{Day3/123:14} - {Day3/124:2}</p>	<p>Q. But Dr Wright, what you didn't explain there was that your part in all of this, in creating these documents, by putting in these entries in March 2020, that wasn't apparent from the chain of custody, was it?</p> <p>A. No, because I didn't do that. Your error is you keep missing the fact that I said I had to create another document. My Lord, the litigation in the US didn't involve Tulip Trading. If I was to bring that in, it would add extra opportunity for Mr Kleiman to seek money from me. So, what I did was separate it. I requested an offline copy so that I could make it so that no online copy of anything from Tulip Trading would go into the American case.</p>	<p>Dr Wright claims the MYOB screenshots had to be created new for Kleiman. Dr Wright has provided no evidence that this assertion is correct.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day3/124:19} - {Day3/125:10}</p>	<p>Q. Do you say that none of those screenshots that we looked at, 4077, 4078, 4079 or 4090, has anything to do with this case?</p> <p>A. I'm saying that the screenshots taken by Ontier had nothing to do with that file. That file was never given to Ontier, so therefore Ontier could not have, at any point, got screenshots from the file.</p> <p>Q. Well, you said a moment ago that none of these documents had anything to do with this case. That's what you said.</p> <p>A. No, as in the QIF -- sorry, the QIF, the MYOB and the email. Sorry, I'm not specific.</p> <p>Q. The documents that we looked at earlier, 4077, 4078, 4079, that I put on screen, are they documents you say have nothing to do with this case?</p> <p>A. They are documents related to this case that have nothing to do with the other MYOB file.</p>	<p>Dr Wright gives muddled answers to evade answering the question.</p>
<p>{Day3/125:11} - {Day3/126:6}</p>	<p>Q. I'm sorry, Dr Wright, do you say that those documents have relevance to this case and are probative of anything in this case?</p> <p>A. As I just said, they're documents related to this case -- I'll emphasise that again. The screenshots taken by Ontier, when they downloaded, themselves, the online version of this document that has nothing to do with the one gave in to the American court case, are directly related to this case. The ones that I created in response to Magistrate Reinhart and an order to do so, they, on the other hand, have nothing to do with this case.</p> <p>Q. The documents you say that do have something to do with this case, were created by you -- as a result of you having transferred entries from a separate QIF file into MYOB on 6 and 7 March 2020, aren't they?</p> <p>A. No, they're not. And as the chain of custody says, and it comes directly from Ontier, those files never touched me. I didn't have a log-in, I didn't download the file, I was never involved. It was directly by paralegals at Ontier.</p>	<p>Dr Wright evades a question, instead using the opportunity to further blame third Parties.</p>
<p>{L5/150/1} 11-08-2009 Information Defense Pty Ltd - Bitcoin Token {L5/471/1} 01-10-2009 Information Defense Pty Ltd - Bitcoin Token {L5/146/1} BCDB - Bitcoin inventory</p>		
<p>{Day3/127:22} - {Day3/128:9}</p>	<p>Q. Now, just to be clear, the findings of Mr Madden, agreed by Dr Placks, were that the entries shown on these documents which we have just seen were as a result of your entries on 6 and 7 March 2020. You dispute that, do you?</p>	<p>Dr Wright claims the MYOB screenshots relate to a 2009 account despite providing no evidence for this.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. I do, because both of these -- or all of those images were taken by Ontier prior to that date, so that can't be true.</p> <p>Q. The reality is that these documents resulted from entries which you made in the system in March 2020 and that they're matters of your invention, aren't they?</p> <p>A. No, they're not. They're from an account that I no longer have admin access to that dates back to 2009.</p>	
<p>{H/209/11} Appendix PM42 (New MYOB Files)</p>		
<p>{Day3/134:5-17}</p>	<p>Q. Page 16, please {H/209/16}, paragraph 51. What Mr Madden then did was to view the session logs in an SQL compact viewer, a tool which shows records in the order that they were added, and he finds log-in and log out records for the session ID which had given the anomalous records, now with the log-in and log out records directly with each other but the timestamps out of order; correct?</p> <p>A. No. As I've noted before, the schema updates. This was part of what I put in my witness statement pointing to an MYOB site. The schema in MYOB will update entries and any of these log entries will record when they have been updated.</p>	<p>Dr Wright refuses to accept an obvious fact., and avoids a question about logs by answering with a reply about schemas.</p>
<p>{Day3/135:10} - {Day3/136:3}</p>	<p>A. As I've noted, all of the schemas are updated. The log-in in MYOB requires updates, and if you don't do them, you don't access.</p> <p>Q. Dr Wright, if there was this automatic, across the board update, surely it would update the product version for all these different record IDs to the same product version?</p> <p>A. No, it won't. It will only do where schema changes happen in an entry.</p> <p>Q. Mr Madden goes on to record that the product version 2023.4.1.6 was one released in May 2023 and therefore narrows the period of use of the software to a period between 15 May and 7 June 2023, and you deny that that's a valid finding, don't you?</p> <p>A. What I noted in my witness statement was a point from MYOB. The MYOB accounting software company noted that there was a major update; they didn't explain why, but they said no user could continue using the software unless they accepted the changes to the schemas.</p>	<p>Dr Wright refuses to accept the obvious truth regarding the effect of system updates to MYOB.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{Q/2/10} Joint Statement of Patrick Madden and Dr Simon Placks		
{Day3/138:9-17}	<p>Q. But your latest story, that you had genuine records from which Ontier captured material, neither they, nor AlixPartners have provided any evidence in support of that, have they?</p> <p>A. Again, you're asking for waiving of privilege.</p> <p>Q. No, I'm asking you to accept as a matter of fact that they haven't provided you with supportive evidence?</p> <p>A. I'm asking -- well, actually, they're not my solicitors any more and you're asking for waiving privilege.</p>	Dr Wright using privilege as an excuse to avoid answering a basic question.
{Day3/139:1-6}	[...] One of the reasons that Martti Malmi got into Bitcoin wasn't digital cash, and it relates, it is trustworthiness of online records. Why I created Bitcoin was to have a timestamp server, as I note, because there is nothing on any system where metadata stays valid --	This is incorrect - integrity for document timestamping had been around since 1990 (https://en.wikipedia.org/wiki/Trusted_timestamping).
{L2/441/1} TimeChain-0.1.odt		
{Day3/140:4} - {Day3/140:11}	<p>Q. Do you see that it presents as a version of the Bitcoin White Paper in OpenOffice ODT format, with an abstract proposing the same basic system?</p> <p>A. No, I recognise it as Timecoin. The similarities are there, but Bitcoin is only a partial implementation of Timecoin. Timecoin went on to be the commercial implementation of Bitcoin that I ran in places like Qudos Bank.</p>	Dr Wright evades the question.
{H/17/5} Appendix PM2 (Timechain ODT)		
{Day3/143:15} - {Day3/144:2}	<p>Q. No, you're missing the point I'm making. Simplicity of reproduction is another point they made. Their first point was the Bitcoin White Paper just wasn't written in LaTeX, and that's something you disagree with, is it?</p> <p>A. I'm saying that they had no testing of that. So they've just made a comment because the metadata says OpenOffice.</p> <p>Q. No, they haven't. With respect, Dr Wright, that's simply wrong. They've made that conclusion on the basis</p>	Dr Wright insists the White Paper was written in LaTeX and criticises both experts.

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>of a whole series of analyses, not just the metadata information -</p> <p>A. A whole series of analyses that are based on things like the metadata.</p>	
<p>{Day3/144:17} - {Day3/147:9}</p>	<p>Q. Happy to call it a diagram, Dr Wright. There's a little OBJ character where the diagram appears?</p> <p>A. There's an object field, yes.</p> <p>Q. And that's an object replacement character, isn't it?</p> <p>A. No, it's where one would go. So it's not a replacement character, it's a marker, an anchor.</p> <p>Q. Well, I'm telling you it's -- I'm putting to you that it's an object replacement character and that it's typically inserted into a document automatically when the document is converted from one source containing embedded objects which can't be displayed in text form; that's right, isn't it?</p> <p>A. No. There's a couple of problems with that. Number one, it's not an embedded object in the Bitcoin White Paper. The diagram in the Bitcoin White Paper has searchable text, my Lord. The reason it has searchable text is, it is actually a LaTeX-created document. It is not just, as you put it, a flowchart or anything else. Now, if that was the case, it would not come up as an object file. Because you have that searchable text, and any of that can be searched, if you go to the actual agreed White Paper, any version, you'll be able to select and search on any of those. Even the verify and sign that are at 29 degrees -- I pick weird angles. The owner signature, etc, if you do a find and replace, will actually bring up, my Lord, so you can actually search on that. So unlike a diagram, where you can't search, that's there. So what you're saying is that text would then be there. If that was an object, then in that place, where objects is, there would be text.</p> <p>Q. I put to you, Dr Wright, that's simply wrong and this is a classic artefact of conversion from a document containing a diagram of that kind.</p> <p>A. I'm putting to you that anyone with a mouse can click on the Bitcoin White Paper, on Verify, and select text, and they can cut and paste it, and they could go, "Find: owner zero signature". And if your proposition was correct, that would be wrong. If you had an image there, an image file embedded, and you tried to search it, you would not be able to do that.</p> <p>Q. But Dr Wright, if you -- based on your explanation, if this was a document written in LaTeX which would compile, then it would compile in accordance with its</p>	<p>Dr Wright further insists the White Paper was written in LaTeX. Dr Wright says that the OBJ character is an anchor marker rather than a replacement character.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>instructions, it wouldn't produce this OBJ character, would it?</p> <p>A. Actually, it would. When you're compiling and you're not going to PDF and there's an error, that can happen. Now, the way that my LaTeX file is set up, my Lord, is I haven't got one. Each of the diagrams is separate so that I could reuse them. So I have an image 1, image 2, I can't remember the names of the things, text file, and each of those are compiled separately and embedded. Now, the way that I have it is that I compile it into a PDF and do a compiled PDF, so when you convert into Word or into ODT, because it is no longer the standard thing from the original PDF, it is now an embedded document. So that object file is because the PDF of the embedded diagram hasn't been found. Now, in the LaTeX files that they have, you'll note that there are also compiled versions of the images that are directly from the text, the TX, file. Those are then embedded. So the reason that you don't have errors like Verify, etc, and you have object, is that it is embedded from a PDF and the PDF hasn't been built before the ODT.</p>	
<p>{Day3/148:5} - {Day3/148:22}</p>	<p>Q. As Mr Madden finds, it would be extraordinary, wouldn't it, for a writer to predict the various indentations required for future diagrams and then make those in blank spaces?</p> <p>A. No, I guess he's not a writer. So, my Lord, if you again look at my compiled text images that are in the Overleaf files, I have those spaces. So without pre-empting your question and with this file here, some of them are like 7.81 centimetres, things like this, so they are actually built into my LaTeX for the White Paper. Now, that is because I already compiled those images. As I noted, they're not an object file. I use LaTeX, but I compile into a PDF, or other format, and then I have that compiled into the document. So, how do I know? Because I wrote them. I have those images, I know the exact size of the images I created and I leave the space what they will be.</p>	<p>Dr Wright claims to have deliberately configured the space around the images in the White Paper.</p>
<p>{Day3/149:5} - {Day3/150:23}</p>	<p>Q. So you went to the extraordinary effort of creating a LaTeX document which specifies coordinates for empty space in this document; correct?</p> <p>A. No, for where the image would go, and which is something in my CHFI forensic book that I note. In the section on steganography, I actually talk about doing this. That was in a 2007 publication.</p> <p>Q. The fourth point, Mr Madden, at page 15 {H/17/15}, finds a series of examples of irregular hyphenation, including "proof-of-work" written without the second hyphen and "non-reversible" with the hyphen deleted, and he found that each time that happened it corresponded to</p>	<p>Dr Wright provides evasive answers to Mellor J's questions, refusing to accept the obvious truth regarding the reason that hyphens were missing from various documents .</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>the word crossing a line in the published Bitcoin White Paper. Would you accept that those indicia are there in the document?</p> <p>A. Yes, I do.</p> <p>Q. Now, that is at least consistent with conversion of a document from PDF to Word, isn't it?</p> <p>A. No, actually, it isn't. If I open up a PDF in something like Soda, which is the PDF sort of program I use, then all of this will come out correctly. I can, for instance, even download the PDF of the White Paper on my phone, open it in Word and it comes out correctly. So, that's not actually correct. Actually, if you --</p> <p>MR JUSTICE MELLOR: Sorry, Dr Wright, when you say "come out correctly", what do you mean?</p> <p>A. I mean the hyphenation will actually be correct.</p> <p>MR JUSTICE MELLOR: Right.</p> <p>A. So it doesn't --</p> <p>MR JUSTICE MELLOR: So how does that explain what Mr Madden observed?</p> <p>A. Basically, what they're assuming is that there are errors in the LaTeX where sometimes I've used per cent forward and things like this, done unusual things, and not always do I hyphenate. So I have different sections of hyphenation and not hyphenation and they carry forward into other documents I create.</p> <p>MR HOUGH: You referred to conversion from PDF. This is of course an ODT document, Dr Wright.</p> <p>A. No, conversion from LaTeX to ODT.</p> <p>Q. You were saying to -- you were talking about PDF conversion just a moment ago.</p> <p>A. No, but when I'm talking about PDF, then that doesn't happen. That's what I said.</p>	
<p>{L4/162/1} Re: Citation of your Hashcash Paper</p>		
<p>{Day3/158:6} - {Day3/159:6}</p>	<p>Q. {D/74/1}, please. {L4/162/1}. Satoshi writes to Adam Back: "Thanks for the pointers you gave me to Wei Dai's b-money paper and others." The real Satoshi was treating the web page which he'd accessed as the b-money paper, wasn't he?</p> <p>A. No, I'd just been told I could Google it, and I hadn't Googled it yet, and basically I'm looking at this as b-</p>	<p>Dr Wright is caught in an obvious lie in relation to how Satoshi came to reference Wei Dai in the White Paper {L4/162} when presented with the contemporaneous documents.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>money paper, so I assumed that I would find a b-money paper, which I didn't.</p> <p>Q. Dr Wright, you're simply saying that black is white in relation to these emails, aren't you?</p> <p>A. No, I'm not.</p> <p>Q. It is perfectly plain from these emails that the real Satoshi did not know about Wei Dai's b-money paper before August 2008, isn't it?</p> <p>A. No. Further down, you'll also see, "I'm going to release a paper that references your Hashcash paper". In that, I note the Hashcash PDF. Now, there is a Hashcash page. I've noted that. So, those are actually different things. So, I knew about both, and the Hashcash page and the paper, well, one was a -- well, basically email type blogpost and the other was a paper, a proposal. So my presumption was that in talking about this, you have paper/page. I know I'm pedantic, it's part of being an Aspie, it's ...</p>	
{Day3/159:10-21}	<p>A. I'm actually saying you're wrong. It's very simple. If you look at the area below, Hashcash paper and page are two different things.</p> <p>Q. The real Satoshi didn't say, "Yeah, yeah, I know all about Wei Dai, I've been profoundly influenced by his work for years, I didn't know he'd gone further than producing a short document into producing a fuller paper". He didn't say that, did he?</p> <p>A. He didn't need to, but I didn't realise he did. The ideas that he posted initially were ones, with BlackNet, that got me started along this path, but he didn't produce anything further.</p>	<p>Dr Wright refuses to accept obvious truth about what the documents show Satoshi knew or was aware of.</p>
{H/20/27} Appendix PM3 (Bitcoin White Paper)		
{Day3/161:6-24}	<p>Q. Mr Madden made a number of findings. First of all, he found that the day, hour, minutes and seconds for the times for the creation timestamp precisely matched those of a control copy of the Bitcoin White Paper as published in 2009, which he'd found to be authentic but the year and month are different. That he found to be either a remarkable coincidence or an instance of backdating; that's right, isn't it?</p> <p>A. No, actually, once again, I used LaTeX. My Lord, as I have explained, you set the time in LaTeX. So, I can actually put in the program used, for instance, in this case, OpenOffice, and I can also say what the different create and modify times are. So, if I'm going to change those, I don't need to change all of the settings. Now, the reason</p>	<p>Dr Wright's refuses to accept the obvious truth of Mr Madden's conclusions on the matching of timestamps.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>you do this in LaTeX is that you have a control copy. So, when you're printing and you want to have something printed later, every version of the PDF you create, even if you print it or compile it from LaTeX, will have the same information. [...]</p>	
<p>{H/29/16} Appendix PM4 (Touchup_Textedit Flags) {H/20/31} Appendix PM3 (Bitcoin White Paper)</p>		
<p>{Day3/166:19} - {Day3/167:9}</p>	<p>A. It dates to 2008. I don't know the exact date because you set that in metadata. So, what I set in metadata and when I printed it are two different things. It dates to 2008.</p> <p>Q. You've just --</p> <p>A. The one from 2009, that you're saying is your version that everyone agrees, was not done in April 2009, it was done in March, so ... And not on the date.</p> <p>Q. Dr Wright, I'm putting to you a different point here, which is that if this has a tag in its raw data referring to nChain Limited, which didn't come into being for years after that, it can't be a document in this form which dates to 2008?</p> <p>A. No, it means that a document has been opened, using, probably, Acrobat DC, at a later time. That is a different issue.</p>	<p>Dr Wright refuses to accept the obvious truth regarding presence of anachronistic metadata relating to nChain in a supposed document from 2009.</p>
<p>{Day3/169:19} - {Day3/170:1}</p>	<p>Q. The natural inference from all of this is that this is a document which has been forged by you to support your claim to be Satoshi.</p> <p>A. No, that's actually totally wrong. As I've already noted, I can print out a perfect version of a PDF at any time with any metadata and any date. So, stating that I'm going in and intentionally changing these things to support my case is ridiculous. [...]</p>	<p>Dr Wright claims he is too good a forger to have forged these documents.</p>
<p>{Day3/174:11} - {Day3/174:18}</p>	<p>Q. That wasn't the question. The first question was: do you accept that both of the fields are identical in byte capacity?</p> <p>A. I'm saying they're the same length. Byte capacity is a little bit different, but they are the same length.</p> <p>Q. Are they identical in byte capacity, both fields? A. It depends on what the formatting and compression is, so not necessarily. They are the same number of fields.</p>	<p>Dr Wright evades answering the question.</p>
<p>{Day3/177:20} - {Day3/178:20}</p>	<p>Q. May we now go to {H/20/64}. Do we see that Mr Madden found that lambda characters which appeared in the original version of the Bitcoin White Paper, or in the published version of the Bitcoin White Paper, lambda characters were replaced, in this document, with these odd little symbols?</p>	<p>Dr Wright refuses to accept obvious truth, evading the questions by responding specifically about the presence of the lambda symbol rather than the question about fonts.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. It's not an odd little symbol, it's in multiple character sets. It's a modified version of an omega symbol that hasn't come out correctly.</p> <p>Q. It doesn't look very much like an omega at all; it's a circle with three dots in the middle.</p> <p>A. It's supposed to be a line.</p> <p>Q. The reality is that, as Mr Madden found, this is an artefact suggesting conversion from PDF to a computer which didn't have the font with the lambda symbol installed, isn't it?</p> <p>A. No. Again, what computer doesn't have the lambda symbol installed, would be my first question?</p> <p>Q. With the relevant font with the lambda symbol installed. That's what I put to you.</p> <p>A. No, again, I don't have a computer in the last 20 years that hadn't had the relevant font installed and that wouldn't have infinity, or even the -- I mean, the thing is, you have the sum symbol in maths, so it is there. I mean, you cannot have the sum symbol in maths without the lambda symbol.</p>	<p>This is inconsistent with his pedantry elsewhere, where he insists that he picks up on the fine details of the question.</p> <p>Dr Wright mixes up theta and omega.</p>
<p>{Day3/179:14} - {Day3/181:1}</p>	<p>Well, he found that the relevant font was Segoe UI, and that the character of three dots and a circle was included in that, in Windows 8, released in August 2012. Which part of that do you disagree with?</p> <p>A. All of it. I mean, I don't disagree that it was included in that font, but saying that it is that font, that it would embed, that if you convert you get an unusual Segoe font replacing Lambda, I mean, all of that beggars belief. I mean, Segoe, I've seen before, but I've never used in my life, so to expect that that becomes a unicode character by default is ridiculous. Next, the same circle with three dots is in a number of symbol fonts, not just your one that you're saying, but actually at least 20 different font types, and in fact, in the symbols that you have in Openleaf, I have it for Lambda.</p> <p>Q. Dr Wright, just this before we finish. Given that, on your account, all of these different independent conclusions of alteration were so plainly wrong, are you surprised that Dr Placks agreed that on these -- the basis of these findings that the document had been manipulated?</p> <p>A. Absolutely, yes, but for a different reason. I'm surprised in that anyone would allow themselves to go into such a level of expert overreach. We're talking about a printed paper document. My Lord, neither of these people profess any expertise in -- I'm not even going to pronounce it, but ligigraphic(?) technology -- there, I did</p>	<p>Dr Wright accuses his own expert of overreach and lack of expertise.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	-- none of them have any paper or printing experience, they haven't worked for printers, they know nothing about that, and what they're doing is analysing a printed document as if it's a computer document. I mean, that beggars belief, in my opinion. Next, your argument is that I have a paper document that I have converted and made an error of intentionally years and years ago, which is ridiculous. So, I do say that.	

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
DAY 4		
CROSS-EXAMINATION OF DR CRAIG WRIGHT BY JONATHAN HOUGH KC		
{L5/150/1} – (ID_004077) - MYOB accounting system records		
{Day4/4:3-23}	<p>Q. Do you recall that yesterday you said that this and three other screenshots were taken by Ontier after they were given access to the MYOB system?</p> <p>A. Yes. This is explained in more detail in the later chain of custody that detailed all of this in - - more than the March one.</p> <p>Q. We've been to that. You also insisted that the information in these screenshots was not affected by the inputting of information you did on 6 and 7 March 2020 which showed up in the audit logs found by Mr Madden; is that right?</p> <p>A. That is correct.</p> <p>Q. And I showed you on screen this image at {L5/150/1}, and I asked if you had made the entry which gave rise to that record when you did your inputting on 6 and 7 March 2020. Do you recall me asking that question?</p> <p>A. I recall you asking.</p> <p>Q. Your answer was that you had not, and in support of that point you said that the screenshot, this one here, had been produced before those dates; do you recall?</p> <p>A. I do.</p>	<p>Dr Wright re-stating that Ontier took certain screenshots of the MYOB system.</p>
<p>{Day4/5:15} - {Day4/6:12} {H/209/5}</p> <p>Appendix PM42 to the Second Report of Patrick Madden</p>	<p>Q. Go to {H/209/5}, please, under subparagraph (d). Now, do you see that in this screenshot, the date has not been cropped from the bottom, unlike in the others we considered, and that date is 9 March 2020?</p> <p>A. I do.</p> <p>Q. I can tell you that that's a Monday. Now, bearing in mind that we'll say this can be further confirmed with Ontier if necessary, would you now accept that these screenshots were created on 9 March 2020?</p> <p>A. No. I will accept that this other one was done. Those or screenshots are not screenshots, they're pdfs in - - produced. So Ontier had earlier produced a series of documents. They then converted those into PDF</p>	<p>Dr Wright blaming Ontier for creating screenshots of the MYOB system and insisting that they were taken before 9 March 2020.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>documents at a later date. They also reaccessed at a later date. So they had downloaded into a local version and they had taken multiple screenshots.</p> <p>Q. So you insist that those other screenshots, those other documents were created before 9 March 2020?</p> <p>A. Yes.</p> <p>Q. Are you able to say on what dates they were created?</p> <p>A. No, I was not. The log - in was given to both AlixPartners and to Ontier in late 2019.</p>	
<p>{Day4/6:13} - {Day4/7:16}</p>	<p>Q. Let me put to you, on the basis of the information we have from the load file and on the basis of this further document, that the shots were taken/produced on 9 March and that the editing you did on 6 and 7 March was just in time for them to take the screenshots of the system you'd edited.</p> <p>A. If you're asking me a question, the answer is, no, I've not edited anything. As I noted, the log - in was provided to Ontier. None of this was in my control or possession, and if they'd downloaded a version onto their own machine, I would have no way of accessing or altering anything. When you download MYOB into a local machine, what happens is it is offline. So, the argument you're presenting is somehow I must have got into the offices of Ontier, compromised their computers and accessed an offline program.</p> <p>Q. To be clear, I'm not putting that to you. I'm putting to you that you modified the records in the way shown in the audit logs that we looked at yesterday and that that was the basis of the records which Ontier then produced to us.</p> <p>A. No, you're actually putting to me, being that this was done inside Ontier, as the chain of custody says, that I accessed a computer in Ontier, that I ran a local version in Ontier somehow on one of the PR -- paralegals' computers and altered this without their knowledge.</p> <p>Q. That wasn't what I was putting to you, Dr Wright, but we'll move on.</p>	<p>Dr Wright is questioned about editing the MYOB audit logs, he is evasive in response and tries to reframe the question, as well as blaming Ontier.</p>
<p>{L2/234/1} – (ID_004011) - draft of White Paper</p>		
<p>{Day4/9:23} - {Day4/10:5}</p>	<p>MR HOUGH: My Lord, this is in our core list of 20. And you say, in your fourth witness statement in its exhibit, that this is a draft of the White Paper and an authentic document; is that right?</p> <p>A. I do.</p>	<p>Dr Wright admits that ID_004011 would support his claim to be Satoshi, if it was a genuine document authentic to 2008.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. If this was a genuine document authentic to 2008, it would support your claim to be Satoshi, wouldn't it?</p> <p>A. It's not what I would use just to support, but it helps.</p>	
<p>Calvin Ayre funding Dr Wright's legal proceedings</p>		
<p>{Day4/10:6-19} {L15/453/1} Screenshot of tweet by Calvin Ayre dated 3 October 2019</p>	<p>Q. May we go to {L15/453/1}. We see here that your supporter, Mr Ayre, tweeted in the context of the McCormack proceedings: "... I have seen some of the boxes of historical documents including old versions of the white paper in Craigs handwriting and printed and with his notes and coffee on them and rusty staples." Do you think that's a reference to this document?</p> <p>A. I've no idea. And two areas that you're wrong. I mean, you're saying my "supporter". Supporter, as in he says things on tweets. But I think you're implying that he is my financial backer. As you've seen multiple times, he's an independent individual who has nothing more than an investment in a company I founded.</p>	<p>Dr Wright denying that Calvin Ayre is his "financial backer" but admits that Mr Ayre has an investment in a company that he founded.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day4/11:6} - {Day4/12:20} {L16/342/4}</p> <p>Wright v McCormack QB - 2019-001430 Amended Reply to Amended Defence - 22 April 2020</p>	<p>Q. Page 4, please {L16/342/4}, paragraph 4B: "Notwithstanding the foregoing, and that the Claimant puts the Defendant to strict proof regarding the relevance of the averment, it is submitted that the Claimant is being funded by a third party in these proceedings, namely Calvin Ayre." You admitted in those proceedings, also concerning your claim to be Satoshi, that you were funded by Calvin Ayre, didn't you?</p> <p>A. No, what I'm saying is I took out a loan and I used the loan against assets. So, no, he's not a funder.</p> <p>Q. "... it is admitted that the Claimant ..." That's you: " ... is being funded by a third party in these proceedings ... " You verified that with a statement of truth - -</p> <p>A. As it says - -</p> <p>Q. Wait a second - - and you now say that you were not being funded by Mr Ayre in those proceedings?</p> <p>A. As it exactly says here: "The Claimant has taken out a Bitcoin ... denominated commercial loan against the Claimant's and the Tulip Trust's Bitcoin ... " So ...: "... [which] will be paid back to Mr Ayre." So I made a deal, a loan from the company, and the company paid him back. So, no, he wasn't a litigation funder, he wasn't funding. I took out a commercial loan.</p> <p>Q. I suggest to you that in denying that you were being funded by Mr Ayre, you are denying words which you verified with a statement of truth.</p> <p>A. The words I said in the statement of truth, and I'll explain if they're not clear to you, are that I have taken out a loan that was held against my assets. That included, later, shareholdings. I've sold some of those assets and I've paid for that loan, but that loan is how it was funded.</p> <p>Q. Was that loan recorded in a formal document?</p> <p>A. It was, yes.</p>	<p>Dr Wright disputing that Calvin Ayre is funding him in the McCormack proceedings, but admits there is a formal loan document in place.</p>
<p>Comparison between ID_004011 and ID_000537</p> <p>{H/238} Appendix PM44 to the Second Expert Report of Patrick Madden</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day4/13:11} - {Day4/15:7}</p>	<p>11 Q. Moving then to Mr Madden’s analytical findings in relation to this document {H/238/4}, please. Now, do we see that Mr Madden noted that this document had the same unusual missing hyphen in ”peer - to - peer” that we saw in the document ID_000537 that I asked you about yesterday?</p> <p>A. Yes.</p> <p>Q. And then page 9, please, {H/238/9}. Do we see that Mr Madden made comparisons between the contents of the documents ID_000537 and this document and found some - - just a couple of differences, one of which was the alignment of the table, as shown on this page? Yes?</p> <p>A. Yes.</p> <p>Q. But he found - - and this is paragraph 28 - - that these differences would disappear if ID_000537, which is a PDF document, was opened in Word and the footer referring to SSRN was deleted. Are you aware of that finding?</p> <p>A. Yes. I'm also aware that it is pure opinion. And what I would say is, rather than using a scientific process, what he has done is provided no evidence. So rather than having a scientific process with method that is replicable, he has just put in a pure opinion of what happens. He hasn't demonstrated anything, he hasn't had an experiment and he hasn't made a procedure. Now, as an example, I've demonstrated to other people that I can open up this on my phone even and convert it to Word on my phone, which doesn't have terribly many things, and keep that formatting. So, what you're saying is, basically, your expert has failed to follow the basic requirements of being an expert that my Lord has mentioned in several cases in patents</p> <p>MR JUSTICE MELLOR: Dr Wright, do you dispute what he says in paragraph 29?</p> <p>A. Completely.</p> <p>MR JUSTICE MELLOR: Have you done what he did?</p> <p>A. I've tried to do what he did, but I haven't got the same results. But unfortunately, there's no methodology presented. Now, what I'm saying is, a scientific process should be used if you're an expert. This is why I deny their experts. Now, it should be like a paper. If I'm writing an academic paper, I will have a methodology, and that methodology section then goes into results and then goes into discussion. What we have is a discussion. We jump from the introduction, where we say, "We're going to do this test", and then we go, "The discussion is I've got an opinion".</p>	<p>Dr Wright confirming that he disputes Mr Madden’s findings in relation to ID_004011 and ID_000537.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{Day4/19:2-9}	<p>Q. Now, is it right that your account is that you had a copy of this document in which the first page appeared as the image on ID_003300? That was the photograph with the slight shadow across it.</p> <p>A. That's correct.</p> <p>Q. And then you took a photograph of that first page and sent it on by WhatsApp to somebody in 2019?</p> <p>A. Yes, I sent it to the litigation team.</p>	<p>Dr Wright admitting that he took a photograph of ID_004011 and sent it to his lawyers.</p>
{Day4/20:4} - {Day4/21:6}	<p>Q. Now, on its face, that note {L2/234/1}: "Stefan - - Will Centrebet use a token that is transferable + audited." Would naturally read as a note asking Mr Matthews, prospectively, whether Centrebet would be able to use such a token, doesn't it?</p> <p>A. No, it does not.</p> <p>Q. How do you say it naturally reads?</p> <p>A. What I did was I took an image of the paper prior to sending it to the lawyers so that they had the original. The US litigation had nothing to do with whether I was Satoshi or not, so what I had done was I put down notes on my own paper as I was working on it and I referenced areas that I needed to find. So, in part of trying to discredit the attack, saying that Dave Kleiman owned half of everything I created, I put down notes about the work I was doing and what I needed to find. So, in this, I put down a note and I put down, "Will Centrebet use a token that is transferable + audited" because I needed to find the references where I spoke to Stefan about this topic. That was then used when I was arguing in the US litigation to say that I'd been doing this with Centrebet, I had been working on these areas, and Dave Kleiman was not a party.</p> <p>Q. This reads naturally as a note to Stefan, not a note to yourself about finding a reference, doesn't it?</p> <p>A. No, it does not.</p>	<p>Dr Wright is questioned about the handwritten note on page 1 of ID_004011 {L2/234/1}, he refuses to accept the obvious interpretation of his notes as being a note to Stefan, and provides an evasive response about it being a note to himself to find a reference.</p>
{Day4/21:7} - {Day4/22:15}	<p>Q. Page 6, please {L2/234/6}. There's a section under "Calculations": "The race between the honest chain and an attacker chain can be characterised as a Binomial Random Walk." And the note in red is: "Negative, should add more detail." Yes?</p> <p>A. Yes.</p> <p>Q. That reads naturally as an author's note to himself to add more detail to the draft, doesn't it?</p> <p>A. No, it does not. This references a negative binomial and the other work that I've done on that later. So in the</p>	<p>Dr Wright refusing to accept the obvious truth of his handwritten notes on pages 6 and 9 of this same document (namely a note to himself to add more detail to the draft and a note to Stefan Matthews).</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Kleiman case, we were not disputing the development of the White Paper, we were disputing the work that came after. So it was in particular the mining in 2009 up to 2011. In that, I had written a number of other papers, including ones on negative binomials and this demonstrates that it was my writing alone. If I'm not writing it with Mr Kleiman, then there's no argument that I'm partly partnered with him to do all of this. So my notes are to find those other aspects of papers.</p> <p>Q. Page 9, please {L2/234/9}. May we look at the - - yes, if we're looking at the top of the page {L2/234/8}: "Stefan Matthews, would Centrebet use this." That, again, reads as a note to Stefan Matthews rather than a note to yourself to find references, doesn't it?</p> <p>A. No, it does not. Stefan was one of the witnesses in the trial and I had to use the areas. So what I was looking for were the areas where I'd had meetings with Mr Matthews, because what I need to search for is the question: would you use this, Mr Matthews. So if I'm searching for that area, I'm putting a note to myself on that.</p>	
<p>{Day4/23:21} - {Day4/24:2}</p>	<p>Q. Dr Wright, taking all these notes on their face value, this was a document which you forged with these notes to provide support for your back story, isn't it?</p> <p>A. No, it's a document I wrote on after taking a screenshot, or a photograph, of each of the pages so that I could send them off to my litigation team to note the original evidence, if it was needed.</p>	<p>Dr Wright not accepting the obvious truth and meaning of the handwritten notes on this document and providing an evasive response.</p>
<p>The SSRN upload {L15/185/1}</p>		
<p>{Day4/25:7} - {Day4/26:10}</p>	<p>Q. Dr Wright, I can show you the various pieces of language from the documents, but would you accept that the version uploaded to this website shown here included language which we see in the March 2009 version which is different from the language in the October 2008 version?</p> <p>A. Again, I had multiple versions - -</p> <p>Q. Do you accept that as a factual proposition? I know what your explanation is, but do you accept it as a factual proposition or shall I have to - -</p> <p>A. I'm denying the way that you're versioning them.</p> <p>Q. Let me ask the question again. Do you accept as a factual proposition, because I think you do in your defence, that the version uploaded to SSRN, linked from this site, included language which appeared in the March</p>	<p>Dr Wright is being evasive not accepting the obvious truth that 2 different versions of the Bitcoin White Paper were uploaded onto SSRN, and will not accept there are even different versions.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>2009 version which was different from language in the October 2008 version?</p> <p>A. Let me rephrase - -</p> <p>Q. Just that factual question and then you can give your explanation, Dr Wright</p> <p>A. Again, you're using the term "version" and I don't believe it's a version. I had multiple versions. The one that was published in 2009, you're correct. But that isn't a version of that date. That one actually predates going back to 2008. As I've noted many times, sometimes I even go back to my first copy. That is evidenced in my LLM. My LLM, the one that got published, was actually the first version I produced. Strangely enough, I made a whole lot of changes and then I undid them.</p>	
<p>{Day4/26:16} - {Day4/27:2} {A/3/17} Dr Wright's Re-Re- Re-Amended Defence</p>	<p>Q. Paragraph 52: "It is admitted and averred that on or about 21 August 2019 Dr Wright uploaded a version of the White Paper to SSRN." Correct?</p> <p>A. Yes, but what I'm saying is I don't individually upload it. I instruct other people to do it. So my upload, as I've noted, is - - I'm not sure who it was in 2019, but it's now Sebastian, probably Alex back then. So I give the document into nChain and nChain runs SSRN. So when I'm saying I uploaded it, as an executive, that basically means I instruct someone to do it.</p>	<p>Dr Wright is taken to the section on SSRN in his Defence. He is evasive in response and blames third parties (namely that staff at nChain uploaded the document).</p>
<p>{Day4/27:24} - {Day4/29:1}</p>	<p>Q. Back to the SSRN upload, please. {L15/185/1}. This stated that the document was yours and it gave a date written of August 21, 2008. The version that was uploaded was not written on that date, was it?</p> <p>A. I'm not - - I'm not exactly sure which version was written when. As I noted, the metadata on the dates was actually typed into LaTeX and changed multiple times, so the exact date when it was written, I don't recall. It was 2008 and it would have been August.</p> <p>Q. You were - -</p> <p>A. Now, the loading of this date was done by one of the people at nChain, so as I've noted, the exact date is an estimate.</p> <p>Q. You were perfectly clear in your defence, the document which you uploaded was produced in 2019 based upon a version issued to the public in March 2009, wasn't it?</p> <p>A. It was issued, yes, but it was produced and created earlier. And, yes, it was given to people at nChain, who loaded it.</p>	<p>Dr Wright blaming third parties (namely "people" at nChain) for the version that was uploaded onto SSRN. Dr Wright also provides a very confusing account of the version(s) of the Bitcoin White Paper uploaded to SSRN.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. But it's my turn to be precise now, Dr Wright. The version you uploaded was different from the version which was written by Satoshi in August 2009, wasn't it?</p> <p>A. No, again, none of those - - that version you're talking about, electronic cash, was not written in August 2009, it was written earlier. So, while I put that detail in it at that point and sent out different versions, again, you're taking that I have one version and I don't change these things. I don't.</p>	
{Day4/29:2-14}	<p>Q. You were trying to present this document, accessible here, as the original Bitcoin White Paper written by you in August 2008, and that wasn't true, was it?</p> <p>A. What you're saying isn't true is correct. What I was trying to do was assert my authorship. I had just filed copyright, which was done in the US, and signed all of that. Prior to this, I'd been forced by a magistrate in the US to admit that I was Satoshi. And because I admitted under oath, I started getting a number of attacks against my identity, etc. So, basically, if I'm going to be attacked for who I am and the fact that I have to say something under oath, then I may as well come out there and assert my authorship fully.</p>	<p>Dr Wright admitting that the Bitcoin White Paper was uploaded onto SSRN to assert his authorship of it.</p>
<p>{L3/326/1} – (ID_000554) - 2 code2flow source code flowcharts</p>		
{Day4/35:15-22}	<p>Q. So Dr Wright, you're saying that years later -- because I think that's what you say in your appendix B -- years later, somebody on your staff produced a code map which looked virtually identical, or visually identical at this level of detail and had the same title and the same date footer but was different?</p> <p>A. There were slight updates and there were different versions of the code base.</p>	<p>Dr Wright implausibly asserting that somebody in his staff produced a code map that looked virtually identical, years later, for ID_000375.</p>
{Day4/36:14-24}	<p>Q. Dr Wright, that is a complete fiction, isn't it? This document, ID_000554, has been created from a prior document in order to support your claim to be Satoshi.</p> <p>A. No, once again, in my evidence, I supply the iDaemon document. That 300 - and - something page document defines that one node structure at a point in time. So, those staff members were working to take my system and scale it, and to do that they needed my original code. I didn't want to do the BTC changed methodology, I wanted my original code, so to do that, they needed to work on my original code.</p>	<p>Dr Wright's response is evasive and does not answer the question.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day4/36:25} - {Day4/37:14}</p>	<p>Q. And none of these employees has been prepared to give evidence for you; correct?</p> <p>A. Well, Stefan Matthews is actually an employee --</p> <p>Q. None of the employees who you say did the coding has been prepared to give evidence for you?</p> <p>A. Ignatius Pang worked for me. Shoaib was a director of my company and involved and saw this. Stefan oversaw these people. So, actually, that's not correct. These are people who were with the companies.</p> <p>Q. You say that there were specific people who produced this document, who did the coding, you knew you were facing an allegation of forgery in relation to it, and the people who you say did the coding are not giving evidence for you, are they?</p> <p>A. No, they're not.</p>	<p>Dr Wright admits that no-one is giving evidence on his behalf in relation to his claims that staff members were working on his "original code".</p>
<p>(ID_000375) - bitcoin_main.h.pdf</p>		
<p>{Day4/38:5-23}</p>	<p>Q. We're just going to see it on page 11. Now, what he concludes is that the text in red, which is specifically encoded differently, is indicative of the document having been edited in those respects. Would you agree with that conclusion?</p> <p>A. No, I don't, but, again, this was sourced from a staff machine and the document is created through a process of extracting from Atlassian. We used, at the time, Atlassian, I believe the team still does, to - - well, basically manage the code development. The system that we're talking about is a scalable distributed database handling 1.5 million transactions a second. We broke Amazon the other day, AWS. Now Facebook, Google and Twitter combined do less than a third of that at peak. So this is important, because that means you need a management system for running the code. So that sits on Atlassian and other systems, I don't know all of them any more, I'm sorry, but for that, these individuals can print out at will.</p>	<p>Dr Wright's response is incoherent and makes grandiose claims, including how his work "broke Amazon".</p>
<p>{Day4/38:24} - {Day4/39:11}</p>	<p>Q. Dr Wright, we've got specific characters which are encoded differently and which relate to Bitcoin and indicative of editing?</p> <p>A. No, once again, if I actually opened something up, like he implies, in a hex editor, it doesn't change any of the characters. So, where I'm saying this is wrong is, if I actually open up, say, UltraEdit, which is a hex editor I use, and I go in there and I change the code in the PDF, then it doesn't change any of the fonts around it. So, the</p>	<p>Dr Wright admitting that he uses a hex editor (UltraEdit).</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	structure here is, what you're saying is that it's been edited and somehow someone has also done it in a way to make it look like it's been edited.	
{Day4/41:22-24}	Q. And over the page {H/63/16}, we see he found that it produced code maps presented very similarly to this one? A. No, they're completely different.	Dr Wright is not accepting the obvious truth of the similarity of the code maps.
{Day4/42:13} - {Day4/43:10}	Q. He also found, I think you're aware, that the metadata of this document show that the version of Adobe XMP Core used to create the PDF dates from 2016 and wasn't available in 2008? A. Well, that's basically the version that's been opened up, because it's been opened with Adobe Distiller. So I don't know why someone's opened it with Distiller, but that's occurred. Q. Dr Wright, all these separate indications go to show that this was a document created in or after 2016 as the first process of producing the reliance document, which is a forgery? A. That's incorrect. As I've noted, it's part of the process of development. In creating a distributed system where, in Hotwire, we had at one point 50 plus staff in Australia and now we have several hundred in Australia, including over 100 developers - - actually more - - they need to be able to access all of this information and tools and run it as needed. The way that you set metadata in LaTeX files is so that you have the searchable documents. If everyone produces them differently, the metadata updates over time, then you don't know which versioning you're going to be using.	Dr Wright provides an incoherent response, and blames third parties (namely, staff at Hotwire).
{L3/474} - Bitcoin.exe - (ID_000739)		
{Day4/44:25} - {Day4/45:8} {H/68/4} Appendix PM12 to First Expert Report of Mr Madden	And he found that despite the differences in text the text in each area occupied the same number of character spaces, yes? A. I do. Q. And would you accept that's consistent with binary editing of a file to avoid the file crashing? A. For an executable file, yes. There are other ways of extending it, but a simple way of doing it would be to overwrite using a hex editor.	Dr Wright making an admission regarding binary editing of a file, and also indicating familiarity with hex editing.
{Day4/46:9-25}	Q. And are you aware that he found, by that test, that the file bearing your name had been corrupted?	Dr Wright admitting that hex editing was used, but

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. That's correct.</p> <p>Q. Now, your version, as I understand it from the -- from your appendix B, part 16 {CSW/2/56}, is as follows, and you can tell me at each stage if I've got it wrong. ID_000739 was created by hex editing, but you didn't do it?</p> <p>A. That's correct.</p> <p>Q. It's your account that it was done, that hex editing was done by an ex - employee of one of your Australian companies?</p> <p>A. That is correct.</p> <p>Q. You go on to say that it was created and introduced into evidence in the Kleiman litigation in order to fabricate the notion of a business partnership with Dave Kleiman?</p> <p>A. That is correct.</p>	<p>blaming third parties for it (namely, an ex - employee of one of his Australian companies).</p>
{Day4/47:1-11}	<p>Q. And do I have this right, you say that the purpose of editing it and then deploying it in the Kleiman litigation was to suggest that you could not have compiled a version of the code?</p> <p>A. That, and the IP address added, 203.57.21.7, that you said, was a VPN that David Kleiman used into my company. So, I provided a VPN access to servers that he could run and do some of his forensic work on, and by adding that IP address, it would make it seem that Mr Kleiman was also sort of part of the code process and part of the development of Bitcoin.</p>	<p>Dr Wright introduces new, unsupported, evidence that the IP address 203.57.21.7 was a VPN that David Kleiman used.</p>
{Day4/47:12} - {Day4/48:7}	<p>Q. Now, when do you say that the ex - employee produced this hex edited version?</p> <p>A. Produced it? I don't know. The interactions between certain people in Hotwire and Ira Kleiman started in 2014. There were two different agendas. Some of those staff members had made a deal where they were going to sell intellectual property, code that had been created in Hotwire, to BNP Paribas(?). The deal was for about \$100 million for investment in companies, and scaling and tokenised solutions, IP that hadn't been patented yet, but is now patented by nChain, as well as doing deals with backers for Mr Kleiman, so they were basically sending information back and forwards with Mr Kleiman from 2014 on. I don't know any of what happened, because I've -- the only reason I have any of this is we have one of the laptops of the ex - staff members. Which is where this came from.</p>	<p>Dr Wright blaming third parties, namely Ira Kleiman and "certain people at Hotwire".</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. So you claim that an ex - employee went to the trouble of hex editing a public version of the Bitcoin executable file to make it look like you'd written it?</p> <p>A. Yes.</p>	
<p>{Day4/51:1-11}</p>	<p>Q. If you had been aware of this document on your system, forged to set you up, you would have made very sure that your solicitors identified it so that you wouldn't face these sorts of questions, wouldn't you, Dr Wright?</p> <p>A. No, actually, this was brought up multiple times, including in the Kleiman case. So, I would have expected that you would have actually looked at that litigation and known.</p> <p>MR JUSTICE MELLOR: Were you cross - examined on this document in the Kleiman - -</p> <p>A. I was, my Lord.</p>	<p>Incorrect, this document {L3/474}, (ID_000739) was not in the Kleiman proceedings, it was in the Granath proceedings.</p>
<p>{L4/188/1} - (ID_000848) - debug.log</p>		
<p>{Day4/54:3} - {Day4/55:22}</p>	<p>Q. And the IP address has been changed from 194.74.129.154 to 174.74.129.154, so the "9" changed to a "7"; do you see that?</p> <p>A. I do.</p> <p>Q. Would you accept that the original email - - IP address, before amendment, was yours?</p> <p>A. Sorry, IP address?</p> <p>Q. The IP address was yours?</p> <p>A. It's on a domain from my company, but it's not mine.</p> <p>Q. L/14 - -</p> <p>A. The original or the changed one, sorry? I missed what you said.</p> <p>Q. I'm so sorry, the original address before amendment?</p> <p>A. The original was actually mine. The changed one was actually in my company.</p> <p>Q. {L14/200/1}. This is a speed test document from your computer, isn't it?</p> <p>A. It doesn't look like my ... I don't know. No, it doesn't have my Google log - in and that's rather slow. We've got gigabit internet, so I don't know.</p>	<p>Dr Wright is evasive and altering his story in relation to which IP address belongs to him.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. We see the IP address below “BT”, don’t we, just on the bottom left of the dial , 194.74.129.154. That’s yours, isn’t it?</p> <p>A. That’s a BT IP address.</p> <p>Q. That’s the IP address you have just accepted was yours?</p> <p>A. No, the one I was accepting was the 129 address, sorry if you go back. So 129.45.46.171 was the one I was saying was mine.</p> <p>Q. I read these out, so let me read them out again?</p> <p>A. My apologies if I got that wrong.</p> <p>Q. The IP address has been changed from 194.74.129.154 to 174.74.129.154 and what I put to you was that the original IP address, before amendment, was yours. You dispute that - -</p> <p>A. 19 - - no, I don’t believe so.</p> <p>Q. So were you wrong a few moments ago when you said that it had been changed from I think your home to your work, did you say?</p> <p>A. I was looking at 12(c), my apologies.</p> <p>Q. I see.</p> <p>A. I looked at the IP address 129 above and the 203 there. So my sincere apologies, I looked at the wrong field.</p> <p>Q. Well, I’ve put to you that the document at {L14/200/1} showed a speed test for your internet IP address and you’ve disagreed, so we’re moving on.</p>	
<p>{L14/201/1} Dr Wright’s Slack: attachment</p>		
<p>{Day4/56:4-24}</p>	<p>Q. Page 201 {L14/201/1}, as the document title indicates, a speed test posted by you?</p> <p>A. No, posted by my account.</p> <p>Q. So are you saying that that was posted by someone on your behalf or someone acting against your wishes?</p> <p>A. I actually don’t know why that was posted and it’s not - -</p> <p>MR JUSTICE MELLOR: Why does it say "Craig" in the top right, Dr Wright?</p> <p>MR HOUGH: "Craig" in the top right.</p> <p>A. Sorry, where am I looking, sorry?</p>	<p>Dr Wright is evasive as to whether the speed test in this document was posted by him and refuses to accept the obvious truth that it was, despite it stating “Craig” in the top right of the document.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>MR JUSTICE MELLOR: Top right. Why does it say "Craig" there?</p> <p>A. I don't know. It also has an Apple Papers icon, so I actually don't know.</p> <p>MR HOUGH: Well, let me suggest to you that what's happened here is that there's been an amendment to change the IP address for one which is in fact yours.</p> <p>A. No, and it wouldn't be mine anyway because, I mean, this is in England. I didn't have a BT English thing until 2017.</p>	
<p>{L4/188/1} - (ID_000848) - debug.log</p> <p>{L4/80/1} - (ID_000840) - debug.log</p>		
<p>{Day4/57:15} - {Day4/58:21} {H/64/14}</p> <p>Exhibit PM11 to First Expert Report of Patrick Madden</p>	<p>Q. And he identified the IP address, at paragraph 30 on the next page {H/64/14}, as relating to the URL "www.whatismyip.com"; do you see that?</p> <p>A. I do.</p> <p>Q. And by his researches he found that that was active up to 2011. That's paragraph 31(a) onwards, if we go down the page and over the page {H/64/15}. And it was active up to 2011; do you see that?</p> <p>A. I do.</p> <p>Q. At page 16 {H/64/16}, inactive by 2013?</p> <p>A. I see that.</p> <p>Q. In paragraph 34 on page 18 {H/64/16}, he reached what I suggest is the natural conclusion that the error message was consistent with this software being run in 2013 or later, at which time that URL wouldn't have been accessible; would you agree?</p> <p>A. Quite possibly, yes.</p> <p>Q. So that would suggest a creation time of 2013 or later, consistent with the 2015 creation time in the provided metadata?</p> <p>A. Quite possibly, and I'll also note that the change from the IRC server to the Ozemail one, which is actually the wrong domain name, would be wrong, because while I worked at Ozemail, back in the 1990s, the Ozemail IRC server was closed in around 2004 or '05. I don't recall exactly when, but it was definitely before Bitcoin.</p> <p>Q. Dr Wright, would you accept, at any rate, given the metadata signs and all the other conclusions that I've put</p>	<p>Dr Wright admits findings by Mr Madden that ID_000848 and ID_000840 debug log files have signs of backdating.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>to you, including the last one, which you agreed with, that these debug log files exhibit signs of backdating?</p> <p>A. Oh, definitely. They've been tampered with.</p>	
<p>{L8/338} – (ID_001546) - email from Satoshi Nakamoto to an addressee, "Ut Ng"</p>		
<p>{Day4/64:3-22}</p> <p>{CSW/2/61}</p> <p>Appendix B to 11th Witness Statement of Dr Wright</p>	<p>Q. And you agree, don't you, that this was a spoofed email?</p> <p>A. Completely.</p> <p>Q. And you agree that it was among your disclosure documents?</p> <p>A. I agree that it was in the documents that have been collected over the years, including ex - staff computers, and this was on a computer that had access to my wife's email, my wife's personal email, my email, several other staff members' emails, and other emails that it should not have had. It had information personal to me and my wife, including all our communications as husband and wife. So - - and it was on a staff laptop. So, no, I was not terribly happy with it.</p> <p>Q. In your appendix B, you say, don't you, that Ms Nguyen probably created the email?</p> <p>A. That's a possibility. I don't actually know. What I do know is "cwright" was never my computer, I don't name my computers that way, and the other information with web box, etc, has nothing to do with the companies that I was associated with.</p>	<p>Dr Wright blaming third parties for spoofing this email (L8/338), namely Ms Nguyen.</p>
<p>{Day4/65:4-16}</p>	<p>Q. Is it your evidence, based on what you've said previously, that whoever produced this had access to your email?</p> <p>A. No, whoever received this particular one. So, someone having this email doesn't mean that they produced - - they created it. So there are two different things. Someone created this email, which is spoofed, and it's on a compromised system.</p> <p>Q. A compromised system of yours?</p> <p>A. No, not of mine.</p> <p>Q. Of whose then?</p> <p>A. My email was compromised, but the compromised system had mine and other people's email.</p>	<p>Dr Wright blaming third parties for spoofing this email (L8/338) and giving incoherent response regarding a compromised system/email.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day4/66:9} - {Day4/67:13}</p>	<p>Q. Do you say that your solicitors identified a number of documents by number which were unreliable, or may have come from compromised sources?</p> <p>A. All of the ones from ex - staff laptops are unreliable sources, but I'm still required to put them in court.</p> <p>Q. Do you say that when giving disclosure, your solicitors identified by number those documents which were - - came from compromised sources or were likely to be unreliable?</p> <p>A. My solicitors basically had all of the documents. I argued that I should not have to put in third party documents, I actually had a fight with my solicitors at one point, arguing that why should I put in a compromised laptop from an ex - staff member, why should I give files that - -</p> <p>Q. Can I pause you there and ask you to answer the question that I've now asked at least once. The question is, when your solicitors gave disclosure in early 2023, are you saying that they identified by document number those documents which came from compromised systems, were unreliable, may have been altered materially to harm you?</p> <p>A. All I know is I filled out chain of custody information, I provided information to my solicitors noting all of this. I stated that I didn't want to give over third party computers, I didn't want to give over information that had been sent to the Australian Tax Office by third parties on the internet. I said a whole lot of that stuff. What ended up being given to you, I don't know, I'm not my solicitors.</p>	<p>Dr Wright blaming third parties in relation to disclosure of documents from compromised systems (namely Ontier).</p> <p>Dr Wright claims that all he knows is that he filled out the chain of custody information, and that he provided information to his solicitors “noting all of this”.</p>
<p>{L9/441} - (ID_002586) - an email supposedly from satoshi@vistomail.com to michelle.m.seven@gmail.com, supposedly copied to Craig S Wright, subject "Digital Fire", 6 June 2015</p>		
<p>{Day4/68:18-24}</p>	<p>Q. Is it your evidence that this is also a spoofed email?</p> <p>A. Definitely.</p> <p>Q. That was another document from your disclosure which wasn't identified as being fake when disclosed, wasn't it?</p> <p>A. No, actually I noted all of the staff and ex - employee laptops, so that's incorrect.</p>	<p>Dr Wright admitting another email from his disclosure is spoofed, blaming third parties (namely Ontier) for it not being identified as such.</p>
<p>{L8/446} - Email from Dr Wright to “Ira K”, subject “FW: Defamation and the difficulties of law on the Internet”, 12 March 2008</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day4/70:23} - {Day4/71:17}</p>	<p>Q. You didn't say in the defence that the email content had been changed or that the email was a forgery, but that it was a real email which had undergone an automatic change through a server migration; that's right, isn't it?</p> <p>A. No, I noted that there was a real email that had been put through that. As with the Kleiman litigation, when this was brought before me, I noted that the email had been doctored and this email, purported to be from me, was introduced by Ira Kleiman. So, basically, the source of some of these emails was, yes, I'd asked Dave to be part of what I wanted to do; I had worked with Dave for a number of years, he was my best friend before he died, and I didn't realise how sick he was, though I had spent two and a half years trying to get him involved and at no point did he tell me that he couldn't be because he was in hospital. Now, Ira Kleiman then used the slightly modified version of what I'd sent to build the case around his brother with other things.</p>	<p>Dr Wright not accepting the obvious truth that he did not say in his Defence that the content of the email had been changed.</p>
<p>{Day4/71:18} - {Day4/72:20}</p>	<p>Q. You said, didn't you, that the body of the email, so the text of the email, is the same as that of the email which Dr Wright sent on 12 March 2008?</p> <p>A. Materially.</p> <p>Q. No, "the same".</p> <p>A. What I mean by that is materially the same.</p> <p>Q. When you signed the statement of truth in that defence, did you believe that the text of the email was different in any respects, what the email actually said?</p> <p>A. I believed that it was materially the same.</p> <p>Q. Did you believe that there were words, passages, whole sentences different between the email that you said was the same and the actual email?</p> <p>A. I believed there were some changes. I had noted this in my testimony in Florida. So I believe that it was based on my original email, but I don't have the original email, so I can't tell you what the changes are.</p> <p>Q. Dr Wright, you were clear in the re - amended defence, understanding the importance of this document, that the body of the email was the same, weren't you?</p> <p>A. Most of it is. So what I'm saying by this is, I'm saying I don't actually have the original, but there are bits that don't sound right. So, the email was one that I sent. I did say to Dave at that time, I did make a comment to David Kleiman, "I wanted you to be a part of this". But I don't have that original email. And while I've told people about it, I don't have the exact copy. That is materially the same.</p>	<p>Dr Wright not accepting the obvious truth that he had previously stated in his Defence that the text of the email was the same.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day4/72:21} - {Day4/73:18}</p> <p>{E/4/31} Fourth Witness Statement of Dr Wright</p>	<p>Q. Let's go to your fourth witness statement {E/4/31}, please, paragraph 93, a question from the RFI asked you how you'd come to believe that the header was different, as you'd said in the defence, setting out full detail. And you said there at 93: "I sent the email set out at paragraph 28 of the Re - Re - Amended Particulars of Claim to David Kleiman on 12 March 2008 using my wright_c@ridges - estate.com email address." You didn't suggest there that you sent an email which was a bit like that one but you think was actually different in some respects.</p> <p>A. I apologise if I wasn't clear, but in 53, you're asking a question as how I believe the header is different. So, I didn't explain anything else, because that's not part of the question.</p> <p>Q. But this was another opportunity, if you thought that the email was actually different from the one set out at paragraph 28 of the re - re - amended particulars of claim to note that difference, wasn't it?</p> <p>A. As I said, I said this under oath in the Florida court. I noted this, so I would presume that people know that I'm not claiming that this is an original.</p>	<p>Dr Wright not accepting the obvious truth that he had not previously stated in his Fourth Witness Statement that the text of the email was different.</p>
<p>{L2/317/1} (ID_000464) & {L2/318/1} (ID_000465) - Further versions of the same Kleiman email "FW: Defamation and the difficulties of law on the Internet"</p>		
<p>{Day4/74:1-20}</p>	<p>Q. {L2/317/1}, another copy of the email, apparently forwarded by you to yourself on the same day it was written, 12 March 2008; do you see that?</p> <p>A. Well, it says "From: Craig S Wright" but you can put any header field in anything.</p> <p>Q. And {L2/318/1}. Now, this is pleaded by COPA as a forgery in its schedule and in the core list of 20, my Lord. It's a document which appears to be an original email from you to Dave Kleiman but with your email address of "craig@rcjbr.org" and a time of "07:39", as compared with the 6.37 on the first email we looked at; do you see that?</p> <p>A. I do.</p> <p>Q. And that's, my Lord, pleaded as a forgery in the schedule because it's the only version in disclosure appearing to be the original. Are any of these emails, and perhaps focusing particularly on this one, the original email?</p> <p>A. No.</p>	<p>Dr Wright stating that no versions of this Kleiman email are the original version.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{L10/74/1} - 9 July 2015 email to Stefan Matthews forwarding 12 March 2008 email (ID_001711)		
<p>{Day4/74:21} - {Day4/77:11}</p>	<p>Q. Q. {L10/74/1}, please. This is an email, again in your disclosure, from you at the rcjbr.org address to Stefan Matthews, 9 July 2015, 08:46. The text is: "More history." Forwarding the Kleiman email of 12 March 2008. Is this a genuine document?</p> <p>A. I don't know. I didn't forward it.</p> <p>Q. You didn't forward it to Stefan Matthews?</p> <p>A. No, I did not.</p> <p>Q. Are you able to give an explanation why a document appearing to be an email from you to Stefan Matthews forwarding that email is in disclosure?</p> <p>A. Yes, I can.</p> <p>Q. Go on.</p> <p>A. Basically, as I've noted, a number of emails were compromised, mine and my wife's and other senior people in the company. One of the problems is, when you appoint people as system administrators, you trust them. So, as much as we tried to run a secure operation, if you have a wolf in your hen house, things go wrong. So, as I've noted, there were a number of staff computers containing my wife's personal emails, my personal emails and even things to do with our children. So, yes, there are a number of things happened right back from then. The engagement with Ira Kleiman started in 2014. By 2015, I'd stopped engaging with him all together and he started building a case. He started sending a variety of information out to journalists, including WIRED and Gizmodo, he started sending information out to others I was involved with. So part of the doxing involved files that came from my computers, but also ones that were modified to look like they were from me.</p> <p>Q. Dr Wright, this document which we have on screen at the moment is document ID_001711. Can you take that from me?</p> <p>A. I can.</p> <p>Q. And you're clear that this is a doctored document? It's not a real one?</p> <p>A. I mean, it's a forward from a compromised email address of mine. Part of the reason I purged and reset up my email, losing a lot of information, in late 2015, was that once I figured out there was a compromise, I knew that there could be malicious code or anything in my email addresses, so I completely shut down my RCJBR</p>	<p>Dr Wright is asked about whether he sent the email at ID_001711. His answer is evasive and he blames third parties (his email account being compromised), asserting that he did not send that email.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>account for myself, my wife, and rebuilt it, losing all of the previous emails. So the reason for that, of course, is, if there's malicious code and I run it, then I'm going to be compromised again.</p> <p>Q. You said - - and you can tell me if I'm wrong, and others can look at the transcript, but you said that this document was not a genuine email. The email, apparently from you to Stefan Matthews on 9 July 2015, is not a genuine email.</p> <p>A. No, that's not what I said. What I was saying is that I had a compromised account. So, a genuine email would include my compromised account. So, if someone sent an email using my Gmail, which now has two - factor authentication but didn't back then, then it's still a genuine email, but not from me.</p> <p>Q. Okay. Do you say that you - - or do you accept that you sent the email from Craig S Wright - - craigs@rcjbr.org to Stefan Matthews on 9 July 2015 with the content that we see on this page?</p> <p>A. No, I accept that my email address was used.</p> <p>Q. But you say that you did not send that email?</p> <p>A. No, I did not.</p>	

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day4/77:12} - {Day4/78:25}</p> <p>{E/4/33} Dr Wright’s Fourth Witness Statement</p>	<p>Q. {E/4/33}, please, your fourth witness statement, paragraph 98: “I have been provided to me by my solicitors document ID_001711, a copy of which is at Exhibit CSW17. This is an email to Stefan Matthews dated 9 July 2015 ... in which I forward an email from me to [Dave] Kleiman.”</p> <p>A. Sorry, is that a question?</p> <p>Q. Was that a falsehood, or was it a falsehood that you've just told me?</p> <p>A. No, I'm saying what it purports to be.</p> <p>Q. No, no, no. At paragraph 98 you say that, "This is an email ... in which I forwarded an email from me to [Dave] Kleiman". That's you saying, "I sent the email". You've just told me that you didn't send the email, so which is right?</p> <p>A. No, if you read this, it says: "This is an email to Stefan Matthews dated [that date] ..." Comma: "... in which I forward an email from me to [Dave] Kleiman." I'm sorry if you don't realise the meaning of a comma, but if you see this: "This is an email to Stefan Matthews ... [date] ... in which I forward an email from me to [Dave] Kleiman". Inside that is a forwarded email from me to Dave Kleiman. I apologise if I ’m not clear on this, but where I dated these two different bits, that’s a separate thing. I did not say, “I forwarded an email to Stefan Matthews that contains ...”</p> <p>Q. Well, Dr Wright, I have to put it to you that there is a clear and stark contradiction between your evidence today and what you attested to with a statement of truth in this witness statement.</p> <p>A. No, I disagree. As I state, "This is an email to Stefan Matthews", of that date. I did not say, "This is an email I sent". I'm going to apologise if I'm not clear on that, but I thought it was.</p>	<p>Dr Wright not accepting the obvious truth that paragraph 98 of his fourth witness statement contradicts his cross - examination answers above, and being overly pedantic in response.</p>
<p>{Day4/80:19} - {Day4/81:10}</p> <p>{H/83/27}</p> <p>Exhibit PM18 to the First Expert Report of Patrick Madden</p>	<p>Q. {H/83/27}, please. Mr Madden, looking at ID_00464, which was the version of the email supposedly forwarded by you to yourself, examining that he found that the transmission timestamp for that email was 9 July 2015, at odds with the recorded date. He went on to find a whole series of further abnormalities. I can take you through them, but perhaps we can short - circuit that by saying, do you accept that that email, the one supposedly forwarded by you to yourself, was not an authentic email to its date?</p> <p>A. What I'm saying is, if you look there, "PCCSW01" isn't me. The IP address, if Mr Madden had checked it, is in the US. I was in Australia, now in Britain; I've never had a US IP address. And "PDT", which is - - well, Atlantic</p>	<p>Dr Wright agreeing that ID_000464 is not authentic to its date.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Eastern Standard time, I believe. So, I agree there's a whole lot of funky alterations that happen to match where Mr Ira Kleiman would be.</p>	
<p>{Day4/81:11} - {Day4/82:17} {L8/443} ID_001318</p>	<p>Q. Page 36, please {H/83/36}, and paragraph 83. Mr Madden addresses the copy of the email forwarded by you to Ira Kleiman, and he looked specifically at Information Defence, and he finds, as per the researches that I mentioned earlier, that it was anachronistic to the face date of the email, and I think you agree with that?</p> <p>A. Completely. As I noted, Ira Kleiman didn't realise that I had Ridge Estates and closed it down in 2008 and moved over to Information Defence; he only knew about the earlier company. So, when he was trying to get evidence to, well, take half of everything I created, he didn't understand some of the history that I know. I know it because I lived it. I started and closed down Ridge Estates.</p> <p>Q. Now, you say, don't you, now that the email supposedly from you to Dave Kleiman on 12 March 2008 which was forwarded in this email to Ira Kleiman, or apparently so, is not a genuine email. That's what you say, isn't it?</p> <p>A. I'm not denying any of that.</p> <p>Q. And we can see that, amongst other things, from the fact that it uses a domain name which is an anachronistic, can't we?</p> <p>A. We can. And my belief on that is, I had shown a screenshot of the email to Mr Ira Kleiman which didn't show the domain. Like when you showed before, you could see the names. Now, from a screenshot, he wouldn't be able to basically go into court and go, "Well, I've got an email, I can prove Craig and Dave". So, my personal belief is that he used the screenshot to try and fabricate one.</p>	<p>Dr Wright admitting that the email at {L8/443} (ID_001318) is not a genuine email.</p>
<p>{Day4/82:18} - {Day4/83:9}</p>	<p>Q. So just to be clear, you're not saying that the domain - - you're not now saying that the domain changed because of a process of genuine changes of server on your part, migrations of server, but because somebody, Ira Kleiman or somebody working for him, edited the email?</p> <p>A. No, I'm saying both. To be clear, I'm actually giving two different things. I'm not always clear, my Lord. I'm saying that I went from Ridge Estates, Ridge Estates ran a sort of domain in X500, and it changed to Information Defense, keeping the same active directory tree structure. Now, when that happens, it changes all of the naming structures in Microsoft. So I did that at a later date, but</p>	<p>Dr Wright acknowledging that he is "not always clear", but does not accept the obvious truth that he has been inconsistent in his account of the changes to the email.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>I'm saying that this email isn't that, that there are both: I did this on my exchange servers, and, after giving sort of a view of this email to Ira, I've got a fabricated one.</p>	
<p>{Day4/84:10-17} {H/83/30}</p>	<p>A. It's not an excuse, it actually happened. As I've noted, on the email I had, I never forwarded that email to Ira Kleiman, I only allowed him to see it. So, the only way he could rebuild it, if I'm saying I don't have it any more, is to rebuild it. And as I noted, after the doxing I deleted all of my emails, all of my active directory, etc, emails on the company, all of my other ones, to purge anything that might be malicious.</p>	<p>Dr Wright blaming third parties (namely Ira Kleiman). Dr Wright's explanation is also inconsistent with his disclosure, in which ridges - estate.com emails have been disclosed.</p>
<p>{Day4/84:18} - {Day4/86:2} {L20/252.79/1} C0003648, IP Address and Domain Name Geolocation Lookup Tool</p>	<p>Q. {L20/252.79/1}, please. Do we see that this is an IP Address Lookup tool showing the IP address 103.39.121.201 being registered in Australia?</p> <p>A. Yes, it is.</p> <p>Q. Can we have that alongside {H/83/27}. Now, do you see at the top, just under paragraph 60, in the transmission header for ID_000464, the IP address is shown received from "PCCSW01" and there's an IP address "103.39.121.201", yes?</p> <p>A. Yes. My apologies, I got this IP address mixed up. Memorising IP addresses is why we have DNS, my Lord. I know what this one is. This is Brisbane, Australia. That was Jamie Wilson. Jamie Wilson was former CFO, chief financial officer, who was dismissed in 2013 and ended up helping Ira Kleiman. He was dismissed because he tried to embezzle money and tried to sell things. So, Jamie is the person who lives in Queensland.</p> <p>Q. I can see you're trying to help my cross - examination by pre - emptying my questions, Dr Wright, but let me ask the question I was going to ask. You'd fingered Ira Kleiman, of course, an American, for confecting this document, and the IP shows its association with Australia, doesn't it?</p> <p>A. Yes, that's correct. Both of them were working together. So, my first patent was created basically with Jamie Wilson. We had a company, FASV, which was a vault system, started in 20 - - like, the idea started in 2010, and the idea was to use Bitcoin with a threshold key system, which Ms Meiklejohn talks about, that I patented in 2011, and Jamie Wilson wrote some false declarations saying that I assigned all of my rights to him for nothing, tried to sell some of my assets to Google, and then ended up helping Ira Kleiman. I collect lots of people like this.</p>	<p>Dr Wright blaming third parties for sending the Kleiman email at ID_000464 (namely Jamie Wilson, former CFO).</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day4/87:2} - {Day4/88:1}</p>	<p>Q. Dr Wright, it's right, isn't it, that when you were first answering the allegation that these Kleiman emails were forgeries, you said simply that the domain name had changed as a result of server migration. That was the excuse or explanation given in your defence; correct?</p> <p>A. Before I looked at them, I knew that I had, in the past, sent an email. So, basically what I'm stating is, if the correct email that came from my domain was in there, this is how it would happen.</p> <p>Q. And then - -</p> <p>A. I did not, at any stage, analyse this email to see how it was created.</p> <p>Q. And then, in your appendix B, you came up with the explanation that the original email as sent had different content because it didn't contain the final paragraph about GMX, Vistomail or Tor. That's your account now, isn't it?</p> <p>A. Yes. I don't have the original email, but I'm very sure that I did not say that.</p> <p>Q. And your account, just to be clear, is that all the versions of this email which we have in disclosure and which have been addressed by Mr Madden have been manipulated?</p> <p>A. It is.</p>	<p>Dr Wright stating that he does not have the original email sent to David Kleiman, and admitting that all versions of the email in disclosure/addressed by Mr Madden have been manipulated.</p>
<p>{Day4/88:2-9}</p>	<p>Q. Now, you say in your appendix B that the real email was tampered with by former employees of your companies who were seeking to help Ira Kleiman?</p> <p>A. Yes. As I said, Jamie Wilson was actually doctoring my signature, and other such things, which we caught him out on. My first filed patent was actually assigned to him, which I never did, I never have received any consideration and in fact never sold it.</p>	<p>Dr Wright blaming third parties (namely Jamie Wilson) for tampering with the Kleiman email, stating that he had concrete evidence of tampering by Mr Wilson (but this is not in evidence).</p>
<p>{Day4/88:25} - {Day4/89:13}</p>	<p>Q. Finally, let me put it to you that while Ira Kleiman certainly deployed that email, there was nothing about the final paragraph that made it critically better for his case against you in Florida, was there?</p> <p>A. Actually, there was. The funding parties behind Ira Kleiman are associated with BTC Core. Now, what they wanted to do was have Ira be like the heir to a dead Satoshi. So, Ira received tens of millions of dollars in litigation funding from some of your clients purposely to make it that the dead brother was Satoshi, I was just the dumb businessman who had no idea and couldn't code, and that thus, Dave, who is dead and can't argue, is now</p>	<p>Dr Wright blaming third parties for funding Ira Kleiman's litigation, including one of the claimants in these proceedings.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	the heir to all of this and therefore we can do whatever we want.	
Return to ID_000739 Bitcoin.exe - discussion in Granath proceedings		
<p>{Day4/92:19} - {Day4/94:6} {L17/202/7}</p> <p>Process Writ to Oslo District Court dated 27 August 2021</p>	<p>Q. Bottom the previous page, please {L17/202/7}: "The plaintiff has been asked to be informed whether Wright possesses or can access other evidence that he is Satoshi Nakamoto, and indicated that Wright has a duty to answer questions about real evidence." Then, following on from that, a number of documents were collected which were said to substantiate that you were Satoshi Nakamoto. These were reliance documents, weren't they, Dr Wright?</p> <p>A. One, there's no reliance documents in Norway, and as it says: "A number of documents have been collected from Wright in connection with lawsuits pending in other jurisdictions. [They're] of relevance to [the] dispute ..." So the 71 documents are there not for the reason you're pointing out. As I've demonstrated in the Kleiman litigation where this first came up, this was promoted by Ira Kleiman.</p> <p>Q. Page 7, please - - sorry, page 10 {L17/202/10}, please?</p> <p>MR JUSTICE MELLOR: Dr Wright, can I just ask. If these documents were not being presented to substantiate that you were Satoshi in the Norwegian proceedings, what were they being presented for?</p> <p>A. Actually, the first lawyers I had in the Norwegian proceedings went down a complete different path as the way I wanted, which is why I dismissed them. What I wanted to do and what happened were two different things. They didn't want to bring a case about being Satoshi, and rather wanted to make it about human right violations and hate crime on Twitter. The incitement aspect was where they put things. So, I didn't actually want a Twitter hate case, but that's what I ended up with.</p> <p>Q. Dr Wright, Wikborg Rein were your lawyers, weren't they?</p> <p>A. I don't remember the name of the firm off the top of my head. I know the people. Was this the first firm or the second firm, I'm sorry?</p>	<p>Dr Wright not accepting the obvious truth that he relied on certain documents to substantiate that he was Satoshi in the Granath proceedings in Norway.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day4/94:15} - {Day4/96:2}</p>	<p>Q. I don't know, but we can go to the first page and see if - - {L17/202/1}. Yes, we see some representatives identified. You might recognise the surname Haukaas. No, sorry. Sorry, Vangsnes.</p> <p>A. Yes, I think this is the first firm that I fired because they refused to do as I actually instructed.</p> <p>Q. So we can see from the front page of this that Wikborg Rein were your lawyers, because it's "Defendant", your name, and then "Process representative", Wikborg Rein, yes?</p> <p>A. If that's the first firm, then, yes, they're the ones I fired.</p> <p>Q. And they identified a series of documents as documents to substantiate you as Satoshi based on this document, didn't they?</p> <p>A. No, I put in those documents to demonstrate that people were actually doing other things, such as trying to falsify evidence against me.</p> <p>Q. Page 10, please {L17/202/10}. We can see that appendix 57, which is Bilag 57, is listed among these: "Original bitcoin v. 0.0.8 bitcoin software (pdf file information + exe.file) [dated] January 4, 2009 at 1:08 pm." Do you see that?</p> <p>A. I do.</p> <p>Q. It's perfectly clear, isn't it, that this, contrary to what you said this morning, is a document on which you relied, among 71, in Granath to substantiate you being Satoshi?</p> <p>A. Two points. In Granath, there was nothing about me substantiating that I was Satoshi. The case was Twitter defamation, so the case had nothing to do with me being Satoshi. I wanted it to be, and I got to a point where I actually fired my lawyers while in there and replaced them. So, the first firm refused to actually run the case I wanted saying that, "It's better if we do it this way", which is very different to over here, so I fired them unceremoniously and replaced them.</p>	<p>Dr Wright is evasive in his response regarding the purpose of the 71 documents in the Granath proceedings and whether they were relied upon to substantiate that he is Satoshi.</p>
<p>{S2/2.1/47} Tulip Trust / Tulip Trading - Dr Wright's evidence in Granath</p>		
<p>{Day4/102:23} - {Day4/103:15} {O2/11/26}</p>	<p>Q. And you then said in the sections that follow that after you'd produced this document in 2011, there were further trust documents that followed?</p> <p>A. When I produced it in 2011? Sorry, I'm not sure I understand what you mean there.</p>	<p>Dr Wright admitting that the document at {S2/2.1/47} was drafted/produced by him.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Well, it's a document dated to 2011, which you said you'd written the day before.</p> <p>A. Yes, I drafted. I don't know whether I typed it or I said it and got it sent or anything like that. As I said, I was drunk.</p> <p>Q. And it's a document you say you produced in 2011, you yourself?</p> <p>A. As I said, I don't know. I was talking to Dave at the time. I definitely drafted it, but as I've said many times, drafting a document can be I say it, I type it, I talk into Dragon VoiceType, it could be many other things. But I definitely was involved in production of it in that way.</p>	
<p>{Day4/103:24} - {Day4/105:1} {S2/2.1/46}</p> <p>Email from David Kleiman to Dr Wright</p>	<p>Q. And that refers to Dave Kleiman having received 1.1 million Bitcoin from you and David Kleiman forming a trust, yes?</p> <p>A. No, what it is is an acknowledgement for when it happened, so that never occurred.</p> <p>Q. So you produced this document, but it never occurred?</p> <p>A. Well, when you write a contract, you fill out the contract saying, "I such and such agree ...", etc, and the same happens with a trust document. So, you create a trust document, and like I said, I was completely drunk, off my nut, and the next day I made sure I actually did the correct one, which was a document created by Diane Pinder of Lloyds solicitors.</p> <p>Q. On the previous page, {S2/2.1/46}, you have an email, apparently from David Kleiman to you, Friday, 24 June 2011?</p> <p>A. Mm - hm.</p> <p>Q. With various attachments?</p> <p>A. Yes.</p> <p>Q. "Tulip Trust.pdf.asc", "Tulip Trust.pdf.tar.asc", "Tulip Trust.pdf": "Craig, "I think you are mad and this is risky, but I believe in what we are trying to do. "Respectfully. "Dave Kleiman." Is that an email that was sent to you?</p> <p>A. I actually don't know.</p>	<p>Dr Wright is evasive in response to whether the email at {S2/2.1/46} from David Kleiman was sent to him.</p>
<p>{L8/17/1} - Deed of Trust between Wright International Investments and Tulip Trading Limited (23 October 2012)</p>		
<p>{Day4/109:2-5}</p>	<p>Q. You swore in Kleiman, didn't you, that this was - - this document was authentic and signed by you on that date, yes?</p>	<p>Dr Wright admits that in the Kleiman proceedings, he swore that the Deed of Trust was authentic and</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	A. Yes.	signed by him on 23 October 2012.
{Day4/109:9-17}	<p>Q. This document was found by Mr Kleiman’s lawyer to be a forgery, this October 2012 deed of trust?</p> <p>A. Mm-hm.</p> <p>Q. You denied that it was a forgery, didn't you?</p> <p>A. Yes, I didn't actually know. I was not involved in anything, so, as I said, I had no knowledge.</p> <p>Q. Well, I can bring up the reference if you'd like, but you denied that it was a forgery, didn't you?</p> <p>A. My understanding was that it was a real document.</p>	Dr Wright is evasive in response to the question of whether he denied the Deed of Trust was a forgery.
{Day4/110:4} - {Day4/111:23}	<p>Q. So you denied it was a forgery, didn't you?</p> <p>A. I did.</p> <p>Q. So, is it your evidence now that this is a genuine document recording the terms of the trust and the trustees?</p> <p>A. No, it is not.</p> <p>Q. Why do you say it's not a genuine document recording the terms of trust and the trustees then?</p> <p>A. Because, as my original statement said, in 2011, I set up everything so that I had no involvement. When I was given the other document in 2012, I saw signatures by people I recognised from Savannah, but I was precluded from even asking them any information about the trust until 2020. After the date in 2020, I validated that this is not sort of a valid document. Now, I did not know which documents were real or not at that point. I was ordered by the American court to give over any documents in my possession, which included staff laptops, to do with the trust. The comment I made many times to the Justice - - the magistrate was that I have no idea and I cannot actually vouch for anything being completely real. I can look at a signature and I can say that that looks like the person's signature, which I did. What I do know now, in that time period when I wasn't engaged in the trust, is that this didn't happen.</p> <p>Q. What didn't happen?</p> <p>A. That document is not real.</p> <p>Q. So this document, which you attested to as genuine in the Kleiman litigation which you denied was a forgery, it's not a real document?</p>	Dr Wright is inconsistent in his responses and now states that the Deed of Trust is not a genuine document. He also acknowledges that he did not know “which documents were real or not” in the Kleiman proceedings.

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. It's a real document, but it's not part of the trust. There was never any agreement between Wright International and Tulip. Now, as I stated, I set up the trust so that I had no involvement until 2020, so until 2020 I was not able to validate anything, whether I wanted to, had to or not. I was nearly put into contempt of court in the American case, which I'll say, in a weird way, was one of the best things in my life, my Lord, because I sought anger management. I threw down one of the documents in front of the justice and the court and he threatened me with contempt, and after that I've spent several years doing anger management and I'm much better.</p>	
<p>{Day4/112:3-13}</p>	<p>Q. And how do you say you discovered that it was not a genuine document - - or, sorry, that it did not reflect a genuine agreement that had been entered into?</p> <p>A. After 2020, actually in '21, I believe, there was a trust meeting held, per the terms of the trust, and I was then allowed to actually get access to the original trust deed, the real one, which I was precluded from having until 2020, at least. The meeting required 70% or more sort of voting shareholding ability of trust members for me to do that, and that was accepted.</p>	<p>Dr Wright proffering new evidence about the authenticity of the Deed of Trust document.</p>
<p>{Day4/113:1-9}</p>	<p>Q. So you thought, after that supposed meeting, and you think now, that this is - - that the document that we looked at was still a complete, genuine document, but just didn't reflect an agreement which was actually entered into?</p> <p>A. Well, there wasn't an agreement between those two companies, I know that. On top of that, I've also spoken to some of the individuals named on the document and they said they didn't sign.</p>	<p>Dr Wright proffering new evidence about the authenticity of the Deed of Trust document, but he has not identified in evidence who the individuals are to whom he spoke.</p>
<p>{Day4/114:13} - {Day4/115:20}</p>	<p>A. That is correct. So this was after the sort of Kleiman issue in 2019, and at this stage I'd now found out that someone had merged multiple documents together. Some of the material involved the trust and others didn't.</p> <p>Q. You told us just a few minutes ago that the document was a single coherent document, albeit not one that reflected a real agreement, didn't you?</p> <p>A. It is a single coherent document made up of other documents.</p> <p>Q. Well, let me put to you, Dr Wright, that there is an inconsistency, a stark inconsistency between saying that this is a single coherent document and saying that it's a mish mash of multiple documents from different sources.</p> <p>A. No, I'd argue that actually taking multiple documents and mish mashing them together makes a document. Now, whether you say that's a coherent document is</p>	<p>Dr Wright is evasive and inconsistent in his responses regarding the provenance of the Deed of Trust.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>another thing. What I do argue is that this was a document purported to be a trust document that added more weight to Ira Kleiman saying that, well, his brother was my partner. So a lot of these things happened because of that.</p> <p>Q. Do you now say it was a fake document produced by Ira Kleiman in support of his case?</p> <p>A. It was used that way.</p> <p>Q. Do you now say it was a fake document used by Ira Kleiman in that way?</p> <p>A. Well, it has to be a fake document used by Ira Kleiman, because if it's used by Ira Kleiman and it's a fake document, then both of those apply. As I stated, there was no agreement ever made between Wright International and Tulip Trading, but between 2011, for over a decade, I had no involvement in those companies, intentionally.</p>	
<p>{Day4/115:21} - {Day4/116:9}</p>	<p>Q. Dr Wright, you swore in the Kleiman litigation that this was an authentic document and you are now saying it is a fake; correct?</p> <p>A. I swore in the Kleiman document - - sorry, litigation that I had no knowledge of what the documents actually were that this appears to be. Basically, when I went in there, I checked the signatures, they were signatures from parties I know. It's a third party document. So I was asked in litigation to validate a document by third parties that I had never seen, and to the best of my knowledge, all of those signatures were the signatures of the individuals. Unfortunately, the terms of the trust precluded me from going to any of those individuals and talking to them directly.</p>	<p>Dr Wright is inconsistent, he has stated above that he spoke to some of the individuals named on the document and they said they did not sign {Day4/113:1-9}.</p>
<p>{Day4/118:5} - {Day4/119:5} {O2/11/27}</p>	<p>Q. Just to be clear, you did not say in the Kleiman litigation, did you, that you simply weren't able to say one way or the other whether it was an authentic document?</p> <p>A. Actually - -</p> <p>Q. You didn't say that, did you?</p> <p>A. Well, no, actually I did. This is - - I said one of the best things that happened to me in a roundabout way, it's why I got anger management. I've - - I'm a terrible stoic, but I'm trying. But what I did, my Lord, was I basically went to the magistrate and I actually threw the document on the ground because I - - I couldn't do anything and I had to accept it in effect. Throwing the document, I got cited because I threw a document in his court, and I understand, and I'm incredibly apologetic and I'll never do that sort of thing in a court again. But I had no sort of option. I knew it was a document in a trust pile, I had no way of invalidating it, I was frustrated because I'm legally not</p>	<p>Dr Wright is inconsistent, he has stated above that he spoke to some of the individuals named on the document and they said they did not sign (Day4/113:1-9).</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>allowed to talk to those people. Under Seychelles law, when I set up that sort of trust, it's a criminal action for me to actually start talking to them. So, I'm sort of in a rock and a hard place, and I accepted that it is a valid document in that pile. As far as I know, there's nothing to say it was invalid at that point.</p>	
<p>{L1/218/1} Dave Kleiman “Risky” email</p>		
<p>{Day4/119:6-15}</p>	<p>Q. Moving on to a related document, {L1/218/1}, please. This is another document in your disclosure in this case and it appears to be a copy of the email from Dave Kleiman to you, "I think you are mad and this is risky ..." email, but this one dated to 17 October 2014; do you see that?</p> <p>A. I do.</p> <p>Q. Now, I presume we can agree, because Dave Kleiman sadly died in April 2013, that this can't be a genuine email?</p> <p>A. That is correct.</p>	<p>Dr Wright admits that the email at {L1/218/1} cannot be genuine.</p>
<p>{Day4/120:19} - {Day4/121:8} ID_001386 (October '14 version of the email)</p>	<p>Q. Now, we've agreed that this document was manipulated and it also, as we saw, included a reference to your email address as sender. Is this a document whose provenance you know anything about?</p> <p>A. Yes, actually, it is. This was sent - - well, one of the ex - employee laptops, which is listed in the chain of custody document, but it was also sent from Ira Kleiman to the Australian Tax Office.</p> <p>Q. In fact, this was a document submitted to the Australian Tax Office on behalf of your company, C01N Proprietary Limited, wasn't it?</p> <p>A. C01N? No it should have been Coin X that that was involved with. But Ira was actually a shareholder of one of the companies and had been, well, basically sending false information.</p>	<p>Dr Wright blaming third parties for this email (namely Ira Kleiman).</p>
<p>{Day4/122:7-17}</p>	<p>Q. "However, the taxpayer has provided two versions of the email from Mr Kleiman to which the Tulip Trust document was purportedly attached. The emails are identical except one is dated 24 June 2011 and the other 17 October 2014." That's right, isn't it, that those two documents were submitted to the ATO by the taxpayer, your company?</p> <p>A. The taxpayer was technically DeMorgan Limited, which was the head group company. That owned both</p>	<p>Dr Wright proffering new evidence regarding Ira Kleiman's involvement in the ATO investigation.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	C01N and Coin X. That, thus, included Ira Kleiman as a shareholder.	
{Day4/123:19} - {Day4/124:13}	<p>Q. "C01N Pty Ltd/Strasan Pty Limited". Was Strasan a prior name for C01N?</p> <p>A. Yes, it was.</p> <p>Q. So when you say that the taxpayer in this document meant DeMorgan and in fact, for the purpose of that document, meant Ira Kleiman, that was wrong, wasn't it?</p> <p>A. No, because you would actually go one level beyond that. Panoptcrypt was the main holding company set up for my wife, myself and my children, and an entity that was the main owner of DeMorgan. So, the top of the pyramid is actually Panoptcrypt, although I didn't run it that way, the limited company was DeMorgan.</p> <p>Q. Dr Wright, the ATO are perfectly clear that "Taxpayer" means C01N, and the taxpayer, C01N, submitted these two documents.</p> <p>A. No, it's part - -</p> <p>Q. That's when the ATO decision says, isn't it?</p> <p>A. It's part of a group. So when you're in a grouped company, same as over here in the UK, the entities actually file together.</p>	Dr Wright is evasive in response and not accepting obvious truth of the meaning of "Taxpayer" in the ATO decision.
{Day4/127:2-11}	<p>Q. Dr Wright, the reality is that all these documents which look like 2011 documents settling up a trust structure and investing assets in Tulip Trading Limited, which bare signs of creation or alteration in 2014, tell a story of you, in 2014, trying to create a documentary record, don't they?</p> <p>A. No, they basically show where we were locked out of our office and we had to rescan documents, reprint documents and get the rest of the corporate documents for the other companies so that we could actually trade.</p>	Dr Wright refuses to accept the obvious truth of the manipulated Trust Deed documents.
Abacus documents: {L9/214/1} ID_001421, {L9/185/1} ID_001397		
{Day4/128:15} - {Day4/129:18}	Q. Now, as Mr Madden finds, the natural conclusion from this is that the first document we looked at has been text edited to suggest it was an invoice for services in relation to an existing company when in fact it's a company which, according to this invoice, was purchased in October 2014; correct?	Dr Wright blames third parties (namely Ira Kleiman) for faking the Abacus documents.

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. No, that's his assumption. I would say neither documents are actually correct.</p> <p>Q. You can elaborate if you want.</p> <p>A. Basically, part of the story Mr Kleiman was putting together was that I never moved any of the assets and that everything went into the American company, W&K Info Defense. There was an agreement between the Australian company Information Defense Pty Ltd and the American company W&K Info Defense that never occurred. Basically, Dave Kleiman was hospitalised from an earlier accident and he was a paraplegic, and because he was hospitalised, the business that I wanted to set up never - - well, never eventuated. The argument by Ira Kleiman was that intellectual property had to basically stay in W&K and that other assets that would have occurred if Dave hadn't been ill had to be, well , accessible , and as such, part of the fabrication there was saying that Tulip Trust/Tulip Trading, any of my companies overseas, didn't exist .</p> <p>Q. So do you say that he faked both these documents, or just one of them?</p> <p>A. I'm saying both of them are actually fake.</p>	
<p>{L7/357/5} Abacus Incorporation form for a Seychelles Company, ID_001930</p>		
<p>{Day4/129:23} - {Day4/130:16}</p>	<p>Q. And on page {L7/357/5}, we see what appears to be your signature with a date of 21 July 2011, yes?</p> <p>A. No, I don't. What I see is a cut and paste where someone's made a mess of it, and it's also not my signature. As part of the Kleiman proceedings, we had this analysed. When I sign, one of the few things I always do that people will now know is a little trick, I do the G separately. So I basically draw a "J" and then draw a "C", and my signature has a little funky thing for that; this doesn't. It also doesn't have an "S". So it's some sort of "Craig Wright" without a - I've always signed "Craig S Wright". We had a handwriting analysis done of this and showed it wasn't my signature. My signature's messy, but it's not that one.</p> <p>Q. Was that a handwriting analysis report which you deployed in the Kleiman proceedings?</p> <p>A. No, none of this actually ended up happening because the other side were fine with not going that way.</p>	<p>Dr Wright is making a new assertion that the signature in this document is not his and referencing a privileged handwriting analysis. This is contrary to Dr Wright's signature on the Claim Form at {A1/1/5}, which appears nearly identical to the one at {L7/357/5}.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day4/132:9} - {Day4/133:9}</p>	<p>Q. Yes. So all the indications are that a document from 2014 has been edited to produce a document dated July 2011, aren't they?</p> <p>A. I'm saying both of them are doctored. Why the first one exists is another question.</p> <p>Q. Dr Wright, just this before the break. This is yet another indication of you, in 2014, trying to doctor the record to create a document that suggests the establishment of Tulip Trading and the trust structure in 2011.</p> <p>A. No, actually the trust structure was set up in the late '90s. The trust actually had a domain name WDI.org, so that was probably back - - actually early '90s. I think it was - - I'd have to look it up, but WDR was set up way back before I even set up DeMorgan version 1. So I had a trust already, multiples, that was first in Belize, I believe, but I also had many other overseas corporations. So, to set up a fake company, again, I have no purpose. I have DeMorgan in Singapore, I have multiple other companies in Panama, Antigua, Belize, Seychelles, Canada, Hong Kong, all dating from before any of this. So this is basically used as an attempt by Mr Ira Kleiman in his litigation, where he wanted - - this is, he believed, \$600 billion was the figure. He was offered a settlement figure of US\$3.4 billion, which he turned down, as 50% cash --</p>	<p>Dr Wright blaming third parties (namely Ira Kleiman) for the doctored documents ID_001930 & ID_001395.</p>
<p>{L9/191/1}, "NetBank - Transfer receipt Part 1", ID_001406</p>		
<p>{Day4/137:6-16}</p>	<p>Q. Well, just so it's clear, Dr Wright, I'm disputing that this is, as you suggest, a fake document.</p> <p>A. I didn't say this was a fake document. I did make a payment. Every single year, I had to pay for nominee shareholding services from DeMorgan.</p> <p>Q. I see, so the email which referred to this transfer receipt was fake, but the transfer receipt isn't?</p> <p>A. There was a transfer done, that is correct. As noted, the email was found on a third party server, which wasn't mine and also had access to my wife's and other people's emails.</p>	<p>Dr Wright is evasive in response and appears to be blaming third parties in relation to the email referred to in the transfer receipt.</p>
<p>{L9/287/1}, email chain between Dr Wright and Abacus</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day4/138:10} - {Day4/139:8}</p>	<p>Q. Then page 1, at the end of this chain {L9/287/1}, ends with Abacus forwarding you the certificate of incorporation and a series of other documents?</p> <p>A. Yes.</p> <p>Q. So there is a substantial documentary record showing that you, in late 2014, reserved Tulip Trading Limited as an aged shelf company, isn't there?</p> <p>A. No, there is not, and this document demonstrates what we get basically every year. This, I had to sign for Panoptcrypt, which became - - which was the director. Panoptcrypt was an Australian company that acted as one of the directors of the overseas companies, so we were also, as I noted, locked out of our offices. That's easily verifiable. There's - - it was in administration for a time, and the records of the administrator are all available and public as well. That's also on ASIC, which is the Australian Companies House. Now, in those documents, you'll see that we had that event, we were locked out of the office, and at the same time we were facing action, like audit from the Australian Tax Office and we were required to basically have all of our documentation constructed. So that was real documents that we went back to the providers for and asked for.</p>	<p>Dr Wright is evasive in response and has not produced the records on which he relies.</p>
<p>{Day4/139:9-20}</p>	<p>Q. Dr Wright, it is no coincidence, is it, that Mr Madden has found editing in the incorporation form and that invoice to suggest the time for this registration being moved from 2014 to 2011? That's no coincidence, is it?</p> <p>A. No, it's not a coincidence. As I stated, because we had an American case where people were trying to plant this on us, when we had people sending false documents to the Australian Tax Office, the entirety of what I was going through at this period were people trying to say that everything was false. Mr Ira Kleiman and several other people in the Australian companies all wanted them closed.</p>	<p>Dr Wright blames third parties for producing fake documents (namely Ira Kleiman and others in Australia) and planting these documents on him.</p>
<p>{Day4/140:16} – {Day4/141:15}</p>	<p>Q. First of all, Dr Wright, none of these documents even appears in the chain of custody, because none of them is a reliance document, so you're just wrong in saying that you look in the chain of custody document to find some answers, aren't you?</p> <p>A. No, actually, I filled out a full chain of custody document and all of these are in Relativity. I don't know what you can see - -</p> <p>Q. Just pause there, please, Dr Wright. Each time you refer to Relativity, you are referring to your solicitors' privileged system, so I just want you to be very careful</p>	<p>Dr Wright is blaming third parties (namely his solicitors) for not passing on information that he claims to have provided on chain of custody.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>about making references to a system which is privileged so that you don't waive privilege, okay?</p> <p>A. No problem.</p> <p>Q. Go on. As long as you're talking about things which have been disclosed between the parties, go on.</p> <p>A. Well, I don't know. What I have done is I've filled out a complete chain of custody document stream. I do not know what the redacted version of that that you have is. I have access to a platform that I'm not discussing, obviously, and that has all of the information. However, what has or has not been attached with ID numbers, I actually don't know. I mean, it's in my view, but I don't know what your view is, so I can't say whether you have it or not, obviously.</p>	
<p>{Day4/144:11} - {Day4/145:8}</p>	<p>Q. My Lord, that's as far as I can go at the moment in relation to that. I've put my case, but obviously I can't go into the detail of an expert report which has yet to be produced. I'm hoping that it won't be necessary to recall Dr Wright to return to this. What all these documents show is that Tulip Trading was bought by you in 2014 as an aged shelf company and efforts were later made to create documents suggesting that it had been bought in 2011. That's the truth, isn't it, Dr Wright?</p> <p>A. No. What it suggests is, because I'm rather close to my chest with most of my corporations and things - - or I used to be; now everyone knows everything about me - - I had a variety of companies that people didn't know about, so they didn't realise that I actually had over 20 overseas corporations that were well documented, they didn't realise that I'd already been in disputes over these companies, they didn't realise that just shutting down a company doesn't give you assets. I mean, that was probably the most asinine bit. Ira and others actually believing that if they liquidated my companies they would somehow get my intellectual property. So, no, that's what it was all about.</p>	<p>Dr Wright blaming third parties (namely Ira Kleiman and others).</p>
<p>The Papa Neema emails</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day4/148:10} - {Day4/150:9}</p>	<p>Q. Let me just see if I can unpick the narrative and if I've got it right. First of all, is it right that you say that on 8 September, you told Christen Ager - Hanssen, the then CEO of nChain, that you would request invoices from Denis Mayaka, formerly of Abacus Seychelles, to show your registration of these companies in 2009?</p> <p>A. Yes, that's correct.</p> <p>Q. Then do you say that Mr Ager - Hanssen, you understand, called Mr Mayaka on 9 September 2023, telling him to expect an email from Maze Cyber and send it on to you?</p> <p>A. I do.</p> <p>Q. Then is this right, you say that on 10 September, Mr Mayaka receives an email from Maze Cyber attaching screenshots of invoices?</p> <p>A. Yes.</p> <p>Q. Then do you say that later that day, Mr Mayaka emailed Stefan Matthews with an email under the name "papa neema@gmail"?</p> <p>A. Well, that's the email address, it's not the name.</p> <p>Q. But the from the email address "papa.neema@gmail.com"?</p> <p>A. Yes.</p> <p>Q. With a ZIP file containing some screenshots?</p> <p>A. Yes.</p> <p>Q. And that was copied to you?</p> <p>A. It was.</p> <p>Q. You say you then emailed him asking for original invoices and he agreed?</p> <p>A. Correct.</p> <p>Q. And your position is that the invoices shown in the screenshots are real?</p> <p>A. They appear to be, yes.</p> <p>Q. Do you believe, do you understand that the screenshots were photographs taken by Mr Mayaka?</p> <p>A. No, actually, he got them. The screenshots are ones he received from Christen Ager - Hanssen, or a representative thereof.</p> <p>Q. So you think Mr Ager - Hanssen sent Mr Mayaka the screenshots which contained real invoices and were then sent on to you?</p>	<p>Dr Wright is evasive in response to questions regarding the provenance of the screenshots of invoices.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. I don't actually know if they were real, but he had been talking to Denis. Because he was the CEO of nChain, Denis believed that he should be able to listen to him and trust him - - which is a silly thing, but then we all do silly things - - and then, when he received those, well, screenshots, he forwarded those on to Stefan. After I received that, I went back to Denis and I went, "Why are you sending us screenshots?", in effect, I don't remember my exact wording, and questioned him about that, because I wanted the invoices.</p>	
<p>{Day4/151:19} - {Day4/152:10}</p>	<p>Q. Now, you insist, don't you, in your 11th witness statement that whatever else, these are not photographs of your monitor?</p> <p>A. No. They are photographs of what I think Christen believed my monitor to be. He's seen videos, etc, but what he didn't realise is I don't run the standard build for nChain. My laptop is a bespoke system, I have it custom made. So while it is Lenovo, it isn't the same as the other ones. And it is still corporate policy at nChain to run Windows 10 because of some applications we have, but I'm a special case and I run Windows 11. So this is basically someone who believes. It was later discovered that Mr Ager - Hanssen had used a policy update from a VPN that was applied to put malware onto my computer. That wasn't discovered until September. Mr Ager - Hanssen was fired from nChain and any day now he'll be facing criminal action.</p>	<p>Dr Wright is evasive and blames third parties (Christen Ager-Hanssen) despite not providing any evidence of Mr Ager-Hanssen putting malware into his computer.</p>
<p>{Day4/152:16} - {Day4/153:3} {P1/20/9}</p>	<p>Q. You have a chain of custody document in the context of these proceedings, don't you?</p> <p>A. I do.</p> <p>Q. "Spyder.rtf" is the name, isn't it, of a deleted file from the Samsung Drive which you provided which Mr Madden recovered and which had been backdated to 2017; correct?</p> <p>A. I don't know if it's a deleted file on that, but I know what Spyder.rtf is.</p> <p>Q. What sort of document do you say it is?</p>	<p>Dr Wright is evasive in response to questions regarding the tabs visible in the screenshots.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. The original would have been a corporate policy document about Spyder. The one on that screen, I don't actually know.</p> <p>Q. So it's certainly a document you associate with yourself?</p> <p>A. Oh, it's one - - I mean, the name is one that I created. Whether it's that version or not, I don't know.</p>	
<p>{Day4/153:13-21}</p>	<p>Q. Dragon Dictate is a form of software you use, isn't it?</p> <p>A. Yes, but I use a different version than that one. The one being displayed and the one that I have are different.</p> <p>Q. Then the "Z" is a logo for the software Zotero, isn't it?</p> <p>A. That's correct.</p> <p>Q. And Zotero is another software you use, isn't it?</p> <p>A. It is.</p>	<p>Dr Wright admits that he uses Zotero.</p>
<p>{Day4/154:20} - {Day4/155:9}</p>	<p>Q. ... It's no coincidence, is it, Dr Wright, that we have a monitor of the same model as yours, with tabs - - a whole series of tabs for programs and files associated with you?</p> <p>A. No, it isn't a coincidence. Mr Ager - Hanssen provided an interview a while back noting that how he met me at an AMEX black card function was basically something he arranged, he paid to be there, and one of the things I found out, like other American lawyers, he spikes drinks. So, my wife remembers how utterly drunk I was. I didn't think I had drunk so much, but neither did Kyle Roche. When you walk away from Mr Ager - Hanssen, you find you have been drinking more than you realised. He actually admitted that in an interview, thinking it was funny.</p>	<p>Dr Wright blaming third parties (Mr Ager-Hanssen).</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day4/155:22} - {Day4/158:5}</p>	<p>Q. So this is another elaborate set up job, this time not by Mr Kleiman or disgruntled employees or people from BTC Core, but by Christen Ager - Hanssen?</p> <p>A. Yes and no. What I do know is he has links to both Algorand and BTC Core, hence why, after all of this started going down, he started tweeting proficiently about how “fake Toshi” was going down and how I’d faked everything.</p> <p>Q. Dr Wright, you’re just making up these allegations as you go along, aren’t you?</p> <p>A. No, it’s actually in one of your witness statements from Sherrell. Mr Sherrell has actually produced this for me. I was not able to capture the tweets in time, but -</p> <p>Q. Your allegations linking Mr Ager - Hanssen to all sorts of other people are just you making it up as you go along, aren’t they?</p> <p>A. No, actually, Mr Ager - Hanssen is using a third party laptop, he is not a skilled hacker, so for someone to actually be displaying my live browsing history, and I mean live, remotely on a screen and tweeting it, well, that demonstrates complete control of my computer. And Mr Ager - Hanssen has no ability to do that, so there are third parties.</p> <p>Q. So you say he has set up a computer to look like yours, put a document on that looks actually genuine and supportive of your position, taken a photograph of it and arranged for it to be sent to Mr Mayaka with a view to it ultimately going to you?</p> <p>A. Yes. I had actually, first of all, told Stefan, look, this is getting ridiculous, why don’t I just go to Denis and ask for the invoices directly. I said that to Ali Zafar KC, who was a person who set up the false, fake trial thing, pretending to be a - - with someone pretending to be a judge, which I found really abhorrent. And then, when I told him this, he said, “There’s no way you can do that, you can’t get those documents, you cannot put them in”. I did it anyway and had them sent, but before I reached out to Denis, I discovered that he’d already reached out to Denis. And then I spoke to Travers, and Christen I found at that point had added his name to my case somehow. Christen Ager - Hanssen told Travers Smith that he was working for Calvin Ayre and Calvin was my funder, and thus, as the litigation funder, and his representative, he has to, well, basically sign off on all of my documents, which led to Travers Smith having a conflict. I actually quite liked Travers Smith, I really did.</p>	<p>Dr Wright blaming third parties (Mr Ager-Hanssen and Ali Zafar KC).</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Please don't tell us about your how your conflict with Travers Smith emerged, because I'm sure your lawyers will consider that privileged.</p> <p>A. So anyway, as I was noting, Mr Ager - Hanssen went into a big panic when I said that I could get documents from Denis. I listened to him and didn't - - but didn't basically act straight away. Ali Zafar KC then told me I couldn't use these documents, no court would accept them. I then went - - I don't know why, I mean, they're directly from Denis. Lawyers believed, because a KC said it, and we're where we are.</p>	
{Day4/158:6-18}	<p>Q. Dr Wright, I'm just going to put it to you again, I think I've probably put it to you already, this is just an elaborate fiction, these were photographs taken by you of your monitor.</p> <p>A. No. As I stated, Christen actually then went and did an interview right after this with a Norwegian court, where he said basically that he set everything up in the first place to get me, to get into nChain, and then said, at the end of this, he was either going to own all the intellectual property in nChain or destroy it. And then he started tweeting to BTC Core and engaging with COPA members, and had a number of files that shouldn't be with him.</p>	Dr Wright blaming third parties (Mr Ager - Hanssen) and referring to events that are not in evidence.
{L1/115/1} - ID_004009 - DeMorgan Notes		
{Day4/159:14} - {Day4/160:2}	<p>Q. Moving on then to a new document ID_004009, which is at {L1/115/1}. Now, this is one of your reliance documents. It's not a pleaded forgery. I'm addressing it in relation to authenticity. Dr Wright, do you recognise this as one of your primary reliance documents?</p> <p>A. I do.</p> <p>Q. It's a set of manuscript notes on a DeMorgan company pad?</p>	Dr Wright admitting that the notes are the early version of BlackNet.

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. It is.</p> <p>Q. Can we agree this, at least the bulk of these notes are written as if they were development notes on Bitcoin or a concept like it before the release of Bitcoin?</p> <p>A. It was the early version of BlackNet.</p>	
{Day4/161:9-23}	<p>Q. And those included a statement from Daniel Bernstein, whose team had developed the digital signature scheme known as EDDSA, didn't they?</p> <p>A. The current version of Schnorr signatures, yes.</p> <p>Q. But they developed the scheme which has the moniker "EDDSA"?</p> <p>A. Correct.</p> <p>Q. And you're aware his statement, which you received in the middle of last year, said that that abbreviation was first used in 2011?</p> <p>A. Yes.</p> <p>Q. And is it right that in your chain of custody information, after the provision of that statement, you gave some information about this document?</p> <p>A. I did.</p>	<p>Dr Wright admitting the date on which the abbreviation EDDSA was first used.</p>
{Day4/162:7-23}	<p>Q. Dr Wright, I'm not disputing that this is written in or after 2011.</p> <p>A. Only the red part.</p> <p>Q. But you say that the document was produced as part of work you were doing in 2002; correct?</p> <p>A. Mm. That's when I started it.</p> <p>Q. You said that the handwritten notes were made between 2005 and 2013? This is from your chain of custody. We can go to it?</p> <p>A. What I'm saying is I've updated there, but the handwritten notes includes the red stuff and there's two separate parts.</p> <p>Q. You've said that the document - - this is, again, from your chain of custody - - was originally written in 2002, but you made further notes in red ink at a later time referring to dates in 2011?</p> <p>A. Yes.</p>	<p>Dr Wright admitting that the document was originally written in 2002 but further notes in red ink were made in 2011.</p>
{Day4/165:3-17}	<p>Q. Can I pause you there, because I think you've probably addressed the question. It was public knowledge, wasn't it, from published emails between Satoshi and Mike Hearn that he, she or they, Satoshi, chose ECDSA over</p>	<p>Dr Wright is evasive in response to questions regarding published emails between Satoshi</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>RSA in part because RSA’s huge keys were out of the question; correct?</p> <p>A. Oh, I mean, it’s public knowledge from a number of communications, including Hal Finney. But you don’t actually need to know --</p> <p>Q. Just answer that question for a start, Dr Wright.</p> <p>A. I would say you even go beyond that into - - so, I wouldn’t actually say that’s why it would be known. It is well known in the industry, where I even taught, that ECDSA is far more efficient than RSA for the same level of security.</p>	<p>and Mike Hearn regarding the choice of ECDSA over RSA.</p>
<p>{Day4/166:13} - {Day4/167:14}</p>	<p>Q. Can I just pause you there. I think, again, we've covered the topic. Back to the document, page 35 {L1/115/35}. Now, just on the language of what's written, "DSA/RSA key size is too large; need to try ECDSA", gives every impression of a note from Satoshi to himself looking forward to the release of Bitcoin and contemplating different signature algorithms to choose between, doesn't it?</p> <p>A. No, it actually perfectly matches up with RRD4. RRD4 is on page number 1 {L1/115/1}. Now, being that I've mentioned RRD4, which is a 2011 project, which is actually doing what I'm talking about, then that just, sorry, doesn't fit. Now - -</p> <p>Q. And this elaborate story of this document being produced over a space of nine years, these manuscript notes being produced over a period of nine years, was first arrived at after Mr Bernstein's evidence was produced, wasn't it?</p> <p>A. I don't know when it was. I told everyone about it. I've mentioned - -</p> <p>Q. So in your - -</p> <p>A. - - all of this - -</p> <p>Q. It was in your chain of custody information, which was first provided in October 2023 after Mr Bernstein's evidence had been produced, yes?</p> <p>A. That's the time for that document chain, yes.</p>	<p>Dr Wright admitting that he first provided chain of custody information for this document after Professor Bernstein’s evidence had been produced.</p>
<p>{L4/371/1} - Information Defense Memo</p>		
<p>{Day4/169:7} - {Day4/170:3} {Q/2/7}</p>	<p>Q. {Q/2/7}, please. This is the joint report of Mr Madden and Dr Placks, their first joint report. In relation to this template, do you see that Mr Madden finds it to be manipulated, on the basis of his conclusions, yes?</p>	<p>Dr Wright not accepting the obvious truth that his expert, Dr Placks, concludes that it is not</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
Joint report of Mr Madden & Dr Placks	<p>A. Yes, I see that.</p> <p>Q. And Dr Placks finds that it's not possible to authenticate it?</p> <p>A. He says it's - -</p> <p>Q. It's unreliable.</p> <p>A. Well, no, what he says - - which one are you looking at, sorry? Which number?</p> <p>Q. 000856.</p> <p>A. Mm - hm. Okay.</p> <p>Q. And he concludes that it's unreliable, doesn't he?</p> <p>A. No, he says he's "unable to attribute document to any specific template given the quality of the scan". So, basically, as he says there, "modify layouts and day - to - day editing", he can't actually do it. But what I'm saying is it came from a third party tool, software repository. So, he doesn't say it's inauthentic, he says that he is unable to say whether it matches. It's a scanned document.</p>	possible to authenticate the document.
{Day4/170:4-10}	<p>Q. Well, I 'm putting to you, on the basis of Mr Madden's findings, that this document is not authentic to 2009, is it?</p> <p>A. I received it in 2012, but I have no reason to believe that it's not in - - inauthentic. The notes were done by Lynn Wright. Cloudcroft was a company that she was running. It took over Information Defense.</p>	Dr Wright blaming third parties (Lynn Wright).
{Day4/170:23} - {Day4/171:6}	<p>Q. Just to be clear, Dr Wright, based on the start of that answer, it's your position, is it, that you have no reason to believe it inauthentic rather than that you positively consider it to be authentic, based on what you know of it?</p> <p>A. I know the text is what I would have told Lynn. All of the material is there. Lynn took all the notes in January 2009. I didn't interact with any of those notes until, sort of, I got them back in 2012.</p>	Dr Wright's answer is implausible.
{L2/243/1} - ID_004015 - Bitcoin code		
{Day4/172:2-13}	<p>A. Well, it's definitely an early copy of the Bitcoin source code, and, yes, I wrote it.</p> <p>Q. And when do you say it dates from?</p> <p>A. I don't actually know. On some of my own copies of documents that I would have printed, I may not have updated the copyright. So all I know is this is a printout that has been in my files since Australia.</p> <p>Q. So since December 2015?</p>	Dr Wright is vague and evasive in response regarding the date of the copy of the Bitcoin source code at {L2/243/1}.

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. It would have been earlier than that. It would date - - I mean, it's pre - Panopticopt and Panopticopt was 2011.</p> <p>Q. So before 2011?</p> <p>A. Well, no, before the mid 2011, is all I could say.</p>	
<p>{Day4/173:11} - {Day4/174:21} {M/2/352}</p> <p>Dr Wright's First Witness Statement</p>	<p>Q. And if we go to the next page {M/2/352}, can we see that paragraphs 75 and 77 of your first witness statement referred to working copies of the Bitcoin Code developed by early 2008?</p> <p>A. I do.</p> <p>Q. And do you see that your solicitors have identified two documents falling within the description of such items, yes?</p> <p>A. I do.</p> <p>Q. One of them is this one, 004015, and the other is 004014?</p> <p>A. I do.</p> <p>Q. So, is it your position that this document was produced by early 2008?</p> <p>A. No, my position is as I've stated. I started creating the code and had a working version in 2008. Now, the way that an SVN like - - and I use TortoiseSVN, but SVN works is that you don't have a local copy, so you do updates and you do updates, etc. So each time I changed the document, I'm basically updating and building on the document. That doesn't mean that I automatically change the copyright. So, when I'm working on a document and I print it, even if I'm printing it in 2009 or '10, it's an extension of my 2008 work.</p> <p>Q. So is it your position that you in fact don't have any documents reflecting, or which represent what you produced in 2008 in the sense that it's either a printout from 2008 or it's a code document dating from 2008?</p> <p>A. Again, that's not correct. Even if I start the work and have it mostly done, but update it, then it's still my work from 2008.</p> <p>Q. So this is asking for documents referred to, and the document that's being referred to is a preliminary version of the code which you had in 2008?</p> <p>A. Which has been updated, as I said.</p>	<p>Dr Wright is evasive in response and not accepting the obvious truth that he does not possess any documents representing what he produced in 2008.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day4/175:6} - {Day4/176:6}</p>	<p>Q. So, is it your position now that this document is a hard copy produced some time after 2008 which you say is a further version, with some development, of code you had in 2008?</p> <p>A. I don't actually know when I printed it out. I know that it goes back to pre - Panopticopt, but more than that I can't say. At that time, I was moving out of home from, like, my ex - wife, and starting a new life and so on, so I don't have proper documentation of which documents were printed when.</p> <p>Q. So you then can't say that this document was the same - - shows that it is the same in content as a version of the code you say you had in early 2008?</p> <p>A. No, what I can say is I started coding this in 2008, and I have an online version of document, and as I'm working on it, I will periodically print it.</p> <p>Q. So this document is itself not evidence of what the code was in fact in 2008?</p> <p>A. I'm not saying it is. The 2008 code is actually still publicly, if difficult to find, available. The SVN had all of that. So, I'm not sitting there going the code proves anything. The code was public. My proof has never been I have the secret source and the code. My proof is, a company such as nChain can do 79 patents a year. I've done 1,000 blockchain patents, 4,000 pending patents, 350 White Papers.</p>	<p>Dr Wright's answer is evasive and incoherent, again resorting to claims to have registered lots of patents.</p>
<p>{Day4/176:7-25}</p>	<p>Q. Just pause there. You said in your statement that you had a preliminary version of the code by early 2008?</p> <p>A. I did.</p> <p>Q. Your solicitors were then asked for, by way of document, that early version of the code, and you - -</p> <p>A. (Overspeaking).</p> <p>Q. - - now say - - just a second - - you now say that the document that was identified was not one of those early versions of the code but something you produced later, which may have changed since 2008?</p> <p>A. No. Again, every line of code doesn't change. So, if I've gone there and updated something, the same way as companies update invoices, then the majority of it is still the same code. So, early code is still early code. I cannot say when it's been updated; I don't have any records, I didn't write the date on the top. I've been schooled on that one now, and every time I write a paper document, I now have the date and other markers, but I didn't at the time.</p>	<p>Dr Wright is evasive in response and will not accept the obvious truth that he does not possess any documents representing what he produced in 2008.</p>

Appendix B: Schedule of Transcript References

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
DAY 5		
CROSS-EXAMINATION OF DR CRAIG WRIGHT BY JONATHAN HOUGH KC		
{H/78/4} - Appendix PM11 - email from Craig Wright to Jimmy Nyuyen		
{Day5/4:7-23}	<p>Q. If we go to {H/78/1}, we can see a copy of that email. Your evidence was that you sent that email, wasn't it?</p> <p>A. It is.</p> <p>Q. Page 5, please {H/78/5}. This is Mr Madden's reproduction of the header of the email, and we see: "Return - Path: <craig@rcjbr.org>." And then: "Received: from ..." An IP address; do you see that?</p> <p>A. I do.</p> <p>Q. It's the same, isn't it?</p> <p>A. Yes. That would likely be nChain in that case.</p> <p>Q. That seems to be associated with your RCJBR.org email, doesn't it?</p> <p>A. I used my computer, which was called "Neo", in the nChain offices. So, yes, that would be my computer being used there.</p>	Dr Wright is unable to accept the obvious truth that the IP address ending in 194 is his own.
{L4/15/1} - {L/15/5} - readme.txt compared against supposed TimeChain v0.0.2 readme file.		
{Day5/5:18} - {Day5/6:4}	<p>Q. Now, please, {L4/15/1}. This is the readme set up notes for Bitcoin released by Satoshi Nakamoto in January 2009. Will you accept that from me?</p> <p>A. Yes. Both of the projects used the same code.</p> <p>Q. And if we go under "Setup", the notes, with the exception of the EXE file name, are materially the same, aren't they?</p> <p>A. They are.</p> <p>Q. And it would have been technically straightforward to take the publicly available text file and amend it to produce your document?</p> <p>A. Yes.</p>	Dr Wright admits that the two readme notes are materially the same, and that it would have been easy to amend the publicly available version, such that the TimeChain.exe file cannot be reasonably relied upon.
{M/1/787} – BlackNet document chain of custody information		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day5/9:2} {Day5/9:16}</p>	<p>-</p> <p>Q. It didn't cast any doubt on the document?</p> <p>A. Well, it says it came from a third party and not me.</p> <p>Q. But it didn't cast any doubt on the authenticity of the document? Simple question, Dr Wright.</p> <p>A. Well, if you don't know anything other than it came from a third party, then that's what you put. It wasn't analysed.</p> <p>Q. And your first witness statement was served at the end of July 2023; do you recall that?</p> <p>A. I do.</p> <p>Q. Do you recall that there's nothing in that witness statement to suggest that the documents you nominated as your primary reliance documents might well have been altered, having been handled by dozens of people?</p> <p>A. Not in my witness statement, no.</p>	<p>Dr Wright is evasive, insisting that the document came from a third party and therefore he couldn't stand behind the chain of custody information he provided.</p>
<p>{K/11/1} - Chain of Custody Reliance Documents / BlackNet Document</p>		
<p>{Day5/11:5} {Day5/12:13}</p>	<p>-</p> <p>Q. And then at the bottom: "Dr Wright is aware that this document is not the native document but a document which has been handled by a variety of custodians as described in the document. The native document (where available) shall be provided in accordance with the letter from Shoosmiths ... dated 11 October ..." So it was Shoosmiths. So it's right to say, isn't it, that in this document, for the first time, we received information from your side saying that there was reason to doubt the authenticity of many of your reliance documents?</p> <p>A. I don't think that's actually a reason to doubt the authenticity, rather it's a file that has been used across a corporation by multiple people in a research effort. As I gave an example yesterday, if I have an invoice and I change the font and the set up, then the data remains the same. So, even though the invoice prints out with different headings, it's still the same data and the same authentic invoice.</p> <p>Q. Dr Wright, just look at what the document says. It says you can't comment on the authenticity of these documents because many people had access to it or copied it from the shared servers. That is plainly raising questions over the authenticity of the document, isn't it?</p> <p>A. No. What I can say is I can look at the text of the document and I can say that's correct. What I can't say is - -</p> <p>Q. Pause there. Where do you say that in this document?</p> <p>A. No, that's what I'm saying now. I'm telling you, I know my document, I can tell you my document, but I can't say whether</p>	<p>Dr Wright is evasive and inconsistent, claiming that a document's use by lots of people is not a reason to doubt authenticity.</p> <p>Implausible and inconsistent nature of Dr Wright's accounts. He claims to write more than a hundred papers a year (he claimed to write a paper every two days {Day3/27:7}) but yet he 'knows his documents' from the early 2000s.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	someone has changed a font or done something else. I don't look at fonts or anything like that when I read a document.	
<p>{E/4/5} - Fourth Witness Statement of Craig Steven Wright Drafting the Bitcoin White Paper</p>		
<p>{Day5/14:5-18}</p>	<p>Q. That was the first time you had claimed in these proceedings to have written the Bitcoin White Paper with LaTeX, wasn't it?</p> <p>A. No, actually, and the document that was provided initially in the Kleiman case that was in the disclosure platform right from the beginning, in handwriting, has "LaTeX" written on it. So right back from before 2019, I'd already had documents saying the White Paper was written in LaTeX.</p> <p>Q. Your first witness statement discussing the way the White Paper was produced said nothing about LaTeX, did it? It didn't use the word.</p> <p>A. I'm not sure, but the evidence that I provided in my handwritten notes does say it.</p>	<p>Dr Wright is evasive, saying that handwritten notes prove he wrote the Bitcoin White Paper in LaTeX, when they merely state that he wrote the word "Latex" in manuscript.</p>
<p>{Day5/15:13} - {Day5/17:17}</p>	<p>Q. And so, is it right to say that you are unable to point to a reliable, unamended version of the Bitcoin White Paper from the 2007 to 2008 period?</p> <p>A. No, that's not correct. The original handwritten document is, and it's been seen by multiple people. Other documents are.</p> <p>Q. Which other documents?</p> <p>A. Other versions of it.</p> <p>Q. Which other versions?</p> <p>A. I don't know the ID numbers off the top of my head, I'm sorry, I don't memorise them.</p> <p>Q. Well, you had the opportunity in this witness statement, and on many other occasions, to say there are some versions which I can absolutely vouch for, but instead you say -- you make here the general observation: "I am ... unable to say ..." Of the Bitcoin White Paper drafts: "... whether the metadata or content ... [had] been altered or amended ..." Correct?</p> <p>A. No. What I said is I don't have memorised the ID numbers from the disclosure platform. I would be able to go back and pull those numbers and say it, but I can't do it without access to the platform. So, what I'm saying is, I haven't memorised every number of evidence.</p> <p>Q. Dr Wright, you are here answering questions generally about drafts of the White Paper and you make this general observation that you are unable to say whether the metadata or</p>	<p>Dr Wright is evasive regarding what his evidence is on whether the metadata or contents of drafts of the Bitcoin White Paper have been altered.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>contents of the drafts have been altered or amended. Is that - - (overspeaking) --</p> <p>A. (Inaudible).</p> <p>Q. Is that evidence, to which you put a statement of truth, correct or incorrect?</p> <p>A. What I said is there may have been changes, such as fonts, there may have been metadata changes. Now, in saying the content, what I'm saying is I know the content of the White Paper, that is correct. The words in the White Paper are correct. If something, such as a font, has changed over time, or someone has re - saved my document, no, I haven't checked that.</p> <p>Q. So there is no version of the Bitcoin White Paper in electronic form which you can hold up and say this is a pre - issue copy of the Bitcoin White Paper which I wrote, which hasn't been -- which can't have been mucked with by somebody else and potentially altered by somebody else?</p> <p>A. No, again, that's incorrect. What I'm saying is I cannot quote a number at the moment. I could look at the Relativity platform, the disclosure platform, and I could bring up the numbers. But without that in front of me, I cannot; I haven't memorised them. So when I leave the court, I could go and pull the numbers for you and I could say, "This one, this one and this one", but I cannot do that by memory.</p>	
<p>{Day5/17:22} - {Day5/18:9}</p>	<p>Q. Dr Wright, you understand the importance of being able to identify a reliable pre - issue version of the White Paper in your hands, don't you?</p> <p>A. Not in the way you're saying. I actually --</p> <p>Q. It was one of the issues identified in his Lordship's judgment of October last year as one of the key issues in the case.</p> <p>A. No, authorship was. So, what you're saying and what I'm saying are two different things. What I'm saying is, the proof of identity and authorship doesn't come down to a key, or holding a file. I could, at any time, create a perfect copy of the White Paper. What I'm saying, though, is, evidence is always by actions. The same way that de Cervantes proved that he was the author of the Don Quixote - many other authors through history have proved pseudonymous authorship, the same way that patent providers have done so.</p>	<p>Dr Wright contends, wrongly, that identifying a pre-release version of the Bitcoin White Paper is not a key issue.</p> <p>Dr Wright claims that he could create a "perfect" copy of the Bitcoin White Paper any time, but that this wouldn't be probative, thereby casting doubt on all alleged documentary proof provided.</p>
<p>{Day5/18:12} - {Day5/19:9}</p>	<p>Q. Let's be clear about this. You are not asking the court to accept your claim to be Satoshi on the basis of any document you say is reliable; is that your position?</p>	<p>Dr Wright is evasive, calling into question all metadata relating to documents.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. No, it is not.</p> <p>Q. So it's legitimate for us to ask you about whether documents which you have relied on in support of your claim are authentic or may have been mucked with; correct?</p> <p>A. Again, that is a misrepresentation of what I've said. Let me explain that so I'm clear. I have said that the information in these documents is correct. I've also noted that, apart from isolated servers that no one interacts with, metadata will never stay the same. You provided the example of the Bitcoin White Paper. That isn't ever interacted with, it's on a web server that it gets downloaded on a local machine. It is never interacted with on the web server. Now, alternatively, what we have is a corporate scenario. In a corporate scenario, people access files. I can say that these people access files, because I give them access so that we do research. That's how we have created intellectual property in this area, including intellectual property such as --</p>	
<p>{L19/257/2} – Fourth Witness Statement of Craig Steven Wright; Exhibit CSW5 (table referred to in witness statement)</p>		
<p>{Day5/22:12} - {Day5/22:25}</p>	<p>Q. Before you received the Madden report, you presented, through all your communications to us, your first set of 107 reliance documents as authentic originals with no suggestion that they would or might have been altered; correct?</p> <p>A. No. It was well known that I'd had challenges on some of those documents in other courts, and those had been explained --</p> <p>Q. Since receiving that report, you've cast doubt on the reliability and authenticity of very many of them, especially those forensically examined; correct?</p> <p>A. No, again, back to the Kleiman case. There were already notifications put in that the various machines from third parties had been unrelated to myself.</p>	<p>Dr Wright is evasive, stating that he did not present all of his original Reliance Documents as genuine.</p>
<p>{Day5/23:8} - {Day5/23:17}</p>	<p>Q. And you claimed that it had been captured - - the drive image had been captured originally on 31 October 2007; correct?</p> <p>A. Yes. Let me explain that term. That doesn't say that it was cloned. A forensic image is a cloned image. A capture means a VMware. So I did an image using DD, then I basically copied files back and forwards until I captured it into VMware, which was in October.</p> <p>Q. 2007?</p> <p>A. That's correct.</p>	<p>Dr Wright confirms the 2007 capture date of the BDO Drive.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{G/5/9} - Third Expert Report of Patrick Madden (including his analysis of the 97 documents from the BDO Drive)		
{Day5/27:6-22}	<p>MR HOUGH: Dr Wright, are you aware that when this report was written, we didn't have access to the drive because we were being told by your side that we shouldn't have that access?</p> <p>A. I don't know when you got access to the drive.</p> <p>Q. And focusing upon what material we had at the time and were being given access to at the time, the metadata in the files, that contained materially less useful information for analysis than that in the file types in your original reliance documents. Can we agree on that?</p> <p>A. No, actually, because there are files, such as Dragon files. Dragon files, while proprietary, have a lot of rich information, right down to voice recording. That would enable extracting WAVE files that you could even replay the background information, and the background information would provide details of where I might have been at the time or - -</p>	Dr Wright is evasive, unable to accept any responsibility for the lack of access provided to the BDO Drive and indirectly blaming his lawyers.
{Day5/28:1} - {Day5/28:21}	<p>Q. Dr Wright, paragraph 16, I'm just going to ask you if this is factually correct: "I note that almost all of the filetypes in the 97 New Documents were not present in the original Reliance Documents. The original Reliance Documents did not contain any LaTeX, RTF, C++, HTM, TXT or DRA files and only a small number of images ..." Are the contents of that paragraph factually correct?</p> <p>A. There were some RTF files, but for the most part, yes.</p> <p>Q. And the explanation for this significant difference is that you had seen what Mr Madden had done to discredit your original documents and you had chosen a set of documents which had very little usable metadata for analysis, hadn't you?</p> <p>A. No, that's incorrect. The distinction is between third party machines and laptops, which I've always stated, right back to 2017, versus my own work habits. I work differently than other people, I use Dragon VoiceType, I use LaTeX, etc, so, my work habits are different to others in the organisation.</p>	Dr Wright is evasive, maintaining his argument that he "work[s] differently" which explains the difference in file types in the 97 BDO Drive documents as compared to those in Dr Wright's original Reliance Documents.
{Day5/28:22} - {Day5/30:4}	<p>Q. Are you also aware that many of your 97 new documents, I think 11 of the 97, include supposed work on Quorum systems? Yes?</p> <p>A. Yes.</p> <p>Q. Do you know how many of your original reliance documents even mentioned the word "quorum"?</p> <p>A. On my original? I don't know. I don't think so.</p>	Dr Wright is evasive, inventing an implausible excuse for failing to provide any disclosure originally of documents he now claims are important.

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. None of them. You've relied upon the work on Quorum systems in the new documents as a key element of your precursor work to the Bitcoin White Paper, haven't you?</p> <p>A. I have.</p> <p>Q. And that didn't appear anywhere in your original reliance documents, did it?</p> <p>A. As I noted, none of the material came from my machines, so the third party machines that the original documents were sourced from had limited information. The information from nChain concerning Quorum documents wouldn't be handed over because that's basically leading to proprietary filings. So, while they have a lot of information, they won't give it to me.</p> <p>Q. That's just a fiction made up on the spot, isn't it, Dr Wright?</p> <p>A. No, actually, it's to do with the fact that we have several thousand pending patents. And as my Lord will understand, companies don't like giving proprietary information that hasn't been filed yet. In fact, I had to rush people because of some of the things I've been mentioning here to get a patent filed, which was lodged on Monday. One of the areas that I communicated with, and will be answering, involves a patent that was only filed on Monday that the original OI goes back to 2008, but because it wasn't considered top of the list - -</p>	<p>Again, he finishes his answer with reference to how many patents he has.</p>
<p>{G/5/9} - Fifth Witness Statement of Craig Steven Wright</p>		
<p>{Day5/31:6} {Day5/31:16}</p>	<p>- Q. Would you accept this, that if you and your solicitors had been doing a proper job of disclosure in the McCormack case, the Granath case or this case, you should have been checking to ensure that all your data sources had been found and imaged? Would you accept that?</p> <p>A. No, actually, I'd gone back multiple times and complained to my solicitors that very few of my files were actually in evidence and I thought that was strange. I said that both in the Kleiman case and the McCormack case.</p>	<p>Dr Wright blaming third parties, his previous solicitors (Ontier), regarding the disclosure exercise carried out in these proceedings.</p>
<p>{Day5/32:2} {Day5/32:15}</p>	<p>- Q. Did it not occur to you in the years between 2019 and mid - 2023, that there was some distinctive material, dozens of documents representing precursor work to the Bitcoin White Paper, which you would have saved and hadn't been disclosed?</p> <p>A. Yes, and it was only in October that I discovered, talking to KLD, after we gave these drives in, that LaTeX files weren't in the search and they were coming up as system files. I went back to Shoosmiths and said, "Where the hell are all the LaTeX files that I know are on this drive", because nothing was in the disclosure platform, and KLD had to change the</p>	<p>Dr Wright blaming third parties, his current solicitors (Shoosmiths), and KLD, for apparently failing to disclose the LaTeX files properly.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	search so that the LaTeX files were no longer seen as system files.	
<p>{Day5/32:19} {Day5/33:4}</p>	<p>- A. No, the QNAP server was taken. The QNAP server was half a petabyte worth of data storage, so that's not a normal home server. I had a number of racks downstairs, part of my basement was set up as a small data centre, and I had computers that were in there. The promise from AlixPartners was that they could not do an image at my home because imaging 500 terabytes was outside of their capability. They said they would take it away and that I would get it back. It is now several years later and that several hundred thousand pound equipment is still unused and sitting in a basement somewhere.</p>	<p>Dr Wright is evasive - he has spent millions on the litigation and yet never invested in getting this server imaged.</p>
<p>{Day5/33:5} {Day5/33:25}</p>	<p>- Q. When you were nominating your original primary reliance documents in this case, did it not occur to you to say, "There's a whole series of other documents which will be on a hard drive at my home which can be nominated, which can be looked at"?</p> <p>A. My understanding was that that drive had been imaged, and I'm not proud of myself, but I had a yelling and screaming match with my solicitors multiple times saying, "Where the hell are my files", and they kept telling me, "They must be in Relativity, you just need to learn how to use it better". So ...</p> <p>Q. So it's another failure by Ontier, was it?</p> <p>A. No, it's probably more a failure by me. I've only recently spent a lot of time learning how to use Relativity properly. I - I'm sorry, my Lord, but the only word is I was a complete arse and I treated some of the paralegals terribly, going, "You must find this", when I should have put it on myself to do it. And no I'm not blaming them, I'm blaming myself. I was an arse at the beginning and, rather than do it myself, I expected people to do it for me.</p>	<p>Dr Wright appearing to admit his partial fault for documents not being in evidence.</p>
<p>{Day5/36:1} {Day5/36:17}</p>	<p>- Q. Then you say: "For the MyDigital Drive, I simply connected it to power up." Yes?</p> <p>A. That's correct as well.</p> <p>Q. You say, you: "... did not access the BDO Drive on the Samsung Drive or any files on either Hard Drive ..."</p> <p>A. No, but I didn't disconnect them right away either.</p> <p>Q. When did you disconnect them, Dr Wright?</p> <p>A. I don't actually recall. I'd left them connected as I went to do other things.</p> <p>Q. Did you leave them open with the encryption down during that period?</p>	<p>Dr Wright provides a new explanation regarding what he did after "discovering" the new hard drives and plugging them into his laptop.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Probably not. I don't think I actually actively logged out. At that period, I had other meetings I had to get to, so I checked and left.</p>	
<p>{Day5/36:18} {Day5/37:7}</p>	<p>- Q. For somebody very concerned with IT security, it seems like a fairly basic failure in the chain of custody that you didn't unplug them, having ensured that you were only looking at them strictly to check that they were working?</p> <p>A. I agree. In this case, I did fail. I should have done that. My presumption was that my laptop was secure. I mean, I use two – factor authentication, etc, and it was my belief that no one had access to my laptop, my own hubris, I guess.</p> <p>Q. You didn't say anything in your witness statement about leaving the drives plugged in, did you?</p> <p>A. No, I hadn't really thought about it.</p>	<p>Dr Wright is evasive when asked why he didn't address the failure to unplug the drives in his witness statement.</p>
<p>{Day5/37:9} {Day5/37:24}</p>	<p>- Q. As we have seen, you say that AlixPartners would have had access to the USB drives, but you speculate on reasons why they didn't image the BDO image; correct?</p> <p>A. Yes.</p> <p>Q. You're aware that AlixPartners themselves have told your solicitors that they had no knowledge or awareness of the Samsung or MyDigital Drives when they did their work in 2019?</p> <p>A. Yes, I'm aware that they said lots of things, including that they failed on the QNAP server, and they've changed their story multiple times.</p> <p>Q. So you are saying that they are telling a falsehood, if I can put it in that way, when they say that they had no knowledge or awareness of these two hard drives?</p> <p>A. Yes, because the serial numbers are actually listed in their list.</p>	<p>Dr Wright blames a third party, AlixPartners, who he appears to claim have changed their story regarding what access they had to the drives (or otherwise) in 2019.</p>
<p>{P1/18/15} - Eighteenth Witness Statement of Phillip Nathan Sherrell</p>		
<p>{Day5/40:10} {Day5/40:22}</p>	<p>- A. Of the five drives, some of them have been imaged because they're basically damaged. Those ones are correct. Like, where AlixPartners have said, "These click and don't do anything", that is correct, and they do, so there's nothing to put forward. And other ones have been imaged in the way that they're saying. The two there have been imaged in a way that wasn't correct.</p>	<p>Dr Wright is evasive regarding the number of drives that he found, and how he then presented that information in his witness statement.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. This suggests that you were putting forward to your team more than two drives, whereas your witness statement was that you'd found two relevant drives; correct?</p> <p>A. No, I found two drives that had no information that has been captured --</p>	
<p>{Day5/41:17} - {Day5/42:8}</p>	<p>Q. But if some had been moved around, you think, because of your son moving things, why did you say in your witness statement that the lack of a sticker told you pretty clearly that the image hadn't - - that the disk hadn't - - drive hadn't been imaged by AlixPartners?</p> <p>A. I didn't say it hadn't been imaged, I said it hadn't been imaged correctly. So what I'm referring to is the sticker associated - - well, the serial number associated with the Samsung Drive relates to a very small partition. It's only in megabytes. Now, that would match with the external partition, so my thought was, you haven't unencrypted this. Now, what I did do was I matched, with my wife, all of the serial numbers in that drive. Even the ones that had been imaged, I validated that they had been imaged and where the information was in the disclosure platform or not. If they had been imaged correctly, then I just put them back and ignored them.</p> <p>Q. Dr Wright, digression aside, this is another contradiction of one of your witness statements, isn't it?</p> <p>A. No, it is not.</p>	<p>Dr Wright contradicts the account given in his Fifth Witness Statement regarding whether the disk had been imaged by AlixPartners.</p>
<p>{Day5/42:20} - {Day5/45:9}</p>	<p>Q. You told us yesterday, in relation to the screenshots at ID_004077, 78 and 79, a number of documents I showed you the screen --</p> <p>A. Yes.</p> <p>Q. - - that you'd given Ontier access to the MYOB accounting software, the log - in details and so on, in late 2019, didn't you?</p> <p>A. Yes, that's correct.</p> <p>Q. And you insisted that they definitely took the screenshots at 4077, 78 and 79 before 9 March 2020, which was the date I put to you?</p> <p>A. My understanding was that they did, yes.</p> <p>Q. Dr Wright, I'm going to put to you a letter which your solicitors, Shoosmiths, have sent to us this morning. Paragraph 2 -- well, I'll read the whole thing. Paragraph 1: "We refer to your letter dated 8 February 2024 to Ontier where you requested information regarding ID_004077, 4076 to 4079 and when the screenshots within those were specifically made." [As read] Paragraph 2: "Ontier has written to us and provided us with the requested information. With the permission of Mr Justice Mellor, we have sought out our client's instructions. Our instructions are to disclose the information Ontier has</p>	<p>Dr Wright not accepting the obvious truth regarding the date that the screenshots at {ID_004077} - {ID_004079} were taken. This has later been disproven by the disclosure provided by Ontier and analysis conducted for the Sixth Expert Report of Mr Madden</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>provided to us. Ontier LLP has stated as follows. "Dr Wright first provided this firm with log - in details for the MYOB accounting software on 9 March 2020 and we first accessed the software on that date. We did not have access to MYOB in late 2019." [As read] And then they make a reference to Bird & Bird's letter: "We created a series of screenshots from that system on 9 and 10 March 2020, including screenshots that correlate with the screenshots which appear at doc IDs 4076, 4077, 4078 and 4079." [As read] And then they say that they've copied the letter to his Lordship's clerk. It's right, isn't it, that, as Ontier say, they were not provided with log - in details in late 2019, as you said yesterday?</p> <p>A. No, and I'm going to be instructing them to release information that is already in the disclosure platform, including 2019 emails to AlixPartners and Ontier, giving those access details. So, no, those emails are already in disclosure.</p> <p>Q. And it's correct, isn't it, that they took the screenshots on 9 and 10 March 2020?</p> <p>A. I wasn't involved with them taking the screenshots. What I do know is that they received the log - in details in 2019.</p> <p>Q. You were very firm yesterday that those screenshots were not taken as late as 9 March 2020, weren't you?</p> <p>A. I know what I was told by my solicitors at the time, and I also know, and I have the emails in disclosure stating that they had access from 2019.</p> <p>Q. So you're saying that you understood from your solicitors that those screenshots had been taken before 9 March 2020?</p> <p>A. That is correct.</p> <p>Q. On that basis, they were either lying to you then or lying to the court now; correct?</p> <p>A. I have no idea. I know most of the people at Ontier who were there are no longer there.</p>	
<p>{Day5/45:19} - {Day5/46:15}</p>	<p>Q. And you said that it was the IP address for nChain, yes?</p> <p>A. Yes.</p> <p>Q. According to an IP address look up facility, that IP address is identified as being located in Cobham; do you see that?</p> <p>A. I do.</p> <p>Q. That's your home area, isn't it?</p> <p>A. It is.</p> <p>Q. NChain's headquarters are in London, aren't they?</p> <p>A. That's - - well, actually they're in Switzerland, but there's an office in London.</p>	<p>Dr Wright is evasive when asked a straightforward question about where nChain's offices are.</p> <p>Dr Wright also fails to accept the obvious truth that the IP address identified is his personal IP address.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. To be clear about this, the parent company is based in Switzerland, but there's a London company with a registered office?</p> <p>A. Yes, there is.</p> <p>Q. So, Dr Wright, you were wrong, weren't you, to say that that IP address was associated with the company and not with you personally?</p> <p>A. No, there are VPNs. What I do know is that I have a BT fibre link and I have a range of IP addresses. I know what the range of IP addresses are. I don't know what the VPNs or anything else that I have might be.</p>	
BDO Drive - Expert analysis		
<p>{Day5/47:12} - {Day5/47:20}</p>	<p>Q. Page 18, please {I/5/18}, paragraph 70, Mr Lynch established that the last time of use of the computer from which the image was taken was 5 July 2007. Do you agree with that finding?</p> <p>A. No, I don't. That was the last time that it was booted as a PC. As I noted, it was converted later into a VMware image. The way that you would run a VMware image when you're doing a capture is that you snapshot it and the snapshots update, but the base image doesn't.</p>	<p>Dr Wright contradicts his own expert, Mr Lynch.</p>
<p>{Day5/50:2} - {Day5/50:13}</p>	<p>Q. You didn't specify it in any of your witness statements - - or in your witness statement when you were describing the initial discovery of the BDO Drive, did you?</p> <p>A. I believe I did. Unfortunately, I didn't think I needed to be clear on the terminology. When I stated that I captured it, that doesn't reference cloning it. I mean, I'm sometimes not clear but, I guess it's a theory of mind issue with being an Aspie, I assume you understand terms I do. I've written textbooks on this topic. So when I say "clone", I mean one thing, when I say "captured", I mean another. I'm pedantic on these sort of terms.</p>	<p>Dr Wright resorts to pedantry in order to avoid inference that he didn't provide full information when describing the initial discovery of the BDO Drive.</p>
<p>{Day5/52:13} - {Day5/53:9}</p>	<p>Q. You're aware, aren't you, Dr Wright, that your witness statement describing your computer environment - - both your witness statements describing your computer environment to explain away these findings have been considered by both parties' experts? You're aware of that, aren't you?</p> <p>A. Yes, and neither of the experts are trained in virtual machines.</p> <p>Q. And each of the experts agrees, you're aware, that the computer environment you describe at great length in those statements does not affect their conclusions, including this</p>	<p>Dr Wright disagreeing with experts' findings regarding the importance of his "computer environment" to their various findings.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>conclusion on which they agree. You're aware of that, aren't you?</p> <p>A. Yes, and they said that there's no evidence of Citrix being used. That is despite the fact that there is a BDO Citrix profile in the image. If you actually go into the image, you'll find a Citrix ICA profile that is a BDO one with the BDO SSIDs that can only be created from the domain at BDO. That image contains that information, demonstrating that what they've just said ignores files that are actually on that device that couldn't be created by me.</p>	
<p>{Day5/53:11} {Day5/53:24}</p>	<p>- Paragraph 76(b), Mr Lynch concludes that: 63 "After the BDO Image was mounted and the transaction logs created, the clock on the computer ... was backdated such that the clock reflected a date of 19 or 31 October 2007." As shown in those transaction logs and as he correctly deduced; that's right, isn't it?</p> <p>A. No, actually, it's not. I've done this myself to check, and if you backdate the clock, it changes the modified time. So the simple sort of test would be to actually do this and log it. But if you actually run this test, you find that the modified time always updates after the other. There is no way that I've found of turning the clock back and doing this.</p>	<p>Dr Wright describes the process of backdating a clock, demonstrating apparent familiarity with the process.</p>
<p>{Day5/54:13} {Day5/55:3}</p>	<p>- "The clock was changed at least 2 other times." Mr Lynch finds, one of them: "... changed the clock from 31 October ... to 30 October ... and that change occurred while information was being recorded in a transaction log. As a result of that change, a transaction log that had been recorded as being created on [the 31st] was recorded as ... last modified on [the 30th] ..." Do you accept that finding?</p> <p>A. No, once again, if - - rather than relying on theoretical knowledge or something you get from a blog, you actually take an image yourself and you try this, you find that never happens. So, basically, all you need to do to validate what I'm saying is take an image, turn the clock back and look at the transaction logs, and when you do, you notice that this never occurs.</p>	<p>Dr Wright disagreeing with his own expert's findings regarding the manipulation of the computer clock.</p>
<p>BDO Drive {L20/223/184} - Stroz Friedberg Memo on BDO drive {I/5} First expert report of Spencer Lynch</p>		
<p>{Day5/55:23} {Day5/56:4}</p>	<p>- Q. And you had the opportunity, through your legal representatives, after that, to ensure that a proper expert was instructed and that that expert was given proper information about your systems; correct?</p>	<p>Dr Wright blaming third parties, his lawyers, for failing to instruct his chosen expert.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. No, actually, I don't believe so. The expert I wanted, I - - my first instructions were any expert needs to be SANS qualified.</p>	
<p>{Day5/56:19} - {Day5/57:9}</p>	<p>Q. No, but this was after the PTR, when the experts were brought in to look at the BDO Drive. At that stage, everyone had to race around and find appropriate experts and get those experts instructed. You had the opportunity, at that time, to ensure that an expert was properly instructed and suitably qualified, didn't you?</p> <p>A. No, I said categorically that the person who did the Citrix tests for me was an expert and I wanted them used. I also said that I don't think Stroz should be used because they have a conflict of interest. Over 30% of their revenue, at the time, was gained through members of COPA. I got told Chinese walls will be in place. My comment on that is I don't believe Chinese walls ever work. So, Meta, who was a member of COPA until - -</p>	<p>Dr Wright blaming third parties, his lawyers, for failing to instruct his chosen expert. Dr Wright accusing his expert of a conflict of interest, and revealing privileged information.</p>
<p>{G/6} Fourth Expert Report of Patrick Madden (BDO Drive)</p>		
<p>{Day5/60:19} - {Day5/61:19}</p>	<p>Q. And you're aware, aren't you, that he found that the identifier linked with the 71 new reliance documents which had been found to have been copied when the clock was setback, the security identifiers for those documents had a number ending in 1002? You're aware of that?</p> <p>A. No, the clock wasn't set back. What I will note is, the SSIDs changed, because it was, one, on a new computer where it was on a virtual machine, and, two, BDO Kendalls merged. So in the intervening period where I'm doing this, BDO merged to form a global firm. Each of the BDOs were separate in Australia at this point. The Melbourne office took over to be the head IT area and new credentials were given. So we moved from a BDO New South Wales domain into a BDO Australia domain. That basically changed all these SSIDs.</p> <p>Q. We'll come back to the SSID in a moment. But you're saying then that these 71 documents were documents which you added in to the drive between July and October 2007; have I got you right?</p> <p>A. I can't look at every single document you're looking at at the moment, but, yes, during the period between July and October, I copied from my external drive, that is currently on the drive as an external link, but not linked because it's not a full machine any more, into the drives so that I would have files.</p>	<p>Dr Wright accepting that it was him that copied the files to the drive (albeit he says this was done in 2007)</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day5/63:1} {Day5/63:16}</p>	<p>Q. That S -- that SID number, 1002, I think we can agree, was different from the user profile assigned to you while you were an employee at BDO?</p> <p>A. Yes.</p> <p>Q. So it is at least consistent, would you accept this 77 much, with the story of these documents being added much later?</p> <p>A. No, it's not. It's consistent with a new computer. In the new computer, I would have both admin and Craig Wright local admin and the admin will have a different SSID, as it says on here, and the Craig will have a different SSID. So when I put the drive as an image and mounted it using Mount Image Pro on the new computer, I don't have the same SSID for my local computer, so copying back and forwards will now have a different one; it must do.</p>	<p>Dr Wright admitting that the SID number was from a different user profile assigned to him whilst at BDO.</p>
<p>{Day5/65:20} {Day5/66:20}</p>	<p>Q. You're agreeing that it could have been modified. Do you say that there were such modifications between those dates?</p> <p>A. Unfortunately, I don't know. What I do know is that, based on your own witness statement from Sherrell and Mr Ager – Hanssen, Mr Ager – Hanssen published pictures of some of those files on that BDO Drive - - files he didn't have access - - well, clearly he did have access to, files he should not have had access to - - on a third party computer, running Linux, showing my browsing history, my communications with my lawyers, my personal communications with my wife, all sorts of things. He had an access to that drive, yes.</p> <p>Q. So you're saying that you think he got access to your drive and modified files on it?</p> <p>A. I actually don't know. The Samsung Drive was taken by KLD, so I haven't been able to do a proper analysis. I would like to. Because it's been taken, I can't do any further analysis. Now, what I do know is that Mr Ager – Hanssen posted extensively on Twitter, before taking down those Twitter posts, pictures of my browsing history on my current computer and pictures of file shares and the structure that he didn't have access to. We hadn't released that drive, it hadn't been given to my lawyers properly even, and yet Mr Ager – Hanssen was displaying it.</p> <p>Q. I'll come back to that later.</p>	<p>Dr Wright is evasive when confronted with Mr Madden's findings regarding the date range in which modifications to the BDO Drive were made {G/6/33}.</p> <p>Dr Wright later retreats to a rote part of his story, blaming third parties (Christen Ager – Hanssen, KLD) for modifications.</p>
<p>{Day5/66:22} {Day5/67:24}</p>	<p>Page 37, please {G/6/37}, paragraph 117. Mr Madden was able to recover two deleted image files from the Samsung Drive, image.raw and InfoDef09.raw, which he concluded were identical to each other apart from blank space and 99.98% identical to BDOPC.raw, the BDO raw image which you put forward in these proceedings; correct?</p> <p>A. The BDO raw image isn't InfoDef.raw, so they're different things. There is an encrypted and not unencrypted drive on</p>	<p>Dr Wright appearing to suggest that the BDO Drive is not the time capsule it was purported to be. Dr Wright then goes on to blame third parties, including KLD, for</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>there called InfoDef, but there is a deleted image of a file, yes, that has been added.</p> <p>Q. And he found that 17 of the -- this is page 41 {G/6/41}, paragraph 134 -- he found that 17 of the 97 new reliance documents existed on ID -- on InfoDef09.raw in slightly different versions. Were you aware of that?</p> <p>A. Not before Mr Madden pointed it out. As I said, the Samsung Drive was taken by KLD, so I haven't been able to do any analysis.</p> <p>Q. Does it surprise you to know that there is a deleted image file containing 17 of the 97 new reliance documents existing in slightly different versions?</p> <p>A. After the image that Sherrell has put in -- Mr Sherrell's put in the witness statement, no. I would have been highly shocked if Mr Ager-Hanssen hadn't told my wife and tried to sort of poison her against me and other people and using these images. Apart from that, now I'm not.</p>	<p>his not being able to analyse the drive with the deleted files contained therein.</p>
<p>{Day5/67:25} {Day5/68:11}</p>	<p>- Q. So you say that this finding of slightly different versions of 17 of the 97 new reliance documents existing in InfoDef09.raw is due to some sort of hack and manipulation orchestrated by Mr Ager-Hanssen?</p> <p>A. By someone working for Mr Ager - Hanssen. I don't believe that he would be able to do it himself. I also don't believe he'd be able to run a Linux laptop. I'm not trying to diss him that way, but he's not a Linux person and the laptop, in the screenshot he showed, running and accessing my files, was Linux. That's very clear from my explanations. You can look at that computer, it's a Linux computer.</p>	<p>Dr Wright blaming third parties (Christen Ager - Hanssen), for the presence of different versions of documents in the deleted files in InfoDef09.raw</p>
<p>{Day5/68:12} {Day5/68:17}</p>	<p>- Q. You're aware, aren't you -- you were just talking about what KLD had done with the Samsung Drive; you're aware that they returned it to your team some while ago, aren't you?</p> <p>A. No, I'm not. I don't actually know where it is. I know they imaged it and I know I haven't got it back.</p>	<p>Dr Wright maintaining a false narrative about how the Samsung Drive was supposedly manipulated by third parties (see above entry), despite it having been returned to him.</p>
<p>{Day5/68:18} {Day5/69:5}</p>	<p>- Q. {E/20/8}, please. Paragraph 25, you describe KLD capturing a physical forensic image of the hard drives, and then at the end, you say that: "KLD Discovery then returned the Hard Drives to me. They left my home and I believe returned to their London office with the captured forensic images. Shoosmiths has since taken custody of the Hard Drives and they remain in Shoosmiths' possession." Is that right?</p>	<p>Dr Wright is evasive about the treatment of the hard drives following KLD returning them.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Yes. I don't know whether it's with the lawyers or with KLD or ... I don't know where they actually are. I know Shoosmiths have signed for them.</p>	
<p>{Day5/69:12} - {Day5/70:1}</p>	<p>Q. These drives in the hands of your solicitors are not documents to which you have access?</p> <p>A. No, I don't.</p> <p>Q. Is that what you're saying?</p> <p>A. I'm saying I have handed them over and I'm not going to have them returned until after the trial. My solicitors don't want me to have access until after then -</p> <p>Q. No, no, no, you said you couldn't run tests on them for yourself because you didn't have access to them.</p> <p>A. I don't have access to them.</p> <p>Q. Well, let me put it to you that if you instructed your solicitors to provide those drives to you so that you could run tests on them, there would be nothing to prevent them complying with your instructions.</p> <p>A. That's not what I've been told.</p>	<p>Dr Wright appearing to share privileged information regarding whether he could have accessed the drives.</p>
<p>{Day5/70:10} - {Day5/71:2}</p>	<p>Q. Page 42 {G/6/42}, we see that the difference between the version on InfoDef.raw and BDOPC.raw is the difference between the words “the original Bitcoin White Paper” on InfoDef and “the proposed Timecoin system” on BDOPC.raw?</p> <p>A. I do.</p> <p>Q. And would you accept that that is consistent with you editing the document to suggest that you’re speaking about a prospective Timecoin system rather than an existing Bitcoin system?</p> <p>A. No. The image that has been left there was something that I’d say Mr Ager - Hanssen or one of his people were involved with. Unfortunately - and I’ll say this again - my own hubris. I get in trouble for this all the time; I believe that I know how to secure a system, so therefore I forget about insiders. From external attack, I’m good, but I keep getting compromised by insiders, because I trust people.</p>	<p>Dr Wright blaming third parties (Christen Ager - Hanssen) for the presence of a manipulated document “the proposed Timecoin system” on BDOPC.raw.</p>
<p>{Day5/71:3} - {Day5/71:14}</p>	<p>Q. So on your account, the findings which show forgery of this drive based upon the transaction logs, the SIDs and the ObjIDs are all findings made by experts who don't know what they're doing; correct?</p> <p>A. They're not qualified. They're not specialised in VMware, they're not specialised in Citrix. Generally speaking, it's not that you can run an imaging and cloning tool that makes you an expert, it's expertise in the area. So you would have expertise in, like, VMware, if you're going to talk about that.</p>	<p>Dr Wright questioning the qualifications of both parties’ experts.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>If you're going to talk about persistence in Citrix, I'd expect at least an introductory Citrix qualification.</p>	
<p>{Day5/72:9} {Day5/72:24}</p>	<p>-</p> <p>Q. So Dr Wright, there are some findings of forgery which you say are due to expert incompetence, and entirely separate findings of forgery which you say are due to an unauthorised hack?</p> <p>A. I'm saying that the experts have not checked a simple validation. They haven't done an experiment, which I would expect from an expert.</p> <p>Q. And you say that the unauthorised hack was possible because you, the great IT security expert, left this drive plugged in, you say, you now accept, very unwisely?</p> <p>A. I do. In part. I presumed that my computer was safe because I had two factor. What I didn't expect was that 22 the group policy update that was pushed from nChain would also contain a back door. I assumed that Christen wasn't working against the organisation.</p>	<p>Dr Wright blaming third parties (Christen Ager - Hanssen) who he says hacked him. Dr Wright also criticises both experts for lack of competence for failing to perform certain tests.</p>
<p>{Day5/74:21} {Day5/75:12}</p>	<p>-</p> <p>Q. You describe those events in one of your statements as taking place in late September 2023. When do you say it first occurred to you that these - - that the BDO Drive might have been manipulated by Mr Ager - Hanssen?</p> <p>A. Not as early as it should have been. Again, my own hubris. I actually saw that he had images and I tried to excuse it away. I went to my solicitors, Travers Smith, and I said, "There's no way he could access my machine, I have no - - I don't know how he's got these images, but they can't be from my computer". I made excuses. I was actually incredibly stupid. I refused to believe that anyone could break into my computer, even someone who was an insider. I sat there telling everyone that, "No way, no one will ever break into my computer, no way he's done this", and it took me a while to actually accept that, well, he's got images of my computer and he must have.</p>	<p>Dr Wright blaming third parties (Christen Ager - Hanssen) for hacking his computer system.</p>
<p>{Day5/75:13-24}</p>	<p>Q. Can you put a date, or a rough time, when it first occurred to you that Mr Ager - Hanssen may have manipulated the content of the BDO Drive?</p> <p>A. I should have known around the 20 - something - - by 23 September, but I refused to believe it.</p> <p>Q. When did it actually occur to you?</p> <p>A. Probably not until December. Not when Stroz and things like that started giving me information back on the drive. It got to a point where my wife talked to me and said, "Something here, you have to start thinking about this", and then it actually started dawning to me that I'm a bit dumber at times than I think.</p>	<p>Dr Wright is evasive in describing when he became suspicious that Mr Ager - Hanssen had manipulated the BDO Drive. Dr Wright claims it wasn't until December, even though he asserts he is an expert in computer security.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{L2/49/1} 004695 - "The King2.rtf		
<p>{Day5/76:15} - {Day5/77:18}</p>	<p>Q. Let's look at some documents from the BDO Drive, {L2/49/1} {PTR-F/52/1}, please. ID_004695. If it's easier to use the ID, it's 004695. This is a file entitled "The King2.rtf" and it presents as an article on network security and Quorum systems, simplifying hugely, doesn't it, Dr Wright?</p> <p>A. No, it's an exam that I had in - - actually, it was held in Las Vegas, for some reason, but SANS were doing testing. I did one of my GSE, global security expert, exams and one of the examinations, they had as a King's WiFi exercise, where I had to breach and work out how to get into the WiFi. We were given a red team/blue team scenario and this was my paper done during that examination, which I subsequently passed.</p> <p>Q. You're aware, aren't you, that Mr Madden has found that this file was created with a version of Windows which was the May 2020 update?</p> <p>A. I've seen his notification of the versioning, yes.</p> <p>Q. Is that a finding you accept?</p> <p>A. I'm saying now it could be possible. It's actually feasible that people could have been on that drive.</p> <p>Q. Ah, so the fact that this was shown as created with a version of Windows which was the 2020 update is down to Mr Ager - Hanssen's hack?</p> <p>A. That's the only explanation I can give you. What I do know is he accessed that drive. I led myself to believe that he wouldn't be able to, and obviously, if there are files on a computer displayed on the internet that are mine, I have to accept it.</p>	<p>Dr Wright blaming third parties (Christen Ager-Hanssen) for hacking his drive and forging The King2.rtf document.</p>
{ID_004715} NG3.tex		
<p>{Day5/81:17} - {Day5/82:6}</p>	<p>Q. You could look at the documents, couldn't you?</p> <p>A. Yes.</p> <p>Q. So, looking at the documents, you didn't notice anything wrong with any of them?</p> <p>A. No, I didn't.</p> <p>Q. Back to {L1/175/1} {PTR-F/72/1}, which is the document. Now, Mr Madden made a finding that there was a previous version of this document on InfoDef09.raw which showed various changes. You're aware of that, aren't you?</p>	<p>Dr Wright disagreeing with both experts as to the order in which InfoDef09.raw and the BDO image were created.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Again, I would say it's the other way round. I would say that there is a changed version of this document on InfoDef09.raw. If you actually look at it - - and if I had the drive, I'd analyse it properly - - I think you'll find that InfoDef09.raw is copied after the BDO Drive.</p>	
<p>{Day5/82:20} {Day5/84:17}</p>	<p>-</p> <p>Q. So what I suggest to you is that these are very clear indications of a document which refers to Bitcoin as an existing system being modified to look like something looking at a Hashcoin system to support your case.</p> <p>A. No, I'd actually say it's the other way round. What it is is someone trying to ensure that there is manipulated evidence on these drives because of my own hubris not believing it. Even having, on an external drive, a 2008 copy of a file would support my claim. So, your argument on being a deleted version, etc, if that hadn't been manipulated more, that would be supportive itself. Now, the BDO Drive would be updated the other way, effectively, which could be easily checked, and the problem is neither expert has actually checked this, they've made a presumption without validation.</p> <p>Q. So you say that Mr Ager - Hanssen - - we'll come back to what the experts did in a moment, but you say that Mr Ager - Hanssen and his team of hackers, whoever they were, manipulated documents in order to seed them onto InfoDef09.raw with the hope that COPA and the developers would gain access to the drive, find them and finger you as a forger, yes?</p> <p>A. I think --</p> <p>Q. That's your hypothesis?</p> <p>A. No, actually, it isn't a hypothesis. One of the things I disclosed to my lawyers was, some of the files that I'd given to Christen Ager - Hanssen, including PDF files, had a web cookie, my Lord. A web cookie calls a web server or IP address when logged. I have a web server running that these files log from. I can't say how, but they recorded, in 2016 - - sorry, September last year, Bird & Bird's IP address. I notified both Travers Smith and other solicitors of this.</p> <p>Q. I'm sorry, what are you suggesting this indicates, Dr Wright?</p> <p>A. I don't actually know, because they've got an open WiFi, so it can't say that it's them. Someone could have stood outside their office, Mr Ager - Hanssen could likely have actually done that to try and implicate them some way. What I do know is Mr Ager - Hanssen is playing a game that I don't understand.</p> <p>Q. I'm going to put to you, first of all, Dr Wright, that Bird & Bird don't have an open WiFi, do they? I'm putting that on pretty clear instructions.</p>	<p>Dr Wright blaming third parties (Bird & Bird, Travers Smith, Ager - Hanssen) for conspiring to compromise the BDO Drive.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. I haven't checked their WiFi.</p> <p>Q. And this is yet another, and may I suggest somewhat scandalous, embellishment to your tale.</p> <p>A. No, it's not. It actually happened, and I did report it.</p>	
<p>{L1/183} - ID_004719 - LaTeX Timecoin fragment</p>		
<p>{Day5/86:3} {Day5/86:9}</p>	<p>- Q. And that's a clear sign that you forged this document, isn't it?</p> <p>A. No, actually, it's not. Even if there was an alternative document with that information, that wouldn't show any forgery, or anything like this. None of that demonstrates what you're saying. What it does say is that someone was trying to access my drive.</p>	<p>Dr Wright blaming third parties, saying that "someone" tried to access his drive.</p>
<p>{Day5/88:19} {Day5/88:22}</p>	<p>- Q. But Dr Wright, it's odd, isn't it, when you're writing an academic piece, to give a reference to a paper but then not include the date, or a citation and put a question mark? That's unusual, isn't it?</p> <p>A. No, actually, generally, now, because I use APA more than anything else, at 7, I do "N.D" for "no date", but when writing, until I've actually figured out what the date is, I will put something in there.</p>	<p>Dr Wright is evasive regarding the acronyms used on a document and his writing style.</p>
<p>{Day5/89:2} {Day5/89:15}</p>	<p>- Q. Dr Wright, it isn't the case, is it, that Mr Ager - Hanssen got strikingly lucky here, this is another sign of forgery by you, isn't it?</p> <p>A. No, he didn't get lucky. It turns out that he'd been actually monitoring my computer for months, including all of my emails, all of my communications, all of my WhatsApp. He had basically been screenshotting everything, he had videoed everything, he had recorded everything I'd said in the room, he had all of my communications. So, being that he had every single email I sent, every WhatsApp I've sent, including to my wife, everything I've talked to my family about, all my communications, I don't think he was lucky at all, I think he just had too much information}</p>	<p>Dr Wright blaming third parties (Christen Ager - Hanssen) for forging documents and seeking to frame him.</p>
<p>{Day5/90:14} {Day5/91:9}</p>	<p>- A. No, it is not. ChatGPT just takes what existing people do, it doesn't make up anything new. I mean, honestly, the concept that AI is anything other than "Actual Ignorance", and that it doesn't take what people blog and things like that and create things is insane, I'm sorry. ChatGPT creates nothing. What it does is it takes what existing people do, everywhere on the internet, and it makes it common'</p>	<p>Dr Wright blaming ChatGPT for characteristics in Dr Wright's work which are similar, saying that ChatGPT replicates work like</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. But it has characteristic indicia which appear in a ChatGPT paper for different referencing and referencing formats, doesn't it?</p> <p>A. No, actually, the way that it does is continuous replication. So, if you were looking at this paper, what you would actually have to be doing is looking at the text. The indicia that you put there are standard, sort of, ways of doing all of this that have existed for the last 20 years. Because they're on blogs, because they're on standard forums, ChatGPT takes these things and replicates them. So people like me, who actually write things, end up having their work in ChatGPT because it steals.</p>	<p>his (rather than the other way around).</p>
<p>{H/278} Appendix PM46 to Fourth Expert Report of Patrick Madden</p>		
<p>{Day5/91:16} - {Day5/91:25} {PTR-F/80} ID_004723 (BDO) and LP1.tex (Idf09)</p>	<p>Q. {H/278/41}, please. In his 46th appendix, Mr Madden found a version of this in InfoDef09.raw. Do you recall that finding?</p> <p>A. I do.</p> <p>Q. And do you see that he found that there had been modifications to remove references which postdated 2006, hadn't there?</p> <p>A. No, I'd say that they've been added afterwards. So, what we have, once again, is Mr Ager - Hanssen, or whoever's working for him, trying to plant things.</p>	<p>Dr Wright blaming third parties (Christen Ager Hanssen) for planting material on InfoDef09.raw</p>
<p>{H/278 Appendix PM46 to Fourth Expert Report of Patrick Madden</p>		
<p>{Day5/94:18} - {Day5/95:8} {L1/377/1} ID_004729 {PTR-F/86/1}</p>	<p>Q. And that is another indication, isn't it, that we have a document which was produced in very recent years, much later than 2007?</p> <p>A. No, it's actually an indication that the original file, which is a BMP, was updated to create the others. The pixelation on this basically is - - well, more pixelated than you would get in a TIFF file, so what we have is a BMP being converted to a TIFF.</p> <p>Q. And I suggest to you, on the basis of that finding that I've just summarised, that this is another document forged by you?</p> <p>A. Again, what I would say is someone has updated this and converted it into a TIFF.</p> <p>Q. This is, as the file name suggests, the BMP file, isn't it, Dr Wright, that we're looking at on screen?</p> <p>A. That's correct.</p>	<p>Dr Wright provides an obviously false explanation, claiming the document is converted to TIFF, when in fact it is a BMP file being looked at.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{ID_004732} (Q.txt) and {ID_004734} (ITI581b.rtf) and {ID_004721} - “Secure and Trustworthy Voting in Distributed Networks: A Quorum - Based Approach with Hash Chains and Public Key Infrastructure”</p>		
<p>{Day5/96:6-17}</p>	<p>{H/278/45}, please. This is PM46 where Mr Madden addresses these documents together. Do you see, at the next page {H/278/46}, in paragraph 134, he finds that ID_004374, the second of those, the second of the documents, can't be authentic to 2007 because it was created with a 2020 version of Windows Rich Text editor; do you see that?</p> <p>A. I do.</p> <p>Q. And is that a finding you account for on the basis of the hack, the supposed hack?</p> <p>A. Well, the only reason I can find the ID drive existing would be that.</p>	<p>Dr Wright blaming third parties (hacking) for the existence of the ID drive with anachronistic documents.</p>
<p>{Day5/98:15} - {Day5/98:22}</p>	<p>Q. What's present here is a full contents table in the InfoDef09.raw version; correct?</p> <p>A. Yes, and what you'll notice is none of the headers are in the other document. So, that would make an incredibly difficult effort of going through and changing all of the header information so that it matches LaTeX. It would probably be about as easy to write the document from scratch.</p>	<p>Dr Wright maintaining that the documents being examined were written in LaTeX, despite multiple indications that they weren't.</p>
<p>{Day5/100:19} - {Day5/101:23}</p>	<p>Q. {H/278/52}, please. Do you see here where he found the metadata anomalies between the two documents?</p> <p>A. I do.</p> <p>Q. And page 53 {H/278/53}, at the top, do we see that the edit which had taken place on this occasion had been to remove the "Data Protection Act 2018" and replace it with "data protection law globally ..."? Do you see that?</p> <p>A. No, Sarbanes-Oxley is American. It actually says, especially SOX. I see the word "globally", but it's ...</p> <p>Q. I wasn't suggesting that Sarbanes-Oxley was UK. I was saying the edit has been to remove "Data Protection Act 2018" and replace it with "data protection law globally ..." --</p> <p>A. And especially SOX.</p> <p>Q. Yes. So we see here a reference to two pieces of UK legislation, the Data Protection Act 2008 and the Companies Act 2006 and the first of those has been changed to "data protection law globally ...", hasn't it?</p> <p>A. It has.</p>	<p>Dr Wright not accepting an obvious truth about editing the document {ID_004733} to remove anachronistic references to the UK DPA 2018.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. And that shows, doesn't it, the direction of the edit to remove the Data Protection Act 2018 and replace it with something that wasn't anachronistic?</p> <p>A. No, it shows that someone has done the other, then left a marker to change. So, basically, when you're taking that, someone's probably done it in Word and then converted it back to DOC.</p>	
<p>{Day5/102:3} {Day5/102:20}</p>	<p>Q. You're accounting for that presumably on the basis of the mythical hack?</p> <p>A. It's not mythical. Being that Mr Sherrell has actually posted it and put it into evidence, your side has actually demonstrated that that hack did occur.</p> <p>Q. Dr Wright, no. Our side has put into evidence some photographs of your screen which were taken by Mr Ager - Hanssen and tweeted; correct?</p> <p>A. No, actually, they're not my screen. That is a Linux computer running in a separate office. They have nothing to do with my screen whatsoever. You'll also notice that they are my files in other machines, so it is not my browsing, but someone monitoring my browsing, someone monitoring my files. If you actually examined that image, it's not my computer, it is remotely accessing my computer. So it is a picture of a Linux computer accessing my computer that Mr Ager - Hanssen has held up to say is his.</p>	<p>Dr Wright not accepting the obvious truth, insisting that Ager - Hanssen's screenshots are evidence of hacking, then insisting that the images didn't show his screen.</p>
<p>G/5 Third Expert Report of Patrick Madden</p>		
<p>{Day5/103:18} {Day5/103:25}</p> <p>{L1/252/1} ID_004736 {PTR-F/93/1}</p>	<p>Q. And his conclusions were, paragraph 53, on the next page {G/5/23}, that those highly unusual timings indicated tampering. Would you accept that deduction?</p> <p>A. Not at all. Again, using Xcopy produces these results. So, files that I would have had at BDO, I still was accessing in 2008. So, when copying from different drives, Xcopy has a different result for modify and creation.</p>	<p>Dr Wright implausibly blaming document anomalies on Xcopy.</p>
<p>{Day5/105:6} {Day5/105:25}</p> <p>{L1/367/1} ID_004682 {PTR-F/39/1}</p>	<p>Q. Let's go to it. {G/5/37}, paragraph 92(b) is 142 referring to this document. He says it is the only Lynn Wright document among these files: "... and like other 'Lynn Wright' documents it has been created with MS Word version 11.9999. It has a Revision Number of 2 and a Total Edit Time of 1 minute ... Internal Metadata stamps dating it to 16 June 2007 ..." Then paragraph 93(b), that version of Word wasn't released until September 2007, that service pack, and that of course contradicts the internal timestamps, doesn't it?</p>	<p>Dr Wright claiming, implausibly and without any evidential support, to have secret early access to Microsoft code releases.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Not necessarily, actually. At that time, I was on the Microsoft developer network and had early access to all of the code. That not only included the Microsoft operating system, but Word, etc. So, that's one possible explanation. But I don't actually know what I was running at that time. I would have to actually analyse it.</p> <p>Q. Has invention run dry, Dr Wright?</p>	
<p>{Day5/106:18} - {Day5/107:1}</p> <p>{L1/236/1} ID_004687 {PTR- F/44/1}</p>	<p>Q. The releases of those packages, selnolig and xurl, postdate the face dating of this file, don't they?</p> <p>A. I agree.</p> <p>Q. And so this file is a later forgery, isn't it?</p> <p>A. No, it's not a forgery, but someone has accessed it, that's correct.</p> <p>Q. So someone's accessed it in order to add in those apparently anachronistic details, have they?</p> <p>A. That would be something to do, yes.</p>	<p>Dr Wright admitting post-dated elements within the file.</p>
<p>{Day5/107:15} - {Day5/108:19}</p>	<p>Q. Would you accept that that also dates this document to much later than 2006?</p> <p>A. No, because that's a standard comment. But if you go down to the bottom of the page again, "pdfcreator ... LaTeX via pandoc", that isn't a Pandoc marker. When using Pandoc, it doesn't add that. This is a manually added comment. So the PDF creator has been updated not by a program, but by a person. There is no Pandoc version and no LaTeX compiler version that I know of in existence, including my tech, including Overleaf, including any of the main programs and any version of Pandoc that adds that statement.</p> <p>Q. Well, Professor MacFarlane, who knows a little about Pandoc, has considered the source commits to determine the date of the template for this document and he dates this to a template current between March and October 2022. Do you disagree with that evidence from him?</p> <p>A. I do. And I also note that he hasn't looked at the PDF creator label. The PDF creator label is manually added. It's not added by Pandoc. And I would love to see him explain which version. I've managed to copy every single version now of Pandoc and check every one of them.</p> <p>Q. So now you understand Pandoc better than its creator?</p> <p>A. I'm quite happy for him to demonstrate which version -- and I have downloaded every one of the versions and also loaded them into the Wayback Machine - - actually puts that tag in there. That tag does not come into Pandoc. Pandoc comes as Pandoc version number.</p>	<p>Dr Wright claiming greater expertise in Pandoc that the creator of Pandoc regarding whether and how tags are added.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day5/110:10} - {Day5/111:19}</p>	<p>Q. -- whether you're able to say which documents you were cross - examined on?</p> <p>A. During this, I was given a folder. That folder had 50 documents that they were going through, saying that there were allegations of fraud and that I was going to lose, and they pressured Stefan Matthews, saying that he would be up for perjury if he didn't drop his evidence in the trial, and that document had the same 50 documents that later came from Mr Madden. The same.</p> <p>Q. So, do you say that Zafar Ali was in on this plan to drop false documents upon you and ensure that they were somehow used against you in the trial?</p> <p>A. I have no idea what anyone's involvement is. What I know is a - - I was forced to spend a day being abused, is the only way to put it, in a mock trial, where I was told by people that if I didn't play ball, they were going to destroy me, where they spent the whole time going - - which I found out they were recording so that they were saying, "If you don't say you're not Satoshi, we're going to make sure that you get no more funds and everything happens in nChain that goes against you", and they said that they'll force Stefan to drop out as a witness, or they'll have perjury charges. They spoke to my ex - wife and abused her, and they went to some of the other people in this trial and tried to get them to drop out.</p>	<p>Dr Wright providing an implausible explanation regarding the circumstances of the mock trial.</p>
<p>{Day5/111:15} - {Day5/112:15}</p>	<p>Q. You think Ted Loveday was involved in pressuring witnesses?</p> <p>A. I don't actually know what he was doing. He was in the trial, which was a mock, fake trial, and -- I'm studying a PhD in law, my Lord, at the moment --</p> <p>Q. Just let's stick to the facts rather than your academic endeavours --</p> <p>A. What I'm saying is, I know it was highly illegal and I got sat down there and told I couldn't leave and locked in a room.</p> <p>Q. Who, other than Mr Ager - Hanssen, was part of the "they" who were pressurising these witnesses?</p> <p>A. I don't actually know. He had other people working for him. He has some really tall guy, I don't know his name, that is supposedly ex - CIA. He has some other guy that he says is Mossad. I don't know if they are or not. And he has a whole lot of other silly people like that, that pretend. He has a whole lot of people that -- Stefan Matthews would know because nChain recorded them all -- that were working for Christen's company that broke in or tried to break into the computer room at nChain, brought the -- Ajay, main person, into tears, threatened them violently, leading to, first, injunctions, which</p>	<p>Dr Wright blaming third parties (Ted Loveday, Christen Ager - Hanssen, the "really tall guy" who is supposedly ex - CIA, and the "other guy" who says he is from Mossad), for the mock trial.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	have been taken, then Christen fleeing the country and now criminal charges pending.	
Back to Reliance Documents		
<p>{Day5/114:12} - {Day5/119:16}</p> <p>{L1/168/1}</p> <p>ID_004712 {PTR-F/69/1}</p>	<p>Q. Page 2, second line down, please {PTR-F/69/2}. Do we see, the second line down has a line of code: "std::this_thread::sleep_for (std::chrono::milliseconds(latency)) ..." Do you see that?</p> <p>A. I do.</p> <p>Q. Now, you're aware that Mr Hinnant, the lead designer and author of the Chrono time utility, has given evidence that it was first standardised for C++ in 2011, yes?</p> <p>A. Yes, and I stated that this was using Project Chrono. Project Chrono first was developed in 1996.</p> <p>Q. He's also - - we'll come back to that in a moment. Mr Hinnant has also explained that "sleep_for" was also standardised for C++ in 2011. Are you aware of that evidence?</p> <p>A. Yes, but I also note that Integrys, the company that I had, the function was producing standardised libraries, so sleep was not an unusual area in C code, and because I was producing code both for simulations and in addition for gaming, what Integrys does, if you look at the Wayback Machine in 2009, it produces standard libraries, statistical libraries, crypto libraries and others.</p> <p>Q. Dr Wright, you're aware that Mr Hinnant's evidence is that looking at this code, it couldn't have appeared in a file actually dating from October 2007. You're aware of that evidence, aren't you?</p> <p>A. Yes, he's made a presumption that the only version that could exist is his. He has overlooked the way that I've said I used Project Chrono and he assumed that no one would actually make standard libraries outside of him.</p> <p>Q. So you know about - - you know more about Pandoc than the creator of Pandoc and more about Chrono than the lead designer of Chrono?</p> <p>A. Firstly, the person who did Pandoc did not note that the header at the bottom was manual and added, so in cross - examination he's going to have to say which version of that that came from. And, next, Project Chrono was a separate project. Not only is it on Wikipedia, but university sites have been running it for ages - -</p> <p>Q. Project Chrono is a physics simulation library, isn't it, Dr Wright?</p>	<p>Dr Wright claiming, implausibly, that he produced his own version of the Chrono code.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Yes, and this is a simulation. So when talking about state - based simulations, this is actually simulation code. The purpose of this code is very, very different from the Chrono code which measures time gaps. This actually measures state gaps.</p> <p>Q. Project Chrono is primarily used, as its own marketing materials make clear, for simulating things like the movements of vehicles and machines, isn't it?</p> <p>A. Yes, state - based analysis. So, when we're talking about state - based and, which we are here, going from one node competition to a next to a next, then we're talking about a simulation. So, this, where we're talking, as it says here, "nextState ... H1", "nextState ... H2", we're talking about a competition between honest and dishonest nodes. So, as you just noted, it is a simulation engine, mapping and modelling different examples in this agent or nodes.</p> <p>Q. So let's just take this in stages. Your claim is that, in modifying the library, you happen to have come up with the standard header now used in the Chrono time library; correct?</p> <p>A. The header for Chrono - - Project Chrono was "Chrono". So, taking "Chrono" and writing it as "chrono", well, I don't think that's a big jump.</p> <p>Q. Secondly, your claim must be that you also happen to have come up with the "sleep_for" syntax, which, as Mr Hinnant says, was also not standard code before 2011?</p> <p>A. No, because what that took is combining other forms of C. C started back in the - - ages back, like in K&R C that I started on, developed into Object C, which developed, as your expert knows because he wrote it, into C++ and NCC. Now, that happened later. Over the years, I was there with each of these. However, what we have are different versions of C and C++, my Lord. You had DEC had their own version, which was both on their Unix and their VMS machines; Solaris, which was my preferred one, had its own version; IBM had its own version; and then these were taken and integrated into Linux and the ANSI free version. So the original was that sleep/sleep_for, etc, was actually in other versions of C.</p> <p>Q. And in addition, your claim must be that you happen to have come up with the name spacing "std::chrono", and the class type milliseconds and the identical syntax which was later proposed and used in the actual Chrono time library, right?</p> <p>A. No, actually, "standard" means it's a standard library. So as I explained in my witness statement, you can embed any standard library that you want. I was a - - as it says on Integrys, my company, I created custom libraries. So if you look at the 2009 web page that I had from that, I created custom libraries. This is also on my Ridge Estates findings going back to 2001/2/3. Now, on top of this, what he's saying there is, this is</p>	

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>standard ":::". The ":::" is a standard C++ format going back to the beginning of C, not C++. On top of that, "milliseconds" is a standard term for milliseconds, and that isn't a standard way of writing, it is one particular out of an unbounded way of listing them. So all you're saying is, that function has milliseconds. A simulation package where you're actually simulating different node agents has time, yes.</p> <p>Q. This is a syntax of a kind which would classically be used in the true Chrono library, isn't it, Dr Wright?</p> <p>A. Actually, no. If we look, once again, "nextState.pow", "nextState.pow", "nextState.pow" and "int total_pow [equals]", what we have is a simulation. So we have taken a simulation system and we are creating a state - based simulate. Like, I was talking earlier, my Lord, in this week about how we had state - based systems where state 1, state 2, state 3 is effectively the hash chain, where you have competitions if there is an orphan fork, ie you have two miners or nodes discover at the same time. Now to simulate that, what I was doing at the time was going, if we have two honest miners and one dishonest miner, then I could simulate that. Now, in here we have "pow", being the amount of proof - of - work, so that I could look at the differences and say where this would occur so I could actually figure out whether I was right in my idea of a byzantine general problem.</p> <p>Q. Once again, Dr Wright, I'm going to put to you that that is, as the creator of the Chrono library has said in relation to this document, nonsense, and he will address it in cross - examination, if it's put to him.</p>	
<p>{Day5/119:21} - {Day5/120/8}</p> <p>{L1/169/1} "Honest2.C++"</p> <p>ID_004713 {PTR-F/70/1}</p>	<p>Q. And once again, the same references to "chrono" and "random", and on the basis of those, I put to you that this is another forged document?</p> <p>A. No. I've been developing random number generation algorithms since the '80s. Now, one of the main functions of being in gaming, which I was, I don't think anyone's disputing that, is, my Lord, you have to have very secure random number generation. So I've been writing random number generators for a long time. I wrote them for Lasseter's, MGM Grand, Playboy Gaming, GCS, Centrebet, Sportingbet. I can keep going on, if you like, but we'll just go through the list of casinos I've worked with.</p>	<p>Dr Wright claiming that anachronistic references to terms associated with C++ were related to his own supposed development of random number generation algorithms.</p>
<p>Overleaf LaTeX Files</p>		
<p>{Day5/122:21} - {Day5/123:14}</p>	<p>I think you're aware of this as a post by Mr Ager - Hanssen in which he claimed that your browsing history showed you accessing an online Q&A, with the heading on the page, "Was</p>	<p>Dr Wright claiming to have shown Shoosmiths the files</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>anything in Satoshi Nakamoto's original Bitcoin paper compiled in LaTeX?". Yes? You see that?</p> <p>A. I do.</p> <p>Q. You did in fact access that site, as shown, in September 2023, didn't you?</p> <p>A. Yes, as he captured. The reason being that - -</p> <p>Q. I'm just at the moment asking you whether you accessed that site, Dr Wright.</p> <p>A. Yes, I did.</p> <p>Q. Then, it was on 27 November 2023, wasn't it, that your solicitors, by then Shoosmiths, for the first time said that you had some files on the Overleaf web - based LaTeX editor which were relevant to this case?</p> <p>A. I don't know when they told you. I had already shown Shoosmiths in September, I believe it was.</p>	<p>associated with the Overleaf based LaTeX editor in September, despite the fact that they were first revealed to COPA on 27 November 2023. This was subsequently contradicted by Shoosmiths, who, in response to Bird & Bird's query, confirmed that demonstrations took place in October and November 2023, but did not confirm that they were shown the files in September 2023, or that any demonstrations took place that month, see {M/3/15}, {M/3/48} (and in fact could not have, as Shoosmiths were not instructed until the beginning of October, per {M/3/48}).</p>
<p>{Day5/125:7} - {Day5/126:21}</p>	<p>A. To make it clear, the use of the US litigation disclosure fell into this. There wasn't another disclosure exercise. There probably should have been, but what happened was the 2019 capture and disclosure, and the subsequent 2020 one, for the US case, was reused in this.</p> <p>Q. I'm going to proceed carefully because of privilege. But we'll get back to this conversation later. Paragraph 17, Shoosmiths record that you told them that a folder entitled "Bitcoin" was on the Overleaf editor containing certain LaTeX files. And then they write this: "We understand from our client that reverse - engineering of LaTeX code which so precisely reproduces the White Paper from the published PDF versions of the White Paper would be practically infeasible ..." Do you see that?</p> <p>A. I do.</p> <p>Q. So your position then was that LaTeX files of yours in the Bitcoin folder on Overleaf precisely reproduced the White Paper?</p>	<p>Dr Wright admits failings in the disclosure exercise in these proceedings.</p> <p>Dr Wright also not accepting the obvious truth regarding when he and his solicitors first provided details regarding his Overleaf LaTeX files.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. With the caveats I gave, noting --</p> <p>Q. You gave no caveats there -- then, did you?</p> <p>A. I gave caveats. I said that the -- what do you call it, the OpenSymbol doesn't run in Overleaf, I said that the IEEE bibliography had been updated by the IEEE, that it was a web - based system, I said that I'm not using MiKTeX and that there had been changes in LuaLaTeX since the version that I had - -</p> <p>Q. Can I pause you there. Can I pause you there. All of that information came much later, didn't it, Dr Wright?</p> <p>A. No, I said that when I talked about it, and I also noted that the bit that would be basically the same would be the images and the images were the most difficult to reproduce.</p> <p>Q. Dr Wright, these differences that you're describing came after the PTR in correspondence from your solicitors, didn't they?</p> <p>A. No, they did not</p>	
<p>{Day5/127:10} - {Day5/128:1}</p>	<p>Q. And do we see that that explained, over the page {E/24/8}, 19.2.6, I think it is, that the Bitcoin folder contained: "... certain LaTeX files which, when the code contained on them is compiled in Overleaf ... produce a copy of the Bitcoin White Paper ..." That witness statement said nothing about any features or processes you used which led to material differences between the Bitcoin White Paper and the compiled versions of yours, did it, Dr Wright?</p> <p>A. No, and I apologise. I'm not very good at explaining technical concepts to non - technical people. So, making people understand the difference between MiKTeX, the original version, which is also in the BDO Drive installed, of LaTeX, and how LaTeX works on Overleaf, a web - based, limited version of LaTeX, all I can do is show people. It's hard to --</p>	<p>Dr Wright claiming not to be good at explaining technical concepts to non - technical people, despite that being a key feature of the Bitcoin White Paper (see paragraph 23(a) of the witness statement of Steve Lee - {C/12/9})</p>
<p>{Day5/128:16} - {Day5/129:5}</p>	<p>Q. We'll come to when you introduced these various qualifications, but I suggest to you that you didn't introduce any of them when you sought an adjournment of this trial at the PTR on the basis of this material, did you?</p> <p>A. I don't know how my solicitors acted. I told them these things. And one example of how I would describe it is, if I had a version of Word, Word 2003, and I loaded the document now in a new version of Word, current version of Office, then both documents are going to display separately, they're not going to be the same. So the same thing happens in LaTeX. If you use an old version of the program, you will get slightly different versions. And this is also in your evidence where some of the experts say that these have changed over time.</p>	<p>Dr Wright failing to accept the obvious truth regarding how his solicitors, whom he instructed, presented the Overleaf information to COPA.</p> <p>In particular, paragraph 19.2.6 of Field 1 says 'when compiled in Overleaf...' {P3/13/8} and did not address the</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
		qualifications that were introduced later.
<p>{Day5/131:6} - {Day5/132:16}</p>	<p>MR HOUGH: Well, I was going to make the point my Lord made, that the advice on this subject has been the subject of a ruling about privilege and that Dr Wright can be asked about this particular advice. But Dr Wright, you must be careful not to go into any other advice. So the question of advice given to the effect that your Overleaf materials were not disclosable, that's something I can ask you about; do you understand?</p> <p>A. I do.</p> <p>Q. So who do you say gave you this advice?</p> <p>A. I would have to look up her name. There was a young solicitor in training at Ontier. I don't have a name on me. I can get it. She was out at the house at the same time when Rivero, the American solicitors, came over, and this was in the initial sort of evidence - collection phases of the Kleiman case.</p> <p>Q. Dr Wright - - and this, my Lord, is the reason why I'm putting this letter - - the reality is that it wouldn't just have been wrong, but very obviously wrong for Ontier to tell you that you just couldn't deploy this material which you regarded as so important. That would have been obviously wrong, wouldn't it?</p> <p>A. No, because in the Kleiman case, there was no dispute over my being Satoshi, so no one wanted anything to do with that. So, the files had no metadata dating back to the time and it was just how the Bitcoin White Paper was created.</p> <p>Q. But Dr Wright, all of these comments are about advice given in the context of this case by reference to the disclosure review document in this case. That's why I took you to the original letter.</p> <p>A. And all Ontier did was they reused the 2019 and 2020 US disclosure documents. Nobody said that we needed to do anything again, they just said, "What we have should be good enough".</p>	<p>Dr Wright blaming third parties, a young solicitor from Ontier, for giving advice that LaTeX files weren't disclosable. Further, it was Dr Wright's position that the Kleiman litigation was predicated on him being Satoshi Nakamoto - see Simon Cohen 1 para 24 {P3/1/7} and COPA's response in Sherrell 1, para 6 "he states that the Kleiman Litigation is premised on the Defendant being Satoshi... I do not know whether this is entirely accurate or not but it does demonstrate the close factual connection between the two pieces of litigation." {P1/1/2}.</p>
<p>{Day5/133:6} - {Day5/134:5}</p>	<p>Pausing there, that is saying that a decision was made in relation to the searches specified for these proceedings, not a judgment made on disclosure for the purposes of the Kleiman proceedings. Do you understand.</p> <p>A. Yes, I understand also that they're the same, because the 2019 US Florida proceedings were just reused. Nobody re - did any discovery. I'm redoing it now for Tulip, but, my Lord, everyone just said we could reuse what we have.</p>	<p>Dr Wright again admitting that no proper disclosure exercise was carried out.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Then: "Dr Wright informs me that Ontier took the view that documents compiled and exported from Overleaf after 31 August 2019 (the latest date range for disclosure of documents in this case) were not disclosable for this reason."</p> <p>A. Again --</p> <p>Q. The advice you were passing on was nothing to do with Kleiman and all to do with the disclosure review document in this case, wasn't it?</p> <p>A. No, they're both the same. AlixPartners, where you have all these files from, they were my US litigation team. They did that over here. That got reused. Nobody bothered to say, "Is there any other files for this case".</p>	
<p>{I/5/34 - First Expert Report of Spencer Lynch</p>		
<p>{Day5/136:14} - {Day5/137:12}</p> <p>“The Bitcoin White paper using LaTeX”</p>	<p>Q. Then in paragraphs 117 to 118, he goes on to say that, by contrast, the Bitcoin White Paper could be replicated using OpenOffice, the program its metadata say was used to create it. Are you aware of that finding?</p> <p>A. Yet he never did it.</p> <p>Q. Then, if we go down to see what he did do, do you see that the first image on the screen is an overlay between the OpenOffice recreation of the White Paper and the actual White Paper; do you see that?</p> <p>A. I do.</p> <p>Q. Do you see, below, there is an overlay between the Bitcoin White Paper and the compiled version from</p> <p>Q. So would you accept from that simple test that the OpenOffice recreation produced a much better replica?</p> <p>A. No, I don't, because the OpenOffice didn't go into the main points I was making. The main point I made was that the image in LaTeX, that was on the BDO Drive as well and has been used in publications of mine going back to 2006, was an exact match. Now, the image, in text, was the hardest part to reproduce and that wasn't.</p>	<p>Dr Wright is evasive in relation to the experts' findings that the Bitcoin White Paper could be easily replicated in OpenOffice.</p>
<p>{G/7/24} – First Expert Report of Arthur Rosendahl</p> <p>{I/5/29} – First Expert Report of Spencer Lynch</p> <p>Cross examination regarding whether the Bitcoin White paper was written using LaTeX</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day5/139:24} - {Day5/141:10}</p>	<p>Q. It's not -- I'm not suggesting to you that it's ugly, I'm suggesting that you went to, on your case, an extraordinary amount of effort to produce something in LaTeX that would look like a document produced in OpenOffice and that would have metadata saying it was produced in OpenOffice.</p> <p>A. I wouldn't say an extraordinary amount of effort. I went to effort, and I did that for those reasons. At the same time that I was actually writing extensively on steganography, I did that with a few documents. So, while I was writing and showing people how you could steganographically do these things, I also produced documents that are steganographically altered.</p> <p>Q. So you went to a lot of effort to produce the White Paper in this form to provide a digital watermark, that's what you're saying?</p> <p>A. Yes.</p> <p>Q. And this would mark you out as the author, right?</p> <p>A. No, it was more just because I could at the time.</p> <p>Q. But the effect of it, on what you say, would be to mark you out as the author, right?</p> <p>A. Yes.</p> <p>Q. Didn't it occur to you to mention that in your first witness statement as a very powerful point on your behalf?</p> <p>A. I didn't think anyone would understand it. I have tried to explain to lawyers multiple times -</p> <p>Q. Don't tell us anything privileged, Dr Wright.</p> <p>A. I'm not going to. I'm going to say I'm probably the world's worst client, I'm an Aspie and I'm a complete ass, and none of my lawyers will deny that. I don't handle people not understanding things very well, and I get frustrated. So, I end up like a three - year - old who doesn't get a lolly when I get frustrated, as people know, and I sit there expecting my lawyers to just grasp these concepts, and then they don't and I get angry.</p>	<p>Dr Wright making a new claim that he engaged in a convoluted process to produce a copy of the Bitcoin White Paper with a digital watermark but didn't mention it in his witness evidence.</p>
<p>Differences between control version of Bitcoin White paper and complied LaTeX version</p>		
<p>{Q/5/2} - Joint Statement on LaTeX of Arthur Rosendahl and Spencer Lynch</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day5/149:19} - {Day5/150:13}</p>	<p>Q. {Q/5/1}, please. Page 2 {Q/5/2}, paragraph 4: "On the subject of reverse engineering, the experts agree that it is not too difficult to reverse engineer the BWP to create a LaTeX source file that compiles a PDF file similar to Dr Wright's, which contain the same text, formulae, and diagrams; and is superficially similar to the [Bitcoin White Paper]. It would however be extremely difficult ... to create a PDF which was an exact match ..." So easy to produce something as good as yours, Dr Wright?</p> <p>A. No, actually, what they're saying in the example was absolutely nothing like it, not even slightly aligned. Not like mine, where most of it was aligned; nothing like. Not - - none of the same line breaks, none of the same images, nothing. And that goes down to a file that instead of being - - like, if mine was - - I can't remember how long it is, but say it was a thousand lines, theirs would be a million lines to take every character.</p>	<p>Dr Wright not accepting the obvious truth that the experts concluded in their joint statement that it would not be difficult to create a LaTeX source file that compiled into something similar to Dr Wright's by reverse engineering the Bitcoin White Paper.</p>
<p>{Day5/150:14} - {Day5/151:14}</p>	<p>On top of that, they didn't actually do it. The simple example - - the simple test wouldn't be to say it, wouldn't be to give an opinion. If you're saying it's so easy, run it up. I did. I used every available LaTeX package after they did this. I have copied all of these and some of them are in the Overleaf disclosure. None of them work. By every one, I used over 120 different packages --</p> <p>Q. Can I pause you there, Dr Wright - -</p> <p>A. -- and none of them --</p> <p>Q. -- because you're starting to give evidence of experiments, which is not admissible, for the simple reason, and perhaps you can accept this, that in this case, whatever else you are, you're not independent, are you?</p> <p>A. No, just like either of the LaTeX people.</p> <p>Q. You're saying that Mr Lynch isn't independent, are you?</p> <p>A. He works for Stroz. I don't believe, no.</p> <p>Q. So both the experts lack independence and Mr Lynch lacks competence as well? That's your evidence at the end of this week?</p> <p>A. Mr Lynch had to follow a cookbook I gave him to follow a simple text program. That doesn't make him an expert in LaTeX. So, just finding someone who has forensic qualifications doesn't make you an expert, and I'm going to stick to that.</p>	<p>Dr Wright tries to rely on experiments in his witness evidence. He then questions his own expert's (Mr Lynch) independence.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day5/151:20} - {Day5/152:10}</p>	<p>A. No, actually, he didn't, and he didn't provide it.</p> <p>Q. {G/7/60}, please, paragraph 196. He found, didn't he, at paragraph 198, that it's: "... very likely that both files (Dr Wright's Images and the Aspose automatic conversion) were ... exactly the same up to a possible translation and scaling factor ... It would have been relatively easy to write a program to check this ..." But given the time that was available to the experts, that wasn't possible. So his conclusion was: close similarity between your document and the product of an online conversion tool?</p> <p>A. No. I actually ran that tool and had a look at the output. The output was, I think, 30 times longer. Every single dot had its own independent area. It didn't replicate the thing very well at all, it had an accuracy of about 60%, so, no, I disagree.</p>	<p>Dr Wright tries to rely on inadmissible experiments in his witness evidence.</p>
<p>{M1/2/103} – IPC(2) – Dr Wright's demonstrations to Shoosmiths</p>		
<p>{Day5/152:21} - {Day5/153:20}</p>	<p>Q. Page {M1/2/103}, please. If we maximise the table. Thank you very much. Now, they plotted the content of the spreadsheet as a graph, showing that the main.tex file, which was the one your solicitors identified as the one which would compile into the White Paper, was edited on 19 to 20 November, 22 November, 24 November and 1, 4, 5, 6, 10 and 12 December; do you see that?</p> <p>A. I do.</p> <p>Q. You were responsible for those edits, weren't you, Dr Wright?</p> <p>A. I was.</p> <p>Q. So the file was being edited right up to the day before the LaTeX files were received by Stroz Friedberg?</p> <p>A. Yes. I demonstrated to Shoosmiths, making a small change, adding a full stop, adding a percentage. And where you say there are extensive edits, that's actually not true. Adding a full stop, removing that full stop, is actually two edits. So, when I add a space, that's an edit. If I go percent, comma, slash, etc, that's three edits. So, at one stage, I typed in Matt's, one of my solicitor's, name. That was probably 10 edits. I then undid it and put the original name back. So I was demonstrating how using that, you could change the date and produce a new version, etc.</p>	<p>Dr Wright claiming that he did demonstrations for his solicitors to show them how one would edit the metadata.</p>
<p>{Day5/154:2} - {Day5/154:13}</p>	<p>A. I downloaded a copy of the file and gave it to Shoosmiths before I did any of this. So, the first thing is, I downloaded the ZIP from Overleaf, sent it to the solicitors. We did that right at the beginning of this process. And as such, once I've given them a copy, I'm saying that I can't change the copy they have,</p>	<p>Dr Wright claiming that he did demonstrations for his solicitors to show</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>therefore my making changes and undoing those changes is not a material change.</p> <p>Q. Do you say that all of those edits were done in the presence of Shoosmiths?</p> <p>A. They were on videos, on calls, I sent them some emails while they weren't on there, I sent, like --</p>	<p>them how one would edit the metadata.</p>
<p>{E/1/4} – First Witness Statement of Craig Steven Wright</p>		
<p>{Day5/157:21} - {Day5/158:24}</p>	<p>Q. Dr Wright, what knowledge or information do you say you've imparted through your witness statement which only the creator of the Bitcoin System could have?</p> <p>A. Generally, looking at how this is described, so I've also talked about characteristics, such as, in scripting, Turing completeness. I got ridiculed, in 2015, for saying Bitcoin was Turing complete. I said it. Nick Szabo basically challenged me and said, "Write a White Paper". Instead, I wrote three papers which I published in academic circles. I did a conference on it. I also published seven patents and we have built it. So not only do I say it is, we have built systems in code proving that it is.</p> <p>Q. I don't want to get into that debate with you at great length, Dr Wright, but even supposing you're right about all of that, why couldn't somebody else very clever, who wasn't Satoshi and knew all about Bitcoin, come up with all of that?</p> <p>A. Because they would have had to know and study the early version of Bitcoin. And as you see from your own experts, like Professor Meiklejohn, people look at Bitcoin post – 2013, 14, 15, 16, 17, and they don't take any of my code, they look at the changes, they look at the narrative that had been promoted by BTC Core. They had this narrative that nodes are run by every person, even back to 2008, James Donald said. They ignore the clear definition in section 5 of the White Paper that says nodes create blocks. So, unfortunately, no, this isn't happening.</p>	<p>Dr Wright is unable to give any clear or comprehensible answer to the (important) question posed.</p>
<p>{Day5/158:25} - {Day5/159:7}</p>	<p>Q. Again, Dr Wright, you're referring to sections of the White Paper. Anyone can read those, can't they?</p> <p>A. They seem to not be able to read them very well, because your side are actually arguing, and including your expert witness, that nodes are something different than defined in the White Paper, despite the fact that, as Satoshi, I said Bitcoin is set in stone. I have reasons for it not to change.</p>	<p>Dr Wright making arguments for his Satoshi Nakamoto candidacy based on an interpretation of the Bitcoin White Paper which is freely available.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day5/161:19} - {Day5/162:14}</p>	<p>Q. And then you began writing code for games by age 11? A. Yes, let me - - Q. Again - - wait a second. Again, in C and C++, yes? A. Yes. Let me clarify that. I started with K&R C. K&R are authors of an early version of C. They developed a number of versions of C that started, including object – orientated code, in the early 80s. So, my first, when I was around nine, was in K&R C. That developed, with the introduction of Smalltalk, into Object C. Object C wasn't to '85 - - '84/'85, my Lord. That was, like, a precursor to C++ but wasn't C++. That integrated in Solaris, my main platform that I used, into a form of library – based Object C. Object C then morphed into the Solaris C that was used, but Solaris had problems, so they're no longer a company, and what ended up happening is, in 1989, a formal version of C++, and then ANSI C++, a year later, were developed. So what I'm saying here, just to make it clear - - I don't always explain myself, my Lord; I'm trying to do it now - - is that I started with these, and as it evolved, I moved towards C++.</p>	<p>Dr Wright backtracking on his evidence that he started writing in C/C++ from age eight – eleven.</p>
<p>{Day5/162:22} - {Day5/163:13}</p>	<p>Q. And you're aware his evidence was that the name "C++" was first coined in December 1983 when you were 13? A. Yes. Q. And your elaborate explanation that you've just given was first provided after you'd read Professor Stroustrup's evidence and in response to it, wasn't it? A. No, because I was actually involved that whole time. And I have his book, by the way; the original. I also have K&R C's first book, and I have the Knuth series, so I have all of this. Q. Your account, that you began using C++ between the ages of eight and 11, clearly given in this witness statement, is a fabricated detail you have now qualified and embellished because it's been found out. A. No. As I just stated, what I'm doing is simplifying so that people understand.</p>	<p>Dr Wright backtracking on his evidence that he started writing in C/C++ from age eight - eleven.</p>
<p>{Day5/168:10} - {Day5/168:22}</p>	<p>Q. Common forms of coding, all this, all the evidence -- A. No, earlier, I said I coded in the C language, so, no. The witness statement's not meant to be rambling, so I made a statement saying that I programmed this using these as an origin - - Q. You're now suggesting that there was something about your work on Millicent where the code specifically prefigured elements of Bitcoin. That's not something you saw fit to mention in your statement, is it?</p>	<p>Dr Wright is evasive regarding the alleged relevance of his Millicent work on development of Bitcoin.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. I've noted right here that Millicent was used in shaping my ideas. I didn't actually take Millicent and make it into Bitcoin, what I did was I designed a system based on those concepts.</p>	
<p>{Day5/171:17} - {Day5/172:11}</p>	<p>Q. There's not a shred of evidence, is there, that DeMorgan did any work on digital cash in that period, is there?</p> <p>A. No, actually, there is quite a lot. BlackNet is actually premised on crypto credits. So, the part you mentioned before with b - money, the first paragraph of b - money quotes Tim May and goes into the history of BlackNet. BlackNet basically had crypto credits. The proposal that you're mentioning that Wei Dai mentioned was, I could extend crypto credits in a new way. He never actually did it. I, actually, at that stage, thought he would have, but he didn't continue. So, what I did was trying to take an encrypted internet, and the only way that is viable to make this sort of distributed encrypted system is to have it economically valued. Now, that meant that proof - of - work tokens would be at small - - small integers of exchanges so that all the transactions you mentioned before, the grabbing a web page, the doing a search, the sending an email, would be both economic transactions and transactions on a server.</p>	<p>Dr Wright discussing supposed work that DeMorgan did on digital cash, without anything to substantiate it.</p>
<p>{Day5/172:25} - {Day5/173:5}</p>	<p>Q. Dr Wright, you produced a whole series of Bitcoin - of BlackNet documents, which we looked at, that say nothing about crypto credits, didn't you?</p> <p>A. You don't actually need to, but if you read BlackNet, you see that the foundational part of it is crypto credits.</p>	<p>Dr Wright admitting that the BlackNet documents do not reference crypto credits</p>
<p>{Day5/173:13} - {Day5/174:16}</p>	<p>{L2/102/1}, please. Back to your CV. Page 3 {L2/102/3}. Your work at DeMorgan is summarised over several paragraphs and it's all about IT security, isn't it?</p> <p>A. Actually, Bitcoin is about IT security. The notion of a secure immutable timestamp server keeping logs - - keeping files so that they can't be changed is the core of the information security. That is one of the things I'm trying to solve. Where my, sort of, opposing counsel here - - I'm not sure if I call him "my learned friend", or anything like that, like you have - - but what you have been saying, all of the metadata changes over time. What I've been working to create is a system where, even if the look of the file changes, we now have a way of proving every paragraph in a document independently.</p> <p>Q. I'm going to stop you on that digression and just put 271 this to you. You said in your witness statement that a major part of DeMorgan was developing digital cash. When you summarised your work at DeMorgan in your CV, while you were working at BDO, there's ne'er a word about digital cash, is there?</p>	<p>Dr Wright is unable to identify any contemporaneous CVs other than that which was put to him, which shows him to have been an IT security professional.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. One, I didn't create that CV. Two, there were four separate CVs at that stage. I ran the programming section of BDO; there's a CV for that. I ran the information security and audit part; there's a CV for that. I ran the financial audit area for computer audits; there's a CV for that. And I ran the digital forensic area; there's a CV for that.</p>	
<p>{Day5/175:25} - {Day5/176:25}</p>	<p>Q. Well, we'll go on to this next week. It may be, shortly, time to draw stumps. But all of these entries, contemporaneously, from your LinkedIn profile and your CV, make clear that your work at DeMorgan was in IT security services, firewalls and the like.</p> <p>A. Two points. One, I don't manage LinkedIn, so I didn't fill it in. And the second point is, no, actually, as I said, the firewalling and logging systems that we're talking about, like for Vodafone, Lasseter's, etc, were all on an early version of what became Bitcoin. They're a hash chain system. So, the error is focusing on cryptocurrency. Bitcoin was never primarily about a cryptocurrency, it was really about timestamp server, as it says in the White Paper, and the concept of immutable logging. So, in 2009, when Martti Malmi got involved, and others, such as Martin - something, their key area was: how do we actually create something and have the integrity of this? And that's why I've talked about Tripwire. A distributed Tripwire system, which we have patents for as well, would enable all of the files in a company to be recorded. So you're saying "just firewalls". No, I developed these systems. They linked into hash chains, they had distributed peer - to - peer logging and enabled the secure management of the server on what is a proto blockchain.</p>	<p>Dr Wright blaming third parties (Martti Malmi, and a "Martin").</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
DAY 6		
CROSS - EXAMINATION OF DR CRAIG WRIGHT BY JONATHAN HOUGH KC		
Dr Wright's CV & Qualifications		
<p>{Day6/5:15} - {Day6/6:3}</p> <p>{L2/102/3} BDO CV</p>	<p>Q. So that's how your CV from the time, or at least the one we have, described that job; correct?</p> <p>A. No, that's a marketing document by BDO. There were actually four or five of these, depending on which stage, and the one that I sent to Gavin talks about high end C++ design and the integration of a number of complex algorithms. Each of these were designed for the particular role, so they were for marketing my - my skills and sort of techniques that I used. The one that focused on GARCH areas, time series, C++ coding, in - depth code analysis, etc, is a different resumé, and none of this, of course, mentions any of the situation, like NIPPA, which was an early peer - to - peer network for the brokers.</p>	<p>Dr Wright is not accepting the obvious truth, namely that the document shown to him was his CV, stating that it was tailored for certain projects.</p>
<p>{Day6/9:4-17}</p> <p>{L2/102/3} BDO CV</p>	<p>Q. Returning to your - the CV from your time at BDO that we have {L2/102/1}. Over to page 2, at the top L2/102/2}: "Career highlights. "Although developing the security measures for the ASX was one of the early highlights of his career, Craig also distinguished himself by designing the security architecture and environment for Lasseter's On - Line Casino ..." That's how the job was described in this CV, wasn't it, Dr Wright?</p> <p>A. Yes, designing the security architecture, which meant completely rebuilding and architecting new systems that didn't exist before.</p>	<p>Dr Wright confirms the work described is IT security work.</p>
<p>{Day6/12:5-9}</p>	<p>Q. Dr Wright, I'm going to ask you the question again. Digital cash, the words or system "digital cash", didn't appear in any of those documents, did it?</p> <p>A. Not in a one liner, no, but "architecture" includes that.</p>	<p>Dr Wright admits that the words "digital cash" didn't appear in these documents.</p>
<p>{Day6/12:15} - {Day6/13:5}</p>	<p>Q. Pause there, Dr Wright. The question was: there isn't a single document setting out a proposal by you for digital cash to Lasseter's, is there?</p> <p>A. Again, wrong. What I was stating is there are multiple documents, I don't know all the ID numbers. I do know, even from third party ones that you have access to, such as Gavin's</p>	<p>Dr Wright is not accepting the obvious truth that the documents don't show any connection between Lasseter's and digital cash.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>disclosure, Gavin's disclosure has my other resumés, the ones that have to do with programming.</p> <p>Q. They don't refer to digital cash work for Lasseter's either, do they? "Digital cash".</p> <p>A. Token systems and digital cash are different. So, apart from that, I have extensively written about this online. And, no, I didn't put "digital cash" per se, because I never had it working at Lasseter's. So while I had a token system, digital cash was never implemented at Lasseter's; I was trying to get it going.</p>	
<p>{Day6/13:21} {Day6/14:11}</p>	<p>- Q. Dr Wright, although you've strained to draw links in your witness statement retrospectively between these various jobs and Bitcoin, your own documents all describe these jobs as straightforward IT security roles, don't they?</p> <p>A. No, that's not correct. And, again, the resumé that you have from Gavin Andresen, which is in his disclosure, because I sent it to him, details extensive high end PhD - level coding projects, many of them, in multiple areas, including token systems and including the logging developed at Vodafone. As noted, Vodafone didn't have 3G back then, this is too early, and to create a logging system for Vodafone required implementing completely new software. That software, of course, had to have the integrity of all of the sends for payment, and to do that we had basically a hash chain - based system.</p>	<p>Dr Wright is not accepting the obvious truth that the documents do not show any connection between Lasseter's and digital cash.</p>
<p>{Day5/15:22} {Day6/16:19}</p>	<p>- MR JUSTICE MELLOR: Dr Wright, last week, you told me, I think, that you didn't prepare this CV.</p> <p>A. No, I did not.</p> <p>MR JUSTICE MELLOR: Yet -</p> <p>A. There were different ones -</p> <p>MR JUSTICE MELLOR: Just wait. Yet it contains a significant amount of detail. This detail must have come from you, mustn't it?</p> <p>A. No. I had an EA. I don't remember her name. And the team was - they had a group that put it together. So I provided some detail to the team and they separated it into four different areas. Because I was working in each of those areas, I headed the digital forensic department, I headed the statistical analysis and fraud detection department, etc, there was a separate CV used for selling in each of those areas.</p> <p>MR JUSTICE MELLOR: But the information about your roles prior to BDO must have come from you?</p> <p>A. They took it from my CV and other things that I'd told, but what they did was they extracted information - my original</p>	<p>Dr Wright is evasive regarding the status of his CVs, failing to answer directly the question being asked.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>one was far more detailed - just for the role. So, because I was in a consulting role in this one, they made it a consulting focus.</p>	
BDO MEETINGS		
<p>{Day6/19:9} {Day6/20:4}</p>	<p>- Q. So is it right that, on your account, all those people knew about your pitch for BDO to provide funding for the Bitcoin System?</p> <p>A. Well, no, it wasn't called Bitcoin back then. What I was talking about was a hash - based audit system that would tokenise all of this using an economic security model. So, I would have talked about "Timechain", or a similar name, not Bitcoin.</p> <p>Q. Do you accept that none of those people has ever come forward and given an interview or evidence in court recalling you pitching a digital currency system, or anything like the Bitcoin System, to BDO?</p> <p>A. No. Neville Sinclair was actually in court and said that I pitched the system. On top of that, each of the other people had been trolled extensively. Allan Granger, I know, doesn't want to give evidence, because he has had death threats, both to him and his wife, from a multitude of people, and as such, he doesn't want to say anything. He was a director of a company that was running Bitcoin research for several years, so he was heavily involved.</p>	<p>Dr Wright provides a different version of events to that which he has provided previously, see Dr Wright's evidence in Granath {O2/11/10}.</p>
<p>{Day6/20:5-14}</p>	<p>Q. Dr Wright, take this in stages. First of all, I suggest to you, and the court can make its own mind up on the basis of Mr Sinclair's transcript, but in the Granath trial, Mr Sinclair made it very clear that he had no recollection of discussing a prospective E cash system with you, right?</p> <p>A. No. As I've noted multiple times, Timecoin was the system I was trying to run. Bitcoin is only the economic system behind it. It's like crypto credits in BlackNet.</p>	<p>Dr Wright claims to be discussing Timecoin with Mr. Sinclair in 2008, which is inconsistent with Dr Wright's own evidence in which Timecoin documents are dated to 2007.</p>
<p>{Day6/21:2-22}</p>	<p>Q. Just pause there. Are you agreeing with me or disagreeing when I say that you've never put forward a single document to support the pitch to BDO, other than the Quill document that I've put to you is a forgery?</p> <p>A. Again, I have also discussed this with Ignatius Pang -</p> <p>Q. Sorry, Dr Wright, that's not an answer to the question. The question is that you've never put forward a single document,</p>	<p>Dr Wright recounting evidence that is hearsay and involving new individuals at BDO.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>other than that Quill page, which I've put to you is a forgery, in support of the pitch to BDO, have you?</p> <p>A. I will quote myself at [draft] line 4. No, and I've also talked to Ignatius Pang. If, my Lord, I can finish my sentence, I would like to say that I discussed with members at BDO some of these things, and that is noted in some of my written documents. Ignatius also mentioned that he discussed this with other people at BDO, including Steve Atkinson and Sonny Susilo. Now, in that, not only does he recall some of those documents, but those other people were involved as well.</p>	
LLM Dissertation		
<p>{Day6/24:16} - {Day6/25:2}</p>	<p>Q. Ms Pearson's evidence is that the text from her paper is her own work, something she prepared and in her own style. That's, for everyone's reference {C/3/3}, paragraph 12. We don't need that on screen. Do you accept that or do you dispute it?</p> <p>A. No, I accept it.</p> <p>Q. Now, comparing the two highlighted sections of her paper and the two highlighted sections of your paper, do you accept that they are identical, except, I think, for using an "S", rather than a "Z" in the word "analogises".</p> <p>A. I do.</p>	<p>Dr Wright admits Ms Pearson's work is her own.</p>
<p>{Day6/27:5} – {Day6/28:18}</p>	<p>Q. Ms Pearson's work, unless you dispute her evidence, came from 1996, didn't it?</p> <p>A. Yes, and both of them discussed the same issues. Ms Pearson's work didn't come up properly because it's not actually an academic thing, it's a blog. So while that should be cited, EndNote didn't include it properly. One of the versions of my document did include it, but the other one didn't. This was brought up by Mr Maxwell, Paintedfrog, and sent to the university with a complaint, the university investigated it and dismissed the claims of plagiarism.</p> <p>Q. Well, this court isn't bound by what the university decided, so I'm going to ask you afresh about this. The initial versions of your dissertation which were produced did not credit Ms Pearson at all, did they?</p> <p>A. No, the initial versions actually did. The update removed her in part because when I use EndNote at the time it doesn't always automatically update these. It was noted in the footnote, but not in the bibliography, so that was a mistake I</p>	<p>Dr Wright is providing new excuses in the box, asserting that the reason why Ms Pearson's work was not cited properly in one version of his LLM dissertation was because it was a blog (contrary to Ms Pearson's evidence that it was a paper), and as a consequence EndNote software did not include the citation.</p> <p>Dr Wright admits that the first version of his LLM Thesis contains</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>made. So while her name was noted in footnotes, it was not put in the bibliography of the document.</p> <p>Q. Dr Wright, there are in this article, and we looked – in your dissertation, we looked particularly from the first page we considered, there are chunks which are identical to Ms Pearson’s not quoted, not in quotation marks and not referenced; correct?</p> <p>A. In that version, yes. The other version actually had it – what do you call it – in italics and referenced.</p> <p>Q. In italics, you say?</p> <p>A. Yes.</p> <p>Q. In quotation marks?</p> <p>A. No, in italics. Italics actually works for block text.</p> <p>Q. Dr Wright, far from your LLM dissertation representing inventive thinking of a very high order, pre – figuring the Bitcoin White Paper, these colour – coded passages show that, in large parts, it was made up of plagiarism, wasn’t it?</p> <p>A. No, that’s not correct.</p>	<p>sections that do not quote or reference Ms Pearson’s paper.</p> <p>Dr Wright is refusing to accept that he has plagiarised Ms Pearson’s work.</p>
{Day6/30:9-23}	<p>MR JUSTICE MELLOR: Can I just ask you, Dr Wright, when you say the “EndNote software ... didn’t handle blogs terribly well”, how on earth would that have affected the presentation of the text in your dissertation?</p> <p>A. Ms Pearson didn’t have a paper, she had a blogpost. Now, I’d referenced that initially and I’d put it in the system, but when it was sent to the editor - and I used an editing service - it came back and I didn’t notice that that had been removed. What then happened was, the version that I’ve got where it is block quoted lost that quoting and the name - well, her material was sort of no longer, well, footnoted and quoted. That is on my, sort of, bad for missing that, but it wasn’t something that I was aiming to intentionally do, it was originally in the document.</p>	<p>Dr Wright provides an evasive and incomprehensible answer when pressed on the relevance of EndNote software to the charge of plagiarism.</p> <p>Dr Wright continues to assert that Ms Pearson’s work was a blog, which is incorrect and contrary to Ms Pearson’s evidence (as above).</p>
{Day6/32:16} {Day6/33:22}	<p>Q. Dr Wright, in the sections we looked at, you directly copied whole passages, not just common terms or words, or graphs and diagrams, didn’t you?</p> <p>A. No, what I’d actually done is I had a block quote - and the version online has the block quote - the block quote was referencing Ms Pearson. The distinction is that her ideas are very different to mine and also Mann and Bezley. So while I did quote her initially, as it states here, when I sent it to the editors with a note to remove some of the material to get it under the word count and just to restructure it, etc, some of that was omitted. Now, I have noted that I am apologetic for</p>	<p>Dr Wright provides a different explanation to that given earlier in his evidence in relation to the use of Ms Pearson’s work in his LLM dissertation.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>that, and the version that is online is the one with her name in it.</p> <p>Q. Dr Wright, just to be clear, an excuse about being asked to reduce size doesn't explain any of the points we've looked at, because adding quotation marks and footnotes shouldn't cause a problem on that score, should it?</p> <p>A. No, actually, it does. So, when you're sending to an editor, my Lord, Zotero and EndNote have their own macros, and if the editing people aren't using them, it means they can be dropped. When loaded back into the software, sometimes these things go missing. So, yes, I am apologetic about not having that, but as I said, I didn't notice that happened.</p> <p>MR JUSTICE MELLOR: Who were the editors?</p> <p>A. I can't remember the name. I - I use First Editing, and I have for a number of years, but there was a woman in Australia, I need to look up - I could look up her name over lunch, if you want, my Lord. I haven't spoken to her since 2010/11.</p>	
{Day6/35:15-21}	<p>Q. Being aware that this is an issue that's been raised in these proceedings, have you ever disclosed any correspondence with the editor to support your version of events?</p> <p>A. No, but the online version with the referencing is available and that's also one of the ones in evidence. It is the longer version.</p>	<p>The online version with the referencing {L2/195} was only corrected <i>after</i> the plagiarism was pointed out, and still does not reference all of the material copied from Ms Pearson.</p>
ACTIVITIES FROM 2007 - EARLY 2009		
{Day6/37:2-6}	<p>Q. You were blogging regularly on IT security issues with a specialist blog entitled, "Cracked inSecure and Generally Broken", right?</p> <p>A. Yes. I actually had one of my staff members load them, but I would write, like now.</p>	<p>Dr Wright is blaming third parties (namely that his staff "loaded" his blogs).</p>
<p>{Day6/40:12} - {Day6/41:12}</p> <p>{L9/97/1} Wayback Capture of "Cracked,</p>	<p>{L9/97/1}, please. This may be the reference. 22 January 2009, did you write a blog in these terms?</p> <p>A. I did.</p> <p>Q. "A Return to Consulting. "I am going back to consulting and contracting. "I will have more details soon, but I am going to be offering: "Security consulting "Forensic analysis and</p>	<p>Dr Wright is not accepting obvious truth regarding his immediate plans for work.</p> <p>Dr Wright's reference to the alleged</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
Insecure and Generally Broken”	<p>Expert witness work "Incident handling response and training "Audit and testing "Data recovery "eDiscovery Services and consulting "Malware analysis and research." Did you therefore present to the world those as being your immediate plans for work in January 2009?</p> <p>A. Not really. That was all I did. I set up the site first for Information Defense, then I set up one for Integyrs. Integyrs was more code - based. Then, with the number of clients that I had, I started selling services, including implementing, well, an - like, Timecoin system, I guess, trying to get that going. Unfortunately, I wasn't able to leverage that and make any money. I sold the systems and managed them for Hoyts, Qudos Bank, Centrebet and others, but I'm not terribly good at commercialising.</p>	Timecoin system is unclear.
{Day6/43:25} - {Day6/44:6}	<p>Q. You didn't say, you didn't express in any of the undisputed public documents that we have in the hundreds, you didn't express any interest expressly in digital cash, digital currency or cryptocurrency at this time, did you?</p> <p>A. Firstly, it's not cryptocurrency. While you can build cryptocurrency on top of Bitcoin, Bitcoin isn't.</p>	Dr Wright states Bitcoin is not a cryptocurrency, contrary to Satoshi's position as set out in the Satoshi/Malmi emails.
{E1} First Witness Statement of Dr Wright		
{Day6/50:16} - {Day6/51:4}	<p>Q. But answering the question, it's more than a small circle of people who knew this identity which was not revealed to the world at large?</p> <p>A. Well, it wasn't revealed to the world at large, no, I didn't intend to, but most people who ended up working at my firms knew who I was as well.</p> <p>Q. So not a small circle of people then?</p> <p>A. I'd still call that a small circle of people. They're people I know of. If you're going beyond, into people I don't know, then that's no longer a small circle.</p> <p>Q. All these people, plus unnamed students and people in the Australian government, that's not too small a circle, is it, Dr Wright?</p> <p>A. It's fairly small.</p>	Dr Wright alludes to more people who "knew" he was Satoshi, but none of those people have given evidence on his behalf in these proceedings.
{Day6/51:25} - {Day6/52:15}	<p>Q. You haven't supplied any previously undisclosed communications dealing with the code design before its release, have you?</p>	Dr Wright blames third parties (AlixPartners, Greg Maxwell) for

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Actually, I have. I've discussed them multiple times. I've now given them over, but most of my stuff I keep in written format, which you don't like, because I use handwriting.</p> <p>Q. No communications, no emails or anything like that?</p> <p>A. As I've noted multiple times, after 2015, with the hack, I basically didn't keep a lot of information. That which I did have seems to have been lost in the QNAP debacle that AlixPartners did. I shut down most of my systems believing that I'd been compromised, which I had. Subsequently, I found out that one of the people in COPA, Greg Maxwell, actually compromised my server, so I'll give him that.</p>	<p>“compromising his server”.</p> <p>Dr Wright claims to have discussed undisclosed communications dealing with pre-release code “multiple times” and to have handed those communications over, without providing any evidence.</p>
{Day6/52:16-24}	<p>Q. Just let's get this clear. I think in a recent statement you referred to having been hacked ten times. Is that the right number, or should we say more or less?</p> <p>A. I don't know. It's at least that. There's the time, as Satoshi, I got hacked on GMX, got hacked on Vistomail; there were multiple vulnerabilities in Bitcoin that most people didn't know about, I discussed some of these in August to October with Gavin, that's part of how Gavin knew who I was.</p>	<p>Dr Wright is blaming third parties (hacking).</p>
{O2/11/11} Wright evidence in Granath		
<p>{Day6/55:20} -</p> <p>{Day6/56:13}</p>	<p>Q. Let's see what he says {C/7/2}, paragraph 7 of his witness statement: "At no point did Satoshi ever send me any source code or software. The first time I found out about Bitcoin source code or software was when it was announced on the mailing list mentioned above, and I downloaded it myself from bitcoin.org." That's what he said in his witness statement, isn't it?</p> <p>A. Yes. I -</p> <p>Q. That's correct, isn't it?</p> <p>A. No, it's not. What he's saying is, "I downloaded it myself", which I said. I was the person who forwarded it to the mailing list and the communications he had were in 2009. So he downloaded what I sent in 2008, he also discussed the code in 2009. Now, what you're trying to say is because he didn't get emailed code when it was in an SVN server subversion, then that's the same thing. It is not.</p>	<p>Dr Wright is not accepting the obvious truth recounted by Mr Trammell in his witness statement regarding his download of the Bitcoin source code (noting that Trammell's evidence was accepted unchallenged).</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day6/56:21} - {Day6/57:12}</p>	<p>Q. And Mr Trammell did not receive any special direct communications for Satoshi about this code; he saw it on the general mailing list and downloaded it. That's completely different, isn't it, Dr Wright?</p> <p>A. No, actually, again, you're trying to twist words. He saw the 2008 mailing list announcement. SourceForge is the SVN, you download it from there. The email said you go to SourceForge to download it. So, when I send someone a link to SourceForge, I'm sending them a link to the code. That's how it works. Now, in 2009, he communicated with me about issues. So what you're trying to say is, because he downloaded my code from my site, that therefore I didn't send him code. Again, that's incorrect. On top of that, he didn't help me code, what he did was he questioned me and I sent responses. So, my answer is completely accurate.</p>	<p>Dr Wright is not accepting of the obvious truth regarding who he supposedly sent the Bitcoin code to.</p> <p>On the basis of what Dr Wright says here, everyone who downloaded the code from SourceForge should have been listed in his Granath testimony.</p>
<p>{Day6/57:13-22}</p>	<p>Q. Dr Wright, of the three people you identified in Granath who received code, two, Dillinger and Finney, were in the public domain, and the third, Mr Trammell was a lie; correct?</p> <p>A. No, it's misrepresenting. Once again, saying I didn't get code, well, actually, you did. I sent you the link, because I sent it out to everyone there, you downloaded from SourceForge, you got my code. So when I send someone a link to SourceForge, I've sent someone my code.</p>	<p>Dr Wright is not accepting the obvious truth regarding who he supposedly sent the Bitcoin source code to.</p>
<p>{L5/154/1} - Malmi emails</p>		
<p>{Day6/61:7-25}</p>	<p>Q. Dr Wright, I'm not going to get into a debate on something which is clear on the printed page, but I'm going to return to the question that I actually asked you and ask you for the courtesy of an answer. The word "MinGW", in the context of writing this code, did not appear in any of your statements or pleadings until you had read Mr Malmi's emails, did it?</p> <p>A. Again --</p> <p>Q. The word?</p> <p>A. I don't know. But what I stated, very categorically, was "Visual Studio". And now, if you actually look on the face of this, it says "Visual C++". Visual C++ runs inside Visual Studio. So where I'm saying "I only used VC for debugging" that still means, in this, I haven't said "Visual Studio", but I'm running it.</p> <p>Q. Well, the court can reach its own conclusions on the consistency of what you are saying, what you have said in</p>	<p>Dr Wright is evasive and not accepting the obvious truth of the words used in emails with Mr Malmi.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	your initial pleadings and witness statement, with what Satoshi said on the printed page.	
{E1/16} First witness statement of Dr Wright		
{Day6/62:6-15}	<p>Q. You haven't identified here, have you, or anywhere else, any individuals with whom Satoshi communicated whose names had not previously been in the public domain, have you?</p> <p>A. No, I don't recall names. Like before, when you were asking me on my supervisors, who I deal with every month, some of them on a weekly or daily basis, I don't recall their names. So, you're asking me who my supervisors are that I've dealt with for five years now and I don't recall their names.</p>	Dr Wright is evasive when questioned on individuals who he supposedly communicated with as Satoshi.
{Day6/63:3-19}	<p>Q. You've never, for example, mentioned communications with Nick Bohm, who exchanged quite a large number of emails with Satoshi and who was one of the very few to whom Satoshi actually transferred Bitcoin, have you?</p> <p>A. No, actually, that's incorrect. There were many people. There was a faucet set up by Gavin. I just don't recall who those people were. So there were probably 100 different people that I communicated with at the time, there were several hundred on the forums, at least a third of them DM'd me. No, I never --</p> <p>Q. But Mr Bohm, early on, received an actual transfer of Bitcoin direct from Satoshi and his name never occurred to you in all your efforts to prove your claim?</p> <p>A. No, I transferred to many people that I don't remember, including funding different things. So --</p> <p>Q. None of those people has ever come forward, have they?</p> <p>A. No. And do I remember any of their names? No.</p>	Dr Wright claims to have communicated with 100 different people without providing any evidence of these communications (aside from publicly available records) or demonstrating any knowledge of who they were with.
<p>{C/28/3}, {D/82/1}, {L3/194/1}, {D/78/1}, {L3/193/1}, {D/74/1} Adam Back / Wei Dai Emails</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day6/64:6-25}</p>	<p>Q. {C/28/3}, please. This is an email from Wei Dai responding to questions from Bird & Bird. Point 1 of his email of 14 October 2023: "I'm not a 'distinguished academic' and has actually never worked in academia." That's right, isn't it?</p> <p>A. If he wants to call himself that. I actually looked at what he wrote and he was also author of code for SSL and wrote papers for this, so I would say that's academic, whether you work in a university or not.</p> <p>Q. Normally referring to somebody as a "distinguished academic" suggests that they've held some post in academia, doesn't it, Dr Wright?</p> <p>A. No, it would mean research and development.</p> <p>Q. So anyone who's written code which you approve of you would refer to as a distinguished academic?</p> <p>A. No, not just code I approve of, it would also mean papers, and Wei wrote extensively on SSL, he developed many of the libraries that were opened and the ones in Bitcoin, so...</p>	<p>Dr Wright is not accepting the obvious truth regarding Satoshi's communications with Wei Dai and refusing to accept that Wei Dai was not a distinguished academic.</p>
<p>{Day6/65:1} {Day6/68:5}</p>	<p>- Q. Back to your witness statement {E/1/19}, paragraph 93, you say this: "Adam Back was known for his work on Hashcash ..." Then you refer to what that is: "He showed little interest in Bitcoin. His attitude was quite dismissive; he stated that digital cash had been attempted before and was bound to fail." That's referring to communications between Satoshi and Dr Back, isn't it?</p> <p>A. It is.</p> <p>Q. {D/82/1}, please. I have a C reference if it's easier. C00002547. No. {D/82/1}. {L3/194/1}. Now, this is an email exhibited by Dr Back, and we see, at the bottom of the page, Satoshi's email to him on August 2008 asking about the citation, and Dr Back responds: "Yes citation looks fine, I'll take a look at your paper. You maybe aware of the 'B - money proposal ..." And so on. Do you see that email?</p> <p>A. I do.</p> <p>Q. And then next {D/78/1} {L3/193/1}, for which I think the reference is C00002544. After the email we looked at earlier, on 21 August from Satoshi thanking Dr Back for the reference to the b - money page, Dr Back writes, at the top of the page: "Sorry still not read your paper yet, but another related paper is by Rivest et al called micromint, which uses k - way collisions to create an over - time computational advantage for the bank in creating coins. What you said about one group of players having an advantage (by compute cycles) reminded me of micromint. In micromint the bank gets an increasing advantage over time as there is some cumulative build up of</p>	<p>Dr Wright is not accepting the obvious truth regarding Satoshi's communications with Adam Back.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>advantage in terms of the partial results accumulated helping create further the partial - collisions more cheaply." Do you see that?</p> <p>A. I do.</p> <p>Q. And then the final email {D/74/1}, which is C00002540. {L4/162/1}. This is Satoshi's email, which I think we looked at last week, of 10 January 2009, expressing gratitude to Dr Back and pointing him to the open source implementation of Bitcoin, yes?</p> <p>A. It is.</p> <p>Q. Now, those are the email communications between Satoshi and Dr Back?</p> <p>A. Not all of them.</p> <p>Q. Well, Dr Back wasn't dismissive at all, was he?</p> <p>A. Oh, completely. He said he hasn't read my paper, and he still didn't later, and he pointed out to other failed attempts and basically fobbed me off going, "Look, other people have tried it".</p> <p>Q. He doesn't say that in any of these emails, does he?</p> <p>A. He actually does. Micromint was an old system that everyone in the industry knew that failed for certain reasons.</p> <p>Q. You say in your witness statement: "... he stated that digital cash had been attempted before and was bound to fail." That doesn't appear in any of these emails, does it?</p> <p>A. No, he hasn't included all of the emails, and he also hasn't included the extensive communications that himself and I had on Twitter and direct messages.</p> <p>Q. But presumably they're not communications you're fortunate enough to have in any copies anywhere?</p> <p>A. No, because all of my Twitter was shut down by a certain COPA member, Mr Dorsey.</p> <p>Q. Put aside your allegations for a moment and answer the questions.</p> <p>A. It's not an allegation. My Twitter was shut down by Jack Dorsey personally, and I was banned for a time until X - well, Twitter was sold and then I was allowed back on. I was completely banned from that platform, I'm completely banned from LinkedIn, where other COPA members are involved, and don't have accounts on them. So I was kicked off that platform and I don't have any of the communications. Of course, some of those are public and in the Wayback</p>	

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Machine, so talks with Adam Back are available demonstrating that I was communicating with him.</p>	
<p>{Day6/68:6} - {Day6/70:3}</p>	<p>Q. Well, I'm going to suggest to you that as Dr Back says in his witness statement, he provided his communications with Satoshi and that you are simply inventing the supposed additional communications where he said things which are flatly inconsistent with his actual emails.</p> <p>A. No, but I'll also suggest that what I've been calling it a chain of hash based proof - of - work, etc, is exactly what I've been calling it, which wasn't publicly known. On top of that, Adam didn't go on the forum, didn't connect to anything, didn't try out any of the system, didn't even read the Bitcoin White Paper, despite my giving it to him, which he did announce and discuss with me, both publicly and privately in '12, '13 and '14. He put that on his Twitter --</p> <p>Q. So when Dr Back says that he's provided a complete set of his email correspondence, he's lying?</p> <p>A. Or he's lost them.</p> <p>Q. He says in his witness statement of these emails, that was the extent of it, and that he's provided a copy of his email correspondence.</p> <p>A. This morning, yesterday and the day before, he also promoted to people that Bitcoin will go up in price and that if you buy now you'll get rich. He has never promoted an actual solution. The only thing that he does every single day on his feeds and promotion is to tell people to buy into a Ponzi, "if you buy BTC, it will go to the moon and you will get rich", that is a quote from one of his things. Technically, that's actually a breach of the financial services legislation, and</p>	<p>Dr Wright asked about Satoshi's email communications with Dr Back. Rather than answering the question, Dr Wright responds by making multiple (unsubstantiated) accusations against Dr Back.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>telling people to buy into a risky asset is not only highly irresponsible, but also criminal. So, where he is saying these things, the only thing he says is about "get rich quick, buy into this, it has to go to a million".</p> <p>Q. Dr Wright, how was that an answer to any of my questions?</p> <p>A. Well, if you're going to be dishonest in selling to people and getting people to buy into a highly speculative asset ... he told people online -</p> <p>Q. Pause there. Pause there. None of this is an answer to any of my questions, is it?</p> <p>A. Actually, yes, it is -</p> <p>Q. These are just allegations against people you don't like, aren't they, Dr Wright?</p> <p>A. No, actually, on his Twitter, where he said, "Sell your house, take out a mortgage, put all the money into Bitcoin because you can't lose it" --</p>	
<p>{L14/482/1} - April 2019 Article by Wright with reference to Toumas Aura (C00001010)</p>		
<p>{Day6/71:3-6}</p>	<p>{Just answering this question and keeping it to this question, when you refer to "the Aurora paper", do you intend to refer to a paper by Tuomas Aura?</p> <p>A. Yes.</p>	<p>Dr Wright is mistaking Professor Aura's surname for "Aurora".</p>
<p>{L3/231/1} Bitcoin White Paper</p>		
<p>{Day6/72:25} - {Day6/73:24}</p>	<p>Q. {L13/492/1}, please. Page 2, please {L13/492/2}. Do you recognise this as a long article written by Andrew O'Hagan called, "The Satoshi Affair"?</p> <p>A. No, I recognise a fiction book.</p> <p>Q. Page 24, please {L13/492/24}, the quotation near the top: "We all have a narcissistic hubris', Wright told me. He wanted to take May's BlackNet idea further. He was also enthusiastic, in those early days, about Hashcash and B - money. The idea behind Hashcash, a 'proof - of - work' algorithm where each of a group of computers performs a small task that can be instantly verified ..." Then there's a short explanation in brackets: "... was 'totally necessary for the building of bitcoin'. Wright said that he spoke to Adam</p>	<p>Dr Wright is not accepting obvious truth of the account given in The Satoshi Affair.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Back, who proposed Hashcash in 1997, 'a few times in 2008, whilst setting up the first trials of the bitcoin protocol.'" Did you say that to Mr O'Hagan as he quotes you saying?</p> <p>A. No, not as he's quoted, no.</p> <p>Q. So he's another person misrepresenting your words, is he?</p> <p>A. There's a reason the book is listed as fiction, not non - fiction.</p>	
<p>{L8/272} COIN - EXCH PTY LTD paper provided to ATO in 2013</p>		
<p>{Day6/74:9-16}</p>	<p>Q. Page 4, please {L8/272/4}. Does it state, at paragraph 3.1, that: "The proposed e-Wallet System ..." Covered by the paper: "... is based on the utilisation of a crypto-currency called 'Bitcoin'." Does it say that?</p> <p>A. Yes. I hate how staff keep putting that term in.</p>	<p>Dr Wright is blaming third parties (his "staff") for using the word "crypto - currency".</p>
<p>{Day6/74:17} - {Day6/75:6}</p>	<p>Q. Page 15 {L8/272/15}, appendix of key terms. The definition of Bitcoin: "Bitcoin is a crypto-currency where the creation and transfer of Bitcoin is based on an open-source cryptographic protocol that is independent of any central authority." That was stated in your company's document as well, wasn't it?</p> <p>A. Yes, it was.</p> <p>Q. And, "Bitcoin Mining" is given this definition: "To form a distributed timestamp server as a peer-to-peer network, Bitcoin uses a proof-of-work system similar to Adam Back's Hashcash ..." And so on?</p> <p>A. Yes.</p>	<p>Dr Wright makes an admission regarding definition of "Bitcoin" in C01N-Ex Paper.</p>
<p>{Day6/75:7-14}</p>	<p>Q. That's how you presented Bitcoin, as its concepts, through your company to the ATO in a document you forwarded, isn't it?</p> <p>A. No, I forwarded the document. I didn't produce it. I still have this problem. People keep putting "cryptocurrency" in patent filings, they keep -- I've actually, multiple times, said we're not to use that term and it keeps getting out there.</p>	<p>Dr Wright not accepting the obvious truth regarding use of term "cryptocurrency" in his documents.</p>
<p>{Day6/75:15} - {Day6/76:2}</p>	<p>Q. So do you say that you submitted this document to the Australian Tax Office without having checked it and made these changes which are, you say, critical to your philosophy?</p> <p>A. Firstly, my EA had access to my email. So, when it's not RCJBR, most of these things were actually submitted on my behalf. And, secondly, yes, I keep saying that I have patents even filed today, despite the fact that I keep complaining to</p>	<p>Dr Wright is blaming third parties regarding documents submitted to the ATO.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	everyone, "Don't you put the term, damn well, 'cryptocurrency' in them". Only two weeks ago, I had that same complaint, even though I'm sitting here going, "Don't call it cryptocurrency".	
{L15/88“1}, Wright’– "Fully Peer-to-Peer" article, 6 June 2019 v {L19/209/11} Wrightson email		
{Day6/81:3-22}	<p>Q. But your article, which we've read at some length, was very clear that your dealings with them were in the context of your postgraduate work from 2005 to 2009, wasn't it?</p> <p>A. Yes, I went through all of the MoneyLab areas at that time.</p> <p>Q. It's very clear from reading those passages that you were saying in your article that you had dealt with Professor Wrightson, and had all these stimulating discussions with him, in the context of and during your 2005 to 2009 degree. That's perfectly clear, isn't it?</p> <p>A. I'm sorry if it's perfectly clear for you, but it's not. One, I'm not good with remembering people. The funny thing is, when it comes to code, when it comes to other things, I have a near eidetic memory; when it comes to people, I don't; I don't even remember faces very well. But when it comes to recalling people, I'm horrible with it. I did have communications with him, I know that they were valuable to me, more than that I can't say.</p>	Dr Wright provides an evasive answer when presented with his prior, clear comments regarding his interactions with Professor Wrightson.
{Day6/81:23} {Day6/82:6}	<p>Q. You wrote an article in which you dated these communications very specifically to your 2005 to 2009 period of doing the MStat degree. You are now saying that you think you just got all that wrong and that it must have been communications on an entirely separate occasion, ten years previously, yes?</p> <p>A. Actually, I don't know. I know I spoke to him many times, but, no, when it comes to time and people and dates, or people generally, I don't recall very well.</p>	Dr Wright is not accepting of the obvious truth about the timing of his interactions with Professor Wrightson, which contrasts with the fact that he recalled well enough to write the article in 2019.
{Day6/82:7} {Day6/84:20}	<p>Q. Let's see further down the page. Professor Wrightson has - claims that he has no recollection at all of meeting you or dealing with you. Does that surprise you?</p> <p>A. No. Professor Rayner, who was my supervisor for a year, was contacted by the lawyers, and they said, "We'd like to speak to you about Dr Wright". His comment immediately was, "I don't recall Craig at all", and they said, "But you just said 'Craig'", and they went, "No, forgotten him". So, I have</p>	<p>Dr Wright not accepting of the obvious truth regarding how Dr Furche characterises his own papers.</p> <p>Dr Wright claims to get people wrong all the time, yet he has produced the names of</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>this effect on people. Either people like me or they want to forget me.</p> <p>Q. Professor Wrightson also says that his department did not have lots of resources, as you suggest, had no patents or papers on transfer instruments, as you suggest, that the paper which you hyper linked to the document, to your article, wasn't authored by anyone in his group, and that he would not have known about any problems of previous digital payment systems, which you say he told you about. Does any of that surprise you?</p> <p>A. Yes, actually, because he has a book and he notes it all, and he has students that researched this. It makes it really difficult for me to believe that someone would be able to say that they have no knowledge of other papers when they're marking students.</p> <p>Q. So do you disagree with him when he disputes what you say about his department having lots of resources?</p> <p>A. Define resources. I think access to papers is lots of resources. If you --</p> <p>Q. Do you dispute --</p> <p>A. -- mean lots of computers, then, probably, but I thought they had a lot of access to material I could use.</p> <p>Q. Do you dispute what he says when he says that they didn't have any patents, contrary to what your article says?</p> <p>A. Actually, Furche does. So, some of the members of the people there do.</p> <p>Q. You dispute what he says when he says that they don't have any papers on transfer instruments?</p> <p>A. Well, yes. His own papers are transfer instruments. So, when he's talking about a digital cash system that he has his name on, I would call that a transfer system.</p> <p>Q. So he's wrong in characterising his own work, is he?</p> <p>A. If he's going to say it's not a transfer system, then, yes.</p> <p>Q. Is he wrong in saying that the paper that was hyperlinked to your document wasn't authored by anyone in his group?</p> <p>A. It's possible. I could have got that wrong. I thought it was.</p> <p>Q. Then at (c) he says he didn't, and in fact still doesn't know who Wei Dai is and has never heard of the paper he supposedly referred you to. Do you find what surprising?</p> <p>A. No. As I said, I'm terrible with names and people, but I still believe it was Professor Wrightson I spoke to.</p>	<p>all the people he gave the BWP to. He later accepts that he could be wrong, but only after extensive questioning.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. So your confident assertion in that paper, and 149 the anecdotes about Professor Wrightson pointing you to Wei Dai and discussing Wei Dai with you, that could be wrong?</p> <p>A. Oh, definitely; I get people wrong all the time. I've gone up to people I should know very well and called them the wrong name many times; I do it at work all the time. I have partial aphasia, which means I don't actually recognise faces properly, so --</p>	
<p>{Day6/85:9-23}</p>	<p>Q. I'll come to that in a moment. He also says - we can take this document down. He also says in his witness statement that he's never heard of Hal Finney, with whom - about whom you supposedly had discussions with him. Is he wrong about that?</p> <p>A. I don't know. As I said, I'm not good with people, and I could have had it wrong, but I don't think I am.</p> <p>Q. He also agrees with Professor Wrightson that the group didn't have a lot of resources, that it never lodged a patent application and that he doesn't recognise the patent paper hyperlinked to your article. Do you accept he's right on those points?</p> <p>A. Yes. I could have got the wrong person and linked the wrong area. I'm not denying that.</p>	<p>Dr Wright appears to accept that he could have been wrong about the discussions he says he had with Professor Furche.</p>
<p>{Day6/85:24} - {Day6/86:16}</p>	<p>Q. An awful lot of mistakes in your blogpost now, aren't there?</p> <p>A. I told you, when it comes to people, I'm terrible. This is the whole thing. When it comes to numbers, code, writing things, a predicate system, I'm great; when it comes to interacting with people ... This is why I work from home, this is why I hide away from the world, this is why I don't interact, why you're asking me about all these people I'm supposed to remember.</p> <p>Q. But you do dispute Professor Furche's claim not to recall you, don't you?</p> <p>A. I would find that difficult. I was at the Australian Stock Exchange for a number of years, and the only way I could put it was, I was a gadfly and I was incredibly annoying to a lot of people, including those in seats and other such systems. And some of the other exchanges that he did stuff with as well, I was involved.</p>	<p>Dr Wright is not accepting of the obvious truth regarding his supposed interactions with Professor Furche.</p>
<p>{CSW/1/82} Eleventh Witness Statement of Dr Wright</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day6/86:22 – {Day6/87:7}</p>	<p>Q. You claim that Dr Furche and you worked together on the surveillance systems for the Australian Stock Exchange from '97 to 2003, don't you?</p> <p>A. I worked on those systems at that stage, yes, and I believe he was there, and he implemented those –</p> <p>Q. Professor Furche –</p> <p>A. – systems at that time.</p> <p>Q. Professor Furche's work on the ASX's surveillance systems didn't start until after 2003, did it?</p> <p>A. Well, I still remember him, and I definitely remember him from the Perth Mint.</p>	<p>Dr Wright is not accepting of the obvious truth, that Professor Furche could not have worked on the ASX surveillance system prior to 2003.</p>
<p>{Day6/87:8-18}</p>	<p>Q. So you worked together at Perth Mint in 2005 to 2008, yes?</p> <p>A. No, I was an auditor.</p> <p>Q. "... then had a joint involvement at the Perth Mint, where I was an auditor for BDO (2005 - 2008)." Yes?</p> <p>A. Yes.</p> <p>Q. In fact, Professor Furche's work in relation to the Perth Mint didn't begin until 2016, did it?</p> <p>A. I don't know, but I'm pretty sure it was him there, and I believe he was also involved with Chi - EX.</p>	<p>Dr Wright appears to backtrack on the clarity of his memory of interacting with Professor Furche in the period from 2005 – 2008.</p>
<p>{Day6/88:1-12}</p>	<p>Q. Dr Wright, the reality is that these weren't an extraordinary series of honest mistakes, your whole article about your dealings with these distinguished people was a set of fictions, wasn't it?</p> <p>A. No, not at all.</p> <p>Q. And it was written as if produced with complete confidence when in fact there was barely a true word in it?</p> <p>A. No, that's incorrect. As I said, I get things mixed up, with people, but I do know I had dealings with them. In particular, some of his references to what he does actually overlap with mine.</p>	<p>Dr Wright explains how he mixes up his interactions with individuals. In doing so, he inadvertently reveals the way in which he sees overlaps in his dealings with individuals and elaborates on them to create his version of events.</p>
<p>{L3/252.1.1.1/1} {L3/252.1.1.1/2} - Microsoft Documents</p>		
<p>{Day6/89:20-25}</p>	<p>Page 3, please, at the bottom {L3/252.1.1.1/3}. Bottom of the page, you were in communication, weren't you, with Microsoft and with Siemens, the IT recruitment people, expressing interest in a job in Microsoft's click fraud team?</p>	<p>Dr Wright admits that his interactions with Microsoft were with the IT recruitment</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	A. That's correct.	team, relating to a job in the click fraud team.
{Day6/90:15-18}	Q. And then page 2 {L3/252.1.1.1/2}, at the top, the job was as a programme manager in a Microsoft team combating click fraud, right? A. That's correct.	Dr Wright admits that his interactions with Microsoft were with the IT recruitment team, relating to a job in the click fraud team.
{Day6/95:14} - {Day6/97:9} {L3/252.1.1/1}	Q. And shortly after the interview, Satoshi actually releases the paper, yes? A. Yes, right after the interview, actually days later, I was told that there was a hiring freeze at Microsoft. Q. And yet there is not a shred of evidence in any of these emails that you showed the Bitcoin White Paper to Microsoft, whereas there is plenty of evidence in the emails that you showed Microsoft some of your other work, isn't there? A. No, there's very little here actually. This is only a work email. The majority of my communications were done on my private emails, on Ridge Estates, so as you might guess, I tried to minimise any emails to and from the work domain. Q. But in this interview process, which you told the court in Granath might have led to Microsoft owning this invention of yours, there is not a mention of it, is there? A. No, because you don't have those. You only have the interviewer ones. What you'll notice is none of the communications between the Microsoft individuals that were done on the Ridges Estate email and myself were there. In the intervening period, I talked to a number of people in the advertising and what is now Bing area. In the communications, I explained that if we could implement a small proof - of - work fee, this would remove any incentive for people to scam the system. Now, one of the things, if you actually read Adam Back's - I'll even quote his, he talks about proof - of - work as a means of stopping spam and - - Q. Can I pause you there, because I asked you a specific question. During the course of this entire exchange, this entire interview process, which you have said could have resulted in Microsoft owning the system which you had developed - you claim to have developed, you never mention the system at any point in any of the documents in any of the communications we have, do you? A. No. As I stated, I only have very limited numbers of emails and things left. I have none of the Ridges Estate emails	Dr Wright refers to further interactions with Microsoft / Bing, without having provided any evidence of them. Further, Dr Wright states that he doesn't have any of the Ridges Estate emails to which he refers, despite there being Ridges Estate emails in his disclosure documents, including some which he seeks to rely on in his 11 th witness statement (ID_000039).

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>or any of those other ones. What’s happened over time is I’ve lost those. It’s many years ago. At the time, I wasn’t also sitting there going Bitcoin’s going to be a multi - billion dollar invention. In one of my early notes, I put down that I thought it might get me either a partnership or a professorship with tenure and that was about the extent of what I thought of my invention.</p>	
<p>{L7/471} - Reliance document ID_004018 Notebook with Bitcoin Notes - BDO/Microsoft</p>		
<p>{Day6/98:19} - {Day6/100:17}</p>	<p>Q. Now, this all reads as descriptions of your discussions with BDO and a forthcoming meeting with Microsoft, doesn’t it?</p> <p>A. I continued discussions with BDO. Alan actually ended up, after he’d left BDO, becoming a director, and also the main audit lead at some of my firms. On top of that, Microsoft came back to me in 2011 and I had further communications with them between ’11 and ’12.</p> <p>Q. But the reference to not being able to get BDO in on this, that’s plainly a reference to things going on in 2008, based on your evidence, isn’t it?</p> <p>A. No, it’s not at all.</p> <p>Q. So you’re saying that these in fact came later?</p> <p>A. Yes, this was notes I was making in 2012. This was a preparation document for the AAT, Administrative Appeals Tribunal. I took these notes working as I was also getting everything together for the dispute with the Tax Office and I put down some of the issues with both BDO and Microsoft at the time.</p> <p>Q. You first dated these notes in communications with our side to 2011/2012 in your chain of custody document of October last year, didn’t you?</p> <p>A. No, the first time I dated this goes back to well before that, back to the Kleiman case.</p> <p>Q. It’s the first time you told us that this document had been produced in 2011/2012, isn’t it?</p> <p>A. I don’t know when you were told. All I can say is that I went through all of this with lawyers earlier, and when it goes from the Relativity and disclosure platform to you, I don’t know.</p> <p>Q. So you’re now saying that it was all written in 2011/2012?</p>	<p>Dr Wright appears to accept that notes which purported to date to 2008/2009, are actually notes he made in 2011/12, although refuses to accept that this story was first put forward when he provided his chain of custody information (following service of Ben Ford’s statement).</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Probably more 2012, but, yes, this is my notes as I was preparing for the AAT.</p> <p>Q. You first came up with that story, didn't you, after COPA had provided evidence from Ben Ford of the Datastation company that that form of notepad was not printed until March 2010, didn't you?</p> <p>A. No, that's not correct.</p> <p>Q. And the only explanation for you giving a period of 2011 to 2012 for these notes, despite all their contents appearing to date them to 2008, is that you were reacting to Mr Ford's evidence, weren't you?</p> <p>A. No, actually, I've got a - a note from Ali Zafar where he put down all this stuff and I explained it --</p> <p>Q. I don't want - I don't want - really, I don't want privileged information.</p> <p>A. It's not. He's not my lawyer.</p> <p>Q. If COPA hadn't tracked down Mr Ford, or if he hadn't kindly helped by providing evidence, you would have sat there and quite happily let the court work on the basis that these notes dated from 2008, wouldn't you?</p> <p>A. No, I would not. I was explaining that these were my notes for the tribunal.</p>	
<p>{Day6/100:25} - {Day6/101:25}</p>	<p>Q. "Gareth", at the bottom of the page: "Gareth - UK system - not full time." Is that a reference to Gareth Williams?</p> <p>A. It is.</p> <p>Q. Gareth Williams died in 2010, didn't he?</p> <p>A. He did.</p> <p>Q. That's another reason that your story about these notes coming in 2011/2012 makes no sense, isn't it, Dr Wright?</p> <p>A. No, I had to go in front of the tribunal in 2012 and I took down all of my other notes and put them into a single thing so that I had them all with me. In that, I had been using Clayton Utz up until nearly before the end, but the fees were over \$3 million Australian and when it came to the tribunal, I had to represent myself, so I collated all my own notes.</p> <p>Q. So when you write: "The following people have agreed to run nodes when the system starts." This was actually something you were writing three years later, three years after the system had started, you're saying?</p>	<p>Dr Wright's implausible attempt to explain away his suggestion that he had received notes from Gareth Williams after he had died.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Yes, back - discussing this with the ATO, with the mining of - what I'm saying is all of this was the start of the system and these people have agreed.</p> <p>Q. That's just a set of lies, isn't it , Dr Wright?</p> <p>A. Not at all.</p>	
<p>Release of BWP - {E/1/20} - First Witness Statement of Craig Steven Wright</p>		
<p>Sharing drafts of the BWP - Kleiman Depo: {L17/327/96-97}, {L16/267/36}</p>		
<p>{Day6/106:23} - {Day6/107:10}</p>	<p>Q. Page {L17/327/98}, line 6, you described who you shared that with, and you said Wei Dai, Gareth Williams, people at uni, Allan Granger, Don Lynam, Dave Kleiman, Adam Back and a few others; correct?</p> <p>A. Yes.</p> <p>Q. And before this case, that was the fullest account you'd given of those with whom you'd shared the Bitcoin White Paper, isn't it?</p> <p>A. No, I've mentioned it publicly and in conferences and other such things, so I said "others", but, no, I haven't gone into everything, and I have to think on people relatively hard, I'm not terribly good with names or people at all.</p>	<p>Dr Wright claims not to be good with names, but has given an extensive list of people he supposedly shared the Bitcoin White Paper with 15 - 16 years ago.</p>
<p>{E/4/21} Fourth Witness Statement of Craig Steven Wright - Sharing drafts of BWP</p>		
<p>{Day6/107:11} - {Day6/109:14}</p>	<p>Q. {E/4/21}, please. Now, in this part of your fourth witness statement, you answered a question, didn't you, asking you to say to whom you'd provided pre - publication drafts of the Bitcoin White Paper, yes?</p> <p>A. Yes.</p> <p>Q. And you gave the 21 names we see there under paragraph 49?</p> <p>A. That's correct.</p> <p>Q. Trying to take this shortly, it's right, isn't it , that if these people received drafts of the Bitcoin White Paper, they would have known that that was a project you were working on?</p> <p>A. One of many.</p>	<p>Dr Wright is not accepting the obvious truth regarding the lack of evidence that he shared his Timecoin paper or any other papers concerned with E - Cash prior to the publication of the Bitcoin White Paper.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Now, is it right that, with the exceptions of Stefan Matthews and Don Lynam, none of these 21 individuals has come out publicly, whether in a court or in an article, and supported your account of receiving and remembering the Bitcoin White Paper from you?</p> <p>A. No. As I said, this is pre - - pre - release drafts. This is a different question to the one in the Kleiman trial. They were asking particularly about the 2008, August, one that I sent to Wei Dai and others. Many of the people here received a Timecoin paper. So the pre - draft version of the Bitcoin White Paper is in multiple iterations, and some of them had it as electronic cash, some of them had it as Timecoin with E - cash, some of them had Timecoin. So effectively, they're all pre - release drafts of the Bitcoin White Paper, but they will be different.</p> <p>Q. Is it right to say that, again with the exception of Mr Matthews and Don Lynam, none of these people has come out publicly in an article or in a court proceeding and said that they received from you a draft paper called Timecoin or E - cash before the release of the Bitcoin White Paper?</p> <p>A. I believe David Bridges has, to my knowledge Rob Jenkins remembers Timecoin. Iggy talked about his communications with Steve Aitken where they -</p> <p>Q. Who did, sorry?.</p> <p>A. Ignatius Pang.</p> <p>Q. None of those people has ever come out publicly saying that they remember receiving a paper from you before the release of the Bitcoin White Paper describing E - cash, Timecoin, a digital currency system created by you, have they?</p> <p>A. No, I just answered that. And Shane Patterson also has talked about this. He doesn't - he's not in court or anything, but he's talked about it publicly. Max Lynam has talked about it publicly. Edward Archer and I have had quite a number of conversations on this. Shoaib's talked about it. Neville has. Andrew Sommer won't because, legal privilege, unfortunately. I mean, a number of people have, yes.</p> <p>Q. Which of them has produced - has provided evidence in other proceedings, or these proceedings, saying that they received a draft of the Bitcoin White Paper, whether it was called Timecoin, or E - cash or whatever, before the release of that paper?</p> <p>A. Robert Jenkins talks about the system I built , which was a hash chain based on a genesis file . Let's see, David Bridges, the same thing.</p>	

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Do you say that they describe in their evidence, because we're coming to their evidence, receiving drafts of what would become the Bitcoin White Paper, whether they referred to Timecoin or E - cash, drafts of that paper, before its publication?</p> <p>A. Yes, but you're referring to different things. You're referring - you're mixing up my larger Timecoin implementation and Bitcoin.</p>	
<p>{L16/116/73 - Lynn Wright in Kleiman</p>		
<p>{Day6/113:5 – 9} {L16/116/73}</p>	<p>Q. So she was lying under oath, was she, in giving that account?</p> <p>A. No, I think she was on a lot of medication, as I said. My ex - wife had just gone through breast cancer operations, and she was on a variety of medication.</p>	<p>Dr Wright seeks to discredit the clear evidence given by his former wife by claiming that cancer medication had affected her ability to testify (even though she had expressly been asked at the beginning of her testimony whether she had any impairment).</p>
<p>{E/4/21} Fourth Witness Statement of Craig Steven Wright - Sharing drafts of BWP</p>		
<p>{Day6/115:6-17}</p>	<p>Q. And you could readily, like the rest of the world, pick that up from the press?</p> <p>A. No, I'd already given his name to the ATO before he was dead.</p> <p>Q. There is no evidence whatsoever of communications between you and him during his lifetime, is there?</p> <p>A. Again, I don't have any of the Ridges Estate, Panoptcrypt or other emails.</p> <p>Q. You've plucked his name out of the air as a mysterious collaborator, haven't you?</p> <p>A. No, actually, I put that under a secrecy provision in the US. We had a closed court, but it got leaked.</p>	<p>Dr Wright fails to accept the obvious truth, that he could have known of Gareth Williams' name and death from press reports.</p> <p>Dr Wright states that he does not have evidence of communications between himself and Mr Williams because he does not have emails from his Ridges Estate or Panoptcrypt email addresses,</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
		despite his disclosure containing emails relating to these addresses (including emails he relies on in his eleventh witness statement - such as ID_006524).
<p>{Day6/116:6} - {Day6/117:17}</p> <p>{L15/125/100} Continued videotaped deposition of Dr Craig Wright</p>	<p>Q. Page {L15/125/100}, do you see that you described him as a former MI6 agent and linked also with GCHQ?</p> <p>A. That's correct.</p> <p>Q. You said you had helped train him and he was participating in the call partially as a UK agent?</p> <p>A. Basically, I met him at BlackNet conferences and I was involved with some of his training on digital forensics and tracing.</p> <p>Q. "Was he working in his capacity as an agent for the [UK] Government when he participated in this call with you?" "Answer: Only partially." Yes?</p> <p>A. Yes.</p> <p>Q. And then, towards the bottom, you said that you involved Mr Kleiman in this conversation because you were wanting to clean up everything to do with Satoshi, yes?</p> <p>A. Yes.</p> <p>Q. And of course that dates the call to 2011, when Satoshi was departing the scene, doesn't it?</p> <p>A. No, I started departing the scene in about August.</p> <p>Q. That's convenient, isn't it, because Mr Williams, of course, was found dead on 23 August 2010? Did you have this videocon just before he died?</p> <p>A. No. I get dates wrong.</p> <p>Q. You described what appeared to be a vivid recollection of a video call with a UK Government agent who had been dead for several months before the video call could possibly have been timed, didn't you?</p> <p>A. No, I did not. What I had was a call where I was very, very angry and I was trying not to respond and I was being difficult.</p> <p>Q. Returning - we can take that down. Returning to your sharing of the Bitcoin White Paper, you've never been able, have you, to provide a single email evidencing sharing the Bitcoin White Paper with anyone, have you?</p>	<p>Dr Wright states that he does not have evidence of communications between himself and Mr Williams because he does not have emails from his Ridges Estate or Panopticopt email addresses, despite his disclosure containing emails relating to these addresses (including emails he relies on in his eleventh witness statement - such as ID_006524).</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	A. No. As I said, Ridges Estate, Information Defense and other emails have all been lost. - {}	
<p>{Day6/117:22} - {Day6/118:4}</p>	<p>Q. Which hard copies do you say were the specific hard copies shared with these individuals?</p> <p>A. Oh, I mean, there'd be copies of those. One of the ones I took back from Stefan, so I don't know which particular one is which, but yes, I'd shared them.</p> <p>Q. So you took back a hard copy you'd shared with Stefan, did you?</p> <p>A. Yes, he didn't want it}</p>	<p>Dr Wright claims to have shared a hard copy with Mr Matthews, and taken it back, which is inconsistent with the evidence of Mr Matthews.</p>
<p>{Day6/118:12} - {Day6/119:11}</p>	<p>Q. Not only have you not got any of these emails or hard or soft copies from your own records, none of these 21 people have obliged you by coming forward with their end of the email, or their hard or soft copy from their systems, have they?</p> <p>A. No. As I've noted, it's been over 15 years. Danielle's moved and started her own business, left her own business, been somewhere else; Shane's no longer with Centrebet, it doesn't exist any more, other people aren't, so I don't know about you, but a lot of people don't have 15 - year old emails.</p> <p>Q. You're very unfortunate that not one of the has ever been able to come forward with the emails or a soft copy or a hard copy, aren't you?</p> <p>A. No, actually, they can talk about all of the systems they've seen, etc; they know about Timecoin, they can talk about those systems; and they know about the implemented code and systems that I built for their companies.</p> <p>Q. Well, I'm going to try with the question again. None of 212 them has actually come forward with a hard or soft copy which they say is a pre - issue draft of the White Paper you provided to them, have they?</p> <p>A. No, and I think if they did, you'd just say that it's all false and made up.</p>	<p>Dr Wright is unable to obtain witness evidence from individuals with whom he says he shared a copy of the Bitcoin White Paper.</p>
<p>{E/5/6} - First Witness Statement of Stefan Matthews - Stefan Matthews / BWP sharing</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day6/121:21} - {Day6/122:10}</p>	<p>Q. He's quite specific about receiving a soft copy and printing it out in the printer in his office, isn't he?</p> <p>A. Yes. That would be the Timecoin paper. That's why I said he only became aware of Bitcoin later. That document didn't use the name Bitcoin.</p> <p>Q. I see. So you gave him the Timecoin paper in soft copy and the Bitcoin White Paper in hard copy? That's what you're saying now, is it?</p> <p>A. Probably multiple times for both. I'm probably the world's worst marketer. As you see, the way I even describe this is terrible. I don't - like you're saying: why didn't I market this, where are my colourful PowerPoints? Basically, asked what is this and I go it's a USB stick. I mean, that's about as good at marketing as I get.</p>	<p>Dr Wright describes himself as the “world’s worst marketer” despite having his own website https://craigwright.net/ and his numerous public appearances where he talks about his alleged work.</p>
<p>{Day6/123:9-19}</p>	<p>Q. You gave the story of handing over a hard copy because it would fit with that false document with the notes about - with the coffee stain and the note about, "Stefan - Will Centrebet use a token that's transferable and audited", didn't you?</p> <p>A. No, actually, that wouldn't be a message to Stefan. So, like I said, that wouldn't have been what I gave him. But Stefan had a habit of just dropping my papers in the bin if he didn't want them, so I actually would have used the USB stick just so that there's something that he won't drop in a bin.</p>	<p>Dr Wright explains that he would have given Mr Matthews a copy of the Bitcoin White paper on a USB stick.</p>
<p>Sharing drafts of the BWP - Kleiman Depo: {L17/327/96 - 97}, {L16/267/36}</p>		
<p>{Day6/126:23} - {Day6/127:18} {L16/267/36} 2020-03-16 Wright Complete Deposition with some Exhibits</p>	<p>Q. You were asked: "Did you type that?" And you answered "No, I did not." Now, that was directly opposite to what you had said a year previously, wasn't it?</p> <p>A. No. What I meant by that was I typed a message that I gave to someone else to send. So in the first one, I typed it, but, no, I did not type the email.</p> <p>Q. And page 140, let's see how you explained it there, you said that it was probably written by Angela Demitrio, your executive assistant, yes?</p> <p>A. Either that or one of the other people, yes.</p> <p>Q. Then you went on, at line 20, not saying that you wanted her to write the words because you wanted to make Louis Kleiman proud of his son, but that she got the instruction to write those words from Louis and Uyen or other people; that's what you said on that occasion, wasn't it?</p> <p>A. I wanted a message sent to Louis, but I didn't handle it.</p>	<p>Dr Wright is evasive, refusing to provide a straightforward answer regarding his testimony in the Kleiman proceedings and whether he wrote a message to Louis Kleiman regarding Dave Kleiman's involvement in Bitcoin.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day6/127:22} - {Day6/128:18}</p>	<p>Q. Then line 10: "That is a mischaracterisation. You asked me a particular sentence. You did not say whether I typed that e - mail. You said a particular sentence - literally one sentence in this e - mail ... 'did you type that'. In discussions with my lawyers, I typed that exact sentence." And then, at line onwards: "Without going into the discussions ... I just need to formulate how I said it without saying my discussions - I had pointed out evidence that my lawyers - I keep hitting discussion points. I discussed that sentence and I typed that sentence. I did not type the whole e - mail." And then you refer to being over - literal. Your account, on that occasion, was that you'd typed the sentence, but in a communication with your lawyers about talking points, yes?</p> <p>A. Like I've just been saying, I typed the sentence, I didn't type the email. I had instructed people to send messages, but I was an executive at the time, and, no, I didn't overlook every single thing that got sent.</p>	<p>Dr Wright is evasive, refusing to provide a straightforward answer regarding his testimony in the Kleiman proceedings and whether he wrote a message to Louis Kleiman regarding Dave Kleiman's involvement in Bitcoin.</p>
<p>Patch Tuesday - {L14/420/2}</p>		
<p>{Day6/135:11} - {Day6/136:3}</p>	<p>Q. So your story, if I have this right, is that Genesis Block is mined, and then Microsoft's regular security update on Patch Tuesday causes the machines to crash, and then you addressed the problem before 10th January by building a domain; correct?</p> <p>A. No, I already had a domain. I hadn't had the Windows XP machines on the domain. So what we're talking about there is, I had a domain but I needed to integrate these systems. What you'll note in the first interview is I mentioned the WSUS system. WSUS is the Microsoft patching server. So I wasn't doing like normal home users do and running, just patching from downloads from the internet. What I had was a patch consolidation system at home. So, WSUS doesn't also - when I say "Patch Tuesday", that's what it's known, but when you're running WSUS, it doesn't run on Tuesday, necessarily, and it doesn't have the patches the way that you're saying the same way.</p>	<p>Dr Wright claims that he received patch updates from Microsoft on a different day to "Patch Tuesday" but provides no evidence for this.</p>
<p>{L14/420/2} - Two steps forward, one step back - Blog post on medium posted 6 April 2019</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{Day6/136:10-23}	<p>Q. But in the course of these, the interview and this blog, you're referring to a problem that occurs to shut things down between 3 and 10 January 2009, aren't you?</p> <p>A. Yes, my systems did an update.</p> <p>Q. You describe that, don't you, the cause of the problems at that time, between the 3rd and the 10th, as being Microsoft Patch Tuesday, don't you?</p> <p>A. Yes, that's what it's referred to in the industry. But when you're running a WSUS server, as you'll note on the first interview that you noted, if you want to go back to that, what you see is WSUS is the Microsoft local patch server. So, WSUS isn't that I'm pulling patches from the internet like most people, it is that my server does it on my schedule.</p>	<p>Dr Wright contends that he had issues with system updates between 3 - 10 January 2009, which were updates that were run on his schedule, and which he continues to refer to as "Patch Tuesday" despite the fact that the January Patch Tuesday occurred after this timeframe.</p>
{Day6/137:3-17}	<p>Q. Patch Tuesday, in January 2009, took place on Tuesday, 13 January 2009, didn't it?</p> <p>A. I don't know. What I do know is I had a WSUS server. So WSUS does it on the schedule that I implement.</p> <p>Q. {L4/60/1}, please. This is referring to Microsoft Patch Tuesday for January 2009 and describing it as taking place on 13 January 2009, which I can tell you is a Tuesday. Do you see that?</p> <p>A. Again, what you're missing at the bottom is their Windows Update, WU, is different to Windows Server Update Services. Windows Server Update Services, which I have mentioned in each of those areas in my witness statement as well, is separate to Windows Update. Home users do Windows Update; servers do the other.</p>	<p>Dr Wright claims that Patch Tuesday updates were done on his time schedule, despite "Patch Tuesday" occurring later.</p>
<p>{L4/262/1} It's Windows Patch Tuesday - Jan 2009</p>		
{Day6/138:2-9}	<p>A. Again, what you're doing is mischaracterising. It is a term for the patching. Patch Tuesday references Windows Update, WU. I specified WSUS. Now, everyone in the industry just calls it "Patch Tuesday". Now, when you have your patches released, it can be over a weekend, it can be on a Thursday, it can be whatever. With WSUS, the server system is configured however you configure it.</p>	<p>Dr Wright claims that patches could be released other than on the second Tuesday of each month, which contradicts the account of Patch Tuesday given in his own evidence (his eleventh witness statement, {CSW/1/200} para 1159) where he confirmed that it occurs on the second,</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
		and sometimes fourth, Tuesday of each month.
{L4/60/1} Microsoft Patch Tuesday for Jan 2009 _ one bulletin		
<p>{Day6/138:10} - {Day6/139:14}</p>	<p>Q. Back to the previous document {L4/60/1}, and if we can put on screen both page 1 and 2 together, please, if that can be done {L4/60/2}. Now, we can see that, at the bottom of the page 1, Microsoft indicates what Microsoft is planning to release on Patch Tuesday, and that includes updates for both Windows Update and Windows Server Update Services, WSUS: "This information is subject to change by Patch Tuesday ..." It's all happening, including for WSUS, on that single Patch Tuesday on 13 January 2009, isn't it?</p> <p>A. No, actually. What you're again missing is the Microsoft Developer Network. Now, I was teaching Microsoft products at Charles Sturt University and I was actively part of the Microsoft Developer Network, MSDN. As an MSDN sort of registered person, not only do I have access to a whole lot of their products, but I have pre - release. So, all of these are pre - tested. So Microsoft Patch Tuesday goes out to individuals in the MSDN network first. Not only that, but even source code for Microsoft. I mean, ironically, people think Microsoft is not open source; it is, if you're signed up. So, first thing happens, internal testing, beta test. Second thing happens, goes out to the MSDN network, including myself. Third thing happens, it goes out to wide, broadcast to everyone. So, again, when you're saying Patch Tuesday, you're presuming that I'm just one of the every day plebs out there and not in the MSDN network.</p>	<p>Dr Wright is evasive, now claiming that he was part of the Microsoft Developer Network, which is not something he has referred to previously and not something he has provided any evidence to support.</p>
{E/1/122} - First Witness Statemen of Craig Steven Wright		
<p>{Day6/141:15} - {Day6/142:5}</p>	<p>Q. And you say that you were - that they were operating a node from Don's farm while you were at the same time running mining operations from systems you had set up, including computer systems in 69 racks, right?</p> <p>A. No, I said 69 systems. What that would actually be would be two external other systems, 67 Windows machines, and they were structured with Virtual Machines, Citrix, etc. I've explained all of that. So the two machines that aren't part of</p>	<p>Dr Wright is evasive in relation to the number of racks or systems he was operating, even where the details themselves are unimportant.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>this are Solaris, but the other machines are Windows and Virtual.</p> <p>Q. Well, you disputed my description of them as computer systems in 69 racks, but that's exactly what your statement says, isn't it?</p> <p>A. That's a typo. It's 69 computers in racks. It should be.</p> <p>Q. I see.</p>	
<p>{Day6/146:20} - {Day6/147:18}</p>	<p>Q. Now, I'm putting this to you on the basis of the expert evidence of Professor Meiklejohn. It wouldn't have been necessary to run a set up of this magnitude to mine Bitcoin in 2009 or early 2010, would it?</p> <p>A. Of course it would. Ms - Professor Meiklejohn is misrepresenting Bitcoin mining and nodes. Section 5 of the White Paper doesn't say that you solve hashing. Now, hashing is only one small component. The majority, at a low level like that, is actually validating ECDSA. ECDSA is a far more computationally intense process than hashing. So what we need to do is actually go through validation of blocks, checking, later running testnet as well, and ensuring that all of that process happens before you distribute the block. On top of that, I had to run multiple systems. Bitcoin was configured so that on a single C class, and I had a C class in each area, the 256 IP addresses in V4, or more in IP v6 would only act as a single node on the network. So even if you had 30 machines on a single location, they only broadcast as one node on the network. Now, that allowed me to have multiple systems, including the logging systems and the rest of the Timecoin server. All of that together was really the cost that I experienced.</p>	<p>Dr Wright's contention that the majority of computational power in the early days of Bitcoin was used validating ECDSA is incorrect. Even today, miners spend more computational power on hashing, rather than verifying transactions, a point that was accepted by his own expert Mr Gao during cross - examination {Day18/60:10-12}.</p>
<p>{Day6/147:25} - {Day6/150:1}</p>	<p>A. I did, because I was running the majority of the network. Other people wouldn't, because they came and went. Now, during 2009, there were periods where there was weeks with no one else other than myself and my familiar mining, and by weeks, I mean weeks. It dropped off totally. So, it was like, towards the end of 2009, there was a complete black period, and to give the sort of node security enough, I had to keep running up more and more servers. Over this time frame, people would try and drop off, and without those people staying and continuing to act not just as a home user, but with an intention to run a system, it wouldn't work. So -</p> <p>Q. And what is more, putting computing power on this scale onto the network would have increased the difficulty level of the target hash for the proof - of - work beyond what it actually was at the period of time, wouldn't it, Dr Wright?</p> <p>A. No, that's a drastic misunderstanding of how Bitcoin works. So like I said, if you have two different areas, in fact</p>	<p>Dr Wright's contention that the bitcoin network was running constantly is incorrect. See Meiklejohn 1, paragraph 77 {G/2/32}.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>what you're only going to get is one of those will act as the mining node. We didn't have a pulled system back then, so only one would act as the major player. However, what you could do is distribute everything. So you have a collection of logs, like I did, you could have all of that bundled and being signed into a binary tree structure, that could be built into the ECDH structure that I used in keys, all of that takes up a lot of processing power. So, the distinction here is, if you're going to be a casual miner, not caring, versus someone who needs the network to be available by 7 - and Bitcoin was, so most operators on the Bitcoin network came and went, they connected a laptop, they turned it off every now and again. Even Hal Finney turned it off after a while, it got too hot. I didn't have that luxury.</p> <p>Q. Dr Wright, it's simply wrong to say that operating a regular node and doing the amount of mining that was called for at that time would have required this volume of electricity.</p> <p>A. No, actually, it doesn't take that much to chew up a lot of electricity, especially server machines. Now, you also need to remember that you don't just have a laptop. Now, when you're running a server machine, my Lord, you have routers, you have switches, you have back up servers, you have UPS, you have air conditioning. This is part of it, I had to have the machines air conditioned as well. So, if I was to sit there going, "Yes, I'm just running my laptop", yeah, that would be true, but then Bitcoin would have gone down. Bitcoin had 100%, and I mean not 99.999999, 100% availability from the 12th on, because my machines sat there the whole time in multiple locations.</p>	
<p>{L15/96/59} - SatoshiVisionBook}</p>		
<p>{Day6/150:8} - {Day6/151:10}</p>	<p>A. It is.</p> <p>Q. Page 59, please {L15/96/59}, the last paragraph: "Far too many people fail to understand what I said. At no point have I said that Bitcoin is a cryptocurrency ..." Right? Did you write - just for the moment, did you write that?</p> <p>A. I wrote the original thing that went into the blog that got taken and put in the book.</p> <p>Q. Do you endorse what is said there?: "At no point have I said that Bitcoin is a cryptocurrency ..."</p> <p>A. Not fully. I try and shy away from it. I have said it, and I have been lax on the term. At times, I'm more draconian than others, but even now, some of our patents just last week went</p>	<p>Dr Wright's suggestion that Satoshi wouldn't have thought about what 'cryptocurrency' means is implausible, especially with the context of Satoshi's emails with Mr Malmi on the subject.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>out saying "cryptocurrency". So I get the term from people and I don't - sometimes I get upset, and others I don't.</p> <p>Q. {L18/121/1}, please, page 50 {L18/121/50}. Towards the bottom of the page, if we can blow it up. A Slack post by you: "Bitcoin is not a Cryptocurrency." You've made this point very many times, haven't you?</p> <p>A. Yes. Originally, when I released Bitcoin, I noted that "cryptocurrency", well, sounded cool, but I hadn't really researched the distinction, and that was pre - Silk Road. So I didn't crack down on it too hard at that point. After 2013/14, I've been very hard on the term.</p> <p>Q. {L5/196/1}, please.</p>	
<p>{L6/193/1} - 0.3.0 released</p> <p>{O2/11/24} - Transcript of Craig Wright Evidence from Granath Proceedings</p>		
<p>{Day6/152:6} -</p> <p>{Day6/153:4}</p>	<p>Q. May we have on screen {L6/193/1}. Now, this is a previously unpublished email exchange between Satoshi and Martti Malmi, 6 July 2010, so the same date, which reads, from Satoshi: "I uploaded 0.3.0 beta to sourceforge and updated the links on bitcoin.org. I still need to post the announcement message on the forum and mailing list. Here's what I've prepared: "Announcing version 0.3 of Bitcoin, the PGP cryptocurrency!" It's right, isn't it, that Satoshi stated that they had prepared that post telling Mr Malmi that that was the case, right?</p> <p>A. No, what I did was I took what Mr Malmi originally wrote and I prepared that. So, the original used the terminology earlier, and then I put in what he put.</p> <p>Q. You have repeatedly said, haven't you, that the post was written by Mr Malmi? You've been quite emphatic about it, haven't you?</p> <p>A. As I said, if you go back into his other emails, you will find that he originally wrote some of this stuff for the page, etc -</p> <p>Q. Focusing -</p> <p>A. -- I, for the announcing part.</p>	<p>Dr Wright is not accepting of the obvious truth regarding Satoshi's preparation of the announcement of v0.3.0, where Satoshi first referred to Bitcoin as a "cryptocurrency".</p>
<p>The Satoshi emails with Mr Malmi introducing announcing version 0.3 of Bitcoin as a P2P cryptocurrency.</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day6/153:13} - {Day6/155:17}</p>	<p>Q. Well, I'm asking about this email, because it says very clearly, from Satoshi: "Here's what I've prepared: "Announcing version 0.3 of Bitcoin, the P2P cryptocurrency!" Satoshi was taking responsibility for that, whereas you have since sought to distance yourself and attribute it to Mr Malmi, haven't you?</p> <p>A. Like I said, Mr Malmi wrote the initial term; I then prepared this. As we will note in his earlier emails, he wrote the stuff about the peer - to - peer cryptocurrency.</p> <p>Q. But you stated specifically in your Granath evidence, and I can take you there, that this post, this particular post had been written by Mr Malmi, didn't you?</p> <p>A. That is written by him. The "peer - to - peer cryptocurrency" bit is from him, which, again, if you go to his earlier emails, you'll note.</p> <p>Q. You said that the post had been written by him, the post we're looking at here, didn't you?</p> <p>A. It has. I added the extra command line bits.</p> <p>Q. We'll go to your evidence in Granath then {O2/11/24}, internal page 90, lines 4 to 11. The post was referred to and you were asked, at line 8: "Is that something you have written? "Answer: That was written by Marty Melmey. "Question: This was written by someone else? "Answer: Marty Melmey." So you were insisting that announcement was written by him, not that you had prepared it but he had contributed in some way, but that you had - that he had written the post, right?</p> <p>A. He wrote the text of the block at the top, which, when we bring up his earlier emails, you'll see, and like I'm saying now, I added the additions at the bottom. He then posted it on the site.</p> <p>Q. Well, I put to you, and no doubt this can be corrected and put in submissions that it is simply not true that Martti Malmi came up with that part of the post, or any part of it. It was prepared by Satoshi, as that email says.</p> <p>A. No.</p> <p>Q. And your evidence -</p> <p>A. Once again -</p> <p>Q. Your evidence in Norway was dishonest, trying to keep up your insistence that Bitcoin is not a cryptocurrency.</p> <p>A. Not at all. Mr Malmi, aka Cobra, or Cobra Bitcoin, is very categorically forgetting one little point: he came up with the text earlier, including the stuff on the peer - to - peer forum,</p>	<p>Dr Wright is not accepting of the obvious truth regarding Satoshi's preparation of the announcement of v0.3.0, where Satoshi first referred to Bitcoin as a "cryptocurrency".</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>so where I have not corrected that and I've put it in there, doesn't mean I wrote it. If I block quote something from someone else, because we're working together, that doesn't mean I wrote it. So I prepared.</p>	
<p>{E/1/24} - First Witness Statement of Craig Steven Wright</p>		
<p>{Day6/156:24} - {Day6/158:2}</p>	<p>Q. You also say what in August 2009, you offered Mr Matthews 50,000 Bitcoin for AU\$100 in order to prove that Bitcoin had monetary value, yes?</p> <p>A. I think we actually started at 500 and I tried to get him down, but -</p> <p>Q. Let's see -</p> <p>A. -- we're Australian, so we haggled a bit. But it started at something like 500, then went down to 100 and I couldn't even get that.</p> <p>Q. {E/1/24}, paragraph 124: "Around August 2009, to demonstrate that Bitcoin had monetary value, I offered Stefan Matthews 50,000 Bitcoin for A\$100. I did try to get less when he said no. However, Stefan chose not to proceed with the transaction." Does that accurately describe your discussion?</p> <p>A. Yeah, the way I would probably put it would be I started at around 500 and went down. That makes it sound more - I mean, like I said, I went less when he said no.</p> <p>Q. Now, Mr Matthews, at that time, had no knowledge of how Bitcoin was working, did he?</p> <p>A. No, actually, he did, because we were running some of the servers, but he didn't understand it as far as token or money went.</p> <p>Q. So you think that at the time you had this discussion, you were running some of the servers along with Mr Matthews, yes?</p> <p>A. No, that's not what I said.</p>	<p>Dr Wright is evasive, providing an answer that directly contradicts what he said about Bitcoin not having any attributable value until 15 - 18 months after its launch, {Day6/142-143}.</p>
<p>{Day6/159:12} - {Day6/161:13}</p>	<p>Q. As you tell the story, this was a meaningless offer, wasn't it? AU\$100 for 50,000 of something of entirely unknown value and quantity?</p> <p>A. No, actually, that's completely wrong. It has value now. It was speculative. I mean, I was hoping someone would buy it so I could add value; a cent per token was something. Now, what you're saying is it's a meaningless offer. No, completely not; anyone who bought it back then, you could actually argue</p>	<p>Dr Wright is improperly using his oral evidence to make baseless accusations against COPA and its members.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>the same. So when Martti did it, is that meaningless for him? When Gavin came in, was that meaningless for him? All the other people in the early days of Bitcoin that saw something in my invention, that saw that this could be something worthwhile that is more than just some money - go - up token scam that your COPA people are running now.</p> <p>Q. Can you stop making irrelevant allegations and answer the question, please -</p> <p>A. They are completely relevant allegations. They're not just allegations, every single one of your COPA team have, this morning --</p> <p>Q. Please stop. I'll stop you there, Dr Wright. You have used the witness box as a pulpit to make allegations against many people. I'm going to stop you there. These are --</p> <p>A. I have stated facts.</p> <p>Q. These are allegations for which you provide, very often, no supportive evidence at all. We'll move on. What I put to you is that at that time, Mr Matthews knew nothing about the operation of the system, unlike these other people, was not participating in it, and so the offer you were making was meaningless. Right?</p> <p>A. No. It supported the system. My Lord, is it possible to bring up Twitter? I would love to show every single one of the COPA members, this morning, pumping - basically making false Ponzi claims saying that Bitcoin - BTC, sorry, will go up to 100,000 or \$1 million --</p> <p>MR JUSTICE MELLOR: Stop --</p> <p>A. -- that if you don't get in --</p> <p>MR JUSTICE MELLOR: Dr Wright, in an earlier hearing, I made it perfectly clear that at this trial I was not going to be assisted by arguments about the current state of the system, and that's what you're getting into. And counsel is quite right to stop you, because it sheds no light whatsoever on the issue I have to decide. Do you understand?</p> <p>A. I do.</p> <p>MR JUSTICE MELLOR: Thank you.</p> <p>MR HOUGH: You don't mention in your statement attempting this exercise, this sort of offer with anyone else, do you?</p>	

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{Day6/163:3-22}	<p>Q. You say, don't you, that the ATO investigations that you were facing were the reason for you retiring the Satoshi persona, right?</p> <p>A. No, the reason that I stopped focusing on Bitcoin and left it to the stewardship of Gavin and others was a combination. I had the Australian Tax Office, I had Mr McArdle trying to bankrupt me, I was involved in, well, basically getting divorced, I'd just, in February, moved house, and I was trying to sort of rebuild my life.</p> <p>Q. But according to your witness statement, the "chief" reason was the ATO investigation, right?</p> <p>A. That was the biggest thing on my mind, but, I mean, you can't, at the same time, discount - I mean, just because, say, 30% was the ATO, then I also had Mr McArdle trying to bankrupt me and that was a, sort of, problem, I had the whole divorce thing, that wasn't exactly pleasant, we can't say, I had trying to redo all the companies through the divorce, that was a mess, so - ...</p>	<p>Dr Wright is evasive when answering even fairly peripheral questions, such as what he says in his evidence about the reasons for his supposed retirement of the Satoshi Nakamoto moniker.</p>
<p>{E/1/26} - First Witness Statement of Craig Steven Wright {L15/131/1} - 2019/06/28 - Transcript re: Evidentiary Proceedings</p>		
<p>{Day6/164:18} - {Day6/167:18}</p>	<p>Q. But that - there was a communication from Satoshi, if we can put it that way, "I've moved on to other things, it's in good hands with Gavin and everyone", yes?</p> <p>A. I said that, because I was focusing on other developments of the system. I believed that Gavin would steward the system and scale it. I needed to work on other scaling solutions, because there were problems. And one of the things I also talked to Martti and others was, what I wanted to do was ensure that there were working escrow and sales systems. Some of the early parts of the code that I wanted to build, including a marketplace, like things to do with poker, mental poker systems, etc, all required that Bitcoin was there and running, and by that stage I thought it would continue.</p> <p>Q. You have complained - this is paragraphs 134 onwards in your statement {E/1/26}, on page 26. You've complained that Mr Malmi, who operated as an administrator of the bitcoin.org website and forum, set up a new forum against your wishes, haven't you? Just is that right or wrong?</p> <p>A. It is right.</p> <p>Q. And it's right, isn't it, that you've made some extraordinary allegations about Mr Malmi before, haven't you?</p> <p>A. I've made plenty of allegations against Cobra.</p>	<p>Dr Wright demonstrates his willingness to make serious accusations against individuals from the Bitcoin community without any evidence.</p> <p>Dr Wright blames third parties for his lack of supporting emails (claiming he was the victim of a hack).</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. {L15/131/1}, please, page 14 {L15/131/14}, line 15. You were describing to the court in Kleiman, in June 2020, why you couldn't be associated with Satoshi, weren't you?</p> <p>A. Yes.</p> <p>Q. And you made reference to Mr Malmi at line 22, didn't you?</p> <p>A. I did.</p> <p>Q. And then page {L15/131/15}, you alleged that Mr Malmi had been responsible for setting up Silk Road, Hydra and other dark - darker websites, didn't you?</p> <p>A. He was involved with it.</p> <p>Q. You alleged that he had worked on setting up assassination markets and the funding of terrorism, if we see at the bottom of the page 15 and at the top of page {L15/131/16}, right?</p> <p>A. That was part of Silk Road, yes.</p> <p>Q. You accused Mr Malmi specifically of doing these things, didn't you?</p> <p>A. He helped set up Silk Road. When I put him in touch, or when we were all talking with Joseph Vaughan Perling, NewLibertyStandard, and himself to set up an exchange, this is not what I expected the exchange to be. The exchange that he mentions in his email is one of the ones that were the back end to Silk Road.</p> <p>Q. You've made these scandalous allegations without ever putting forward any documentary support for them, haven't you?</p> <p>A. We have documentary support: his emails. The exchange that is being mentioned in there is the one behind Silk Road. I didn't have my emails any more; my server was hacked.</p> <p>Q. Back to the previous page {L15/131/15}, line 21: 289,290 "Martti also started working on a reputation system to allow assassination markets." You've never given a shred of evidence for that scandalous allegation, have you?</p> <p>A. The system that he talks about, where he says I contacted him briefly, etc, the "identify", or whatever he wants to pronounce it, was actually linked to that.</p> <p>Q. The reality is that that evidence, like the evidence you've happily given about Mr Malmi and others in these proceedings, is simply a set of scandalous and unsupported allegations, isn't it?</p> <p>A. No. And the comments I've been making for years about how Bitcoin was funded on accommodation of Liberty</p>	

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	Reserve and WebMoney are ones that only Satoshi and Malmi knew, even though I said it before I had access to his emails.	
{L6/282.7/1} - Re: TEST network: bad blocks getting accepted?		
{Day6/169:6-13}	<p>Q. He was proposing the use of GitHub as a source control system from July 2010, yes?</p> <p>A. Yes. He wanted it, but it didn't move at that point.</p> <p>Q. And there's no vehement objection from Satoshi in any emails, is there?</p> <p>A. No, I kept running it for all the months later, and I didn't move. So he suggested something, and I didn't accept it.</p>	Dr Wright maintains that he (as Satoshi) was against moving the code to GitHub, without having provided any contemporaneous evidence for that (and despite the contemporaneous evidence pointing to Satoshi's acquiescence, at least).
{L6/500.2/1} Project management: Satoshi doesn't scale?		
{Day6/170:17} - {Day6/171:4}	<p>Q. {L19/255/1} - I'm sorry {L6/500.2/1}, please. This is Satoshi's response. The middle of the page, he responds to the suggestions: "I don't know anything about trackers, but people seem to like github so that sounds like a good choice. I wouldn't pick SourceForge." So he was responding positively to the proposal for the GitHub branch, isn't he?</p> <p>A. No, his response - I am responding there to the bug tracking, GitHub was far better, I admit that</p>	Dr Wright claims that the Satoshi response to the GitHub proposal was in relation to bug tracking, rather than the move to GitHub generally.
{L19/255/1} - Capture {L7/16.1/1} - Links/documents on SourceForge		
{Day6/172:1} - {Day6/173:18}	Q. Then {L18/437/1}, a Satoshi email to Mike Hearn, 29 December email. In the second full paragraph, he says: "Code for client - only mode is mostly implemented. There's a feature branch on github with it, also I'm attaching the patch to this message." So, that shows Satoshi using GitHub, doesn't it?	Dr Wright is evasive, insistent that Satoshi was using a "client - only" mode of GitHub.

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. No, we're talking about the client - only mode. Going back to September/October, I first sent a patch to Gavin, and then Gavin and I started sending back SPV software. SPV is not a full node or other structure, SPV is the Simplified Payment Verification mode. So, what was happening here was there was a branch for a trial version of an SPV system. This would be a walleted node that didn't mine.</p> <p>Q. Next, {L17/16.1/1} - sorry, {L7/16.1/1}. I gave a wrong reference. It's an email from Mr Andresen to Satoshi and Mr Malmi saying he wants to make changes to SourceForge and asking for administrative privileges. One of these is to make the support tab link to the GitHub issue tracker. Do you accept that's a genuine email?</p> <p>A. I do. It was linking in to the page and the main project system.</p> <p>Q. Then {L7/16.2/1}, Satoshi writing to Gavin Andresen on 4 January 2011. He says he's given Mr Andresen admin. That means administrative privileges, doesn't it?</p> <p>A. Yes, on the SourceForge site.</p> <p>Q. He says that Mr Andresen's ideas, including about the support tab link, are good, yes?</p> <p>A. Yes. I thought that a better, like, help desk type function would be great.</p> <p>Q. And that he could disable or delete SourceForge forums if he thought it would help?</p> <p>A. Yes. We already had set up the bitcoin.org forums. The bitcoin.org forums, which is now BitcoinTalk, were a separate forum. So, the forums on SourceForge were horrible. I mean, I like SourceForge for SVN, but their forums and their bug tracking is just horrible, still. So, those, what we talked about were archiving all of those communications, doing it in a way, because there were private communications, we didn't want any of them shared, and then saving everything.</p>	
<p>{R/12/2} - Annex 1 to COPA's Skeleton Argument</p>		
<p>{Day6/177:19} - {Day6/178:6}</p>	<p>Q. The highest concentration was from 4.00 am to 5.00 am, right?</p> <p>A. That's generally when I'm up doing things, yes.</p> <p>Q. Very low in the afternoon and virtually none in the evening?</p>	<p>Dr Wright states that he did most of his work as Satoshi between 4 - 5am, which is implausible.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. In the evening, I rest.</p> <p>Q. Next page {R/12/3}. This is a scatter plot showing the emails and posts over time -</p> <p>A. Mm-hm.</p> <p>Q. -- which tells a similar story.</p> <p>A. Yes, it shows that the majority of stuff and why I posted that I was so, well, basically, trashed, in August, to Gavin, can be seen there.</p>	
<p>{E/1/33} - First Witness Statement of Craig Steven Wright</p>		
<p>{Day6/180:14-22}</p>	<p>Q. Then, now, please, page 33 {E/1/33}, paragraph 186. You're here dealing with the steps you took to gain access to private keys when you were involved in the big reveal in early 2016; do you see that?</p> <p>A. Yes, although what I must note is you're confusing the Tulip Trust with "The Trust". The key sharing system that you have here was a scheme that I created, a software program called "The Trust". The Trust isn't the Tulip Trust, The Trust was owned by the Tulip Trust.</p>	<p>Dr Wright has a convoluted explanation for the difference between "The Trust" and the Tulip Trust.</p>
<p>{Day6/181:3} - {Day6/182:9}</p>	<p>Q. And when you made that statement, you understood the importance of being accurate and precise about all those details, right?</p> <p>A. I do.</p> <p>Q. In these proceedings your position is that the Genesis Block does not have, and never has had, either a private or public key associated with it; correct?</p> <p>A. Well, what you can actually do is you can generate a public key structure that doesn't have a private key, or at least no known private key. I've explained this and blogged about it.</p> <p>Q. You've given evidence in your statements that there isn't either a public or private key associated with the Genesis Block, haven't you?</p> <p>A. You're misrepresenting what I've said, again. What I've stated is that the key structure that is hashed doesn't actually act as a key. While it looks like one, has the same representation, it is a keyless key.</p> <p>Q. One second. (Pause). So we take it from you that the hard drive didn't have a private key associated with the Genesis Block?</p>	<p>Dr Wright provides an explanation regarding "keyless keys", but it is not possible to have a public key without a private key, even if no - one knows it, see Meiklejohn 1, paragraph 32 {G/2/11}.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. It did not.</p> <p>Q. And there was no technical or cryptographic means for you to prove your claim to have created the Genesis Block specifically; is that right?</p> <p>A. No, I actually can show how you can do it, and I can show the mathematics between creating a keyless key.</p> <p>Q. But you couldn't prove by some cryptographic means that you had an association with the Genesis Block?</p> <p>A. Not by cryptographic means, no.</p>	

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
DAY 7		
CROSS - EXAMINATION OF DR CRAIG WRIGHT BY JONATHAN HOUGH KC		
{L5/104/1} - Re: Bitcoin		
<p>{Day7/5:3} - {Day7/7:18}</p>	<p>Q. And do you recall that I challenged your claim that Martti Malmi had written that post by showing an email from Satoshi saying that they had prepared the post?</p> <p>A. Prepared isn't written.</p> <p>Q. And do you recall saying that if you go back to Mr Malmi's earlier emails, it can be seen that he wrote that part of the post?</p> <p>A. Yes. And I'll just correct you, it wasn't "they", there's only one Satoshi and it's me.</p> <p>Q. Obviously we disagree about that, but let's go back to the emails {L5/104/1}. I think this is one of the earlier emails between Satoshi and Mr Malmi to which I think you were probably referring. Do you see here an email of 11 June 2009?</p> <p>A. I do.</p> <p>Q. If you go to the middle of the page, Satoshi writes this, just at the bottom of their email: "Sourceforge is slow right now ..." Sorry, just above that: "Someone came up with the word 'cryptocurrency' ... maybe it's a word we should use when describing Bitcoin, do you like it?" Do you accept that that's a genuine email?</p> <p>A. I do.</p> <p>Q. Then {L5/106/1}, please, an email of 12 June 2009, a response from Satoshi to Mr Malmi, and they say, specifically addressing that suggestion, towards the bottom: "It sounds good." Mr Malmi says, "It sounds good": "'The PTP Cryptocurrency' could be considered as the slogan, even if it's a bit more difficult to say than 'The Digital P2P Cash'. It still describes the system better and sounds more interesting, I think." Again, do you accept that's a genuine email?</p> <p>A. I do.</p> <p>Q. And were those the emails that you were referring to yesterday when you said you need to look back at the earlier emails?</p>	<p>Dr Wright is questioned about Satoshi's use of the term "cryptocurrency" in emails with Martti Malmi and is evasive in response, not answering the question being asked.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. In part, yes. On top of that, there are also communications on SourceForge via direct message, and on top of that in the forums.</p> <p>Q. I think you referred to earlier emails yesterday.</p> <p>A. I did, and I'm saying both that and the others.</p> <p>Q. So, based on these emails, Satoshi raised the idea of calling it a cryptocurrency, we saw in the first of those emails just now?</p> <p>A. No, actually someone else on the forums had mentioned that.</p> <p>Q. Satoshi raised it between them and Mr Malmi?</p> <p>A. No, Mr Malmi was actually in part of the forum discussions.</p> <p>Q. And then Mr Malmi agreed with the idea in the email we're looking at on the screen - in the email we're looking at at the moment on screen?</p> <p>A. And then he wrote the changes to the page, etc.</p> <p>Q. Later, Satoshi wrote the July 2010 post describing it as a cryptocurrency?</p> <p>A. No, I prepared the additions there. At that point, you will realise that the cryptocurrency reference had already been put on the page. So at 0.3, that's way after the Bitcoin web page, which you can find out by checking the Wayback Machine, and also other forums had already described it that way. So, when you're saying that this had been created by me, that's postdating the changes.</p>	
<p>{Day7/7:19} - {Day7/8:4}</p>	<p>Q. Can we at least agree on this. Based on these emails, Satoshi had no problem at all calling Bitcoin a cryptocurrency, despite you saying that that is a radically incorrect description?</p> <p>A. One, I agreed at the time and didn't have any arguments. Afterwards, as I've noted, I've basically gone and decided that it's the wrong term. I've been saying that for some time. Now, cryptocurrency is actually something that's anonymous. Now, while I haven't, at the time, gone into that deep enough, I have subsequently.</p>	<p>Dr Wright ultimately accepts that Satoshi called Bitcoin a cryptocurrency "at the time", but that he decided it was the wrong term later. This contradicts his book at {L15/96/59} in which he states "At no point have I said that Bitcoin is a cryptocurrency", which was put to him in {Day6/150:1}.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{O2/11/29} - Transcript of Dr Wright’s Evidence from Granath Proceedings		
<p>{Day7/9:15} - {Day7/10:17}</p>	<p>Q. And then you said that what was on that hard drive was the first 12 keys, as well as a number of key slices?</p> <p>A. Not exactly. What I'm trying to explain to people is, the drive was an encrypted system that was accessed using an AES key that was collated using the slices. The slices were collated at that point. The AES key unlocked the drive. When the drive is unlocked, what you access is the algorithm that I used as part of Timecoin for mining. That enables recalculating the keys. The keys are homomorphically calculated.</p> <p>Q. But you're clear here that what you extracted, by whatever means, were keys to the first 12 blocks on the blockchain associated with Satoshi, right?</p> <p>A. Yes, they had been completed and basically recalculated.</p> <p>Q. So not the first 11, as you said in paragraph 186 of your witness statement in these proceedings, which I put to you yesterday?</p> <p>A. My first 12.</p> <p>Q. Well, I'm not going to go back to it because I put it to you, but you said that you had an encrypted hard drive containing the keys for "all of the blocks mined by me, including blocks 1 through 11", whereas you said in Granath that the keys you had access to were "the first 12". That's a difference, isn't it, Dr Wright?</p> <p>A. It is.</p> <p>Q. Which do you say now is right?</p> <p>A. I definitely had 1 to 11.</p> <p>Q. So you were wrong when you said 12 to the court in Granath?</p> <p>A. Fairly much, yes. I made a mistake.</p>	<p>Dr Wright admitting that he made an error in the Granath proceedings in stating that he had access to the keys to the first 12 blocks on the blockchain, rather than the first 11 blocks (as stated in these proceedings).</p>
{L14/409} - Transcript of Wright Deposition in Kleiman Proceedings		
<p>{Day7/12:15} - {Day7/13:1}</p>	<p>Q. Then at line 23, you were asked: "What assets were controlled by the Tulip Trust in 2011?" Which is when you say it was first settled, yes?</p> <p>A. In the current format, yes.</p>	<p>Dr Wright provides an evasive and confusing response in relation to when the</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. You'd been asked, at line 6, when the trust was created, and you said simply "2011"?</p> <p>A. Like I said, it was actually an earlier trust that was resettled. So technically it is a different iteration of an earlier trust. So the current one was settled in 2011, but that is taking over from an earlier trust where I've added other members.</p>	<p>Tulip Trust was first settled.</p>
<p>{Day7/13:23} - {Day7/14:16}</p>	<p>Q. Page {L14/409/293}, line 13, as part of the same answer, you said that: "Dave was asked simply to hold a part of some documents and keys that were split using Shamir Secret Sharing scheme so that he did not even know what he was actually holding."</p> <p>A. Once again, that was The Trust. That was the Shamir system, which was an algorithmic code.</p> <p>Q. A Shamir sharing scheme is explained in the reports of the experts and allows, in simple terms, a private key to be broken into slices so that they can be reassembled in different combinations to gain access, yes?</p> <p>A. No. The Shamir system I'm talking about is White Paper 222 and 479, as well as other things. We have granted patents on this. The system described by Ms Meiklejohn and others is a radically simpler system. I created new forms of threshold systems, including automated ones and non - interactive methods, and these are very different to the system she's describing.</p>	<p>Dr Wright provides an explanation of his own version of the Shamir sharing scheme, and does not agree that it is the scheme as explained in the expert reports.</p>
<p>{Day7/14:17} - {Day7/15:23}</p>	<p>Q. Let's carry on with your evidence and see where you go with it in the Kleiman proceedings. Page {L14/409/294}, line 6, you were asked if you put Bitcoin into the trust in 2012, and you answered no; do you see that?</p> <p>A. I do.</p> <p>Q. Question: "Did you ever put Bitcoin into the trust?" "Answer: No."</p> <p>A. Correct.</p> <p>Q. And: "Did anyone ever put Bitcoin into the trust?" "Answer: No." Yes?</p> <p>A. That's correct.</p> <p>Q. And those were questions about Tulip Trust, weren't they?</p> <p>A. There's a bit of both. There's The Trust and there's Tulip Trust and people keep confusing the two. As I've noted, the Bitcoin was held by a company, and The Trust owned shares. So shares in the company were held by the Tulip Trust. It holds multiple companies, I think about 11, not 100% in the majority of them, but it holds the shares in its sort of shareholding.</p>	<p>Dr Wright is questioned about whether questions he answered in Kleiman were about putting Bitcoin into the Tulip Trust. Dr Wright is evasive in response and explains there was also "The Trust", a company which held Bitcoin, but the shares in this company were held by the Tulip Trust.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Those companies hold a variety of different assets. That includes intellectual property, it includes software, it includes research and development and it includes Bitcoin.</p> <p>Q. So your evidence now is that Tulip Trust, amongst its assets, had companies and those companies owned Bitcoin?</p> <p>A. Yes, and being that I don't own 100% of any of those companies, I cannot say that the trust owns Bitcoin. The trust owning - if I own a share in News Limited, that doesn't mean I own News House.</p>	
<p>{L15/51/1} - Wright Declaration in Kleiman Proceedings</p>		
<p>{Day7/16:6} - {Day7/18:5}</p>	<p>Q. {L15/51/1}, paragraph 4, you recorded that you mined Bitcoin during years 2009 to 2010 directly into a trust, the name of which is redacted but was located in Panama, yes?</p> <p>A. Yes, which is very different to what we were talking about before. The trust structure was Information Defense had a trust to Wright International. At this point, this is pre-tulip Trust, so when I was asked how I set this up, Information Defense, which is a registered - or was a registered Australian Pty Limited company, did the mining and had a conditional agreement to basically transfer the assets into Wright International.</p> <p>Q. {L15/51/2}, paragraph 5: "In June ... 2011, I took steps to consolidate the Bitcoin that I mined with Bitcoin that I acquired and other assets. In October 2012, a formal trust document was executed, creating a trust whose corpus included the Bitcoin that I mined, acquired and would acquire in the future. The name of that trust is Tulip Trust. It was formed in the Seychelles. I refer to ... [it] as Tulip Trust I." So at that point, you were saying that Tulip Trust was the subject of a formal trust document in October 2012 and its corpus of assets included the Bitcoin that you'd mined, acquired and would acquire in the future, right?</p> <p>A. Not in the way that you're implying. As I noted, the company, there were two different ones, one where I'd had the purchased Bitcoin, which was Tulip - well, Tulip Trading Limited, and the second was Wright International. That was the first company that was set up in 2009. Now, by "corpus", what I mean is that includes all the assets of these companies. At this point, Wright International was 100% owned by bearer share structures and then through the trust.</p>	<p>Dr Wright is asked about his declaration in which he stated that he mined Bitcoin directly into a trust during 2009-2010, and is evasive in response, re-interpreting the meaning of his previous sworn declaration.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. So what you say you mean - you meant in this sworn declaration is not that the assets of the trust included Bitcoin that you mined, acquired and would acquire in the future, but its assets included companies which owned such Bitcoin?</p> <p>A. Effectively, that's what I used the word "corpus" for. I was ordered directly by the court to respond to any Bitcoin I might have, including through any corporate structure. Now, including through any corporate structure meant that I had to list if there's a trust in companies and I'm a beneficiary of those, and they explicitly - the magistrate told me explicitly that any beneficiary agreements need to be included and I did.</p>	
<p>{Day7/18:21} - {Day7/20:3}</p>	<p>Q. Paragraph 7, you identify the trustees for that trust as COIN Limited, with its company number, Uyen Nguyen, yourself, Dave Kleiman, Panoptcrypt, Savannah, and the holder of certain PGP key IDs; do you see that?</p> <p>A. I do. This was when I went through documentation and I basically were handed from machines, including third party ones, employees', a variety of trust documents. I explained to the court that I cannot actually validate these, I have no right to, until after meetings that cannot be held before 2020, but I was still ordered, saying that, "These are trust documents and you have to accept them". So, based on the fact that I was unable to validate anything, I basically said, "This is what this document says".</p> <p>Q. So based on this document, your evidence previously to the court that David Kleiman had nothing to do, no involvement with Tulip Trust, was wrong, because he was a trustee?</p> <p>A. No, actually I've noted already, you brought this document up earlier last week, this document is false. It actually is three different documents that have been tacked together by somebody, and on top of that it's been altered. As you yourself noted, the signature has been applied just by an image.</p> <p>Q. Dr Wright, I'm not at the moment talking about the trust document. We'll come back to that in a moment, but just on the basis of your sworn declaration, you say there that "the trustee was initially David Kleiman" and then "additional trustees were appointed". If that is correct, you were wrong to tell the court previously that David Kleiman had no involvement with the trust and his only connection was holding some key slices which he didn't really understand.</p>	<p>Dr Wright is shown his declaration identifying the trustees for the trust, and asked about David Kleiman's involvement with the Tulip Trust. Dr Wright's response is evasive and does not answer the question that was asked.</p>
<p>{Day7/20:4} - {Day7/22:1}</p>	<p>A. No, I was not. As I have already explained, I had no access to anything and I was only shown documents. At this point in time, I had no reason to sort of not believe any of the documentation, they hadn't been analysed, and being that the</p>	<p>Dr Wright is not answering the question that he was asked; he was being asked what he did</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>documents came from third party laptops, it was only later that we started analysing them.</p> <p>Q. Sorry, I thought you just said about five minutes ago that you didn't have access to trust documents at this time, at the time you were making this declaration?</p> <p>A. No, I didn't. These actually came from employee laptops. If you sort of check the chain of custody, which was listed right back at the beginning in the disclosure platform going back to 2019, you'll find out that these came from two employee laptops, the ones that held my wife and my own emails and other areas they weren't allowed to have access to.</p> <p>Q. Dr Wright, which is it? Are you saying that you gave this declaration based on your own knowledge without access to trust documents that David Kleiman was a trustee, or are you saying that you gave this declaration not knowing whether David Kleiman was a trustee but based on access to trust documents? Which is it?</p> <p>A. It is not a trust document, it's fabricated. I gave this based -</p> <p>MR JUSTICE MELLOR: Dr Wright, can you just focus on the question. It's about the status of Dave Kleiman. Was he a trustee or not?</p> <p>A. No, he was not, my Lord.</p> <p>MR JUSTICE MELLOR: So why did you say he was a trustee in paragraph 7?</p> <p>A. I was handed, by the magistrate in the US, these documents and I was told that I had to answer the question. I said, "I don't actually know", and he said, "Do you accept this could be a trust document", and I went, "I don't know", and he said, "Yes or no", and basically I was under the - I answer yes or no, and I had no idea, and if I didn't answer I'd be in contempt and my answer was, "I'm a beneficiary who has no access to any of the trust deeds, trust documents, I have no knowledge of any of the trustees at this point; I set it up so I couldn't", and I was forced to answer that. I said I had no reason to argue that this wasn't a valid trust document at the time. Some of the signatures, like those from Nobel and Savannah, were people I'd worked with in the past, so I answered based on, if this is a real trust document, this is what it would be.</p>	<p>historically in relation to the trust, not what was stated on the documents. Dr Wright is also inconsistent with his answers given earlier regarding whether he had access to trust documents or not {Day7/18/6-20}.</p> <p>Mellor J queries Dr Wright's responses and requests that he focus on the question about whether David Kleiman was a trustee or not.</p>
<p>{Day7/22:18} - {Day7/23:18}</p>	<p>Q. Well, let's take this in stages. First of all, we don't accept that that was a document you threw down in court, but secondly, we established last week that you did attest to the authenticity of a trust document in the Kleiman proceedings dated 23 October 2012, didn't you?</p>	<p>Dr Wright is blaming third parties (namely Diane Pinder of Lloyds solicitors) in relation to the set up of the trust document dated 23 October</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Yes, there was one done at that time. It was done by Diane Pinder of Lloyds solicitors in Brisbane Australia, but I wasn't involved in any of the set up, so the structuring after 2011 didn't involve me at all. So, I've been answering questions, as I've been noting the whole time, about a trust where I was a blind beneficiary with no rights to view any documentation.</p> <p>Q. So your evidence to this court is that when you said in the sworn declaration: "While the trustee was initially David Kleiman ..." And then you set out further trustees, including Mr Kleiman, what you meant to say was: "I don't know who the trustees were, but I've been shown a document which I've been pressured by the judge to accept is genuine that gives this information." Is that your evidence?</p> <p>A. No, actually, I got told by my solicitor - well -</p> <p>Q. Sorry, please don't go into anything privileged.</p> <p>A. Well, that makes it hard to answer, because my attorneys told me this was a real trust document.</p>	<p>2012, and that they told him it was a real document.</p>
<p>{Day7/24:1} - {Day7/26:4}</p>	<p>MR JUSTICE MELLOR: In paragraph 7(c), you nominate yourself as a trustee of the Tulip Trust I.</p> <p>A. Yes, I was listed on that document, which -</p> <p>MR JUSTICE MELLOR: Just wait for the question. How could you carry out your obligations as a trustee without seeing the trust documents?</p> <p>A. Because I'm not actually a trustee, my Lord. The document stated that I was, but that's - my signature's not on it. I've never signed the document. So this document was created, I don't know by whom. It was on two staff laptops, ones that also went and sent information to Ira. Savannah was a real company, the people there I know; Uyen I know, but I wasn't allowed to discuss the trust, based on the provision that I set up in 2011, until at least 2020. So that made answering any of this difficult, because I couldn't go to anyone and say, "Can you show me the trust document".</p> <p>MR JUSTICE MELLOR: So why did you nominate yourself in paragraph 7(c) as a trustee?</p> <p>A. I'd listed what were on - so "trustees for Tulip Trust I are", and I listed exactly what the document said.</p> <p>MR JUSTICE MELLOR: And did you include anywhere in this declaration the qualification that you've just mentioned, that you weren't a trustee?</p> <p>A. Well, I had no idea how I could be. I had told my attorneys in the US basically that I'm not allowed to act for the trust or anything, and I don't actually know. There were multiple trust</p>	<p>Mellor J asking further questions of Dr Wright in relation to Dr Wright's role as trustee of the Tulip Trust I. Dr Wright is evasive in response and blaming third parties (Lloyds solicitors).</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>deeds, many of which were conflicting. One of those was actually the real deed. I only know which one is the real deed now, because it's post 2020. At the time, I wasn't able to ask anyone.</p> <p>MR JUSTICE MELLOR: So who created all these multiple trust deeds?</p> <p>A. The first one was Diane Pinder of Lloyds solicitors.</p> <p>MR JUSTICE MELLOR: You're saying she drafted it?</p> <p>A. She drafted a trust, not this document.</p> <p>MR JUSTICE MELLOR: Who was responsible for the making of these multiple trust deeds?</p> <p>A. I settled the first one in 2011. After I settled the document in 2011, I had no further part in it other than I spoke to Diane about some of the terms that she needed to clarify when she was redrafting it. I also put people in touch with Bakers and was in some - like, engaged in communications with them as the new trust deeds were structured in 2016. But I didn't actually maintain - or didn't get a copy of the deed.</p> <p>MR JUSTICE MELLOR: And who was responsible for the new trust deeds in 2016?</p> <p>A. As in managing them, holding them ...?</p> <p>MR JUSTICE MELLOR: No, who initiated those?</p> <p>A. My wife.</p>	
<p>{L8/17/5} - Deed of Trust between Wright International Investments and Tulip Trading, C00000560. {L15/51/2} - Dr Wright's Declaration in the Kleiman Proceedings</p>		
<p>{Day7/26:10} - {Day7/28:15}</p>	<p>Q. It's from the Kleiman proceedings. It's a deed of trust between Wright International Investments and Tulip Trading, dated 23 October 2012, reference C00000560. Page 5, please {L8/17/5}, we looked at this earlier. Do you see that that records the list of trustees which appeared in your declaration, essentially?</p> <p>A. I do. I also note, on the first page, that it says it's for a joint endeavour and partnership. Now, that's what I was being sued for as part of the Kleiman proceedings. In that, I noted that I've never been a partner and I wouldn't ever be a partner. I'm a shareholder in many things, but I don't engage in partnerships.</p> <p>Q. Was this the document which you say you were shown which led you to make the declaration which you now say was so significantly wrong?</p>	<p>Dr Wright is evasive and incomprehensible in his interpretation of his sworn declaration in the Kleiman proceedings, stating that the Deed of Trust is now "just the prep for pre-drafting for what ended up in the 2016 document".</p> <p>Dr Wright admitting that the encrypted file referenced in his</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Yes.</p> <p>Q. Moving back to your sworn declaration {L15/51/2} - thank you very much - page 4 {L15/51/4}, paragraph 18, you refer to settling a further trust, Tulip Trust II, in 2014. Is this right, the claims to have placed assets in trust in 2011/2012 are separate from Tulip Trust II?</p> <p>A. No, no. Basically, this is just the prep for pre - drafting for what ended up in the 2016 document. That's now with the registered trust number. So, in 2014, that was initiated. At the point when this was done, the majority of members were miners, so it still needed sign off from a certain number of people, so even though I wasn't involved in all of the details, I signed off on it happening.</p> <p>Q. Paragraph 22: "Access to the encrypted file that contains the public addresses and their associated private keys to the Bitcoin ... I mined, requires myself and a combination of trustees referenced in Tulip Trust I to unlock based on a Shamir scheme." Now, you seem here to be referring to the same encrypted file or drive described in your witness statement that we looked at yesterday, paragraph 141; is that right?</p> <p>A. No, because that document's wrong. There wasn't anything properly documented for what is Tulip Trust I, but a document was created. That document is one of the ones that you'll note have metadata problems.</p> <p>Q. Were you referring in your declaration, when you referred to an encrypted file, an encrypted file which included the key slices giving access to the algorithm, giving access to the early keys to blocks 1 to 11 or 1 to 12?</p> <p>A. The encrypted file was accessed when you use an AES key. The AES key was reconstructed using key slices.</p> <p>Q. But is the encrypted file that we're talking about in your witness statement for these proceedings and this sworn declaration the same one?</p> <p>A. That encrypted file is, yes.</p>	<p>witness statement in these proceedings {E/1/27} and his sworn declaration in the Kleiman proceedings are the same.</p>
<p>{L15/131} - Transcript re: Evidentiary Proceedings in Kleiman Proceedings (Dr Wright's cross - examination by Mr Freedman)</p>		
<p>{Day7/30:3-11}</p>	<p>Q. And then, at line 3, you were asked: "So the manner in which it was set up with Dave Kleiman potentially allows for the fragmented keys to come to you so that you can decrypt</p>	<p>Dr Wright confirming that accessing the encrypted file would</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>the file and obtain a list of the public addresses; is that right?" And you confirmed that, yes?</p> <p>A. Yeah, it's a bit more complex than that, but, yes, accessing the file would allow me to reconstruct all of those.</p>	<p>allow him to reconstruct the keys.</p>
<p>{Day7/33:24} - {Day7/35:4}</p>	<p>Q. And line 15, Mr Freedman asked: "What were you going to do to the blockchain with the Genesis block, Dr Wright?" Yes?</p> <p>A. Mm - hm.</p> <p>Q. Your answer is: "Again, you're confounding two different things. There's a loan of Bitcoin held on a separate organisation and the key controlling the Genesis key. They're not the same thing."</p> <p>A. That's correct.</p> <p>Q. Now, you refer repeatedly there to a key in association with the Genesis Block. Was that the private or public key for the Genesis Block that you were referring to?</p> <p>A. Neither. Earlier I mentioned a HMAC scheme. Now, when I was talking about that, a HMAC is a combination of a secret and a - basically a hash algorithm. Now, in this, the HMAC used a key that was generated using what I call a "number 42 process". That is a type of ECDH exchange. Now, while there is no private key to the Genesis Block, what can happen is, a public key and the Genesis Block can calculate a shared secret in a standard ECDH methodology. That is Genesis buy private key, gives you a secret; that secret is then used as part of the generating string that allows you to create all of the other keys that I have in the list. So the algorithm that I'm talking about of a HMAC is based from the Genesis first.</p> <p>Q. Page --</p> <p>A. So the key isn't a public/private key scheme, it's a symmetric key scheme.</p>	<p>Dr Wright is asked about his references to a "key" in association with the Genesis Block, and whether this was a reference to the public or private key. Dr Wright provides a new explanation regarding the "number 42 process", which is a type of ECDH exchange (presumably a reference to certain of his patents).</p>
<p>{Day7/40:11} - {Day7/41:14}</p>	<p>Q. Dr Wright, please, next question. Even on your own evidence, you were putting a sum of Bitcoin, which you say at \$1 a Bitcoin was \$1 million, you say beyond your reach and only accessible either through Mr Kleiman or, if something happened to him, through a mysterious bonded courier arrangement which he had to arrange. That was your evidence to the court in the Kleiman proceedings, wasn't it?</p> <p>A. My Lord, if I can finish. When I set this up, Bitcoin was worth around 30 cents.</p> <p>MR JUSTICE MELLOR: Can you just concentrate on the arrangement that you set up --</p> <p>A. I am, my Lord.</p>	<p>Dr Wright is asked about his evidence on the bonded courier arrangement in the Kleiman proceedings, he is evasive in response.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>MR JUSTICE MELLOR: - that you described to the court in Kleiman.</p> <p>A. I am. That's what I'm trying to do. What I set up was an arrangement for the companies. The companies owned intellectual property. I wasn't caring about the Bitcoin per se, I was caring about the IP. The IP is the thing I care more about than anything. The intellectual property, at that point, was still valuable; it is now. The intellectual property must be valuable, because BTC Core have integrated granted patents that I've created into BTC. If they're not valuable, they wouldn't. Now, what I was doing was making sure that that intellectual property would be protected, more than anything else, all of my ideas, all of my research, everything, so what I cared about was locking that away.</p>	
<p>{Day7/42:12} - {Day7/43:1}</p>	<p>MR JUSTICE MELLOR: Can we just be clear. You were putting these assets beyond reach. Was it under the arrangement that counsel put to you, those assets could only be recovered with the assistance of Dave Kleiman or the arrival of the bonded courier in 2020?</p> <p>A. Not fully. There were two areas. The ownership of the assets, yes. But the intellectual property, all my notes were on the drives, but everything was still in my head, my Lord. So, no one can force me to write down something in a patent. If it's locked and they can't access it, then they can't access it. So, my belief, at the time at least, was that the worst case would be I get bankrupted, and then in 2020, when I'm out of bankruptcy, I basically come out and patent all my information.</p>	<p>Mellor J asking Dr Wright for clarification regarding his arrangements for recovery of his Bitcoin assets, Dr Wright is evasive in response.</p>
<p>{L12/203/1} Wright/MacGregor email exchange and slices/trustees</p>		
<p>{Day7/44:14-24}</p>	<p>Q. {L12/203/1}, please. I said I would refer to the email exchange that you had with Mr MacGregor that was discussed in Kleiman. May we go to page 2 {L12/203/2} to see his email. We see here an email from Mr MacGregor dated 17 April 2016, about which you were asked in the Kleiman proceedings. Do you accept this is a genuine email?</p> <p>A. Possibly. There's modified versions of it.</p> <p>Q. There are indeed, but this one, dated 17 April 2016, do you accept that as genuine?</p> <p>A. I can't tell by its face, I'm sorry.</p>	<p>Dr Wright is evasive when asked about whether he accepts that the email at {L12/203/2} is a genuine email.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{Day7/47:15-22}	<p>Q. Further down the page, the key distribution is set out for the 7 trustees as follows. In this version of the document, which is {L12/203/1}, ID_002639, do you think that that key distribution is correct?</p> <p>A. I listed what I had from a spreadsheet.</p> <p>Q. Do you still have that spreadsheet?</p> <p>A. I don't know. It's probably in the discovery platform.</p>	<p>Dr Wright is asked whether he considers the key distribution for the seven trustees is correct, and is evasive in response.</p>
{L13/447/1} - ID_002629 - Dr Wright/Mr MacGregor emails		
{Day7/49:11} - {Day7/50:1}	<p>Q. For the lawyers, they're ID_002624 to 002628. I don't plan to go through all of them with you, Dr Wright. Were you aware of why there were so many different versions of this email?</p> <p>A. Some of - at least one of the emails ended up on a staff laptop. How it got there, I don't know. Probably because Ramona's email was being accessed by a staff member, or ex - staff member.</p> <p>Q. Dr Wright, why do you say it would assist some disgruntled staff member to adjust the numbers of key slices in the allocation in this email and date it to a later point?</p> <p>A. Why exactly, I don't know. I mean, I know people were working with Mr Kleiman and I know that people wanted my companies to go into liquidation. More than that, I can't answer.</p>	<p>Dr Wright blaming various third parties for the different versions of the Wright/MacGregor emails and the manipulation of the same, namely staff or ex-staff members, as well as implying that Ira Kleiman had an inside man at Dr Wright's company.</p>
{Day7/50:20} - {Day7/51:12}	<p>Q. But he was saying, "I've got a trust document, it gives me this information", and you didn't respond by saying, "Well, I have no knowledge of this trust document", did you?</p> <p>A. I didn't answer. It wasn't my place to and I wasn't going to. He was fishing for information, he wanted more, I wasn't going to tell him.</p> <p>Q. Well, you gave him the information he requested in terms of key allocation, didn't you?</p> <p>A. I gave what was necessary for the exercise I agreed to be part of and no more.</p> <p>Q. But you didn't say in the course of that, "You're referring to this trust document, I have no knowledge of that, I certainly don't know how you got it", did you?</p> <p>A. I wasn't going to talk to him about anything at all. Already by this point I didn't trust Mr MacGregor, so the relationship</p>	<p>Dr Wright is evasive when pressed on the inconsistencies between his account of the trust document above, and the content of this email exchange with Robert MacGregor.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>was already starting to fray. I wasn't going to go into anything more than I'd already agreed.</p>	
<p>{Day7/52:10-20}</p>	<p>Q. Dr Wright, the reality is that the Tulip Trust is a fiction, originally invented for the ATO investigations, isn't it?</p> <p>A. No, actually it goes much further back than that. It was originally invented to hold the shares of the company I'd listed through a back door listing, which was DeMorgan, back in the 1990s. That was originally structured as WDI, it had the domain WDI.org, and it was then transferred into a variety of like Craig Wright R&D, etc, entities that acted as a trust until that point.</p>	<p>Dr Wright now asserts, for the first time, that the Tulip Trust goes back much further than the dates of the ATO investigation, to the 1990s.</p>
<p>{Day7/53:4} - {Day7/54:7}</p>	<p>Q. No, Dr Wright, denying you were Satoshi in the context of the Kleiman litigation would only have devastated your credibility further, because you had committed by that stage to being Satoshi, right?</p> <p>A. No, actually, I hadn't. I had not mentioned again. I didn't talk about it at all. It was my being asked in the Kleiman thing under oath and then being forced that brought that out. That then led to some of your clients de-listing Bitcoin, BSV, because I wouldn't go back and retract. CZ from Binance came out and publicly said no more of this -</p> <p>Q. Dr Wright, I'm going to stop you there because you're a long way away from my question. You made your claim to be Satoshi in mid-2016, if not earlier, you gave your evidence in Kleiman materially after that. If you had denied being Satoshi in the Kleiman proceedings, you would have been publicly confessing to being a liar in a very public big reveal, wouldn't you?</p> <p>A. Not really. I could have said it was all sorts of other things. I could have said I've lost the keys, I could have lied. If I did lie in the court case, I could have ended it very quickly. Now, what I am saying, though, is I didn't want to come out in 2016, I didn't want to reveal anything, and I didn't want to later. Between 2016 and when I was forced in court to answer the question under oath, I hadn't said anything more, I hadn't built anything requiring that I was and I hadn't discussed it at all.</p>	<p>Dr Wright is evasive when pressed about the consequences of denying that he was Satoshi in the Kleiman Proceedings.</p>
<p>{E/1/21} First Witness Statement of Dr Wright {O4/23/1} GQ Interview - Cryptographic means of establishing control/association with the Genesis Block</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day7/54:16} - {Day7/56:8}</p>	<p>Q. Moving back to the Genesis Block, {E/1/21}, please, on screen, paragraph 107. You stated in your witness statement for these proceedings: "Contrary to popular misconception, no public or private key is associated with the Genesis Block." Correct?</p> <p>A. That is correct.</p> <p>Q. You confirmed to me yesterday that there was no cryptographic means of establishing control of or association with the Genesis Block, right?</p> <p>A. That's correct.</p> <p>Q. {O4/23/1}, please. This is a transcript of an interview you gave to GQ in April 2016, I think. On page 4 {O4/23/4}, by letter A, when being asked about giving proofs, you said this: "I'm not going to jump through everyone's fucking hoops. Bullshit from Maxwell that we've had to pay money to get bloody disproven because the code's fucking out there. I'm not doing this every fucking time. I'm not going to cite(?) ..." And I think that's "sign": "... every fucking key I own in the world. I've got the first fucking nine keys, I've got the fucking genesis bloody block, I've got the fucking code, I've got the fucking papers ..." And so on. You were suggesting there, weren't you, that you had the means to establish proof of control of the Genesis Block, weren't you?</p> <p>A. No. While I was a little bit angry at this point and - very angry, what I was stating is what I've said before. The anchor is part of a hash chain. The generation of, like, ECDH key values for a HMAC system allows the Genesis Block to be the anchor in that system. So you need to choose something when you have, like, the start of a hash chain. So, for my own key structures, I also chose the Genesis Block. So the genesis key here is a symmetric value, not controlling the blockchain itself.</p> <p>Q. There is a public key associated with the Genesis Block, isn't there?</p> <p>A. No, there's a number that people attribute to being a public key. That doesn't make it a public key. I've explained in my blogs, which you have in the book there, how you can actually generate a public, like, what looks like a public key that has no private key.</p>	<p>Dr Wright not accepting the obvious truth that the transcript of his GQ interview suggested that he had the means to establish proof of the Genesis Block.</p>
<p>{Day7/56:9-24}</p>	<p>Q. The cryptocurrency technology experts in this case are agreed, let me put this to you, that there is a public key which was used in the Coinbase transaction with the Genesis Block. Do you agree with their evidence in that regard?</p> <p>A. No. Neither are cryptographers. I mean, Ms Meiklejohn -</p>	<p>Dr Wright disagreeing with the evidence of both cryptocurrency technology experts in this case, in relation to whether a public</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Professor Meiklejohn.</p> <p>A. Professor Meiklejohn studies sociology and socio, sort of, legal aspects of Bitcoin, etc. Dr Gao looks at other aspects of scalability and Bitcoin. Neither have studied cryptography in any real depth. What I will note is, saying that something is a string of numbers doesn't make it a key. Now, while you can take any string of numbers and say that it is a key, that doesn't mean that you can actually get a private key from it.</p>	<p>key was used in the Coinbase transaction with the Genesis Block, and stating that neither of them are cryptographers.</p>
<p>ATO Claims and Investigations</p>		
<p>{Day7/59:22} - {Day7/60:6}</p>	<p>Q. And that claim included tax offset claims for sums paid to W&KID, a company set up by yourself and Mr Kleiman, for operating a supercomputer, didn't they?</p> <p>A. It did.</p> <p>Q. And they also included claims for US\$ 2 million for materials and assistance supposedly received from Professor David Rees, a UK - based mathematician, didn't they?</p> <p>A. Yes, that was all given to the ATO a year before he died.</p>	<p>Dr Wright admitting his company C01N made tax claims that included tax offset claims for sums paid for operating a supercomputer and for materials and assistance supposedly received from Professor Rees.</p>
<p>{L11/354/1} - ATO Reasons for Decision</p>		
<p>{Day7/60:11} - {Day7/61:3}</p>	<p>Q. {L11/354/1}, please. Do you recognise this as a paper giving reasons for the ATO's decision on the tax offset claims - R&D tax offset claims by C01N Pty Ltd for the 2012 to '13 tax year?</p> <p>A. Sort of. It's only an interim document, and what this is is the high net worth individuals took over the claim rather than the R&D, so it's not really the way you're putting it.</p> <p>Q. It's a set of reasons for decision by the ATO, isn't it?</p> <p>A. No, it's actually the high net worth team, who have no rights to actually do this.</p> <p>Q. Well, I'm going to suggest to you that it is what it says, "Reasons for decision", prepared and issued on behalf of the ATO.</p> <p>A. No. I know all about this. I've gone through it multiple times. Arna Synnot was also there in 2013 when everything got reversed by the ATO as well.</p>	<p>Dr Wright not accepting the obvious truth that the document being displayed on-screen is the ATO reasons for decision in respect of the tax offset claims by C01N Pty Ltd.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day7/62:11} - {Day7/63:12}</p>	<p>Q. Were you responsible for the ATO being informed that Professor Rees was provided with private keys and - on 28 June 2013 and the other information set out in paragraphs 267.1 and 267.2?</p> <p>A. No, that's not what they were told. They were told he was transferred Bitcoin at a particular time, and they were initially told one year before this. They then chose to do the audit after he died, on his stuff, saying that he couldn't prove anything.</p> <p>Q. So you say that the ATO misrecorded the information which had been provided to it, do you?</p> <p>A. Oh, consistently. That was the whole point of the - being in the tribunal. Every single thing that they put in. That's why they didn't actually have the R&D team involved.</p> <p>Q. You're aware, aren't you, as they record here, that the ATO recorded that they had communicated with all four of Professor Rees' daughters, yes?</p> <p>A. And? Sorry.</p> <p>Q. You're aware that they recorded that?</p> <p>A. Yes, they called them afterwards.</p> <p>Q. You're aware that none of the daughters had any knowledge of you, or the payment, or the Bitcoin, or the supposed suggestion that Professor Rees was doing consulting work, right?</p> <p>A. Again, they were never involved. I've never met them either.</p>	<p>Dr Wright blaming third parties, namely the ATO, for mis-recording the information that had been provided to it regarding Professor Rees and the transfer of private keys to him.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day7/63:13} - {Day7/64:18}</p>	<p>Q. But on your account, Professor Rees was doing substantial work, providing materials and assistance for - valued at US\$2 million and none of his family knew that he was even doing any consulting work, or that he did such work in principle, right?</p> <p>A. No. Again, that's completely wrong. I agreed to transfer a certain amount of Bitcoin in the early days. That was based on the transfer of notes. Those notes go back quite a long way. So, when I made the agreement, this was actually worth a lot less, but Bitcoin goes up in price, I still transfer it.</p> <p>Q. Go to the top of the page, please: "All four of Professor Rees' daughters advise they have never heard of the taxpayer or Dr Wright. Professor Sarah Rees also advised that Professor Rees did not undertake consulting work." Now, Dr Wright, one can understand that they might not have heard of you, but it would surely be surprising, if Professor Rees' daughter was unaware of him even doing consulting work when you claim that he did that work which produced materials valued at US\$2 million? That would be surprising, wouldn't it?</p> <p>A. Again, that's not how I framed it. What I noted and what I said, very categorically, which I have said in all of these things, was I had, going back to the '90s, discussed a number of mathematical concepts with Professor Rees. What I then did was I said I would give him a certain percentage of what I've created back when I first created it, and I did. When I made the promise, it was a nominal amount. He acted basically just as a professor.</p>	<p>Dr Wright is questioned about the implausibility of Professor Rees' family being unaware of his consulting work for Dr Wright's company. Dr Wright does not answer the question that is asked and provides an evasive response, refusing to accept the obvious truth that Professor Rees' daughters had never heard of this collaboration and therefore, bearing in mind his ill health, it was very unlikely to have happened.</p>
<p>{Day7/64:19} - {Day7/65:5}</p>	<p>Q. Dr Wright, this is another instance of you relying on a fictitious collaboration with a well known person who's died, just like Gareth Williams, isn't it?</p> <p>A. No, actually, the contact was given to the ATO in 2012. They could have contacted them any time. It's like Liberty Reserve. They knew about Liberty Reserve in 2009. They then complain, after 2013 when it shut down, that they can't get records. Or High Secured. They had High Secured records going back to 2013. It was only in 2015 that they jumped up and down going, "We can't get into your records because they're shut down now" in 2015.</p>	<p>Dr Wright blaming third parties, namely the ATO, in denying that his collaboration with Professor Rees was fictitious.</p>
<p>{Day7/65:6-20}</p>	<p>Q. Dr Wright, how old was Professor Rees when he was doing the supposed consulting work for you and receiving these - access to these Bitcoin addresses?</p> <p>A. As I explained, what he did was he accessed -</p>	<p>Dr Wright refusing to accept the obvious truth that Professor Rees was in declining health when he was supposedly doing the consulting work and</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Just a simple question, Dr Wright. How old was he when he was doing the consulting work and then receiving the Bitcoin addresses?</p> <p>A. Around the same age as my grandfather.</p> <p>Q. Which is?</p> <p>A. I don't know. Old.</p> <p>Q. He was in his 90s, wasn't he, in declining health, and at the time that he supposedly received the Bitcoin addresses, in a nursing home, not using a computer?</p> <p>A. When he originally did that, he still had his computer. That was four years before, of course.</p>	<p>receiving the Bitcoin addresses.</p>
<p>{L9/89/1} Cracked, Insecure and Generally Broken Blogpost</p>		
<p>{Day7/66:17} - {Day7/68:10}</p>	<p>Q. I'm just asking you about the capture. It's shown as captured on the Wayback Machine on 2 June 2014, isn't it?</p> <p>A. That was the first capture, yes.</p> <p>Q. We can see the text for an article on Saturday, 10 January 2009: "Bitcoin. "Well ... e - gold is down the toilet. Good idea, but again centralised authority. "The Beta of Bitcoin is live tomorrow. This is decentralised ... We try until it works. "Some good coders on this. The paper rocks." And then a web link. Dr Wright, do you say that this was a genuine post which you put on your website on 10 January 2009?</p> <p>A. So, firstly, it's not my website. Secondly, I don't post on my blogs. I haven't posted on my blogs. I don't ever post on my blogs. Every single blog I have had has been run by third parties. My current one, the Craig Wright.net is run by third parties. The one before that, third parties. The medium post, third parties.</p> <p>Q. Pausing there. Do you accept that this is - or do you say, because we certainly don't say that it's authentic to 10 January 2009, but do you say, to the best of your knowledge, that this post was put up on 10 January 2009?</p> <p>A. I have no idea. I don't run blogs. I never have.</p> <p>Q. Who was responsible for running this blog on Saturday, 10 June 2009?</p> <p>A. In early - early 2009, David, an American. Not David Kleiman, another David. I don't remember his name. After that, there was another person. After that, another person. After</p>	<p>Dr Wright asserting that he is not responsible for any posts on his blogs and that they are all run by third parties, and therefore does not know the date on which this blog post was uploaded.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>that, people working for Panopticon. Then Uyen, then Hotwire, then DeMorgan.</p> <p>Q. But you can't actually say who was running the blog and would have been responsible for any posts on 10 January 2009?</p> <p>A. David, but I can't remember his last name.</p> <p>Q. Who was he employed by?</p> <p>A. He was a consultant with Information Defense.</p> <p>Q. Did he work as a self - employed person or through a company?</p> <p>A. I don't recall. I think he was self - employed, but I'm not actually sure. I paid him part - time.</p>	
{Day7/68:15-20}	<p>Q. If that post of 10 January 2009 was an actual post issued then, it would have been rather blowing your cover as Satoshi, wouldn't it?</p> <p>A. Not necessarily. It just could mean, like Hal Finney said, running Bitcoin. But, no, I didn't actually post it, so I can't say.</p>	Dr Wright is evasive, claiming he did not post this blog post.
{Day7/70:10-11}	<p>Q. And page 6 {L8/368.1/6}, we now see two articles, yes?</p> <p>A. We do.</p>	Dr Wright accepting that a copy of the page captured on 18 February 2014 shows 2 articles appearing on the blogs between 4 January 2009 and 11 January 2009.
{Day7/71:2-23}	<p>Q. Would you accept that that set of captures suggests that the Bitcoin post was likely added between 12 December 2013, the last time there was just one article shown, and 18 February 2014, when there were two articles shown?</p> <p>A. No, not necessarily. The reason being that, in blogger, you can actually hide posts. It's also possible to use a robot.txt to have things displayed or not. What I would say, though, is all of this is linked to the Gizmodo outing. So this was used as part of that, and then also by Mr Maxwell as part of the discrediting. So that was - he must have known, of course, how this came about.</p> <p>Q. Well, I can certainly agree with you that the article that we looked at in the first place, the Bitcoin article featured in the WIRED and Gizmodo pieces, is something leaked to them, but I'm going to suggest to you that the plain meaning of all of these captures is that this article was added, backdated, in either late 2013 or very early 2014.</p>	Dr Wright accepting that the blog post was likely added in 2014, and blaming third parties for its backdating, possibly Ira Kleiman.

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. I would say more likely 2014, which is when my problems with Mr Kleiman started.</p>	
<p>{Day7/71:24} - {Day7/72:22}</p>	<p>Q. Now, if the captures are right, it was added by 18 February 2014, and if that's right, that was before you had had any problems or disagreement with Mr Kleiman, isn't it?</p> <p>A. I thought so, but I was wrong. I discovered that Mr Kleiman actually had already had legal advice and litigation sort of - what do you call it - lawyers engaged before he even sent his first email to me.</p> <p>Q. So you're saying that Mr Kleiman may have been responsible for putting this backdated post on your blog even before you sent your email reaching out to him in February 2014?</p> <p>A. No, I said it would be linked to what happened there. As I noted, I had other disgruntled employees already at this point and they worked with him. Why anyone started setting any of this up, I don't know.</p> <p>Q. So your working hypothesis is that some disgruntled employee, perhaps working with Ira Kleiman, put that blogpost on your blog in early 2014, backdating it to 2009? That's your working hypothesis, is it?</p> <p>A. No, I don't really have one. All I know is that shouldn't have been up there, someone put it there, and someone used it with the ongoing communications with Gwern and then WIRED and Gizmodo.</p>	<p>Dr Wright blaming third parties (possibly Ira Kleiman) for the backdated blog post, even though 18 February 2014 pre-dates Dr Wright's email reaching out to Mr Kleiman.</p>
<p>Dr Wright telling ATO in 2009 that he had created Bitcoin</p>		
<p>{Day7/73:6} - {Day7/74:14}</p>	<p>Q. Well, you know that's disputed, Dr Wright. {L10/367/1}, please. Just before I ask you about this, your last answer was that you'd told people in the ATO in 2009 that you had created Bitcoin, right?</p> <p>A. Yes, actually, I did.</p> <p>Q. Are there any documents that you have showing that you told Australian taxation officials in 2009 that you'd created Bitcoin?</p> <p>A. Yes, I communicated as part of all of this. That's why the private ruling in 2013 included mining in 2009.</p> <p>Q. Dr Wright, is there a single document which has been disclosed in these proceedings which demonstrates you</p>	<p>Dr Wright is pressed as to whether he has any documents that demonstrate he was telling the ATO he was Satoshi in 2009 or 2010, he is evasive in response and does not answer the question.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>telling the Australian tax authorities, dated to 2009, that you were Satoshi?</p> <p>A. Yes, I communicated as part of all of this. That's why the private ruling in 2013 included mining in 2009.</p> <p>Q. Dr Wright, is there a single document which has been disclosed in these proceedings which demonstrates you telling the Australian tax authorities , dated to 2009, that you were Satoshi?</p> <p>A. Again, the 2013 is based on 2009 documents -</p> <p>Q. Well, Dr Wright -</p> <p>A. - they had.</p> <p>Q. - we're disagreeing about whether the private ruling is based upon what you say you said in 2009 or, as we say, a set assumed facts. Setting that to one side, is there any document from 2009, or indeed from 2010, showing you telling the ATO that you were Satoshi?</p> <p>A. Two points. One, I don't have any Information Defense or Integrys files any more. The second point is, I know you're saying you're disputing this, but the simple fact is, you don't just say something after an extensive audit when the ATO already have all the documentation, when it's gone through a court process, when multiple audit firms, including KPMG, etc, have been involved, then sitting there going, "Oh, they just assumed".</p> <p>Q. Well -</p> <p>A. Sorry, that's just claptrap.</p>	
<p>{Day7/74:18} - {Day7/75:7}</p>	<p>MR JUSTICE MELLOR: Dr Wright, I just need to tell you something. If you don't answer the question, I'm going to assume you have no answer to it, okay? So the question was: "Setting that to one side, is there any document from 2009, or indeed from 2010, showing you telling the ATO that you were Satoshi?" Now, you haven't answered that question.</p> <p>A. I don't actually know, my Lord. I know there's a lot of documents in there. I didn't run the accounting, I don't actually know which ones are part of that in disclosure. So some of the accounting documents are in there. My simple answer is, I don't actually know what, in the million documents in that file, happen to be from that.</p>	<p>Mellor J reminding Dr Wright that he has not answered the question asked above. Dr Wright ultimately states that he does not know if there are any documents that demonstrate he was telling the ATO he was Satoshi in 2009 or 2010,</p>
<p>Dr Wright's dealings with Stefan Matthews and Robert MacGregor</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day7/79:7} - {Day7/80:10}</p>	<p>Q. In any event, the contact with Mr Matthews and Mr MacGregor began again by early 2015, didn't it?</p> <p>A. Yes, I contacted Stefan again in 2015.</p> <p>Q. And by that stage, your businesses were in pretty desperate straits, weren't they?</p> <p>A. I wouldn't say it that way. What I didn't know how to do was get out of the problems we were having with the Tax Office.</p> <p>Q. Mr Matthews gave an interview to CoinGeek, and we can ask him about this, in which he described your businesses as having gone down to staff numbers of pretty much zero and being in all sorts of problems at that point in time, early 2015. Is he wrong about that?</p> <p>A. No, we had reduced staff members, but it wasn't zero. We still had a few developers and - but it was probably a quarter of what it was. What we did have problems were getting - transferring any money, exchanges, etc, for Bitcoin were nearly non - existent and difficult, we were having a lot of problems with the ATO. I did have other options. So where you're saying "desperate", we had an offer from Macquarie Bank for 10 million a year funding for four years, which would have actually been more money.</p> <p>Q. Is that an offer that you provided any documents in relation to?</p> <p>A. They're in the disclosure. I don't know what's been disclosed, but they're in the disclosure.</p> <p>Q. We can ask about that, but they don't ring a bell with me.</p>	<p>Dr Wright not accepting that his businesses were not doing well in early 2015, referring to an "offer" from Macquarie Bank for funding that does not appear to be in his disclosure in these proceedings.</p>
<p>{L9/395/1} "Investment Pack: Stefan - Calvin Ayre" meeting invitation, ID_004092</p>		
<p>{Day7/80:11} - {Day7/81:2}</p>	<p>{L9/395/1}, please. Now, this appears to be a meeting invitation suggesting that a reasonably detailed investment meeting was planned for 27 April 2015 involving yourself and Mr Matthews; correct?</p> <p>A. No, this was Stefan had put together one with Calvin Ayre, which was one of the first times I met him. The initial thing wasn't investing in the companies, Rob ended up doing - Rob was separate, and what was proposed was selling Bitcoin to him, but Calvin wasn't interested at the time.</p>	<p>Dr Wright claiming, implausibly, that this meeting was about selling Bitcoin.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. If we look at the invitation, it's referred to as: "Investment Pack: Stefan - Calvin Ayre." Do you say the meeting wasn't about investment?</p> <p>A. Well, it was, but it was going to sell Bitcoin as well as then try and bring him into the company. So, Stefan was there, who brokered it, with Calvin Ayre.</p>	
<p>{Day7/81:13} - {Day7/82:18}</p>	<p>Q. So you say that in this initial meeting on 27 April 2015 you were upfront with them that you were Satoshi and you were going to be selling Bitcoin to them?</p> <p>A. No, I didn't mention that I was Satoshi at all. My selling Bitcoin had nothing to do with my identity. I didn't tell Rob, at this stage, that I was Satoshi, I didn't tell Calvin. That happened later. They basically -</p> <p>Q. So what do you say you were selling to them at this meeting?</p> <p>A. Bitcoin. As in -</p> <p>Q. As in Bitcoin assets?</p> <p>A. Yeah. As in tokens</p> <p>Q. I see.</p> <p>A. As in BTC. I wasn't able to sell the quantity I needed on market, so I was going to do an over - the - counter trade.</p> <p>Q. So, at least we're clear on that. Where, in the many bullet points of this document, does it refer to you selling Bitcoin tokens rather than participating in an investment discussion?</p> <p>A. It doesn't.</p> <p>Q. So you were having a meeting which was about selling Bitcoin tokens, but in fact the entire content of the invitation and all the agenda bullet points were completely irrelevant to the real discussion?</p> <p>A. No, not at all. Calvin was the head of Bodog, which was a gaming company. So, what I wanted to do was basically show off what we're doing and how this would actually be good for his company. I didn't only want him buying Bitcoin, I wanted Bodog using Bitcoin.</p>	<p>Dr Wright claiming that this meeting was about selling Bitcoin, but that he did not mention he was Satoshi.</p> <p>Dr Wright admitting that the meeting invite ({L9/395/1}) does not refer to selling Bitcoin.</p>
<p>{Day7/83:3-9}</p>	<p>Q. And you were seeking investment to get your companies out of a very big financial hole, weren't you, Dr Wright?</p> <p>A. No, I was making a very big financial hole. The cost of running everything I was doing was my financial hole. I was spending over 60 million a year, continuous, at that point.</p>	<p>Dr Wright confirming that his company was in financial need when he met with Stefan Matthews and Calvin Ayre.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{L9/489/1} - email from Craig S Wright to JLP, Robert MacGregor, Stefan Matthews, Ramona Watts re: Escrow arrangements</p>		
<p>{Day7/87:15} - {Day7/88:5}</p>	<p>Q. So, you were - the response to your request for the fighting fund was for Mr Ayre to send Mr Matthews and Mr MacGregor to Australia to drill into your books and business, yes?</p> <p>A. No, Robert's running a separate company, but Rob had extensive dealings with Bodog. So, Rob ran a payment processing company and also IT company that had extensive interactions with Bodog, and if all of this would work, it would help with the - what nTrust did. NTrust did money transfers, and if Bitcoin could be used, it would make that simpler. That would make Calvin's life simpler as well. So, there are actually two things. There's Stefan coming down to represent, sort of, the broader deal, Rob as a possible deal, and then Calvin talking about the escrow deal.</p>	<p>Dr Wright explaining the nature of his requests for a "fighting fund".</p>
<p>{L9/491/1} - email from Allan Pedersen to Ramona Watts Re: Canadian investors in</p>		
<p>{Day7/89:20} - {Day7/90:14}</p>	<p>Q. Fine. This email shows that your wife was desperately trying to gather together employees and ex - employees to make it look like your office was actually in business, doesn't it?</p> <p>A. Not the way that you're saying. But, yes, we needed the other people in there. Some of them were only part - time at this point, and others worked from home to reduce costs. So, having them in the office was important.</p> <p>Q. As Mr Matthews told CoinGeek, your business was in desperate straits and basically down to nil employees, and here you were trying to set up a fake office to impress the investors. That's the position, isn't it, Dr Wright?</p> <p>A. No. We still had some employees. We were down to a quarter or so of everyone, we had people working part - time, others from home, and the offer that I had at the moment, the alternative was with Macquarie and I didn't particularly want to sell out to a bank.</p>	<p>Dr Wright confirming that having employees in the office was important for the meeting, and that he was down to a quarter of his employees.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{L10/33/2} - Term sheet DeMorgan/NewCo - ID_004127		
{Day7/92:11-20}	<p>Q. Then the next section, a services agreement directly between the NewCo and yourself, consisting of a \$1 million initial rights payment and subsequent payments of \$500,000 per year for five years, yes?</p> <p>A. Correct.</p> <p>Q. And that refers to there also being a grant of exclusive rights to your life story for subsequent publication or release?</p> <p>A. Yes, detailing the growth of the company, etc.</p> <p>Q. We'll come to that in a moment.</p>	<p>Dr Wright confirming that the agreement between NewCo and himself granted “exclusive rights to [his] life story for subsequent publication or release”.</p>
June 2015 Bailout		
{Day7/94:18} - {Day7/95:1}	<p>Q. We can take that off screen now. So by this stage, so the end of June 2015, a deal had been done for a bailout of you and your companies, hadn't it?</p> <p>A. No. As I said, there was a thing to basically lock the IP away so that we didn't have problems with the ATO. As I noted, I had other options, hence why I wasn't as worried as Stefan, but my choice was I didn't want to sell it to Macquarie Bank.</p>	<p>Dr Wright denying that the deal with Stefan Matthews was a “bailout”.</p>
{Day7/95:2} - {Day7/98:5}	<p>Q. And at some point in these negotiations, you had made your claim to be Satoshi, hadn't you?</p> <p>A. Not at all. There was nothing to do with Satoshi in any of these.</p> <p>Q. So you're saying that the life story agreement at that stage had nothing to do with your life story to being Satoshi?</p> <p>A. No. We have 1,000 granted patents, I have 1,900 original ideas. That in itself is a life story. So what they were looking at is the development of all that intellectual property.</p> <p>Q. Well, the life story payment was separate from the intellectual property, or the concept of a life story was separate from the intellectual property, Dr Wright. Are you saying that the life story, as far as Mr Matthews and Mr MacGregor were</p>	<p>Dr Wright is asked about whether he made his claim to be Satoshi during the negotiations with Mr Matthews et al. Dr Wright is evasive in response, claiming that the life story agreement had nothing to do with his being Satoshi.</p> <p>Dr Wright admits that Mr Matthews knew he claimed to be Satoshi when the</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>aware, at that stage, June 2015, did not include your claim to be Satoshi?</p> <p>A. I have no idea what Mr MacGregor thought, ever. So you're asking me to say what someone else thinks. I can't do that. I'm an Aspie.</p> <p>Q. Well, let's focus on the two of them and just, rather than what they felt, what they knew.</p> <p>A. Again, I don't know what they know. I don't know what they think, believe, know, feel.</p> <p>Q. Just listen - let me ask you the question and you can see if you can answer it. As at the time these heads of terms were entered into, to your knowledge, did Mr Matthews know that you were Satoshi, on your claim?</p> <p>A. Well, he would have. I gave him the White Paper.</p> <p>Q. To your knowledge, at that time, when you entered into this term sheet, did Mr MacGregor know that?</p> <p>A. I've no idea.</p> <p>Q. So Mr Matthews, who was the actual signatory, knew that the life story was of somebody who claimed to be Satoshi?</p> <p>A. No, he did not. All of the talks and negotiations were about having basically the new company recorded as it's growing, building, etc.</p> <p>Q. But just, again, focusing on the question. At the time of this agreement, you say that Mr Matthews, who was the signatory, knew that the life story was of you and knew that you claimed to be Satoshi?</p> <p>A. Again, no. It was the life story to do with all the building and the intellectual property. You keep twisting the words. I'm not going to agree to that, because that's not what it was. I sat down and I spoke to Stefan about this, and what he said was, "We're going to document the growth of the company".</p> <p>Q. So, even though Stefan was the - was a signatory to that agreement and you say he knew that you were Satoshi, the life story at that stage was not going to include this biographical detail of you being Satoshi?</p> <p>A. I have no idea what it was going to include. What they said was they were going to document the growth of the company.</p> <p>Q. But you were entering into a multi - million dollar deal which required you to assist in providing a life story and you say you just didn't know whether that life story you were being required to provide included your claim to be Satoshi; is that what you're saying?</p>	<p>Heads of Terms were entered into.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Again, I entered into the smaller deal where I didn't have the restrictions, where the promise was I get to basically go out and invent and not have to run the company. The nature of the deal was, rather than being the CEO, I'm chief scientist, my whole role is I sit in an office and I invent things all day.</p> <p>Q. How many patents had been applied for and granted, by that stage, which were the subject matter of this agreement?</p> <p>A. Patent applied for, no; that's why we needed help. I didn't know how to. What I had at this stage was 1,300 ready to be turned into patents documents. So, when Cerian and the Australians came in, I had 1,300 research projects. The average of those is about five to six patents per document.</p> <p>Q. I'm going to stop there, because I think you've answered the question.</p>	
<p>{L10/66/1} - Email Ramona Watts to Craig S Wright forwarding email from Andrew Sommer (Clayton Utz) 7/4/2015</p>		
<p>{Day7/98:6} - {Day7/98:11}</p>	<p>After that deal, or shortly after that deal, Clayton Utz, the solicitors who had been acting for you in your dealings with the ATO, terminated their retainer, didn't they?</p> <p>A. Yes, people sent in false information and fabricated documents to them.</p>	<p>Dr Wright blaming third parties for fabricating documents and sending false information to Clayton Utz.</p>
<p>{Day7/98:12} - {Day7/99:6}</p>	<p>Q. {L10/66/1}, please. Mr Sommer was a solicitor at Clayton Utz, wasn't he?</p> <p>A. He's a partner.</p> <p>Q. And at the start of July 2015, he wrote this email to your wife explaining why they had to terminate their retainer, didn't he?</p> <p>A. He did.</p> <p>Q. And he recorded, didn't he, that they had submitted supposed emails from various individuals at your instruction?</p> <p>A. No, actually, those came from third parties. We had them forensically analysed and it showed that the claims were false.</p> <p>Q. He - the purport of this email is that they'd submitted emails on your behalf, apparently from ATO officials, and the ATO were now saying that these emails weren't genuine?</p> <p>A. They said that until we had them forensically analysed and demonstrated that they actually came from an ATO server.</p>	<p>Dr Wright blaming third parties for sending false emails to Clayton Utz, who then submitted them to the ATO on his behalf.</p> <p>Dr Wright now blaming the ATO itself for these emails; referring to forensic analysis to demonstrate these emails came from an ATO server. There is no evidence of this</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
		analysis in these proceedings.
{L10/68/1} - Clayton Utz termination of engagement DeMorgan Limited		
{Day7/99:7} - {Day7/101:11}	<p>Q. {L10/68/1}, please. Do we see that on 6 July 2015, Mr Sommer terminated the retainer on the basis that information had been provided to the firm which raised serious questions about the integrity of documents provided by you; correct?</p> <p>A. No, by the firm.</p> <p>Q. 6 July 2015: "It is with regret that we inform you in your capacity as Director of DeMorgan Limited ..." This is to your wife: "... that Clayton Utz has decided that we must terminate our engagement with DeMorgan Limited. "Information has been provided to our firm which raises serious questions about the integrity of documents provided by Dr ... Wright, both to our office and to the Australian Taxation Office. We believe this information to be credible. In these circumstances, we can no longer represent DeMorgan Limited in the disputes it and its subsidiaries has with the Australian Taxation Office." That's what he wrote, isn't it?</p> <p>A. That's what the firm wrote. He actually called and said that he didn't want to.</p> <p>Q. It's his signature at the bottom, isn't it?</p> <p>A. He signed it, yes.</p> <p>Q. So he, on behalf of the firm, was refusing to act for you because he considered there to be credible evidence, raising serious questions about the integrity of documents provided by you?</p> <p>A. No, he was actually put under pressure. Clayton Utz was also dealing with the Tax Office and they were a large part of their revenue, so when the Tax Office said that, they had no choice. When we had the documents forensically analysed, all of this turned out to be false.</p> <p>Q. So do you say that when he signed that letter, he did not believe the words he was writing?</p> <p>A. Yes, he spoke to my wife and myself and he said he was under extreme pressure from the firm and if he didn't do it, basically there would be problems.</p>	<p>Dr Wright claiming that Andrew Sommer phoned him and told him something different from the termination letter at {L10/68/1}, that he did not want to terminate the retainer, and that he has evidence to corroborate this.</p> <p>Dr Wright not accepting the obvious truth of the words in the email at {L10/66/1} and this letter.</p> <p>Dr Wright blaming the ATO for the fake emails, referring again to the forensic analysis that shows the emails originated from the ATO server and asserting (falsely) that this is in his witness statement and/or disclosure.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. And do you say that when he wrote the email that we looked at a moment ago, private, to your wife, that he didn't believe the words he was writing in that email?</p> <p>A. Yes, I do.</p> <p>Q. Dr Wright, have you ever obtained any evidence from him to corroborate your position on this?</p> <p>A. Yes, I have, and everyone keeps going "privilege". I also have the forensic documents analysing that the emails that were purported to come from me actually came from a server inside the ATO.</p> <p>Q. Well, Dr Wright -</p> <p>A. They're in disclosure.</p> <p>Q. Well, once again, you keep making assertions about what is in disclosure. We do have -</p> <p>A. They're in my witness statement.</p>	
<p>{L10/66/1} - Email Ramona Watts to Craig S Wright forwarding email from Andrew Sommer (Clayton Utz) 7/4/2015</p>		
<p>{Day7/101:17} - {Day7/102:10}</p>	<p>Q. And when you say that this partner of Clayton Utz, who had been working for you for some time, wrote documents which were, on your account, dishonest in expressing his view, that's just wrong, isn't it?</p> <p>A. Yes, I didn't say dishonest; I said that he had to do it because of the firm.</p> <p>Q. Well, if he wrote, "We believe this information to be credible", when he didn't believe it to be credible, that would be a dishonest statement in his letter, wouldn't it?</p> <p>A. No, "we" refers to the firm. And if he gets outvoted by other partners who don't like me, then that's it.</p> <p>Q. Back to the email at {L10/66/1}. Over the page {L10/66/2}, after explaining how serious the matter is, Mr Sommer urged you to tell Mr MacGregor and Mr Matthews of the matter urgently. He said that, didn't he?</p> <p>A. He wrote it.</p> <p>Q. Did you inform them as a matter of urgency?</p> <p>A. Yes, of course.</p>	<p>Dr Wright not accepting the obvious truth that Mr Sommers would have been dishonest if he wrote the email and retainer letter expressing one view and terminating the engagement, and then phoned Dr Wright expressing another regarding the ATO emails.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{L10/339/1} - Email Stefan Matthews to Carla Hontiveros Orbeta FW: The book 11/09/2015</p>		
<p>{Day7/102:19} - {Day7/104:10}</p>	<p>Q. Thursday, September 10, 2015, "Subject: The book": "Good morning noon or night. "I had a discussion with Stefan today. "When we do the book, I want to make sure it is honest. I am not looking at being St Craig and I feel the best will be to go into all the story." Did you write an email with this content, looking at it now?</p> <p>A. I don't recall.</p> <p>Q. Reading the text, does it look like your style, as far as you can see?</p> <p>A. Not really, no.</p> <p>Q. The "PS" at the bottom {L10/339/2}, please: "PS "I may have to have a special chapter for Stefan. And asked him to review the White Paper and it was on his desk at one stage for months yet he still never got round to it. In 2009 I had begged him to invest in some of the ideas I had. So is a little bit of a jab and poke at someone that I do respect, but I need to say how wonderful it is that he passed up that opportunity because if he had, and he had invested in buying 50-100,000 bitcoin at that point you would not be here now and we would not be discussing anything today." Do you think you wrote those words at that time?</p> <p>A. Not at all. I don't generally - I can't ever think of a PS I've used, and a lot of the other stuff doesn't look like mine. I do use the term "vulture capitalists".</p> <p>Q. Then, page 1 again {L10/339/1}, further up the page, we see what appears to be a positive response from Mr Ayre and a positive response from Mr Matthews. Are you able to say whether or not you received emails of those kinds on those dates, 10 and 11 September 2015?</p> <p>A. Not to my knowledge.</p> <p>Q. {L10/424/2}.</p> <p>A. Actually, I do know something. Tyche was the British company of Robert's, and I had no involvement with that at that point. The first time I visited the UK and over here was in October. So this is September.</p> <p>Q. So you think that isn't a genuine email?</p> <p>A. I don't recall it, and it doesn't look familiar.</p>	<p>Dr Wright refusing to admit any aspect of this email chain.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{L10/424} - Email Ramona Watts to Robert MacGregor, Craig Wright, Stefan Matthew, c, JLP, Rob Gillespie 27/10/2015 RE: Publication</p>		
<p>{Day7/104:11} - {Day7/105:12}</p>	<p>Q. We're now on {L10/424/2}, an email at the bottom of the page from Robert MacGregor to you and others, 21 October 2015, as I say, to you, Mr Matthews, Ramona Watts, Calvin Ayre, Rob Gillespie and "JLP", I think that's Mr Phillips. You may not remember. Do you recall this as an email that you received around that time?</p> <p>A. I don't.</p> <p>Q. Now, this is an email which is contained within your list of documents associated with your first witness statement, your PD57AC list, which suggests that you reviewed it at the time that you were making your first witness statement. Do you recall doing so?</p> <p>A. I went through my first witness statement, yes.</p> <p>Q. Do you recall reviewing this email when you were preparing your first witness statement?</p> <p>A. Not off the top of my head, no.</p> <p>Q. Mr MacGregor writes, as this email is transcribed, that he: "... had a very productive call yesterday ... with the William Morris agency's lead literary agent in [New York] regarding ... manuscripts and having them represent ... interests globally for the media rights to your autobiography and history, Craig ..." Do you remember, in October 2015, having those sorts of discussions?</p> <p>A. No. I was travelling to the UK at that point.</p>	<p>Dr Wright refusing to admit any aspect of this email chain, despite it being listed in the list of documents associated with his First Witness Statement {E/1/40}.</p> <p>His evidence also conflicts with {L16/406/7}, a blog post which shows that he entered London via Heathrow on 25 October 2015, not at the date of the email (21 October).</p>
<p>{Day7/105:13-23}</p>	<p>Q. And if we go down - if we go to page 3 {L10/424/3}, do we see that he, at the top of the page, asks a series of questions all about Satoshi and the Bitcoin project?</p> <p>A. I can see what it's writing there, yes.</p> <p>Q. If this email is a genuine one, then in late October 2015, he was asking you for details about Satoshi and the Bitcoin project with a view to dealing with literary agents, wasn't he?</p> <p>A. No. Can you have a look at the - who the Craig Wright is on this email? Just typing in "Craig Wright" doesn't make it Craig Wright. So maybe page 1?</p>	<p>Dr Wright not accepting the obvious truth that he was the "Craig Wright" on this email chain.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day7/106:16} - {Day7/107:22}</p>	<p>Q. May we have {E/1/40}, please. This is the "List of Documents Shown to Dr Wright During Witness Interviews" for preparing your first witness statement. Now, Dr Wright, I don't want you to tell me anything privileged, but item 7 is this document, according to this list. Would you accept that you saw this email in the course of preparing your first witness statement?</p> <p>A. Yes, and I didn't recognise it then either.</p> <p>Q. Now, Dr Wright, if I had seen an email which looked as though it was fake and conflicted with aspects of my story and I was preparing a witness statement, having been pointed to it, I would be jolly sure to make clear in the witness statement that there was a fake document. Would you feel the same?</p> <p>A. No, I wouldn't, actually. There are multiple fake documents and I've been noting that for quite some time. I'm not going to sit there and pull out every fake document in the pile. I've noted multiple times that there are documents that don't involve me.</p> <p>Q. Back to the document {L10/424/1}. Your wife gives a response, according to this email, about when the project began, why, with whom, lots of details, including you being: "Captivated by Tim May's and Wei Dai's contribution to BlackNet ... in 1998". Do you say that that's a genuine email written on 26 October 2015?</p> <p>A. Can't say. What I do know is, at that time, I was travelling and going to London, so there's a part in this where Rob's saying, "I'll meet you in London later", but that would be meeting me in London then. I mean, that's wrong.</p>	<p>Dr Wright refusing to admit any aspect of this email chain, despite it being listed in the list of documents associated with his First Witness Statement {E/1/40}.</p> <p>Dr Wright admitting there are multiple fake documents in these proceedings "I'm not going to sit there and pull out every fake document in the pile. I've noted multiple times that there are documents that don't involve me."</p> <p>Dr Wright stating that he could not have met Rob in London conflicts with {L16/406/7}, a blog post which shows that he entered London via Heathrow on 25 October 2015.</p>
<p>{L11/47/1} Email from Mr MacGregor to various including Dr Wright "Bakers"-24 November 2015</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day7/107:23} - {Day7/109:8}</p>	<p>Q. Next {L11/47/1}, please, an email dated 24 November 2015 from Mr MacGregor to you and others. Do you recognise this as a genuine email, or is this another one you say is fake?</p> <p>A. No, this is one I do recognise. The "To" includes Craig at Tyche, which isn't me. Even though it says "Craig Wright". I don't actually have that domain and that email.</p> <p>Q. This doesn't, I think, refer to you as - by reference to Tyche.</p> <p>A. I thought this did. One of them did.</p> <p>Q. Can we go down the page -</p> <p>A. I'm pretty sure it was this one.</p> <p>Q. Go down the page. And this is - I think this is a one - page document. Yes, the operator is confirming. So all this says at the top is that it's from Mr MacGregor at Tyche to you, amongst others?</p> <p>A. Yes, but in the original. In the actual email, which I've seen of this one, I believe that's Tyche.</p> <p>Q. Do you say that this is an email which - the content of which is genuine?</p> <p>A. I've no idea. You're asking me about an email sent from someone else to an email address I don't control, so I can't say whether it's genuine or not.</p> <p>Q. Well, this one refers, at item (5), to Mr MacGregor proposing creation of a proof package - proof packet rather, including establishing control of Satoshi Nakamoto's private keys and so on. Was that being discussed by that stage, 24 November 2015?</p> <p>A. God, no. There's no way on earth I'd give over my damn private keys to someone.</p> <p>Q. No, but was that being discussed by Mr MacGregor at that stage?</p> <p>A. I don't know what he was discussing. I mean, honestly, if I'm not the person receiving it and it's a thing set up as Craig Wright and his company, no idea.</p>	<p>Dr Wright denying the obvious truth that this email was sent to him, even though it says "Craig Wright".</p>
<p>{L11/54/1} Email from Craig (Tyche) to Robert MacGregor, c, JLP, Rob Gillespie, Stefan Matthews 25/11/2015 Re Bakers</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day7/109:9} - {Day7/111:15}</p>	<p>Q. {L11/54/1}, please. This is an email dated 25 November 2015, ostensibly from you, "cwright@tyche.co.uk", to Mr MacGregor and others. Do you say that this is another non - genuine email, something you didn't write?</p> <p>A. I didn't write it, no. Tyche is a British company belonging to Rob that I never worked for.</p> <p>Q. So all this content saying - referring to the original White Paper being a good start and engaging with Mr MacGregor's ideas, that's all fake content, is it?</p> <p>A. I've no idea what it is.</p> <p>Q. Are you aware who supposedly created these non - genuine documents, Dr Wright?</p> <p>A. Probably someone at Tyche.</p> <p>Q. Who are you fingering for this?</p> <p>A. I've no idea.</p> <p>Q. Why did you say "probably somebody at Tyche"?</p> <p>A. Because it uses the Tyche domain. It's either someone at Tyche or someone who's compromised Tyche. I don't know. I'm not Tyche. Never have been.</p> <p>Q. Would you accept that if any of these emails is genuine, if the court concludes that any of them is genuine, then you were discussing all of these matters concerning Satoshi outing before the WIRED and Gizmodo outings; correct?</p> <p>A. No, that would be like saying if I put down justicemellor@gmail.com, I could send one as my Lord, but I can't. It's not real, just because my name's on it.</p> <p>Q. Dr Wright, one of your - one point you have stuck to is that you didn't engage in any discussion about coming out as Satoshi until after the WIRED and Gizmodo outings of early December 2015, right?</p> <p>A. I did not.</p> <p>Q. And so these emails were flat against that account, weren't they?</p> <p>A. Not really. They're from Tyche. I have no idea what it is and where it comes from.</p> <p>Q. These are emails that were disclosed by your solicitors on your behalf from material in your possession. It's right, isn't it, that when they were disclosed, nothing was said to the effect that these were all fake documents which you didn't accept, was it?</p>	<p>Dr Wright denying that he wrote this email, blaming third parties, "probably someone at Tyche", but unable to identify who. Dr Wright also blaming his solicitors for including this email in his disclosure.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. No, the disclosure was basically everything from 30 staff laptops, from a server that had access by 200 people, from the third party disclosures in the Kleiman trial, which included everything that Ira Kleiman sent in, everything that Greg Maxwell sent to the ATO, by the way, your client, going right back to 2014. All of that stuff is in my disclosure, so I'm not owning any of it because - just because it's in a pile of something that I'm a corporate executive or have been a corporate executive for doesn't mean I'm owning it. I had to basically give over everything and return everything that matched a search term. There's no requirement and nobody ever asked me to go through and go, "Please pick out any documents you don't agree with".</p>	
<p>{Day7/112:3} - {Day7/114:1}</p>	<p>Q. {L17/164/1}. This is your reply in the Wright v Granath libel proceedings in the High Court, isn't it?</p> <p>A. It is.</p> <p>Q. Page 22, please {L17/164/22}, paragraph 35.2, the reply pleads this: "Save as follows, the Claimant was not made aware of any plan, whether pursuant to any nCrypt Agreement or otherwise, for a big 'Satoshi reveal ', ie an unmasking of the Claimant as Satoshi Nakamoto, as alleged or at all. The Claimant had no wish ever to be revealed publicly as Satoshi. However, following publication of the articles in Wired and Gizmodo in December 2015, which linked the Claimant with Satoshi Nakamoto, the Claimant was reluctantly persuaded to extend the scope of the sale of his life story to include his story as Satoshi Nakamoto ..." Yes?</p> <p>A. Yes. That was in March/April of 2016.</p> <p>Q. So, if anyone recalls detailed discussions about your life story - discussions with you about your life story being published, including Satoshi Nakamoto and Bitcoin, in September 2015, they must be wrong, mustn't they?</p> <p>A. The discussions I had were about my intellectual property and the birth of the company and what I was building. Now, that will include Bitcoin, because I was talking about the scaling solutions I had, the development of patents and the technology that I'm still building. That was what I discussed.</p> <p>Q. So when you were having the discussions in September and October 2015 about the book, it did include a life story that would discuss your role as Satoshi Nakamoto creating Bitcoin -</p> <p>A. I didn't -</p> <p>Q. - are you now saying that?</p>	<p>Dr Wright is asked about whether he had discussions about his life story in September 2015, he is evasive in response and answers by reference to discussions in 2016.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. No, I just said I did not have discussions in September. Tyche is not my email.</p> <p>Q. I'm struggling to understand what you're saying here, Dr Wright. It may be my fault. In September to October 2015, were the discussions, such as you had, about the life story with a view to a life story including your work as Satoshi Nakamoto or excluding that work?</p> <p>A. What discussions at that period? I had discussions in 2016 that then extended things. I talked in July and a little bit in August about documenting the company. So, basically, we weren't going on about a life story discussion, we were talking about someone to document the company, and that didn't go into the period you're talking about. And in October, I was here in England.</p>	
<p>{E/5/15} - First Witness Statement of Stefan Raymond Matthews {L10/338/1} - Re: The Book</p>		
<p>{Day7/114:19} - {Day7/115:24}</p>	<p>Q. Paragraph 70: "During this period I had discussions with Dr Wright about the idea of a book dealing with his life story and the history of Bitcoin. I have refreshed my memory of the discussions taking place around this time by looking at an email I sent to Mr Ayre on 10 September 2015 ... By this stage I had helped Dr Wright get to the point where he was more comfortable with the idea of the book." Do you see that?</p> <p>A. I do.</p> <p>Q. May we have on screen ID_004276, the email which he's refreshed his memory from. This is {L10/338/1}. This is the email chain which you've told the court is not genuine, isn't it?</p> <p>A. Again, that's Tyche. And Stefan's forwarded something that I don't know who it's come from. But, no, I was comfortable with documenting the company, my intellectual property, my patenting.</p> <p>Q. The email which he's refreshed his memory from and which he says tallies with his recollections is the email which refers to your life story, including Bitcoin, which we looked at earlier, from 10 September 2015, doesn't it?</p> <p>A. No, it's Craig Wright - cwright@tyche.co.uk, which was Rob MacGregor's company. Robert wanted me to do this, so what I see here is Robert sending an email to Stefan and Calvin to make it look like I actually wanted to, and not even doing it really well, because it's the wrong domain. I guess they wouldn't have known that.</p>	<p>Dr Wright is evasive when presented with the email referenced in Mr Matthews' statement {L10/338/1}, blaming third parties (namely Robert MacGregor) for sending this email.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{E/1/38} - First Witness Statement of Craig Steven Wright</p>		
<p>{Day7/116:18} - {Day7/117:19}</p>	<p>Q. Moving on to the - {E/1/38}, please, paragraph 222. You're discussing events on 2 May 2016. You say: "Following [a call that day], I ... began checking my online presence from the train. I discovered that Rob had been accessing and managing my email addresses, craig@tyche.co.uk and craig@ncrypt.com ..." That is inconsistent, isn't it, Dr Wright, with saying that you had never had an email address craig@tyche.co.uk?</p> <p>A. No, there's two points here - actually, three. Number one is, the other email was C Wright, not craig@tyche. Two, Tyche was a forwarding email, so if something came in, it got forwarded to my DeMorgan number one. And it's true that I also know that these were manipulated and accessed.</p> <p>Q. Dr Wright, you say - you told us not very long ago that you couldn't possibly have had a Tyche email, and now here in this witness statement you say that craig@tyche.co.uk was your email address?</p> <p>A. No, what I'm saying is the difference between an email address and a box. As an example, my Lord, I have craigswright@acm.org, that is a forwarding address for ACM members. I don't receive email there. It forwards to RCJBR.org. So all it does is, if you send to it, it goes to an email of my choosing. That's what was meant to happen on this one. And "Craig" and "C Wright" are also different.</p>	<p>Dr Wright not accepting the obvious truth of the inconsistency between his First Witness Statement and his answers just now regarding his possession of a Tyche email address, and he is evasive in response.</p>
<p>{L11/181/1} Email from Craig Wright to Ramona - government leak 08/12/2015</p>		
<p>{Day7/118:13} - {Day7/119:11}</p>	<p>Q. So, you refer to them having obtained some material which was stolen, yes?</p> <p>A. All of it was stolen.</p> <p>Q. And you also say - you refer to two of their points and say: "This is a government leak. So much for privacy laws."</p> <p>A. I do.</p> <p>Q. Were you saying that the government was responsible for the entire leak, or only part of the leak of the material which was leading to your outing?</p>	<p>Dr Wright blaming third parties for leaking documents to Ira Kleiman, namely the Australian government and Greg Maxwell.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Only part of it. They sent material to Ira Kleiman and he forwarded things. Others did as well. He should have no rights to have received those in the first place.</p> <p>Q. So, thieves gained some access to your material and leaked it to name you as Satoshi, right?</p> <p>A. I don't know what they were trying to do. I can't - I can't get in their minds, sorry.</p> <p>Q. Well, the leak had the effect that you were outed as Satoshi, yes?</p> <p>A. Not properly. It was designed so that it could be taken down right afterwards. Mr Maxwell, who is one of your clients, was actually part of all of that.</p>	
<p>{K/2/25} - Section 2 DRD</p>		
<p>{Day7/119:25} - {Day7/120:23}</p>	<p>Q. {L11/212/1}, please. Just before we go there {K/2/25}, please. If we can go to the first page of this {K/2/1}, please, to identify the document. This is the disclosure review document addressing the disclosure to be given by each party in these proceedings. Do you recognise that?</p> <p>A. I've seen it, yes.</p> <p>Q. Page 24, please {K/2/24}. Do you see here annex 3 setting out "Sources containing Irretrievable Documents" completed on your behalf?</p> <p>A. I do.</p> <p>Q. Page 25, please {K/2/25}: "Email servers and Webmail accounts ..." Identified with you. Do we see one of them, about just over halfway down, is listed as "cwright@tyche.co.uk"?</p> <p>A. I do.</p> <p>Q. So do you say that your solicitors were wrong in nominating that as one of your email accounts?</p> <p>A. No, it's an email account that was listed with documents. It's listed as irretrievable because it's not one that I have control of. So I'm not saying that it doesn't exist as an email account, I'm saying it's not one in my control.</p>	<p>Dr Wright is asked about the cwright@tyche.co.uk email listed in his DRD and is evasive in response.</p>
<p>{Day7/121:3-17}</p>	<p>Q. Are any of the others email addresses which you say are completely fake and were used to produce documents which were themselves fake?</p> <p>A. Tyche.co isn't a fake email address, it's one that's set up with my name that I don't control. That's not the same as saying it's</p>	<p>Dr Wright claims that the Tyche email is set up with his name, but he does not control it.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>fake. It's used for whatever reason it's used, but it's not one that I control.</p> <p>Q. Well, let me just put this to you. If the position taken by your solicitors was that you had lost access to material in this account, you must have had access at some point.</p> <p>A. No, it's not saying lost access, it's saying I don't have access. So, in filling this out, given a list of all of the things in disclosure, the answer is I don't have access to this.</p>	
{L11/212/1} - Wired article		
{Day7/123:8-24}	<p>Q. And WIRED went on to speculate that this might be an elaborate hoax orchestrated by you, didn't it?</p> <p>A. No, actually, Greg Maxwell and a few of the other COPA members contacted WIRED and put together what has already been debunked, false information, as well as some of this other stuff that they put together. So one of the people involved was Mr Greg Maxwell -</p> <p>Q. I'm going to dispute - just to stop you on all of these allegations, Dr Wright. I've asked a simple question, which was that the article speculated that it might be an elaborate hoax. If we look page 13 {L11/212/13}, at the bottom, over to page 14 {L11/212/14}, we can see that it did speculate that, didn't it?</p> <p>A. No, it was changed after information came in to them. And it's not a speculation, Mr Maxwell actually published it.</p>	<p>Dr Wright blaming third parties for the documents in the WIRED article, namely Greg Maxwell, and not accepting the obvious truth of the documents.</p>
{Day7/124:18} - {Day7/125:22}	<p>Q. You went to great efforts, didn't you, Dr Wright, to produce articles to try to rebut the suggestion that these keys were unreliable, didn't you? You produced papers and articles about it, didn't you?</p> <p>A. I produce papers every day. I've produced two papers today, I filed two yesterday. So, yes, I produced one. What I demonstrated was that he was wrong. What I noted was that he was basically out there slandering me for something that was completely false.</p> <p>Q. You now say, don't you, that many, or most, or all of the pieces of evidence that WIRED and Gizmodo had were fake or doctored, don't you?</p> <p>A. No, some were, some weren't; there was a mixture. But what happened was, they mixed the real evidence and tainted evidence so that all the real evidence is just tainted with the same brush now.</p>	<p>Dr Wright provides an incoherent and implausible explanation in relation to the evidence that WIRED and Gizmodo had, and blames third parties (Greg Maxwell).</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Well, Dr Wright, I suggest it's pretty extraordinary to go to great efforts to rebut Mr Maxwell's piece undermining keys which you don't say were your own anyway.</p> <p>A. No, one of them was mine. That's the whole point. There were one known key, one my key and three other keys, so the whole thing is you throw everything at the wall, like this whole case, and you hope something sticks. So, what happens is, you say that my key's also fabricated, as well as the other keys. So you throw in three fabricated keys, two real keys, and then you can run round going, "See, they're all fabricated; don't look at these ones over here, don't look at the real one".</p>	
<p>{L11/285/1}-3. Implementation Deed 07 01 16 Final Fully Executed</p>		
<p>{Day7/126:8} - {Day7/127:23}</p>	<p>Q. You physically moved with your family after these articles, didn't you.</p> <p>A. I physically moved before. My son started school here in July. My daughter started school shortly after that. My wife first came in September. I went in October. I came back to do the transitioning, then I came back here. So, we'd already found a house, we were living in a hotel at that point, but we were transitioning back and forwards. So my argument is, I'd already moved, I'd already become a resident.</p> <p>Q. Moving on to early 2016 at {L11/285/1}, please. Do you recall this document, an agreement being entered into with you, on Baker & McKenzie regalia, dated 7 January 2016?</p> <p>A. I mean, it's on a Baker & McKenzie letterhead, because they did it, but I don't actually know if I'd call it "regalia".</p> <p>Q. Just focus on the document, please. {L11/285/3} was a document that, on its face, provides for the various elements of the term sheet you'd entered into in June 2015 to be brought into effect. Do you remember signing an agreement to that effect?</p> <p>A. Not the way you're describing it. The January document was changed quite a lot. Robert changed it significantly after all the WIRED and Gizmodo stuff came out.</p> <p>Q. What does Robert MacGregor have to do with this agreement?</p> <p>A. Stefan and Sterling Group is only brokering it; Robert was the person doing it. NewCo was mostly - what do you call it - Rob MacGregor, and he was the person behind the deal.</p>	<p>Dr Wright is asked about the Implementation Deed at {L11/285/1} and whether he entered into this, Dr Wright is overly pedantic in response but when pressed accepts that he entered into this agreement.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. So do you say that this isn't a genuine agreement, this document we're looking at here?</p> <p>A. No, it is an agreement, but if it's brokered by a company, that's still an agreement. And as you note, I have already got an address here in - well, at that point, Wimbledon. I'm not in Wimbledon any more.</p> <p>Q. Simple question: did you enter into an agreement on the terms of this document?</p> <p>A. Like I just said, yes.</p>	
<p>{Day7/127:24} - {Day7/128:14}</p>	<p>Q. Page 6 {L11/285/6}, we can see it included further provision on each aspect of the heads of terms, here for the IP asset purchase, yes?</p> <p>A. Correct.</p> <p>Q. Page 10 {L11/285/10}, section 7 addressed the rights and services agreement; do you see that?</p> <p>A. I do.</p> <p>Q. And clause 7.2(c) on the next page {L11/285/11}, said that you would also: "... in due course, enter into an additional services agreement with Ncrypt Holdings ... for completion of certain services relating to recounting and transcribing [your] history [for] \$750,000 ..."</p> <p>A. I do.</p> <p>Q. So that was a term to which you agreed at that time?</p> <p>A. I didn't really have much of a choice, but, yes.</p>	<p>Dr Wright admitting that he agreed to clause 7.2(c), about entering into a services agreement for "completion of certain services relating to recounting and transcribing [your] history...".</p>
<p>{L11/342/4} - Life Story Rights and Services Agreement</p>		
<p>{Day7/128:15} - {Day7/129:21}</p>	<p>Q. And {L11/342/1}, "Life Story Rights and Services Agreement", between you and EITC Holdings Limited. Is this a genuine agreement into which you entered on 17 February 2016?</p> <p>A. It is.</p> <p>Q. And if we go to the final page of this document, which I think is either page 3 or page 4, we'll see the signatures. If we could click back to the signature page. Is that your signature and that Mr Matthews' signature? {L11/342/14}.</p> <p>A. That's one I authorised to be signed for.</p> <p>Q. Is that your signature on the signature page?</p>	<p>Dr Wright is asked about whether it is his signature on the Life Story Rights and Services Agreement and is very evasive in response, stating that somebody else signed it for him. This is inconsistent with paragraph 78 of Mr Matthews' statement {E/5}.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. I agreed to be bound.</p> <p>Q. Is that your signature?</p> <p>A. Like many other executives, I've had people sign things for me.</p> <p>Q. So somebody else signed this for you?</p> <p>A. Yes.</p> <p>Q. Who?</p> <p>A. I can't remember, my EA or anything at the time, sorry.</p> <p>Q. It doesn't say, "Signed by X for and on behalf of Craig Wright", it says "Craig Wright" and then a signature.</p> <p>A. I agreed. I had a message sent saying that I agreed. I electronically basically sent something saying, "I agree to this", and then had it applied.</p> <p>Q. It didn't trouble you that somebody was signing with your signature, not for and on behalf of you, but with your actual signature on this document? That didn't trouble you?</p> <p>A. No, because I sent a message saying that, "Please sign for me", so there was a record saying that.</p>	
<p>{Day7/132:5} - {Day7/133:2}</p>	<p>Q. In short, by signing up to this agreement, you were committing to a major media exercise which would involve revealing your claim to be Satoshi, yes?</p> <p>A. Yes and no. What really happened was, after I'd moved into - into the UK, Robert used that as leverage.</p> <p>Q. Used what as leverage?</p> <p>A. The rest of the money, the ongoing operations in Australia. Basically, the terms were: you've moved over here, your children are here, you don't - everything's now here, your companies are tied up, you're going to do this. So, I was given a choice, which he later quite succinctly put, "Basically you're all going to be shipped back with absolutely nothing if you don't do what I want".</p> <p>Q. So this was an agreement that you really didn't want to enter into and which was entered into under pressure against your wishes?</p> <p>A. More than just pressure. Basically, he said the money for the Australian companies that we had agreed would be withheld, he said the intellectual property has already been effectively transferred and "I'll make sure that you never get to work on it", so the things I cared about most, yes.</p>	<p>Dr Wright stating that he did not want to enter into the Life Story Rights and Services Agreement, blaming Robert MacGregor for applying leverage to him.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day7/133:3} - {Day7/133:14}</p>	<p>Q. Mr Matthews signed this agreement, didn't he? A. I don't know. Possibly. Q. Let's go back to the signature page {L11/342/14}. Mr Matthews signed this agreement, didn't he? A. He did. Q. When he signed this on behalf of - as a director of the company EITC, did he know that you were entering into it under duress, not wanting to? A. He knew I was very unhappy about it, yes. Q. He knew you didn't want to enter into this agreement at all? A. Fairly much, yes.</p>	<p>Dr Wright claiming that Mr Matthews knew he didn't want to enter into this agreement.</p>
<p>{L11/395/1} - 00000389_item.msg - email from Andrew O'Hagan to Dr Wright</p>		
<p>{Day7/139:13} - {Day7/141:5}</p>	<p>Q. He then goes on to complain, doesn't he, about the lack of Satoshi Nakamoto email correspondence? A. He mentioned it, yes. Q. A few lines down: "Weeks ago I asked you to use the SN email in correspondence with me. Nothing. Months ago, I asked for the emails. Nothing. Last week, Rob suggested a meeting to discuss my role." He was pressing, wasn't he, for some form of objective proof that you were Satoshi? A. I'm not actually sure. What I do know is, where he's saying, "Months ago, I asked for the emails", he didn't ask me. So he might have been talking to - to Rob, but I didn't even know Andrew O'Hagan had been involved until sort of way into 2016, like February or something like this. I found out later that Rob had been talking to him for at least six months before this, but never signed a contract or did anything, so I had no idea. Q. Mr O'Hagan, here, was threatening to down tools because he had been asking for a long time for some form of objective proof and he hadn't had anything, right? A. I don't really know. I wasn't involved in any of that. Q. And if, at that point, you had had access to the Satoshi Nakamoto email account, that was plainly a time to use it in order to satisfy his requirements, wasn't it? A. No. I didn't give a rats what he thought.</p>	<p>Dr Wright is asked questions about Mr O'Hagan's email pressing for objective proof that he was Satoshi, Dr Wright's answer is inconsistent with his First Witness Statement, paragraph 172, regarding when he first met Mr O'Hagan {E/1/31}.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. You didn't give a rats what he thought even though you had contractual obligations to assist in the production of this story?</p> <p>A. I had been forced, basically in duress, to go through something I didn't want to do. The promise, and why I selected Rob over Macquarie Bank was a promise that was categorically put as I will get to be CSO, chief scientist, I will sit in a room, I will invent, I will spend 80 to 100 hours a week working on my inventions; I will have a team to document those, I will have a team to file my patents, I will have people like Cerian and the other, like, what do you call it, patent attorneys, to teach me how to turn my inventions into patentable things; I will have a development team to make them real. That's what I was promised. That wasn't delivered.</p>	
<p>{Day7/141:6} - {Day7/141:17}</p>	<p>Q. Dr Wright, you were the one who signed an agreement committing you to provide full support for a big media reveal of your claim to be Satoshi, weren't you?</p> <p>A. I agreed to do it my way. I would prove to people who I am, because I'd spoken to them, because I knew things, because of my work. I went up to Gavin and I told him about the development issues, I explained what we did, things that were not public. I went on an email - not just emails, but I had phone calls with him, and I talked him through things that only he and Satoshi knew, and that's why he came out to England. I had nothing to do with any of this.</p>	<p>Dr Wright's explanation is inconsistent with his evidence, in which he has not revealed anything that Satoshi knew that was not already in the public domain.</p>
<p>{L12/2/2} - 00000547_item.msg</p>		
<p>{Day7/144:18} - {Day7/145:9}</p>	<p>Q. Let's forget about proof in - several hundred years ago. You were rejecting every form of objectively verifiable proof, weren't you.</p> <p>A. No -</p> <p>Q. Objectively verifiable?</p> <p>A. Again, it's not several hundred years ago. A certain author who did a Harry Potter series only did it recently. A certain author who did a whole lot of -</p> <p>Q. You're still not answering my question.</p> <p>A. No, I am. You're trying to equate something that is exactly the opposite of British law, for a thousand years, actually going back to Roman times, on identity law, and people want to equate that, because there are a lot of people in Silicon Valley who hate the idea of having identity; they want to have an</p>	<p>Dr Wright is not answering the question that is asked, and provides an evasive and irrelevant answer.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>anonymous system, mainly because there's more money in Google outside -</p>	
<p>{Day7/146:22} - {Day7/148:17}</p>	<p>Q. I appreciate you're desperate to make Mr MacGregor the villain. But if we look to the top of the page, you object to signing on the basis that it would be definitive proof of your controlling the keys and it was that proof that you controlled the keys that was objectionable to you. That's what you said, isn't it?</p> <p>A. No, it is only proof that I controlled the keys. It isn't proof of identity.</p> <p>Q. "A signed message is definitive ... I control the keys completely. If it is copied ... there is no way to control it. Even deleting a file is not removing it. Files can be recovered and I doubt Gavin would allow us to wipe his machines." That's objecting on the basis that the keys could be compromised, not on the basis that you had a principled objection to signing at all, isn't it?</p> <p>A. No, what you have just said is utterly wrong. Now, what you've just said is the key is compromised. This is wrong. I could give you a signed message and you can validate it on a third party computer, but what I'm saying here is, I can no longer control who has that message. When I did the exercise for the Australian Tax Office, the way that I did it was I encrypted a file - or, sorry, they encrypted a file and I decrypted it. Now, that proves categorically that I have the key. If I can answer the question you put in that file, I must have decrypted it. If I can send you back the file, I must have decrypted it. But there is no proof I have the key other than the party who sent it to me. My requirement, very simply, was Gavin can know, he's not telling anyone.</p> <p>Q. Okay, we'll move on. You go on to say that you were objecting, in the last paragraph, because you'd said that you couldn't control the keys without help. You said that to the government. That was the nature of the objection you were pointing out to Mr MacGregor, isn't it?</p> <p>A. No, that's a different issue. We could have gone through things like signing off on the trust and everything like - that we ended up doing, but, no, I wasn't going to just have it out there. I wasn't going to go into attributing myself to Satoshi publicly that way. No way I was going to basically have this mantra that everyone wants of possession equals identity.</p>	<p>Dr Wright is asked about the basis of his objections to the signing session, he is evasive and rambling in response and refers to an "exercise" he did for the ATO.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day7/148:24} - {Day7/149:7}</p>	<p>Q. You agreed, didn't you, and you undertook signing sessions with GQ, the BBC and The Economist, right?</p> <p>A. No, I had sessions where I showed keys. The agreement was that all of the other stuff would be put in. What was called a "proof pack" was meant to go out. That was meant to put together my history, my work, the patents I'd been filing. None of it went. The proof pack was actually sending the proof, but none of the proof got sent.</p>	<p>Dr Wright blaming unidentified third parties for not providing the "proof pack".</p>
<p>{L12/172/1} - 00000671_item.msg</p>		
<p>{Day7/150:8} - {Day7/150:22}</p>	<p>"My view remains that we verify the early blocks for the media. I sign a message to prove my control of these. What I also do is do this as a signed - only session with JM [Jon Matonis] and [Gavin Andresen] and not move blocks." You were proposing, at that stage, to Mr MacGregor that you would conduct a signing session with the journalists, just as you had with Mr Matonis and Mr Andresen, weren't you?</p> <p>A. No, as I just explained, it's not signing. I would show that I could verify the early blocks. I did not say sign, I said control and possession. I agreed that I would do that for the - what then had to happen was a proper proof session. You verify all my stuff, you go through how I created the Bitcoin White Paper -</p>	<p>Dr Wright not accepting the obvious truth of his email to Mr MacGregor, denying that he said "sign" even though the email refers multiple times to "sign".</p>
<p>{Day7/150:23} - {Day7/151:6}</p>	<p>Q. But you were proposing, weren't you, a signature session with the journalists as with Mr Matonis and Mr Andresen, weren't you?</p> <p>A. No, actually, I know what digital signature is, I have been teaching it since 2000. I said we will "verify the early blocks". "Verify the early blocks" doesn't mean I'm doing a digital signature. I can't do a digital signature unless I've given proof. Having a key is not proof. You will not budge me on that one.</p>	<p>Dr Wright not accepting the obvious truth of his email to Mr MacGregor regarding the basis of the signing session.</p>
<p>{L14/671/1} - GQ Interview with CSW</p>		
<p>{Day7/155:7} - {Day7/155:19}</p>	<p>Q. Well, let's take an example of that. May we please have the recording at {L14/671/1} played. And can we play it from 1 minute and 40 seconds. Actually, we'll play it from the start, so it's fully heard. From the start. I think there may be a problem with the audio? (Video footage played) Pause there,</p>	<p>Dr Wright making baseless allegations against Professor Courtois.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>please. This was a discussion with GQ, who had an academic cryptographer with them, Dr Courtois, right?</p> <p>A. No, the only way I saw it is that he's a university academic who was basically a fraud, who goes out there claiming that he can break cryptographic keys when he has never done so.</p>	
<p>{Day7/156:15} - {Day7/157:25}</p>	<p>Q. Okay, let's play on. (Video footage played) I think we can stop there. That's what I wanted to ask you about. Now, Dr Wright, I'm not going to ask you about the language in which you spoke, you were obviously under stress, but you insisted, didn't you, that you had only ever transferred Bitcoin to Zooko and Hal Finney, full stop, didn't you?</p> <p>A. No, that's not what I'm saying. I was noting in the earliest keys, now, when I'm referencing this, all of the other, what people call, Satoshi Bitcoin were actually owned by Information Defense which was transferred to Wright International. So any of the other things I did were company transfers.</p> <p>Q. Dr Wright, it's true, isn't it that Satoshi, as well as transferring Bitcoin to Hal Finney, transferred Bitcoin to many other people, or a number of other people?</p> <p>A. Technically, I enacted the process, but it was from Information Defense. So when I did it for Mike or Gavin or all of the different many, many people, and there would probably be about a hundred, then that's not from me, it's from my company.</p> <p>Q. Dr Wright, you were answering questions about what could be proved in terms of movement of early Bitcoin and you said that you had transferred them only to Zooko and Hal Finney. That was your meaning, wasn't it?</p> <p>A. No, it's not. The --</p> <p>Q. And in reality, Satoshi never transferred any Bitcoin to Zooko Wilcox - O'Hearn, did he?</p> <p>A. Actually, I did. Zooko was very interested because he had been working on a similar thing, MojoNation, beforehand.</p> <p>Q. So he's wrong in his witness statement when he says he didn't receive Bitcoin from Satoshi, is he?</p> <p>A. He is.</p>	<p>Dr Wright is asked about the individuals to whom he claimed to transfer Bitcoin. Dr Wright is evasive in response and claims that other transfers were not from Satoshi, but from his company, Information Defense. He also claims to have transferred Bitcoin to "about a hundred" people from his company.</p> <p>Dr Wright claims Zooko Wilcox O'Hearn's evidence is incorrect when he states he did not receive Bitcoin from Satoshi.</p>
<p>{Day7/158:1} - {Day7/159/14}</p>	<p>Q. And of course Satoshi transferred Bitcoin to Nick Bohm, but you weren't to know that at that point, were you?</p> <p>A. Oh, of course I did. But do I remember people? No. I transferred to a lot of people in 2009.</p>	<p>Dr Wright is asked about the people to whom Satoshi transferred Bitcoin, he gives an evasive and rambling</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. But what really got you exercised in the course of this discussion was the idea that your signing sessions might not be valid because your keys that you had used might have been obtained by somebody - by you without having been Satoshi, right?</p> <p>A. Not at all. My Lord, what that guy said is Bitcoin was not secure. He said that he could compromise literally tens of thousands of addresses. My system is the most secure software system ever created. I find it not only offensive, but it's flimflam people like that, who sit there saying that they can do these things, that's technobabble, when you write papers and you can't do it. He could verify nothing. So - called experts who cannot verify their work; I hate that. I loathe it. People like that, who falsely, fraudulently claim to have cracked tens of thousands of Bitcoin addresses, write papers about it, go to conferences about it, which he has, it is disgusting.</p> <p>Q. Can I just stop you. You have made the point - you've made your point. Let me ask this question then. You've said that you transferred Bitcoin as Satoshi to hundreds of people. Can you name some of those to whom you transferred Bitcoin whose receipt of Bitcoin from Satoshi is not in the public domain?</p> <p>A. God knows. I don't remember everyone now.</p> <p>Q. So you can't remember any of the hundreds?</p> <p>A. No.</p> <p>MR JUSTICE MELLOR: Not even one?</p> <p>A. I don't know who is and isn't in the public domain. I know the funding stuff I did for Gavin, but he's talked about that now. But, no, it had no value at the time, my Lord. I just sent whoever asked, and most of them were pseudonymous. The majority of people on the forum didn't actually use their name.</p>	<p>response, and when pressed by counsel and Mellor J, is unable to give the name of a single individual to whom he transferred Bitcoin (whose name is not already in the public domain).</p>
<p>{L13/88/1} - 000005363.email {L14/327/1} - If I sign myself Jean v2</p>		
<p>{Day7/165:4} - {Day7/165:17}</p>	<p>Q. Well, it took - it didn't take very long, but it took a little time and the production of special programs to go through the blockchain and find this signature, didn't it, Dr Wright?</p> <p>A. No. The key for block 9 was actually published back in 2011 on BitcoinTalk forum. On top of that, Mr Maxwell, Willie - actually, every one of the BTC developers have extensively talked about this between 2011 and 2016, right up to this. Every one of them. There are public posts on this key by every single one of the developers, at least - and I'll stake</p>	<p>Dr Wright making unverified claims regarding the key for block 9.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>my reputation on this, at least ten different occurrences, minimum, per one. On this, they've discussed this key, this verification method, all of this. Every one of them knew it.</p>	
<p>{Day7/166:6} - {Day7/167:7}</p>	<p>Q. Let's be direct about this. If you had had access to the private keys associated with any of blocks 1 to 9, you could have taken a message, produced a signature?</p> <p>A. No, I could have produced a message digest that would be associated with it as a signature if I had already proved my identity.</p> <p>Q. But just in terms of what was logistic - what was possible.</p> <p>A. No. No, sorry, you won't get me to agree to that. There is no feasible way to prove identity, it's a one - way function. You cannot. It is against the very law of what that means.</p> <p>Q. Just in terms of proving possession, if you'd wanted to prove possession, possession of one of these private keys, there would have been no technical problem and nothing insecure about simply putting on your blog a message, a new message, cryptographically signed with one of the keys associated with the early blocks, would there?</p> <p>A. It would have been the biggest lie in human history. It would have been going out there and signing up for a cyperpunk lie. It would have been signing up for not what identity is, it would have been removing the function of identity as it is in the Bitcoin White Paper, not pseudonymous, not private, going back to the whole lie of anonymity. It would have been undermining my life's work.</p>	<p>Dr Wright is asked about whether he could have produced a signature if he had the private keys associated with blocks 1-9, he is evasive in response.</p>
<p>{Day7/167:17} - {Day7/169:10}</p>	<p>Q: Dr Wright, your own team and supporters, including Mr Matthews, as well as Mr MacGregor and all the media people, expected this post to contain a message actually signed with one of the private keys, didn't they?</p> <p>A. The biggest lie in your statement is my own team. I didn't have a team, I had Rob trying to sell me. Rob had made a deal with a Silicon Valley group to sell me, packaged as Satoshi, as a cypherpunk, and he gets a \$1 billion figure that I'll get a freaking few crumbs of. His deal was to sell me, put a little bow on me and turn me into a cypherpunk, put me in a hoodie and do everything I hate in life.</p> <p>Q. Can we at least agree on this, having listened to the GQ interview. If you had produced a signed message as proposed, that would not have involved a security risk of the private keys being derived by anyone else?</p> <p>A. Not if I had it on a separate machine. If I had it on -</p>	<p>Dr Wright is pressed on whether his team expected his post to contain a message signed with one of the private keys, Dr Wright is evasive in response and blames third parties (Robert MacGregor).</p> <p>Dr Wright is also asked whether it would create any security risk if he had put a signed message out in the public, he is evasive and does not answer the question.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Just to be clear, what I'm putting to you is, if you had put the message out there, the signed message out there, and the message text, you'd informed the world of which key you had signed with, which block's key you had signed with, that would not have created a risk, a real risk of the key being compromised and the private key being found by a bad actor, would it?</p> <p>A. Again, that has nothing to do with Bitcoin or anything like this. It is the opposite. The security risk, as you're putting it -</p> <p>Q. Dr Wright, that was an important question, it may be important for the court. Are you prepared to answer that question?</p> <p>A. I am answering it. You cut me off. The security risk was the security of my work undermining the whole value of everything I've created, not that the key will be taken. If I give a signed message, then I can hand that without the private key. That's why you have digital signature messages, that's what the blockchain is about. One, the other. The whole purpose here, though, is identity. That is the thing all of your team want to remove. That is the whole purpose behind my invention, that it's private, between individuals, but that means it has to be there.</p>	
<p>{L18/257/3} - Capture of Sartre signing certificate</p>		
<p>{Day7/169:20} - {Day7/171:3}</p>	<p>Q. And then if we go down through {L18/257/3}, we can see that it included the same process of key verification using OpenSSL that was in your draft, yes?</p> <p>A. Yes, but they've taken a few parts out.</p> <p>Q. Page 11 {L18/257/11}, and we have the same signed message, which was from a publicly available Satoshi signature on the blockchain, yes?</p> <p>A. Yes, and he put it down as "signature verification", which isn't what I ...</p> <p>Q. Dr Wright, just this. Are you saying that if the blog had been posted in precisely the form that you had drafted it, it would have satisfied people and it would have been a less dramatic disappointment for everyone?</p> <p>A. Probably not. The argument was already coming, that I would have stolen the keys. So, before I even did this, there was a big movement from BTC Core people: even if Craig has</p>	<p>Dr Wright blaming third parties (“BTC Core people”) and refusing to accept the obvious truth of the contents of his blog posts.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>the keys, he must have stolen them; it must be Dave Kleiman and he stole them from his dead friend.</p> <p>Q. The reality is, Dr Wright, that each of these presented itself as a blog to prove possession of a private key, just as Mr Matthews and Mr Andresen expected, and each of these blogs failed by that standard, didn't it, both your draft and the final version?</p> <p>A. No, as I said, if I sign as Craig Wright, Satoshi. So, no, I was never intending in that one. What I promised was, if you did the proof session, if you did everything that I wanted put together, if you put together my hundreds of papers, if you put together my thousands of patents and all the work I'd been doing, if you showed the scaling work I was doing and you went through that process, then I would have signed. The only way that I could sign is to have my identity known first, because of what I am, what I've done.</p>	

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
DAY 8		
CROSS - EXAMINATION OF DR CRAIG WRIGHT BY JONATHAN HOUGH KC		
{L11/285} Implementation deed, dated 7 January 2016		
<p>{Day8/6:15} – {Day8/7:21}</p>	<p>Q. Page 10, please {L11/285/10}, middle of the page, clause 7, "Craig Wright", 7.2(a): "Craig Wright has entered into an Employment Contract with Tyche Consulting Limited dated 26 October 2015 at a salary of £160,000 [sterling] per annum. The parties acknowledge and agree that Craig Wright may subsequently become employed by a related body corporate ..." Do you say that that statement, that you'd entered into an employment contract with Tyche Consulting Limited of that date, in this contract which you signed is wrong?</p> <p>A. I do. There was never any tax with HMRC filed, and on that day, the documentation that I had to sign with my wife was approximately 1,200 pages in total, a little bit more, probably. We had 100 different documents to sign for all of the IP, I didn't have any solicitors with me, because I was in the UK, not Australia, and I had no chance to read them. So, I looked through the things very quickly, I didn't analyse them in detail.</p> <p>Q. So, you say that you signed this agreement, including the term headed "Craig Wright", without reading the agreement or the term headed "Craig Wright"?</p> <p>A. In full, no, I hadn't. I'll also note, the email you brought up yesterday has a statement saying that my wife and I are ready to start a family. When we came to the UK, my wife and I were in our mid-40s, my wife had three children already, we weren't looking at having children and family, as that email states. So, my Lord, it was well known that my wife and I were not looking at having more children.</p>	<p>Having admitted that he stated he was not Tyche, Dr Wright is asked about the Implementation Deed that states that he entered into an employment contract with Tyche Consulting Limited. Dr Wright is evasive in response, claiming that he did not read the agreement fully.</p>
{L10/426} - Tyche Consulting Limited, Employment Contract, Craig Wright, 26th October 2015.		
<p>{Day8/7:22} - {Day8/8:7}</p>	<p>Q. {L10/426/1}, please. This is a document in your disclosure, "Tyche Consulting Limited, Employment Contract, Craig Wright, 26th October 2015". Page 2, please {L10/426/2}, I</p>	<p>Dr Wright denying, implausibly, that the signature on the Tyche Consulting</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>think an introductory page signed apparently by you. Is that your signature?</p> <p>A. Actually, no, it's not. I've said how I sign with "G"s etc. That's actually not my signature. There's no Wright, there's no anything else and there's a big flourish at the end with a "G". There's plenty of fake my signatures and that's definitely one of them.</p>	<p>Employment Contract at {L10/426/2} is his.</p>
{Day8/8:8-15}	<p>Q. So you say that this contract was not signed you despite the apparent signature, yes?</p> <p>A. At that date, I wasn't living at that address, we had already moved out. A lot of people thought we were still living at 43 Gordon in October, and that's why WIRED and Gizmodo camped out, but actually, in August of that year, we already had the shipping containers come in and we moved, so that's incorrect.</p>	<p>Dr Wright denying that the signature in the Tyche Consulting Employment Contract at {L10/426/2} is his.</p> <p>His evidence here is also inconsistent with Mr Matthews' witness statement at paragraph 72, in which he states that the family's belongings were shipped to the UK "in or around October and November 2015".</p>
{Day8/8:16} - {Day8/9:11}	<p>Q. So, this employment contract, apparently bearing your signature, was not one of the many hundreds of pages of documentation that you signed on that date without reading them?</p> <p>A. Well, it doesn't contain my signature. If you look at my other signatures, where I have them, as I've said, I have a little trick where I do a sort of "C" on the "G". That doesn't really look like a "Craig S Wright". I've never once in my life signed without putting "Craig S Wright" individually, and I can't make out "Craig S Wright" out of that signature at all.</p>	<p>Dr Wright discussing his signature - see also his comments at {Day4/129:23} - {Day4/130:16}.</p>
{Day8/9:3-23}	<p>Q. Would you accept that this is yet another document in your disclosure which you've identified as a fake which was not identified as a fake when disclosure was given?</p> <p>A. No, actually, that's incorrect. This document comes from one of the ex-staff laptops. That is in the disclosure platform. It's listed that it comes from a staff laptop accessing Ramona, my wife's, email, when that employee had no legal rights to access her email.</p>	<p>Dr Wright blaming third parties (his solicitors) for disclosing this document, claiming that he told them that it was from an unauthorised source.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Pause there, a couple of simple questions. This was a document disclosed by solicitors on your behalf in these proceedings; correct?</p> <p>A. Yes.</p> <p>Q. And when disclosing this document, your solicitors did not identify it in correspondence as a fake, did they?</p> <p>A. I don't know what they did. I told them that – and it's in the disclosure platform, that it's from an unauthorised source. So in the disclosure platform, it notes it. I can't say what the solicitors have done after the disclosure platform notes that it's from an unauthorised source.</p>	
<p>{L10/358/1} – Emails between Stefan Matthews and Kelly Connor (copying Robert MacGregor and Kate Brenneke) “Re: Job title and salary for Craig”</p>		
<p>{Day8/9:16} – {Day8/11:5}</p>	<p>Q. {L10/358/1}, please. This is an exchange of emails involving both Mr MacGregor, whom you've seen fit to cast as a villain, and your friend Mr Matthews, from September 2015, making the arrangements for you to be given a job title of chief science officer, a salary of £160,000 by Tyche or by Kelly Connor speaking on behalf of Tyche. Do you see that email?</p> <p>A. No, I don't. What I see is a job title. I don't see anything about Tyche there. As noted, I was given the chief science officer role at nCrypt, now nChain, so my filing with HMRC for that year has me as chief science officer for nCrypt.</p> <p>Q. Bottom of the page, please, Kelly Connor of Tyche writes on 21 September: “We will be submitting information for Craig’s visa very soon and as such, I need to confirm: “Job title – Chief Scientific Officer or Chief Scientist? “Salary.” Then over the page {L10/358/2}, that’s Kelly Connor writing as the HR manager for Tyche Consulting Limited. Are you really saying she was setting up a job title and salary package for a company other than Tyche Consulting Limited?</p> <p>A. Well, they’re Tyche Consulting, or Tyche Consulting. What they actually do is they have HR consulting roles. So the consulting for the first three years of nChain, nCrypt, was Tyche. We didn't have a HR function. Until Rob was out – or actually, we did two years, 2016/17. So when Rob left, that changed, but Tyche ran the HR, payees, payroll and accounting for nCrypt.</p>	<p>Dr Wright not accepting the obvious truth that this email discusses a job at Tyche for him.</p>
<p>{Day8/11:6-16}</p>	<p>Q. Dr Wright, all the documents tell a consistent story, you were employed by Tyche between October 2015 and early 2016, don't they?</p>	<p>Dr Wright is referring to his HMRC filings, which have not been</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. No, actually, I've had to give over my HMRC filings, both here and in the US case, they were put into disclosure, and HMRC, for 2016, '17, '18, only has nCrypt, or nChain – same company. So all of my tax filings, from this period on, are from a single company. My visa was done for nCrypt, my – everything else, so all of the documentation related to this that this consulting firm has put in refers nCrypt.</p>	<p>disclosed in these proceedings.</p>
<p>BBC/GQ/Economist Articles - Big Reveal</p>		
<p>{Day8/13:14-25}</p>	<p>Q. Dr Wright, are you aware -- are you seriously saying that you're not aware that in the hours after the Sartre blogpost went up, that a number of people online discredited it, or claimed to discredit it, saying that it did not provide a newly signed message?</p> <p>A. I didn't read them, no.</p> <p>Q. And you're not even aware now that they said that, are you?</p> <p>A. I haven't been reading them, no. I don't read a lot of that material. I know people accuse me of being on Reddit. I don't have a Reddit account. I actually don't use Reddit, I never have.</p>	<p>Dr Wright is asserting that he had not read articles discrediting or claiming to discredit the Sartre blogpost.</p>
<p>{L13/97/1} Emails between Wright/MacGregor/Ayre - May 2, 2016</p>		
<p>{Day8/14:17} - {Day8/15:14}</p>	<p>{L13/97/1}, please. We see, at the bottom of the page, an email that Monday, May 2, 2016, from Mr MacGregor to Mr Ayre and yourself, copied to Mr Matthews: "The signature -- the fundamental part of the entire story -- has fallen apart. This has to be corrected right now, or there will be no way your reputation or the project can come back from this. It's mid-morning already in NYC and that media coverage is already souring badly." Do you recall receiving an email of that kind?</p> <p>A. Not particularly. I don't have a good recall of that period.</p> <p>Q. Then Mr Ayre responds: "How could the signature fall apart?" Do you see that?</p> <p>A. I do.</p> <p>Q. And you reply: "The wrong copy was uploaded." Don't you?</p>	<p>Dr Wright claiming that he has no recall of the email at {L13/97/1} despite its importance to his proof, and not accepting the obvious truth of the words of the email.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	A. Probably not. Around this time, nCrypt was run by the consulting company Tyche, so my email at nCrypt was actually taken over and I was excluded from it.	
<p>{E/1} First Witness Statement of Dr Wright (inc PD57AC List) {L13/109/1} Emails between Robert MacGregor, Calvin Ayre, Dr Wright, Stefan Matthews and Ramona Watts</p>		
<p>{Day8/15:15} - {Day8/16:9}</p>	<p>Q. Dr Wright, this is another email chain which you reviewed in the course of preparing your first witness statement. I'm not going to go to it, but for the lawyers, this is a chain which is at ID_002274, which is item 5 in the PD57AC list at {E/1/40}. So this is an email, among not very many, which you reviewed for the purpose of your first witness statement and you didn't identify it there, did you, as a fake email which had been written by somebody who had taken over your account, did you, Dr Wright?</p> <p>A. No, I have no need to. Again, I have noted that these all came from third party computers. In the disclosure platform, it notes it. It's very clear that it comes from a compromised staff computer in the disclosure platform.</p> <p>Q. Dr Wright, you keep referring to a disclosure platform which is your solicitors' privileged platform. Please stop doing so, because it's privileged information and I don't want you to waive privilege without proper advice.</p>	<p>Dr Wright blaming third parties (compromised staff computers) for disclosing this fake email.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day8/16:16} - {Day8/17:23}</p>	<p>Q. You can answer this question. There is nowhere in your witness statement where you identify this email, which you had reviewed for that statement, as a fake email, is there?</p> <p>A. Well, yes. I would have relied on it if it wasn't. So, a lot of these things I haven't used because I've noted that they're from third parties and can't be relied on. So --</p> <p>Q. So are you saying that all the emails in your PD57AC list are fake documents, or that some are fakes, some are real and you haven't told us which is which in your statement?</p> <p>A. No, I said everything that comes from a compromised computer owned by staff is unreliable. I categorically said that. I said it in the Kleiman trial, I said it in the McCormack trial, I said it in Norway, I said it to my lawyers here. I said it on the stand in front of the jury.</p> <p>Q. So, for all your nominated primary reliance documents which come from other laptops than your own, are you saying that they should be treated presumptively as fakes, Dr Wright?</p> <p>A. No, what I've noted is that they have been updated and touched. Where I've noted that these were documents I created, they've been sent now to third parties. So this is part of the story. Why I am relying on them in some parts is to say that third parties have interacted with my documents. It is not just to say I wrote them, but the entire story needs to be told, and the entire story includes ex-staff members who had gone rogue, it includes people who have tried to compromise the integrity of what I'm doing, because they get paid, it includes people who get put under pressure.</p>	<p>Dr Wright is pressed on the fact that he did not identify emails in his PD57AC list as fake documents, and refuses to accept that he failed to identify fake documents in these proceedings.</p> <p>Dr Wright is asserting that he is relying on some of his documents to "say that third parties have interacted with my documents".</p>
<p>{L13/168/1} Andresen/Wright emails</p>		
<p>{Day8/21:8} - {Day8/22:4}</p>	<p>Q. {L13/168/1}, please. This is another of the Andresen exhibits from the Kleiman proceedings, an email from you in response to that email: "Please hold that thought. "I am going to re sign the message and post a new never used signature from 9. "I will explain soon. I will call Stefan soon to explain the message. "I am on route from Paris. There is nothing ... I can do before I arrive home." You gave that commitment at that time, didn't you?</p> <p>A. No, I did not. As was noted, I was actually under the tunnel in the Eurostar. At this time, I'd lost control of that email, it had been taken over from me, and Rob used this. He then told me, "I've told Gavin that you have -- told Gavin, who's your</p>	<p>Dr Wright is asserting that he had lost control of this email address and blaming Rob MacGregor for the content of this email.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>friend, that you're going to do this; you're going to look like a complete fool if you don't".</p> <p>Q. Okay, so that's another email you say is fake?</p> <p>A. No, I'm not saying it's fake, I'm saying I didn't control the email address. It's a real email from someone else.</p>	
<p>{L13/116/1} MacGregor emails “a final full offensive”</p>		
<p>{Day8/23:12-21}</p>	<p>Q. Do you agree that the message that's being delivered in this email was precisely the message Mr MacGregor wanted to deliver that evening?</p> <p>A. Yes. What I later found out was that literally Mr MacGregor had a \$1 billion with -- sounding very like Austin Powers "1 billion" -- deal, exactly US\$1 billion. And the deal was that I had to do this by signing with keys and there could be no proof. The only way, it had to be a cypherpunk thing from certain Silicon Valley companies --</p>	<p>Dr Wright is questioned about the email at {L13/116/1}, he is evasive in response, digressing and blaming third parties (Robert MacGregor).</p>
<p>{Day8/24:2-18}</p>	<p>Q. Next question. It would be pretty strange, wouldn't it, for Mr MacGregor to deliver a real message, aimed at you, to an email address that wasn't you?</p> <p>A. No. This is part of what I was explaining before, Mr MacGregor came up with the idea that if he's saying that I'm sending and telling everyone that it's mine, that that's going to be evidence that I'm on board with this and thus I need to follow what he's saying. So, part of the -- the whole thing with Tyche running all of the IT and other systems for nChain was that as soon as I didn't agree, they could cut me off my own email. That was probably one of my stupidest mistakes. By deciding just to be chief science officer, I handed over the control, the CEO or CIO, of all of the IT systems to Robert, and while I wanted just to be the research guy, the problem is, as soon as I did that, other people get to control what I do.</p>	<p>Dr Wright is not accepting the obvious truth of content of the email and providing an implausible explanation in which he is blaming Robert MacGregor.</p>
<p>{Day8/24:19-23}</p>	<p>MR JUSTICE MELLOR: Did your wife have access to this email address “nCrypt Ramona”?</p> <p>A. At that point, I don't know. She was originally set up with one, but none of this is going to our RCJBR emails, my Lord.</p>	<p>Dr Wright is evasive as to whether his wife had access to the email address “nCrypt Ramona”.</p>
<p>{L13/123/1} - Ramona nCrypt email re: blog</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day8/24:24} - {Day8/26:11}</p>	<p>MR HOUGH: {L13/123/1}. We have Ramona responding to that email that evening: "Craig is still working on the blog and triple checking to make sure there are no mistakes. "Craig can resign a transaction on blocks 1-9 as you said, but nothing can be taken away as discussed today." Is the message that Ramona delivered that evening, according to this email, a message consistent with what you intended at that point?</p> <p>A. No, and it's not consistent with what my wife would say. I -- my wife wouldn't go behind my back that way and -- and -- I mean, unless she'd been told other things, but she was with me. If my wife had been separate with someone and talking to them thinking that she'd communicated with me, it might be true, but my wife and I were home together at this time.</p> <p>Q. So all these emails were going through, including to Mr Matthews, and they were all emails from somebody else who'd taken over this account, right?</p> <p>A. Well, I wasn't running the account, so I can't really tell what was happening at the time.</p> <p>Q. And it wasn't something that Mr Matthews spotted during those hours and days, is it?</p> <p>A. No, Mr Matthews at that point trusted Robert, he thought he was on side, but it's amazing what people will do for \$1 billion.</p> <p>Q. Mr Matthews was spending time with you those days, including in your home in Wimbledon, wasn't he?</p> <p>A. That was after this, not on the 2nd, so --</p> <p>Q. But on the 3rd and the 4th?</p> <p>A. He came over on those days, yes. I don't recall much of it, but he did.</p> <p>Q. And Mr Matthews, you say, was simultaneously sending him fake messages about what you were up to even though he was spending time with you?</p> <p>A. Well, this isn't when Mr Matthews was with me. I'd only just come back from Paris on the 2nd. Next, what Mr Matthews did after that is a different thing.</p>	<p>Dr Wright is denying that the email at {L13/123/1} was consistent with what Ramona would say, asserting that he was not running the email account.</p>
<p>{L13/104/1}, email from Mr MacGregor to Mr Ayre</p>		
<p>{Day8/27:1-10}</p>	<p>Q. {L13/104/1}, an email from Mr MacGregor to Mr Ayre, Mr Matthews, yourself at the nCrypt address, 2 May, that afternoon: "Craig and Stefan are both en route to Wimbledon now to get access to the computer Craig needs." You say they</p>	<p>Dr Wright is claiming his memory around the signing session</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>weren't en route to Wimbledon at that time -- you weren't en route to Wimbledon with Mr Matthews at that time?</p> <p>A. As I've said, I don't believe so, but my memory of that period is very fuzzy.</p>	<p>period is “very fuzzy”.</p>
{Day8/28:11-18}	<p>Q. Dr Wright, you were happy for all the world to know through these major publications that you had proved possession, supposedly, in the private signing sessions, weren't you?</p> <p>A. Do you actually recall the video yesterday? Does that sound like someone who sounded happy to you? I mean, I was very angry, I was very upset, I swore a lot, I was agitated. I don't think that sound like a happy person.</p>	<p>Dr Wright is evasive and answers a different question.</p>
{Day8/28:24} - {Day8/29:14}	<p>Q. Dr Wright, I'm not disputing that you were under stress when you were doing those interviews. You were perfectly content, and you agreed, for articles to come out to the world reporting that you had carried out the cryptographic process to prove possession, weren't you?</p> <p>A. No, actually, that was Robert's bit. I was very happy for people to prove my identity. I've detailed to you multiple times what that means.</p> <p>Q. And the reason you ultimately failed and refused to perform a public signing was the simple one, that you couldn't; that's right, isn't it?</p> <p>A. Not at all. Actually, I could. At that point, it would have been the easiest thing to do, but the problem is, then I'm not actually going to have anyone ever look at what I've done.</p>	<p>Dr Wright is stating that it would have been “the easiest thing to do” to perform a public signing, and yet he did not and still has not, despite the importance to him of proving that he is Satoshi.</p>
{L13/261/1} Wright / Andresen email		
{Day8/29:15-23}	<p>Q. {L13/261/1}, please. We're moving to 3 May, an exchange on 3 May between you and Mr Andresen.</p> <p>A. No, it's not.</p> <p>Q. And the email from craig@ncrypt.com says that coin will be moved but trust permissions need to be got in place. Do you say that that's another email not written by you?</p> <p>A. Definitely. I told everyone there's no way I'm moving coin and I'm not doing this, so that's definitely not me.</p>	<p>Dr Wright is denying that the email at {L13/261/1} about moving coin was written by him.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{L/13/268} MacGregor/Wright/Ramona email		
{Day8/30:7-12}	<p>Q. Dr Wright, it's a really simple question. Do you say that this is another email that didn't reach you and your wife? A simple question.</p> <p>A. And it's a simple answer. I had no urgency, so this is an email to nCrypt, where I had lost control of that account.</p>	<p>Dr Wright is evasive in response to the question about whether this is an email that did not reach him and Ramona.</p>
{L13/209/1} "Extraordinary Claims Require Extraordinary Proof" (attachment to {L/13/268})		
{Day8/30:13} - {Day8/31:9}	<p>Q. {L13/209/1}, please. This is the attachment: "Extraordinary Claims Require Extraordinary Proof." We see that after a preamble, the draft says, in a paragraph towards the bottom, you will be laying the foundations for your extraordinary claim to be Satoshi: "... including signing ... with the 'Satoshi' PGP key ... posting independently-verifiable documents and ... transferring Bitcoin from block 9 ..." Ending on page 2 {L13/209/2} with a request that this proof be independently validated. Is that a draft blogpost which you saw on 3 May, whether received by email or in any other way?</p> <p>A. Oh, I saw it at my house when people showed it to me. I basically said that it was a load of four letter words starting with C.</p> <p>Q. So Mr MacGregor and his people bothered to show it to you at your home, but the email attaching it is a fake; is that right?</p> <p>A. I've told you, it's not a fake. I didn't control the email address. So someone sending an email doesn't make it a fake, it means that the address isn't mine.</p>	<p>Dr Wright is evasive when asked about whether the email attaching the draft blog post at {L13/209/1} is a fake.</p>
{L13/252} Ramona email to MacGregor		
{Day8/31:10-25}	<p>Q. {L13/252/1}. This is another document which is on your list of documents which you referred to for your first witness statement. For the lawyer's reference, that's {E/1/40}, item 19. And do you see that in the middle, your wife replies to Mr MacGregor in relation to the draft blogpost: "Ok Satoshi "Your writing is REALLY impressive. "Did you get Craig's email</p>	<p>Dr Wright's answer in relation to whether his wife wrote the email at {L13/252/1} is evasive.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>about adding a bit saying he was 'outed' by leaked documents etc in December? He wants to dispel the myth of his 'self outing'." Is that an email your wife wrote on that Tuesday, early in the afternoon?</p> <p>A. I know she got kicked off nCrypt. I don't know when. But it doesn't sound like something my wife would write, no.</p>	
<p>{Day8/32:14-23}</p>	<p>Q. You don't say anywhere in your statement, despite your desire to blacken Mr MacGregor, that he took over your nCrypt account and sent all these emails to try to alter history while it was happening?</p> <p>A. Well, I don't actually know who did it. I mean, you're asking me to speculate there. It's quite possibly. But what I do know is that emails were being sent so that I would be put in a position where Gavin was going, "Why did you do this, why - you promised me that you'd sign".</p>	<p>Despite stating multiple times that Robert MacGregor took control of his nCrypt email account, Dr Wright rows back and asserts that he does not know who sent the emails.</p>
<p>{L13/231/1} - Email from Mr MacGregor, "PGP Key?"</p>		
<p>{Day8/33:2} - {Day8/34:4}</p>	<p>Q. {L13/231/1}, please, another email from Mr MacGregor, under the heading "PGP Key?", asking: "Have you got the slices yet?" And you're recorded as responding: "I will chase them up soon." And Mr MacGregor saying: "... critical ... we get this today." You're saying that that's another email, are you, where the apparent emails from you weren't actually from you?</p> <p>A. Well, yes. I mean, if you actually read this, it makes it hard to actually believe that it could be my story, because the slices were ones that I'd already used. So I'd already done, in April, all of this. The slices don't disappear. I don't need to contact people every time I get it. Once I've decrypted the drive and made the Bitcoin wallet with those in there, I had them. I didn't need slices any more. So the story from Robert --</p> <p>Q. This isn't discussing Bitcoin keys relating to a Bitcoin wallet, this is discussing the PGP key.</p> <p>A. Well, I told you, that's not a signing key. But again, when we're -- it says in -- in the last line here: "Have you got the slices yet?" And then says: "I will chase them up soon." So, no, that's incorrect. This is talking about chasing up key slices. I didn't need those, I had them.</p>	<p>Dr Wright is evasive when asked for confirmation that the email at {L13/231/1} is not from him, confusing the Bitcoin keys relating to a Bitcoin wallet with the PGP key.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{L13/236/1} Emails between MacGregor/Wright Denis Mayaka		
<p>{Day8/34:12} - {Day8/35:11}</p>	<p>{L13/236/1}. This is another of the documents in your PD57AC list which you reviewed for your witness statement. Item 20. The email goes on, doesn't it, with you saying -- denying that you had signed anything publicly with the PGP key, and then, further up the page, saying that you had a slice from Denis Mayaka, but not yet from the people from Savannah, yes?</p> <p>A. Yes, well, this demonstrates the error in what you're thinking. While Savannah and Denis ran Seychelles companies, I don't think Rob knew at the time. Denis actually lives in Kenya, in Nairobi, so arguing about getting late in the Seychelles has nothing to do with Denis. So, I didn't explain that, but that's where he lives. So that, in that part, is an error.</p> <p>Q. Dr Wright, I'm not suggesting to you for a moment that these were real key slices giving access to a real private PGP key, but these were emails which Robert MacGregor wrote that day, copying Mr Matthews in, and to which you responded, aren't they?</p> <p>A. No. As I stated already, I'd already had my access revoked, so what I do know is, well, I was being put in a position where everything's set up so that: obviously, Craig, you're agreeing, you've told everyone, you've told Gavin, you've told Jon, you've told Ian that you will sign publicly.</p>	<p>Dr Wright is evasive when shown the contents of this email, and provides an incoherent response about access to the key slices.</p>
{L13/257/1} Email with Matthews re: slices		
<p>{Day8/35:25} - {Day8/36:12}</p>	<p>Q. Dr Wright, the reality is that all these emails involved real communications by you, you approved the blogpost through your wife, you were giving your backers the run around over these hours. That's the truth, isn't it?</p> <p>A. Not at all. I had no interest in any of that. What I do know is I was being put under pressure to sign.</p> <p>Q. Moving back to the PGP key, would you accept this, that there is a well known PGP key which has been attributed to Satoshi and the public key for which has been hosted on the bitcoin.org website?</p>	<p>Dr Wright is denying that there is a PGP key attributed to Satoshi, the public key for which has been hosted on the bitcoin.org website.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. No, the public key was -- for that version was only posted in 2011. There was actually an earlier version associated with the site. That isn't there.</p>	
<p>{A/3/24}, Para 83(2) of Defence - Wright claims to demonstrate control of Satoshi's Private Key</p>		
<p>{Day8/37:9} - {Day8/39:2}</p>	<p>Q. {A/3/24}, please, paragraph 83(2) in your defence. Responding to a contention that if you were Satoshi you could demonstrate control over Satoshi's private key, you plead this at 83(2): "It is not clear from paragraph 61.1 what 'private key' is referred to. There has been public discussion of a key created in 2011 after Dr Wright 'retired' his Satoshi Nakamoto persona." Pausing there. That's the key that you were - that we just looked at, isn't it?</p> <p>A. That is the key that has been loaded -</p> <p>Q. Is that the key we just looked at?</p> <p>A. No, actually, not in the way that you're talking. If you'll let me finish, what I'm stating is that the key that had been used for Gavin, Martti and others, as an encryption and decryption key was loaded as if it was a signing key. They're different things.</p> <p>Q. You're not answering my question.</p> <p>A. I actually am.</p> <p>Q. You refer in paragraph 83(2), second sentence, of the defence, to there having been "public discussion of a key created in 2011". Are you referring, by that sentence, to the key we were just looking at or to some completely different key with a completely different set of figures and numerals?</p> <p>A. Do you understand that private keys and public keys are separate? 83(2) is answering a question about a private key.</p> <p>MR JUSTICE MELLOR: Would you answer the question, Dr Wright?</p> <p>A. Yes, my Lord. PGP allows updates, so -</p> <p>MR JUSTICE MELLOR: No, okay, the question was, the key that's referred to at paragraph 83(2) of your defence, is that the key that we've just been looking at?</p> <p>A. No. In 82(2) [sic] is referencing a private key. That's referencing a public key.</p> <p>MR JUSTICE MELLOR: Okay.</p>	<p>Dr Wright is evasive when asked about the key referenced at paragraph 83(2) of his Defence, not answering the question asked until prompted twice by Mellor J.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>MR HOUGH: Are you then referring to the private key, which is the pair of the public key we looked at a few moments ago on the screen?</p> <p>A. What I'm saying, again, is the difference between a signing and encryption key. The encryption key is related to that one, and the private key would be the same, but you can update algorithms, etc, in these.</p>	
<p>{L6/477/1} Emails response to Satoshi's GMX account</p>		
<p>{Day8/40:14} – {Day8/41:15}</p>	<p>Q. {L6/477/1}, please. Do you see an email response from Satoshi at his GMX account --</p> <p>A. I do.</p> <p>Q. -- providing the PGP key? Do you accept that's a genuine email?</p> <p>A. Yes. I see the decryption and encryption key being sent.</p> <p>Q. And do you accept that the PGP key there is the same as the PGP key hosted on the bitcoin.org website from 2011 or earlier, which we looked at earlier?</p> <p>A. What I'll note, once again --</p> <p>Q. Is it just -- is it the same key?</p> <p>A. Not one that was originally there. It's the one that Martti loaded.</p> <p>Q. Are the figures and numbers the same on the page, beginning "mQ ..." --</p> <p>A. It is the key that Martti loaded --</p> <p>Q. -- "... GiBEkj"?</p> <p>A. -- in 2011. It is not the original one.</p> <p>Q. I didn't ask that question. I asked the question whether the key we are looking at, with all the -- with the long string of letters and numbers, is the same as the key we looked at, just in terms of numbers and letters, that had been hosted on the bitcoin.org website which we saw on the Wayback capture, yes?</p> <p>A. To answer once again, it is the key that Martti loaded in February 2011, yes.</p>	<p>Dr Wright refusing to accept that the key sent by Satoshi is the same key as then uploaded publicly by Martti Malmi.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{L19/111/2} Satoshi post posting his public key; {E4} Fourth Witness Statement of Dr Wright		
{Day8/42:10-24}	<p>Q. And then, over the page {E/4/34} to paragraph 104, you write this, don't you, that the reference in paragraph 83(2) was a reference to the PGP encryption key at the Wayback capture website that we look at. That's something you've just denied, isn't it, Dr Wright?</p> <p>A. No, if you look at the first sentence I said in this section, I say, one, I'm not quite understanding what you're asking -- I'm paraphrasing, of course, because I can't see it in front of me. In this, I explain to you that that was a key that I'd privately sent to Gavin and Martti and others, and it isn't the same key. I had updated that for encryption reasons with different people and I've received different ones from Martti and others.</p>	Dr Wright is rowing back on his denial of paragraph 83(2) of his Defence.
{Day8/42:25} - {Day8/43:24}	<p>Q. That's wrong, isn't it, Dr Wright, because as you know, Mr Madden has authenticated the key, establishing that it is the same key that was first uploaded in October 2008? You're aware of that, aren't you?</p> <p>A. No, he hasn't. He has given a link that goes to February 2011, which I think is actually very -- I mean, it's a little bit dishonest to give a 2010 link and say that it's actually -- when you click on it, it goes to a 2011 site. So that's wrong.</p> <p>Q. Well, he's identified metadata for the key file which showed that it was first uploaded on 30 October 2008, hasn't he, Dr Wright?</p> <p>A. No, actually, he hasn't. Again, he is making a statement that's actually not true. And the metadata that he's providing on a text file, I believe you actually stated, and I'm quoting you, there is no forensic evidence on a text file, no metadata to be found, yet Mr Madden's saying there's metadata in this text file.</p> <p>Q. So this is another respect in which you disagree with the expert evidence?</p> <p>A. Because there isn't any. He's actually saying an opinion. If there was evidence, he could easily just show it, not just saying an opinion, going, "It must be there".</p>	Dr Wright is accusing Mr Madden of dishonesty, and criticising him based on a misunderstanding that experts are not supposed to be expressing opinions.
{G/6/50} - Fourth Expert Report of Mr Madden}		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day8/45:3-17}</p>	<p>MR JUSTICE MELLOR: Who’s saying that this date is false then? Are you saying that?</p> <p>A. I’m saying that that date was set back to the beginning of the project -</p> <p>MR JUSTICE MELLOR: By whom?</p> <p>A. By myself.</p> <p>MR JUSTICE MELLOR: Why would you do that?</p> <p>A. Because that’s when the project started.</p> <p>MR JUSTICE MELLOR: Right.</p> <p>A. I do this sort of thing all the time.</p> <p>MR JUSTICE MELLOR: Yes.</p> <p>A. When you’re setting up keys, you’ll notice that there are a variety of keys in there, my Lord. You can change the algorithms and update keys, etc, but key creation dates, I generally leave to the project.</p>	<p>Dr Wright is admitting when questioned by Mellor J on the output of the PGP key at {G/6/50} that he set the date back to the beginning of the project, and that he does “this sort of this all the time”: an admission of backdating documents.</p>
<p>{Day8/45:18} - {Day8/47:4}</p>	<p>MR HOUGH: Last point before the break. Would you accept that this output also shows distinct signature packets showing that this can be used as both a signing key and an encryption key?</p> <p>A. No, it shows that -</p> <p>Q. Do you accept that that’s what the output shows, first of all?</p> <p>A. I accept that you can use PGP in that way, but that is bad practice.</p> <p>Q. Do you accept that the signature packets in this output show that this case could be used as both a signature key and an encryption key?</p> <p>A. I accept you can have bad practice, and someone such as Satoshi would know not to do that.</p> <p>Q. Last chance to answer the question, Dr Wright, before we assume that you have no answer. Do you accept from this output that this key has always had the functions of signature key and encryption key, it can be used for both, based on its signature packets?</p> <p>A. Again, there are two questions there. One, do I accept that it always has? No. When you’re doing PGP, you can update the items and add or remove algorithms at any time. That doesn’t change anything or - like, there’s no metadata that you can use from a key file to say when that’s created. So I can add a new algorithm because one’s been compromised and my key will still be valid.</p>	<p>Dr Wright is not accepting obvious truth that the output at {G/6/50} shows that it can be used as both a signing key and an encryption key.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. And it's right, isn't it, that this story you've now been giving the court about backdating the output and adding functions to the key is something you haven't said in any of your statements on this subject?</p> <p>A. No, that's actually incorrect. I've noted that this was actually how you run PGP; I've noted many times that you should not use an encryption key and a signing key together; I've noted that with Gavin and Martti, I used this for them to send me encrypted files that would be decrypted on the server. So, yes, I've said that multiple times.</p>	
{L6/477/1} Emails between Satoshi and Martti Malmi		
<p>{Day8/47:17} - {Day8/48:18}</p>	<p>Q. {L6/477/1}, please, back to the email exchange with Mr Malmi which you said is genuine. After setting out that key block, Satoshi wrote, at the bottom of the page: "It's also at ...www.bitcoin.org/Satoshi_Nakamoto.asc." Didn't they?</p> <p>A. No, the version that I had was actually slightly different. So where I've said that, the one that was up there, like I said, was linked, but you can change and update. So, where you're saying that this version is there, that's the incorrect part.</p> <p>Q. Doctor --</p> <p>A. They are related keys, they have the same private key, but they are updated.</p> <p>Q. Dr Wright, this public key block that's on this email is identical to the public key block shown on the 2011 web capture, and Satoshi is here saying that, as of 6 December 2010, was on the bitcoin.org website. You're denying plain fact, aren't you?</p> <p>A. No, I'm not. You're misunderstanding how PGP works and the update process. If I have the private key, I can update all the algorithms. So the version that I had loaded and that was available actually had less and different. So anything that they sent me using this key, or the other, would both work with my private key that I had on the server.</p>	<p>Dr Wright is not accepting the obvious truth of the words in the email exchange between Satoshi and Mr Malmi (which he has accepted is genuine) regarding the public key.</p>
<p>{Day8/49:8-17}</p>	<p>Q. Satoshi's emails, the metadata, Satoshi's post, all indicate that this key in this form has been - this public key in this form has been available on the bitcoin.org website from 2010 and earlier; you are just denying plain fact, aren't you?</p> <p>A. No, I'm not. Your own person and your own thing that you used yesterday, with Mr Maxwell and keys that I had, say that they can be updated. So, saying that there are different versions of the same key that I can still decrypt is the not same thing.</p>	<p>Dr Wright is not accepting the obvious truth of the words in the email exchange between Satoshi and Mr Malmi (which he has accepted is genuine) regarding the public key.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{L13/276/1} Email exchange with MacGregor re: moving block 9		
<p>{Day8/50:2} – {Day8/51:5}</p>	<p>Q. And yet you say that this was on – ah, well, no, let’s see, these emails include emails to both “nCrypt Ramona” but also to you at RCJBR.org. Do you accept that these emails are real and in fact the ones attributed to you came from you?</p> <p>A. Quite possibly. I don’t recall. But as you can see here, “craig@rcjbr” is a different email so ... So at this point I was getting these ones, but not the others.</p> <p>Q. I see, so you accept you were getting these ones, right Down to the bottom, please. Here, you are saying that you’ve been desperately trying to get in touch with the people at Savannah Limited, which appears to link in with the emails previously which you’ve denied, doesn’t it ?</p> <p>A. No, I don’t recall any of that part.</p> <p>Q. Even though this is from an email address which you’ve accepted is genuine and you suggested was the email address that we could treat as reliable?</p> <p>A. No, that’s not what I said. What I also said were each of these were found a staff laptop. The reason that you have that and the ones from my wife are that both craig@rcjbr and ramona@rcjbr were on that employee laptop, neither of which should have access.</p> <p>Q. You don’t say in any of these emails, do you, that the emails shouldn’t be copied to ramona@ncrypt because she doesn’t have access to an nCrypt email, do you?</p> <p>A. No, I don’t recall much of what happened on the 3rd, but what I do know is each of these come from a third party machine, a compromised machine.</p>	<p>Dr Wright is initially appearing to accept that the email at {L13/276/1} could have come from him, but then backtracking and blaming third parties (compromised employee laptops).</p>
{L13/325/1} – Emails between MacGregor/Matthews/Ramona/Dr Wright		
<p>{Day8/51:6} – {Day8/52:8}</p>	<p>Q. {L13/325/1}. We see here Stefan Matthews, on the morning of the 4th, asking for an update, including in relation to the “final required slice of the PGP key”. Do you say that’s an email or communication that never reached you?</p> <p>A. The one from Stefan definitely didn’t. I’m not on it at all. Not in any form. And the other one is “nCrypt Craig” once again.</p> <p>Q. So it’s another email that never got through to you over these days?</p>	<p>Dr Wright is refusing to accept he was copied in on these emails relating to the proofing sessions.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Well, it would never get through to me because I never had that email at that point; I was cut off.</p> <p>Q. So all this email traffic was going on, including with Mr Matthews, who was spending time with you, and it never came out that there were a whole series of emails being written by somebody else purporting to be from you?</p> <p>A. No, it would --</p> <p>Q. (Overspeaking – inaudible).</p> <p>A. It would explain why Mr Matthews seemed strange at the time. I’m not good with people and I’m not good with trust, part of being autistic, but I found – at the time, I thought Mr Matthews was acting weird. I’ve known Stefan for a long time and I didn’t understand what was going on at the time. So I don’t think he had any reason to believe that any of the emails weren’t me, so he’s sort of saying things and doing things that I thought were strange.</p>	
<p>{Day8/52:9} - {Day8/53:5}</p>	<p>Q. Once again, Dr Wright, an incredibly high risk strategy for whoever was behind it - you suggest Mr MacGregor - to be producing these emails supposedly from you to people who were spending time with you over those days, yes?</p> <p>A. I said Mr MacGregor was pressuring me. I don’t know whether Mr MacGregor was sending emails or not. As I noted, all of these emails came from a machine that was put into the not only disclosure, but chain of custody as compromised. The only reason any of these got in was because the Kleiman case required that employee laptops also got imaged.</p> <p>Q. Dr Wright, first of all, none of these appears in the chain of custody referred to as compromised, because these don’t feature among your primary reliance documents.</p> <p>A. I’m not sure what’s been listed there. I know what I filled out, and when I filled out -</p> <p>Q. Please don’t tell us anything privileged.</p> <p>A. Well, I filled out the document that got put in, so I don’t know what was put in chain of custody after I filled out the full document.</p>	<p>Dr Wright is blaming third parties, claiming that these emails came from a compromised machine, but nothing in Dr Wright’s disclosure certificate referred to compromised machines.</p>
<p>{L13/328/1} MacGregor email re: Matonis on TV</p>		
<p>{Day8/53:6-18}</p>	<p>Q. {L13/328/1}, the morning of 4 May, yet another message from Mr MacGregor about Mr Matonis going on TV and asking you for input on what he can say, again, because we see that’s to craig@ncrypt, that’s a message that didn’t get through to you, is it?</p>	<p>Dr Wright is claiming that he could not have sent this email, despite not being in</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Yeah. I mean, later this day - I believe that was the day I attempted suicide - there were emails being sent while I was in hospital unconscious.</p> <p>Q. Well, this was in the morning. This was well before you were in hospital, Dr Wright.</p> <p>A. I know, but I'm just saying, if I'm unconscious sending these emails as well, it makes it difficult, or beggars belief that I'm sending while unconscious.</p>	<p>hospital until much later that day.</p>
<p>{L13/357/1} Emails re: Matthews involvement making arrangements</p>		
<p>{Day8/54:18} - {Day8/55:16}</p>	<p>Q. Moving on in 4 May, Mr Matthews' evidence - and this is also in "The Satoshi Affair" by Mr O'Hagan - is that early that afternoon, 4 May, you had a call with Mr Andresen on the telephone discussing moving coin as planned; is that right?</p> <p>A. I don't recall.</p> <p>Q. And Mr Matthews' evidence is that this call was on speaker in his presence; do you recall that?</p> <p>A. I don't recall.</p> <p>Q. And presumably then you do not recall anything about what you wanted to get across to Mr Andresen that day?</p> <p>A. No, I don't.</p> <p>Q. Because Mr Matthews said that you were looking for an excuse for not performing the transactions and wanting to explain that there were some imperfections in the early code. First of all, do you recall saying that?</p> <p>A. I don't.</p> <p>Q. Secondly, do you think it's something you might have said, based on just what he attributes to you?</p> <p>A. I can be vague; people can take what I say in the wrong way. So I don't know. I hadn't slept for over 24 hours at that point, so I don't think I was explaining myself terribly well in any event.</p>	<p>Dr Wright is claiming that he does not remember the events described in Mr Matthews' evidence on 4 May 2016.</p>
<p>{E/2} Second witness statement of Dr Wright</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day8/64:23} – {Day8/66:1}</p>	<p>Q. We’ll come to Mr Andresen’s session in a moment. With all – with the journalists and Mr Matonis, you could have adopted, rather than this complex multi-system approach, the simple approach of putting a new message and a signature on a USB stick and then saying, “There you go, get somebody who understands the Bitcoin System to validate that”.</p> <p>A. No, actually, once again, the entire purpose of this was, I wanted control of what happened. I had stated categorically that the reason I’m not doing this, the reason I’m not doing it on block is I want to control the process and make sure that people prove things first. So, to do that means that I’ve then given a signature that I have no control over. I would then have Rob being able to say whatever he wanted, any of the others. There’s no way of stopping someone releasing it.</p> <p>Q. The journalists were supposed to report you doing this signature. That was the whole point of them going through this with you, wasn’t it?</p> <p>A. No, the whole point was, first, they be journalists, they be reporters, they actually do journalism and they go through and they look at all my degrees, all my qualifications, all of papers, all my patent filings first. That was their job. That’s why we said journalists. My understanding of journalism is that you go through, and maybe because I’m an Aspie, you – I’m very particular on these things, but journalism isn’t just writing blogs.</p>	<p>Dr Wright is admitting to social engineering in relation to the signing sessions for the journalists.</p>
<p>Signing Session with Gavin Andresen</p>		
<p>{Day8/66:17} - {Day8/67:9}</p>	<p>Q. He initially expected you to put a signature on that stick which he could verify on his own laptop, didn’t he? That was his initial expectation?</p> <p>A. I don’t know. I said categorically what I would do, which is if he wanted it on his laptop, I take the laptop home.</p> <p>Q. Well, Mr Matthews has given an account, so I’ll give you the opportunity to give a different one if you wish, that Mr Andresen positively suggested verifying on his laptop and you objected to that; is that right?</p> <p>A. My objection, as I just said -</p> <p>Q. Did it happen, first of all? We’ll get to the reasons in a moment. Did it happen? Did you object to a suggestion from Mr Andresen that he use his own laptop?</p>	<p>Dr Wright is admitting to objecting to Gavin Andresen using his own laptop.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. I said, as my objection, not that I objected to him using his laptop, but if he used his laptop, I wouldn't let him take it home.</p>	
<p>{Day8/67:15} - {Day8/69:2}</p>	<p>Q. And there was then a signing session which took some hours, wasn't there?</p> <p>A. No. The signing session was quick. The some hours was the process. It was a brand new laptop in a sealed box, so we had to take it out, we had to install Windows, we had to install applications, we had to set up the environment, and Gavin and I worked on that together. There was no point where neither of us were alone on the laptop, but sometimes he was on the laptop, sometimes I was, during the process.</p> <p>Q. Now, you said in your evidence in Granath - I can take you to it if you'd like - that the connection was to the hotel WiFi but a third party hot spot might have been used; is that right?</p> <p>A. I don't actually know. I know that WiFi was connected, but I don't actually know which particular WiFi it was.</p> <p>Q. Now, in your first witness statement you say that on the laptop that had been brought in, Gavin did the installation of Windows and he downloaded Electrum, the Bitcoin wallet software, directly from the website. That's what you say in your first witness statement, isn't it?</p> <p>A. Well, yes. Exactly who downloaded each'bit, I am not 100% sure. What I do know, my Lord, is both of us were in and out of the chair. So there were different parts. Either I was sitting on the chair typing, or Gavin - with Gavin looking over my shoulder or vice versa, and we took turns on each part of the set-up.</p> <p>Q. {E/1/35}, bottom of the page: "Once the laptop arrived, Gavin took the lead in setting it up from scratch. He downloaded Electrum, a Bitcoin wallet software, which could be utilised to verify a digital signature." You were very categorical in your witness statement, but rather less sure now, right?</p> <p>A. I 'm not 100%. I do believe that he did, but there were multiple bits of software and I can't recall every single thing we did.</p>	<p>Dr Wright is admitting that he does not know the WiFi that the laptop was on for the signing session with Andresen. Dr Wright is backtracking on the evidence in his first witness statement regarding Gavin installing Windows and downloading Electrum, and admitting he cannot recall the details.</p>
<p>{Day8/69:3} - {Day8/70:19}</p> <p>{E/1/35}</p> <p>First Witness Statement of Craig Wright</p>	<p>Q. You're aware, aren't you, that Mr Andresen, giving evidence in the Kleiman case, was very clear that you had chosen and downloaded the software, right?</p> <p>A. I chose it. I mean, we were going over different options, and I was using BTC Core on one machine, etc, so the option</p>	<p>Dr Wright is admitting he can't remember details due to it being "many years ago".</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>was, like, we went over things and that was a quick, easy option.</p> <p>Q. It's right, isn't it, that as Mr Andresen told the court in Kleiman, you did not take the step of verifying the Electrum download by checking the HTTPS SSL security certificate on the website, did you?</p> <p>A. No, actually, that's incorrect. The browser at the time comes up with that. So, Electrum uses the secure browser certificate function, and, now, that's been hidden by modern browsers, but at the time in 2016, this was actually a main function and it would display a green lock. So it would either come up in Chrome, or whatever, as a big red thing saying "not secure", or green. That's been depreciated, but at the time of this download, Electrum ran that and was part of that program and that - you don't need to click the lock, it's a function of the browser itself.</p> <p>Q. So you say that's a function that operated in relation to the Electrum site that day?</p> <p>A. Yes, it did. They're actually signed up for secure certificates.</p> <p>Q. Dr Wright, in your ninth witness statement, you said you couldn't remember if the download was from the Electrum site or from GitHub; is that right?</p> <p>A. The GitHub is connected to the Electrum site. I know we went through both. I don't know which one we clicked.</p> <p>Q. You were just referring to a security validation by reference to the Electrum site when in fact you can't remember whether the Electrum site was used?</p> <p>A. No, that's incorrect. What I said was we went to the Electrum site. Now, Electrum site has a main download, but it also has the link to GitHub, and GitHub also runs the security keys for each of these. So I don't recall whether I downloaded clicking the one click, I mean it is many years ago, or whether we clicked the GitHub full version of all this and then chose one.</p>	
<p>{Day8/71:9-21}</p>	<p>Q. Turning to your second witness statement, you say that you produced a digital signature using an agreed message, yes?</p> <p>A. Yes.</p> <p>Q. You say that you pasted the digital signature into a file, which you saved on the USB stick?</p> <p>A. That Gavin gave me, yes.</p>	<p>Dr Wright is evasive in his responses to questions about the session with Mr Andresen, continuously disclaiming knowledge of</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. You say that you gave the USB stick to Gavin, who inserted it into the laptop that had been brought in, yes?</p> <p>A. Yes, something like that. Exactly who was sitting in the chair, etc, at the time, I don't recall, it's years ago.</p>	<p>specific things even where not asked.</p>
<p>{Day8/71:22} - {Day8/73:13}</p>	<p>Q. You say, don't you, that he performed the verification?</p> <p>A. Yes.</p> <p>Q. Now, in fact, as Mr Andresen told the court in the Kleiman proceedings, you performed both the signing and the verification, didn't you?</p> <p>A. No. What happened was we, first of all, typed in the message, I cut and pasted the - the signed value, but the message I read out, and when we first put that in, it was incorrect. Then what happened was, I came over and we corrected it in the tool. I - if you're even one character out, space wrong, etc, I can't remember what the error was, but there was something, like one - one letter was off -</p> <p>Q. Let me put to you what the error was, based on Mr Andresen's evidence in the Kleiman proceedings. His evidence is that the message was meant to be "Gavin's favourite number is 11 CSW", because you'd asked for "CSW" to be added, and the error was that the "CSW" was missed. Does that ring a bell?</p> <p>A. It's quite possible. I know he said something, I said something, and then a joint message isn't one - like I couldn't pre-empt what Gavin would say, and adding "CSW" isn't something he could pre-empt.</p> <p>Q. Why was it important for you to add something to this message?</p> <p>A. It just makes it a mix, something extra.</p> <p>Q. Why is that valuable?</p> <p>A. Because it just makes it more likely it is a combination message, if you're signing something.</p> <p>Q. It doesn't make it any more valuable, does it, Dr Wright? It just has to be a new message; why were you adding these extra letters?</p> <p>A. Again, it actually makes it more likely that someone hasn't planned anything. I know you're saying that adding "CSW" makes the software run differently, but that's actually ridiculous, I'm sorry.</p> <p>Q. And it was you, rather than Mr Andresen, who noted the supposed error in the first attempt, wasn't it?</p>	<p>Dr Wright is unable to provide a clear answer as to why he added "CSW" to the message to produce a digital signature.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Yes, it didn't actually work, and that's why I jumped in. So, Gavin was still there watching everything I typed, but then we looked at it and then I noted, "You missed this", and when we typed it in, then it verified.</p>	
<p>{Day8/73:14} - {Day8/75:8}</p>	<p>Q. I'm going to put to you what Professor Meiklejohn says of this session in a part of her report which is agreed by your expert. First of all, it would have been technically straightforward to create software designed to look like Electrum that would produce a false positive output on verification, wouldn't it?</p> <p>A. You can do it fairly -you could actually change Electrum, yes.</p> <p>Q. And it would have been entirely feasible to create a program which would interfere with the genuine Electrum software and cause it to provide a misleading output, wouldn't it?</p> <p>A. Actually, no. What you're presuming is that something was installed on that machine. It was a new machine. If I had a machine remotely and I'd had time to do this, then that would be correct. But in both cases, the Electrum software was downloaded from Electrum, and I know people want to argue otherwise, but that was validated, Gavin actually contacted the person and the logs are there, and, secondly, to do what you're suggesting, it was Gavin's USB stick, it was Gavin's everything else, so...</p> <p>Q. Dr Wright, staging this signing session would have been straightforward for someone with your experience, wouldn't it?</p> <p>A. No, incredibly difficult. One of the things I do understand is malware. I've got one of only about five people globally to have ever done the global security expert in malware, I have the GREM, which is a PhD level malware certification, I have a dissertation on the topic, and what I can say is, while you can do this, this is incredibly difficult. Some of the exercises I did, my Lord, for anti-virus companies, for small analysis, would take three months. This is where the asymmetry of the industry is.</p> <p>Q. Sorry, Dr Wright, I thought you'd agreed that it would have been technically straightforward to create software intended to look like Electrum that would produce a false positive output, and now you're telling us it's very difficult?</p> <p>A. No, I said if I had a machine of my own, not fake sites, not everything else. Your presumption is, yes, you can alter the code to make these things happen, but downloading it from either GitHub or the other isn't an option.</p>	<p>Dr Wright is initially agreeing with Professor Meiklejohn's proposition that it would have been straightforward to create software intended to look like Electrum that would produce a false positive output, but then backtracking and saying it would be "incredibly difficult".</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day8/75:9} - {Day8/76:9}</p>	<p>Q. All this assumes, Dr Wright, that there has been a genuine download and for that we have just your word, right?</p> <p>A. No, you have Gavin's as well.</p> <p>Q. No, we don't have Mr Andresen's word, do we, because all he can say and all he said to the court in Kleiman was that you performed a download which he didn't check by hash or by security certificate?</p> <p>A. As he said, he was watching. The security certificate is on the site. Now, you can validate both GitHub and Electrum at the time we're running the secure browser platform. Now, either - I can't remember whether we used Chrome or the internet browser that came with the thing, I think we actually downloaded Chrome, but in each case, then those browsers at the time supported actually bringing up any invalid websites in large red sort of displays. That has been depreciated because there's a lot of problems with normal sites and they were looked at as being malicious. But in 2016, to go to either GitHub or Electrum, the server, would have brought up a huge red marker across all of the browser saying that this was not secure. So that's not correct. People forget now that in the last seven years this has changed, but at the time, there was no way to get away from that without having a big red marker right across the page saying "insecure". That didn't happen.</p>	<p>Dr Wright provides new (unsupported) factual evidence of security warnings from going to GitHub or Electrum in 2016.</p>
<p>{Day8/76:22} - {Day8/77:12}</p>	<p>Q. What about your expert, Dr Wright? Mr Gao doesn't give any evidence and agrees this part of Professor Meiklejohn's report. He doesn't give any evidence?</p> <p>A. Well, he's not an expert on this either. What he's an expert in is the technology behind Bitcoin. So, he's not going into areas that are overreach.</p> <p>Q. So you chose or approved the choice of an expert who wasn't competent to speak on probably the most important aspect of that expert evidence, right, Dr Wright?</p> <p>A. Not at all. Again, we chose an expert on Bitcoin. Now, that's a different topic. What we weren't allowed to do was bring in extra experts. So we don't have an expert who was a malware topic expert, we don't have any experts who have done any experimentation. No one has been able to demonstrate how this could be done.</p>	<p>Dr Wright is stating that Mr Gao is not an expert on this aspect of the signing session.</p>
<p>{Day8/77:13} - {Day8/79:2}</p>	<p>Q. Nobody requested additional expert evidence on this subject from other disciplines, did they, Dr Wright?</p> <p>A. I did, multiple times.</p> <p>Q. No, no, don't tell us anything privileged. Nobody on your behalf did so, did they?</p>	<p>Dr Wright is admitting that he cannot recall all the details of the session. Dr Wright is not accepting the obvious</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Actually, I think they did. I'm not sure what happened with Travers, but I wanted the Citrix -</p> <p>Q. Please don't tell us anything privileged?</p> <p>A. Well, I'm not. I'm just saying the Citrix person that we've mentioned that I had do exercises was someone that I was trying to bring in. I wanted them rather than Stroz.</p> <p>Q. And Dr Wright, not only could these signing sessions have been straightforwardly staged, but your recollection differs from Mr Andresen's on subjects which are of particular relevance to tampering, so whether the software was downloaded by him and whether it was properly verified, right?</p> <p>A. No, that's actually incorrect. Both of us moved in and out of the chair in different times, and we're talking seven years ago. So, I'm sorry, but I doubt you could remember an event that happened seven years ago with exact clarity. What did happen was Gavin saw everything I typed, Gavin overlooked everything I typed. He saw the site; I spoke to him about it. There was no instance where he was ever not looking at the screen or not able to see something. There was not a second where that was not the case. There were plenty of times when he was on the computer where I was going off, but there was no instance where I was on the computer where he didn't see it.</p> <p>Q. That's not - that - he doesn't say anything like that in his evidence in Kleiman, does he, Dr Wright?</p> <p>A. Actually, he does, he says -</p> <p>Q. Well, the court can form its own view then. If these sessions had been genuine, they would have been carried out under controlled conditions, properly minuted, with the kind of precautions that Ms Meiklejohn identifies, wouldn't they?</p> <p>A. No, they were, actually --</p>	<p>truth that Mr Andresen provided a different account of the session in Kleiman compared Dr Wright's account in these proceedings.</p>
<p>Destruction of USB containing the private keys {E/4/15} Fourth Witness Statement of Craig Wright</p>		
<p>{Day8/79:3} – {Day8/80:15}</p>	<p>Q. Moving on to your supposed destruction of the USB containing the private keys. May we have {E/4/15} on screen. At paragraph 33, you say that you destroyed the hard drive containing the private keys or access to them in around May 2016, you don't recall the exact date, done at your former residence in Wimbledon: "I threw the hard drive with enough force to shatter the glass platters in the hard drive. This destroyed the physical components of the drive rendering the</p>	<p>Dr Wright is stating that he was not clear on how he destroyed the hard drive, contrary to the statements in paragraph 33 of his</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>data stored on it irretrievable.” That was the evidence you gave in your fourth witness statement; correct?</p> <p>A. Yes. I’m not exactly clear on this. I know I destroyed them. I’d come back from hospital a little bit earlier, I had been sedated and I was on medication. I was also very angry, I was upset, I hadn’t slept very much, apart from when I was unconscious, and I know I destroyed the thing.</p> <p>Q. You didn’t express that agree of uncertainty about the method of destruction in this statement, did you, Dr Wright?</p> <p>A. No, but I’m telling you, I – you actually know that I came back from being unconscious at the hospital, and was medicated as well. So when I came back, not only was I tired and upset and angry, I overreacted in doing this and I don’t know if you’ve ever been angry, but recollection’s never good.</p> <p>Q. A simple point, Dr Wright. You don’t say in this statement that you’re really not sure about this, but this is the best recollection you can give?</p> <p>A. No, I’m very sure I destroyed the hard drive.</p> <p>Q. But the method of destruction, given that the question was, “Please explain how he destroyed it”?</p> <p>A. I basically destroyed it. I know I threw it to the ground at one stage. I could have hit it with a hammer as well. The exact recollection I don’t know. I can’t go through the particular stages, but I know I destroyed it.</p>	<p>witness statement {E/4/15}.</p>
<p>{Day8/83:4} - {Day8/84:14}</p>	<p>Q. Do you agree that there is a difference, and quite a significant difference, between saying, “I destroyed something impulsively” and, “I destroyed something because I wanted to ensure that judges and courts understand that Bitcoin is not encrypted”?</p> <p>A. Oh -</p> <p>Q. Do you understand there’s a difference between those two things, first of all?</p> <p>A. Absolutely, no. No. The way that I focus is, that has been my life. I have spent decades creating a system that works within the law that is being misrepresented, where people are saying that there are thousands of Bitcoin nodes or BTC nodes, when in fact there are two that control 60% of the network, both - one of which is a listed company that will take any order my Lord gives them, another one that is controlled on AWS that will give any order my Lord takes it, that is acting within the law, a system that I did an LLM for, that I did another postgraduate qualification in law, that I’m studying a PhD in law for -</p>	<p>When pressed on his motivations for destroying the hard drive, Dr Wright is evasive and digresses into a speech, not answering the question asked.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Dr Wright, I'm going to stop the speech there because we need to make some progress. I suggest to you that there is a material difference between saying, "I destroyed something impulsively", and, "I destroyed something to prove a point".</p> <p>A. Not at all. This is my life's work. When someone does something that impacts what you've been putting your whole career in, that you work 100-plus hours a week on, that you develop intellectual property for, where I'm not making an anti-government thing, that I want it so that child smuggling, child porn, all these other things can be stopped, to be seized, so that the British law that I respect can be implemented, no, that gets me riled. I mean one of the things with Aspies is we focus on certain things and mine is justice and the law, and I want that done.</p>	
<p>{Day8/86:11} - {Day8/87:8}</p>	<p>Q. So, between 2016 and 14 September 2022 when you gave that evidence, you had not even tried to regain access to these keys?</p> <p>A. No, until 2019. After that, I knew I couldn't, because I didn't have those machines and I wouldn't be able to get anything unless I had those machines, back. So I haven't tried, because I haven't got the QNAP servers back.</p> <p>Q. Wait a second. You say now that, from 2019, you knew you couldn't regain access to the keys, and yet here we have you, in the Granath proceedings, in September 2022, telling the court that, in theory, you could obtain access to them again by tracking down some people and doing some things that might gain access? That's a clear contradiction, isn't it, Dr Wright?</p> <p>A. No, it's not. The QNAP servers still exist. While they haven't been imaged correctly, I believe that when I get them back I'll be able to see what's happened to them. At the moment, I don't actually know. Those machines have been floating around the world somewhere with, well, around 250 terabytes worth of my data or more for years when I was told I would have them a week, or maybe two weeks away.</p>	<p>Dr Wright is claiming that there is good evidence out there which he has done nothing to obtain, namely regaining access to the keys stored on the destroyed hard drives.</p>
<p>Dinner with Mike Hearn in July 2016</p>		
<p>{Day8/87:9} - {Day8/88:18}</p>	<p>Q. Dr Wright, new topic. We can take that off screen. After the debacle of the Sartre post in early May 2016, it's right, isn't it, that in July 2016, some arrangements were made for you to meet Mike Hearn, an early member of the Bitcoin developer community who'd corresponded with Satoshi; that's right, isn't it?</p>	<p>Dr Wright's concern that Mr Hearn was probing into the patents he/his company were filing contradicts what he has said throughout about wanting patent ideas to be released as</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Basically, Jon Matonis, sort of, tried to set something up. I don't know why he wanted to, but he wanted me to meet him, yes.</p> <p>Q. A dinner was set up in London at a restaurant called Wild Honey; correct?</p> <p>A. Yes. I don't know who set it up, or exactly all the details, but yes.</p> <p>Q. During the course of that dinner, Mr Hearn asked a number of specific technical questions about the early operation of Bitcoin, including about the use of a certain SIGHASH mode, right?</p> <p>A. Not in the way that's said. He actually -</p> <p>Q. Not in the way that he says?</p> <p>A. If you'll let me finish. What Mr Hearn was actually doing was probing areas that I was doing research into. Mr Hearn, in particular, spent a lot of probing into some of the patents I've filed and where they're going.</p> <p>Q. Well, Dr Wright, I'm going to stop you there. The reality is, he wasn't asking you about your patents, he was asking about - he was asking technical questions to try to establish whether your claim to be Satoshi was valid, asking about the early elements of Bitcoin, wasn't he?</p> <p>A. No, he was asking, in particular, about things that he then, a few weeks later, filed a patent on, that, luckily, I'd actually filed the patent on the day before our meeting. So, Mr Hearn went into areas that I know very well, such as with iDaemon, that we'd covered many, many times and I've posted on.</p>	<p>part of his 'proof' (e.g. the proof pack for journalists).</p>
<p>Dr Wright's legal claims</p>		
<p>{Day8/88:19} - {Day8/89:13}</p>	<p>Q. Dr Wright, that's disputed, but moving on to a further topic, it's right, isn't it, that since 2020 you've asserted intellectual property rights over the White Paper, the Bitcoin file format, the name Bitcoin and the Bitcoin Blockchain? That's correct, as a matter of fact, isn't it?</p> <p>A. No, not the name Bitcoin; that's a trademarked area. What I've asserted is that --</p> <p>Q. Passing off rights in relation to it?</p> <p>A. Passing rights -- passing off rights in relation to calling an altered system that has no relationship to Bitcoin, that has</p>	<p>Dr Wright is not admitting parts of his claim in the Claim Form signed by him {A/3/1}.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>separated these signatures, that doesn't follow the Bitcoin White Paper, that your own --</p> <p>Q. Okay, I'm going to stop --</p> <p>A. -- team has said --</p> <p>Q. I'm going to stop --</p> <p>A. -- is not like --</p> <p>Q. I'm going to stop --</p> <p>A. -- Bitcoin.</p> <p>Q. -- you there, because it's another digressive rant.</p>	
<p>{Day8/89:25} – {Day8/91:16}</p>	<p>Q. It's right, isn't it, that since then you have engaged in a series of legal actions asserting those IP rights and defamation claims against those disputing your claim to be Satoshi; correct?</p> <p>A. No. The defamation claims happened because of a round of attacks led by Jack Dorsey and others, funded by him, doing the Lightning Torch and other such things, basically calling Craig a fraud, saying that all my patents should be taken, with a campaign to try and invalidate –</p> <p>Q. Dr Wright, I'm going to stop you. I asked simply about whether you had issued defamation claims and you're now going into a digressive rant, so I'm going to stop you there. C –</p> <p>A. Can I read your question again? You didn't actually ask me that, you asked me a different question.</p> <p>Q. I asked you if you had pursued defamation claims against those who had disputed your claim to be Satoshi, and it is right as a matter of fact that you have issued defamation claims against people disputing your claim to be Satoshi –</p> <p>A. Can I look at your question again, please? “We obviously don't accept that ...” Sorry, where's your first ...: “... a series of legal actions asserting those IP rights and defamation claims against those disputing your claim to be Satoshi ...” That isn't the correct term. I did defamation claims, as I'm explaining, because I didn't care if they didn't believe I'm Satoshi, I cared that they were actively attacking me. They were calling the systems I'm building a fraud, there was a campaign on Twitter, on Lightning, to say that using BSV means you're a fraud. I cared that they went to every exchange and got me de-listed, I cared that they called up every person using my system and every one of – like, people in governments starting it, and they started putting out things saying that, “This is all fraudulent, they're going to steal your money”. I cared all about that.</p>	<p>Dr Wright is asked about his legal actions asserting certain IP rights and defamation claims against those disputing his claim to be Satoshi. Dr Wright is evasive and does not answer the question asked, going into digression, and then claiming counsel had asked him a different question. When pressed, Dr Wright is argumentative, accusing various people of a campaign against him and the “systems” he was building.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Well, the court can form its own view of your defamation pleadings.</p>	
<p>{C/12/6} Witness Statement of Steve Lee (Dr Wright’s Twitter Campaigns</p>		
<p>{Day8/91:17} – {Day8/93:3}</p>	<p>{C/12/6}, and the subject of Twitter campaigns. Dr Wright, as we can see from these examples, you have yourself been extremely active on social media, like Twitter, threatening Bitcoin developers with bankruptcy, criminal action, losing their families, the death penalty and so on, haven’t you?</p> <p>A. No, that's incorrect. I've threatened people who are criminals. One of these is CZ. CZ was a founder of Binance. He is now facing several hundred criminal charges. That has changed today with the introduction of terrorism funding charges, which have been added to him. That was part of what I’m talking about here. One of them was a BTC Core developer, Amir Taaki. He used BTC, making a mixer, to enable the funding of terrorists in Hamas and others. He promoted that openly.</p> <p>Q. Dr Wright, I’m going to stop you there, because if we look at the post on the left: “If you decide to run an alternative protocol, I’m not being nice anymore, the only option is cybercrime legislation and I will be prosecuting those though those who breach the protocol under criminal law to the full extent of the criminal law in whichever country it happens to be including those with the death penalty and some do.” That’s not, “I’m going to attack those who are committing criminal offences in relation to funding terrorism”, it’s anybody who wants to run an alternative protocol is in your crosshairs; correct?</p> <p>A. No. What I stated was things like Taproot. Taproot, my Lord, was introduced for the sole purpose of anonymising transactions, so that there could be mixer, such as CoinJoin. I was talking about when Taproot and other systems were introduced, these people were doing it to make illegal exchanges outside of the law, outside of the ability to control, outside of the current legislation being introduced into the British Government that enables all of this being linked.</p>	<p>Dr Wright is not accepting the obvious truth of the words in his Twitter posts, denying that he has threatened Bitcoin developers and asserting that he has threatened criminals. When pressed on this, Dr Wright gives an evasive response.</p>
<p>Calvin Ayre/nChain {S2/2.1/13} Granath Proceedings</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day8/93:23} - {Day8/95:10}</p>	<p>Q. Page 13 {S2/2.1/13}. Mr Ayre's tweet of 13 April 2019: "Judge only needs one troll to pass judgment ... no need to sue everyone ... just waiting for a volunteer to bankrupt themselves trying to prove a negative and then letting Craig show the proof. Who will be this moron?" That's Mr Ayre positively tweeting about you taking defamation claims and bankrupting people who dispute your claims to be Satoshi, right?</p> <p>A. I don't actually know. I'm not reading Mr Ayre's Twitter. I don't read much Twitter at all these days, but I know Mr Ayre supports me.</p> <p>Q. Do you follow Mr Ayre on Twitter?</p> <p>A. I don't actually know. I don't run my Twitter account. I have posted things there myself, but --</p> <p>Q. To your knowledge, are you a follower of Mr Ayre on Twitter?</p> <p>A. To my knowledge, no. NChain runs the account.</p> <p>Q. Mr Ayre has a controlling interest in nChain, doesn't he?</p> <p>A. Not directly. I'm not sure what his percentage is. Mr Ayre owns companies that own companies, so --</p> <p>Q. Well, I'm going to put to you, and I'll deal with the documents with Mr Matthews, I'm going to put to you that the Ayre Group has a majority of nChain, the parent entity, and the Ayre Group lists nChain amongst its investments. Would you deny either of those things?</p> <p>A. Oh, I know he's an investor.</p> <p>Q. But that nChain is one of its companies, one of the companies it controls?</p> <p>A. Let me be more specific. I know that he invests in nChain.</p> <p>Q. And nChain, and Ayre Group company, of which Mr Ayre has the majority stake, has provided funding for your litigation, hasn't it?</p> <p>A. No, not at all. I have never received any funding from any part of nChain, either here or overseas. The only money I've received, which I get from them, is now a consulting fee, and before, a salary.</p>	<p>Dr Wright is claiming that nChain runs his Twitter account, even though he no longer works for nChain. This is also inconsistent with {Day8/91:17} – {Day8/93:3} above, where he states that “I’ve threatened people who are criminals” (referring to Twitter posts).</p>
<p>Mock Trial Exercise {M1/1/707} Letter from Clyde & Co dated 10 November 2023</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day8/95:11} - {Day8/96:13}</p>	<p>Q. {M1/1/707}, please, a letter from Clyde & Co on behalf of Zafar Ali and Ted Loveday answering concerns raised about the mock trial exercise, written by a partner at Clyde & Co. At paragraph 2: “In relation to the events you mention, our clients were instructed by nChain UK Limited, the funder and supporter of litigation involving Dr Wright ...” Were they wrong about that?</p> <p>A. In this, what they're doing is taking action now against Mr Ager-Hanssen, so they're funding that. So the litigation, they have an injunction against Mr Ager-Hanssen, a preliminary one --</p> <p>Q. No, this is talking about the -- what Mr Ali and Mr Loveday were doing before the bust up with Mr Ager-Hanssen.</p> <p>A. No, it's not. This is 10 November. This is post. That is when the litigation started against Mr Ager-Hanssen and there is a filing going to be done with the Bar against Mr Ali Zafar. So this is post all of that. This is litigation that, any day now, will be going into criminal matters.</p> <p>Q. Dr Wright, this is nothing to do with that litigation, it is a firm of solicitors writing on behalf of Mr Ali and Mr Loveday to explain what was happening at the time of the mock trial?</p> <p>A. Not by nChain. I don't know who the solicitors, etc, are, but what I can tell you is, in the 10 November, Mr Ali Zafar had nothing to do with nChain.</p>	<p>Dr Wright is stating that Zafar Ali KC had “nothing to do with nChain”.</p> <p>On day 11, Mr Matthews also stated that Mr Ali was not instructed by nChain.</p> <p>Zafar Ali KC’s lawyers, Clyde & Co, state that he was instructed by nChain {M1/1/707}.</p>
<p>Calvin Ayre - financial gain from BSV trading</p>		
<p>{Day8/96:14-17}</p>	<p>Q. Another question about Mr Ayre. Are you aware that he's seeking to gain financially from your claim through trading in BSV?</p> <p>A. Not really. He actually loses a lot of money.</p>	<p>Dr Wright is denying that Calvin Ayre is seeking to gain financially from his claim through BSV trading, claiming that Mr Ayre “loses a lot of money.”</p>
<p>{Day8/96:18} - {Day8/97:14} {L20/252.3/1} {L20/252.4/1} Capture of Calvin Ayre X Posts</p>	<p>Q. {L20/252.3/1}. Could we maximise the top? A tweet from Mr Ayre on 28 December 2023. “So I tell my guy to tell one of our banks in Europe yesterday to start to buy slow as I am all in on Craig winning and the market roars today ... they were just waiting for me to put my money where my mouth is.” Are you aware of Mr Ayre making those sorts of communications, Dr Wright?</p>	<p>Dr Wright is asked about Mr Ayre’s Twitter posts regarding BSV trading, he denies having read any of these posts.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. No, I'm not, but what you're missing is, that's not in cryptocurrency trading. BSV has been de-listed by all of your clients and people related to them.</p> <p>Q. So he's not talking about trading in tokens, is he?</p> <p>A. I doubt it. He would be looking at the companies.</p> <p>Q. {L20/252.4/1}. A tweet from Mr Ayre on the same day: "I never talk tokens but BSV is for sure over 1000 in the run up to the COPA case ... they were watching my money and I said buy but do not move the market [yesterday] and this happens ... watch what happens when I start to buy for real in Jan." He's talking about BSV, isn't he, Dr Wright?</p> <p>A. Looks like it, but I don't know. As I said, I haven't read any of his stuff.</p>	
<p>{L19/212} Email from Calvin Ayre to Dr Wright-23 September 2023</p>		
<p>{Day8/97:15} – {Day8/98:17} {S1/1.35/614} Capture of Calvin Ayre X Post</p>	<p>Q. Aftermath of the mock trial {L19/212/6}. This is an email ostensibly from Calvin Ayre to you, 23 September 2023, immediately after the mock trial exercise, or the day after, which Mr Ager-Hanssen posted. Do you recall receiving this email?</p> <p>A. No.</p> <p>Q. You're aware, aren't you, that Mr Ayre has acknowledged having sent the email?</p> <p>A. No, I'm not.</p> <p>Q. {S1/1.35/614}. Posting about this: "The letter was me trying to talk Craig into signing. Craig being Satoshi is still [an] obvious fact to anyone smart." That's Mr Ayre acknowledging that email was sent by him, isn't it?</p> <p>A. It doesn't look like it. If you go back to the email for a second, I can see nothing about me being forced into signing in that email.</p> <p>Q. Okay, let's go to the email {L19/212/6}. Second paragraph, bottom last sentence: "It no longer matters if you have the keys or not as it is my opinion based on advice from Zafar and others that you cannot win the COPA trial if you do not sign at Harvard so I have no choice in what I have to do." He was trying to push you into signing, wasn't he?</p> <p>A. I don't recall the email, but, no, I mean, not something I was going to do, and we're still dealing with each other.</p>	<p>Dr Wright is denying that he recalls receiving the email from Mr Ayre, but admitting that he and Mr Ayre are still dealing with each other.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day8/99:9} - {Day8/101:8}</p>	<p>Q. "If you have the keys, your best play is to now use them." Contrary to what you just said, the email was trying to press you to use your keys, wasn't it?</p> <p>A. I don't know. I mean, I haven't been looking at any of these emails. I haven't seen one and that's not what's happening. I'm dealing with all of the people at nChain still, I'm -- I'm consulting there, despite this case, and Teranode is still happening.</p> <p>Q. Last paragraph proposes what he will do covering the matter in CoinGeek, saying that: "We will say ... we believe you did forge some documents to replace ones you destroyed earlier to try to pretend you were not Satoshi." Are you aware of Mr Ayre making that suggestion to you?</p> <p>A. No, I'm aware that it came from Ali Zafar. Christen and Zafar had put together a thing saying that I needed to basically go to my Lord and say that these documents were fake and that there would be more, and the only way that I could win this case is to beg you for forgiveness for altering files.</p> <p>Q. This isn't an email from Zafar Ali, this is an email from Calvin Ayre.</p> <p>A. I know what he was saying and I know what Zafar Ali said in front of Calvin Ayre when I was there.</p> <p>Q. Bottom of the email: "This is not how this would play out in the media if we spend toe to toe with COPA and they still win which is what is most likely ... in addition to the massive waste of my kids wealth." Are you really saying that Mr Ayre has not been providing financial support, directly or through nChain?</p> <p>A. No. I've sold shares and done other such things, which I have done with Mr Ayre, but that's a different issue. Selling shares isn't funding my litigation. And if you look at the next page {L19/212/8}, I don't believe that --</p> <p>Q. Look at the next page: "Its clear that once you lose you will need me more than ever. I will be the only one standing between your family and the soup kitchen." Yes?</p> <p>A. No, the bottom. Although that's wrong as well: "By the way ... you lost both contempt of court cases. Christen was the one that saved you and you are acting ..." That's just wrong. So I don't know where this particular email came from, but it doesn't look like the one -- any of the ones I've got.</p>	<p>Dr Wright is not accepting the obvious truth of the words in Mr Ayre's email. Despite stating he does not recall receiving this email, Dr Wright refers counsel to the next page of this email, therefore indicating that he has read it.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
Dr Craig Wright Making a Speech		
<p>{Day8/102:20} - {Day8/104:15}</p>	<p>Q. And then you say in your answer that {L17/285/45}: "... at least three, four hundred people knew that I was Satoshi in Australia ." That's an answer you gave, isn't it?</p> <p>A. It is.</p> <p>Q. Next --</p> <p>A. My Lord, can I just have an indulgence for a second? There's a false premise in both sides of this case that I need to just make totally clear. My premise isn't that I want to prove that I'm Satoshi, it is that I am Satoshi. Everyone keeps going on that I wanted this. I didn't. I still don't. The premise is that I wanted to come out and be Satoshi, or that I need to be. I have never wanted and I still don't want to. What I don't want, my Lord, is my invention, my life's work misrepresented. So everyone keeps going on about how I didn't say something, or I said it to these people, etc. The whole point was, I wasn't trying to ever come out as Satoshi, I didn't ever want to be Satoshi, as in own all of this; I want to be left alone to invent. All I want now is to be left alone to invent. This week I've written three patents, in lunchtimes and things like that. I'm not kidding on that one, I've sent them in. I've done this the whole time. I'm doing five doctorates. I'm doing mini degrees. I never wanted, in 2016, to be out. I don't want to be out now. I don't want anyone to know. I just can't help it, because I am. I will keep inventing, I will keep doing this, and no matter what the outcome of this case is, I'll hit 10,000 patents and then I'll keep going. My whole point is very simple: I never, ever want anyone to believe in me. I'm an ordained Wesleyan minister, a pastor, the only thing I believe that you should believe in is god, that's it. Everyone keeps wanting to believe in me, my Lord, I just want one simple thing: my invention not misrepresented. And that's what BTC are doing and that's why I'm here.</p> <p>Q. Dr Wright, you appreciate that that is disputed and that it's our position that you have been asserting your claim to be Satoshi. {O2/11/37}, please.</p> <p>A. No, I don't --</p> <p>Q. Dr Wright --</p> <p>A. I don't agree --</p> <p>MR JUSTICE MELLOR: Just wait for a question, Dr Wright. You've made your speech.</p>	<p>Dr Wright is interrupting counsel's questions to give a digressive speech, Mellor J requests Dr Wright to wait for a question.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
Dr Wright’s Witnesses & Documents		
{Day8/105:3-22}	<p>Q. Dr Wright, here we all are, after millions spent on your behalf, and there are just two witnesses who actually claim to have had the Bitcoin White Paper from you, or to have known specifically of your work on Bitcoin before its release: your backer, Mr Matthews, and a brief hearsay account from your elderly uncle; that’s right, isn’t it ?</p> <p>A. That is utterly false. Firstly, Mr Matthews is not my backer. While he is now the chairman of nChain, he does not, has not, has never provided funding to me. Next, I don’t get any money from him. He doesn’t pay for any of this litigation and he’s never been behind it. Now, where you’re then going into the rest, Ignatius Pang was involved in early parts of what I’ve invented. The other people, such as Rob, actually talk about the invention, including a Genesis file, etc. Now, while I didn’t call it Bitcoin back then, I talked about Timecoin and the concepts, because what you’re saying is this concept of anti-government money was never what I promoted.</p>	<p>Dr Wright is claiming various people were involved in “early parts” of his invention, but that he called it “Timecoin” back then. This is inconsistent with the witness statements of Stefan Matthews, Rob Jenkins and Ignatius Pang, none of whom refer to Timecoin (although note Rob Jenkins’ re-examination on Day 9).</p>
{Day8/106:3} - {Day8/107:5}	<p>Q. You’ve called none of the people from BDO, to whom you claim to have pitched Bitcoin in 2007, as witnesses in these proceedings, have you?</p> <p>A. Neville is actually old. The only reason he’s not here is health. Neville would have been. Unfortunately, his health is failing. My uncle’s health is now failing; his wife died last year and since then he’s had two strokes. So unfortunately, a lot of the people involved are getting older.</p> <p>Q. You’ve called none of those from Microsoft or Pornhub, to whom you supposedly pitched Bitcoin in 2008 and 2009, have you?</p> <p>A. I don’t have any of the records from Pornhub, but the people from Microsoft, I haven’t been able to reach out, I don’t know how to.</p> <p>Q. You’ve called none of the employees of your companies, who you claim in the chain of custody document had access to your White Paper drafts and precursor work, have you?</p> <p>A. None of the people want to be involved in this industry. Every single one of them have -- that I’ve spoken to have received either death threats or other hate mail. Anyone involved in actual Bitcoin, as I originally created, like the Bitcoin White Paper says, who puts their name out there, receives a lot of hate mail, emails, actual things in the post,</p>	<p>Dr Wright is confirming that he has not been able to obtain corroborative evidence regarding his early work on Bitcoin from other witnesses.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>threats, threats to their employer, etc. So there are campaigns, not just normal campaigns, funded ones.</p>	
<p>{Day8/107:6} - {Day8/110:2}</p>	<p>Q. Moving on from witnesses to documents. You've never produced a single email from or to Satoshi which was not already in the public domain and which has been verified, have you?</p> <p>A. No, actually, I've talked about lots of these. I don't have the originals. It is well known that Satoshi's GMX account was hacked around a decade ago. The Vistomail was closed and then bought, and then closed and then bought and then closed again. So, basically, all of that information has been taken over.</p> <p>Q. You've never identified a single correspondent of Satoshi or person who received Bitcoin from Satoshi whose name wasn't already in the public domain, although, like Mr Bohm, there clearly were some, right?</p> <p>A. As I've noted, I don't even remember my own supervisor names many times. So while I might be smart in some ways, I might be able to do maths, even write history, what I don't do is people.</p> <p>Q. You've never provided any reliable evidence of paying for or setting up the emails or websites linked to Satoshi, have you?</p> <p>A. No, actually, I have, and that has been put in with ATO documentation, etc.</p> <p>Q. None of the 21 people to whom you claim to have provided pre-issue copies of the White Paper has kept an email or a copy of the paper; that's right, isn't it?</p> <p>A. This many years later, I don't know. If they do, they would have to be asked, but they have seen each of those.</p> <p>Q. You have, over the last seven to eight days, raised doubts over the provenance, authenticity and reliability of most of your own chosen primary reliance documents, haven't you, Dr Wright?</p> <p>A. No, actually, that's not correct either. Ones, such as the written documents, that I have had that have been around for a long time have been ones that I'm not denying.</p> <p>Q. So handwritten manuscript documents?</p> <p>A. That date back the time, yes. On top of that, I've also had conversations etc with people such as Gavin.</p>	<p>Dr Wright is referring to Satoshi in the third person ("It is well known that Satoshi's GMX account was hacked...").</p> <p>Dr Wright is confirming that he has not produced any reliable documents such as emails from/to Satoshi that were not already in the public domain, and that he has not provided cryptographic proof.</p> <p>Dr Wright asserts he has a basis to be Satoshi, but refers to patents that date from many years after the Bitcoin White Paper.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Cryptographic proof. You've consistently failed to give any reliable proof of possession of private keys associated with Satoshi, haven't you?</p> <p>A. Again, there's no such thing, other than what is hearsay. Even the Hal Finney one is purely hearsay. The argument is, again, cryptographic proof. There is no such thing of cryptographic proof of identity. In the Bitcoin White Paper, the section notes that it is like where I worked, at Exchange, with a ticker tape.</p> <p>Q. Dr Wright, without genuinely supportive witnesses, reliable documents or cryptographic proof, there's just no basis for your claim to be Satoshi, is there?</p> <p>A. No, absolutely wrong. I have more patents developed than anyone in this industry going back even further; I have a workload that when, in 2016, the company was sold, shows 1,300 completed and 600 in progress papers, of that now 1,000 have been granted patents, 4,000 are pending. That in itself is evidence. The early people, like Gwern, trying to discover people and say identity and falsely say them, basically based it on one or two patents. Some of the first people outed were falsely, because they had three cryptographic patents. Mr Maxwell outed someone falsely because of one patent. Mr Back made suggestions based on a single patent. All of those people have denied it. On top of that, despite years of this, there is no Satoshi, no family, no anything who has ever come forth and nor will there ever be. But 20 years from now, there still won't be. If I don't win this case then what will happen is I will create more patents, we'll have another government sign up, we've already got four governments now signed up --</p>	
<p>Blaming Lawyers</p>		
<p>{Day8/110:15} - {Day8/111:9} {S1/1.13/20} Fifth Witness Statement of Dr Wright (Tulip Trading)</p>	<p>Q. {S1/1.13/20}. Paragraph 61, last four lines. Referring to the findings in that case: "My Norwegian legal counsel chose to disregard my instructions and pursued a legal strategy that diverged significantly from what I had desired and expected. This has been a source of frustration and disappointment for me ..." That's evidence you gave in the Tulip Trading case, isn't it?</p> <p>A. Yes. The one that I didn't recognise the name of at first, that first firm, refused to run the case that I wanted, thinking that they would do better. Only weeks away from the case, I had to replace and get a different firm in.</p>	<p>Dr Wright is blaming third parties, namely accusing Ontier of tampering with a document.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Dr Wright, you've also blamed Mr Justice Chamberlain's findings of dishonesty against you in the McCormack case on failures by your lawyers in that case, haven't you?</p> <p>A. Oh, Ontier actually put -- they changed the header on a document at one point, and we had a witness that would testify and they didn't --</p>	
<p>{Day8/112:2} - {Day8/114:1}</p>	<p>Dr Wright, bearing in mind the reaction you have made to other cases, which was not to accept findings but to blame your lawyers, let me ask you a few questions looking to the future. If the court in this case decides that you are not Satoshi, you will still maintain that you are, won't you?</p> <p>A. Well, I am. If you're asking will I lie, no.</p> <p>Q. If this court decides that you are not Satoshi, you'll still want to make claims, here and around the world, based on Satoshi's supposed IP rights, won't you?</p> <p>A. Again, I don't actually need to be Satoshi to have those rights. A Champagne case, which my lawyers wanted to run, would not require anything other than a change to the protocol. So --</p> <p>Q. But the claims you are currently making are based explicitly upon Satoshi's IP rights and contingent on you being Satoshi?</p> <p>A. Only because if I ran a Champagne case, the first thing your side would ask is, "You're Satoshi", and you would have me do this.</p> <p>Q. So the question again, if this court decides you are not Satoshi, you would still want to make claims, here and around the world, based upon you being Satoshi and having IP rights as such, wouldn't you?</p> <p>A. No, I'd move to patents. Taproot is based on three nChain patents, which is integrated into the core of BTC. We would actually pull the plug on that, and we have already investigated, and we would have the European courts start patent action on that. We would then --</p> <p>Q. And Dr Wright --</p> <p>A. -- go -- we would then start patent action in the US and, if I had to, I'll basically force them to shut down. We will go to vendors, such as AWS, who we're partnered with, and we will notify of the patent violations and it will be a patent case. So if I lose this, there are approximately 80 patent cases already waiting.</p> <p>Q. If this court decides that you're not Satoshi, you will still want to threaten those who dispute that claim, the claim to be Satoshi, with legal action, won't you?</p>	<p>Dr Wright admits that he will maintain that he is Satoshi even if this Court decides that he is not.</p> <p>Dr Wright is admitting that if he loses this case, he will start patent actions and "force them to shut down".</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. No, it's not that I'm Satoshi that I care about. I don't give a rats whether you believe I'm Satoshi. I don't care. I would prefer if you ignored the fact. I didn't want it out there. I would love everyone just to ignore the fact and just leave me alone and let me invent. So what I would say is, as long as they stop and they leave me alone, I will leave them alone.</p>	
<p>{Day8/114:2} - {Day8/115:5}</p>	<p>Q. Dr Wright, let me conclude, please, by putting COPA's case to you. You are not the author of the Bitcoin White Paper or the Bitcoin source code or the person who invented and released the Bitcoin System, are you?</p> <p>A. I am the person who invented Bitcoin, who invented the hash chain system, who invented a timestamp server, as section 3 of my paper --</p> <p>Q. The claim --</p> <p>A. ... notes. I am the person who created over 1,000 granted patents on that technology --</p> <p>Q. Your claim --</p> <p>A. -- 4,000 pending patents.</p> <p>Q. Your claim to be Satoshi Nakamoto is a lie and a hoax, isn't it, Dr Wright?</p> <p>A. No, actually, the opposite. We have spent and we are spending millions of pounds per month testing the scaling that I said would work in the first place, despite --</p> <p>Q. Dr Wright --</p> <p>A. -- the fact that I could sit back, like your clients, and pump money and con people out of theirs.</p> <p>Q. Dr Wright, it's a lie which you have supported with the forged documents we've identified in the schedules of forgeries that are known to you, isn't it?</p> <p>A. No, it is not.</p> <p>Q. And it's a lie you have sustained with a series of other lies over the last eight days, isn't it?</p> <p>A. It is not.</p>	<p>Dr Wright is again relying on his patents (which post-date the Bitcoin White Paper) as one of the main factors in his claim to be Satoshi.</p> <p>Dr Wright is making an unsupported allegation against COPA: “despite... the fact that I could sit back, like your clients, and pump money and con people out of theirs.”</p>
<p>CROSS - EXAMINATION OF DR WRIGHT BY ALEX GUNNING KC</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
Remedies Claimed		
<p>{Day8/115:25} - {Day8/117:21}</p>	<p>Q. So let me ask you this. Are you claiming any monetary remedies other than the recovery of legal costs in the BTC Core claim?</p> <p>A. Not directly. What I will do is, every single cent I get past my costs goes to Burnside and other charities. I'm categorically stating, under oath, I will accept no money, not a cent, from recovered BTC.</p> <p>Q. I just want to understand your answer. Are you saying that you are seeking monetary remedies against the defendants to the BTC Core claims or not?</p> <p>A. I will seek to cover any damages people have had from losses, not to me. I will not accept any money from BTC. I will accept money that goes to third parties.</p> <p>Q. Are you making any claim, on your own behalf or on behalf of your companies, for the payment of a monetary remedy in the BTC Core claim?</p> <p>A. Not to me. If you basically agree to follow British law, and I don't even care if you like me or not, if you agree to admit that you've changed Bitcoin from the White Paper, pay my original offer, I would be happy. Not to me. If you give that money to a charity that's part of my church, I'm signed off.</p> <p>MR JUSTICE MELLOR: Dr Wright, it's a simple question. Leave the question of costs aside. What you're being asked about is, are they going to have to write a cheque for any money at all other than costs? It doesn't matter who it's going to, are you going to insist on them writing a cheque for money as a result of the BTC Core claim, if you win it?</p> <p>A. My Lord, if they implement the required changes so that the British legislation as it is now is supported, I will forego any money. That would be the value I would accept. If the current legislation that has passed is implemented and supported by the developers, that one thing, I want no money.</p> <p>MR JUSTICE MELLOR: And where are these required changes set out?</p> <p>A. British legislation. There's cryptocurrency --</p> <p>MR JUSTICE MELLOR: Have you explained the required changes you need to the defendants in the BTC Core claim?</p> <p>A. They know what I want, but I would sit down with them and have these explained in full. I would very happily sit in a</p>	<p>Dr Wright is asked about whether he is claiming any monetary remedies (other than legal fees) in this claim, Dr Wright is evasive and refusing to answer the question asked. When pressed by Mellor J, Dr Wright confirms that if they “implement the required changes so that the British legislation as it is now is supported”, he will forego a monetary claim.</p> <p>Mellor J asking Dr Wright whether he has explained the required “changes” to the defendants, Dr Wright provides a vague and evasive response.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>room and go, you need to do X, Y and Z, no more money laundering, no building Taproot for enabling secret transactions, the facility -- micropayments can be anonymous, large payments, like million pound ones to Hamas, stop. If that -- if that's agreed, I'm good.</p>	
<p>{CSW/1/107} Eleventh Witness Statement of Dr Craig Wright</p>		
<p>{Day8/118:24} - {Day8/120:13}</p>	<p>Q. Can we move on then to {CSW/1/107}. This is paragraph 578 of your 11th witness statement, and we can see there that you say that: "Over time, the people developing Bitcoin systems adopted the term 'UTXO' ... to describe transaction outputs that have not been spent." Do you see that?</p> <p>A. I do.</p> <p>Q. And stopping there, that seems to accord with the agreement between Professor Meiklejohn and Mr Gao, that this occurred in 2012; is that fair?</p> <p>A. No, it's actually erroneous. It had been used. It was used going back to 2009, but like the term "block chain", it evolved.</p> <p>Q. That's not true. The expression had actually first been used in the developers' chat logs in June 2012, hadn't it?</p> <p>A. No, actually, that's incorrect. It had been used prior to that, in 2009, but it was less common. The development then became the common thing. The same as "block chain" morphed into blockchain.</p> <p>Q. That's not correct. It's first referred to by -- if we go to {D1/6/11}, we can the developers' chat logs and we can see at line 437, somebody called "etotheipi" says: "... I'm going to start using utxo to refer to unspent-txout." Do you see that?</p> <p>A. I do.</p> <p>Q. That's the first occasion in which somebody in relation to Bitcoin had suggested referring to unspent transaction outputs as UTXO; right?</p> <p>A. No, unspent transaction outputs, "utxout" had been done before. So, at times, it had also been done as "u-txout", etc, but, no, it had been. It wasn't --</p> <p>Q. That --</p> <p>A. That person's saying that they're going to do it, but it had been done earlier.</p>	<p>Dr Wright refusing to admit that both cryptocurrency experts agreed that the term UTXO was adopted from 2012, but is unable to provide any evidence supporting his contention for an earlier date (2009).</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Are you able to point to any evidence of any earlier use of the expression "UTXO" than that?</p> <p>A. Not while sitting here, no.</p>	
<p>{L4/97.1/21} main.cpp, 10 January 2009 issue of Bitcoin code file</p>		
<p>{Day8/121:19-24}</p>	<p>Now, CheckBlock had six checks, didn't it?</p> <p>A. At the particular time, I don't recall.</p> <p>Q. The issue of the Bitcoin Core software?</p> <p>A. There are multiple version and talking about my software from 15 years ago, I don't recall the exact structure without it in front of me.</p>	<p>Dr Wright is admitting that he cannot remember the details of what is claimed to be his own source code.</p>
<p>{Day8/123:6} - {Day8/125:18} {L4/97.1/22} main.cpp {L4/98.1/8} main.h</p>	<p>Q. And then, fourthly, we can see that it checked transactions?</p> <p>A. Yes.</p> <p>Q. What was that?</p> <p>A. That it checks transactions?</p> <p>Q. Yes, what was the check of the transactions?</p> <p>A. Basically making sure that they are valid, that the transactions that have been received follow the rules, etc.</p> <p>Q. So what sort of thing?</p> <p>A. What sort of thing. So, basically, Bitcoin uses script. The way that you'd have to then check would be does the key work, does other policies work, are the output and script valid. It's a predicate. So, what we're functionally doing in here is ensuring that all of the input and output is structured correctly, that if there's a message with an ECDSA key that the correct previous block had been signed.</p> <p>Q. So I remember you talking the other day -- I can't remember which day it was -- about how, when you were first running the Bitcoin software, it hadn't been -- the mining that had been absorbing all of your electricity, as it were, it was doing ECDSA checks in relation to the underlying transactions; is that right?</p> <p>A. And much more.</p> <p>Q. Okay, but when you're talking about ECDSA checking, is that what you're talking about in relation to --</p> <p>A. That particular part, yes.</p>	<p>Dr Wright incorrectly identifies ECDSA signatures as one of the transaction checks carried out by the CheckBlock function.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Okay. Can we go then to what check transactions actually is. It's at {L4/98.1/8}. And there were just three checks in check transactions. We can see it at the bottom. They were just: "Basic checks that don't depend on any context." Do you see that?</p> <p>A. It's a bit more than that. Each of these calls other areas. If you look at --</p> <p>Q. I'm going to go to them. If we can turn over the page {L4/98.1/9}, we can see the first one: "if (vin.empty ... vout.empty ... "return error ..." That was checking that there was at least one input and one output, right?</p> <p>A. Yes.</p> <p>Q. Secondly, it was checking that the amount spent wasn't negative, right?</p> <p>A. Correct.</p> <p>Q. And then, thirdly, it was checking that if there was a Coinbase transaction, the scriptSig was of a certain size between 2 and 100 bytes, right?</p> <p>A. Mm-hm.</p> <p>Q. And if it wasn't a Coinbase transaction, then the input had to be the output of another transaction, right?</p> <p>A. Yes.</p> <p>Q. It did not involve checking ECDSA signatures, did it?</p> <p>A. Again, that then calls these other functions.</p> <p>Q. Dr Wright, you're wrong about that?</p> <p>A. I am not wrong about that. If you note this, the diagram that you had is hierarchical. So, that particular function calls the next function, and when you're talking about checking CheckSig in that particular one, then that's ECDSA, but it's not in that core.</p>	
<p>{Day8/126:11} - {Day8/127:22}</p> <p>{L4/97.1/23}</p> <p>main.cpp</p>	<p>Q. Now, it is within AcceptBlock that the signatures are checked, isn't it?</p> <p>A. Basically what we have is a series of functions that each of these call other functions. So, where you're trying to say that each of these don't do all of that, the diagram that these guys don't like is a functional call mapping each of these areas down.</p> <p>Q. I'm not asking you about any diagrams, I'm asking you about what is in the CheckBlock function, and you told me that within the CheckBlock function were checks of ECDSA signatures.</p>	<p>Dr Wright is pressed on his incorrect assertion that the CheckBlock function contains an ECDSA signature check, and denies that is what he said.</p> <p>Mellor J requesting Dr Wright to identify where the calls are for</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. If it's a header and everything else is underneath it, then that is part of the entire function and you are checking everything. So when you have one function follow another to be correct, then all of those sub functions are part of the same function.</p> <p>Q. I'm afraid you're wrong, Dr Wright. If we want to explore how you get to signatures from the AcceptBlock function, I can take you there. Do you want me to do that?</p> <p>A. Like I said, the block includes both the full check and each of these. So when you have a transaction that you have checked, it then goes into the block and it's put into a binary tree structure. All of that is checked as part of the entire function. What you're doing is pulling out each individual call and saying that it's separate. It isn't.</p> <p>Q. We have looked at what the CheckBlock function contains and you have said it contains an ECDSA signature check. It doesn't, does it?</p> <p>A. That's not what I said.</p> <p>Q. Well, we can see what you said.</p> <p>A. What I said was, the function includes all of the processes in that. CheckBlock doesn't work unless each of the called functions are there.</p> <p>MR JUSTICE MELLOR: You're going to have to show us where you say these calls are in the code, Dr Wright.</p>	<p>the ECDSA signature check in the code.</p>
<p>{Day8/129:13} - {Day8/130:11}</p> <p>{L4/97.1/16} main.cpp</p>	<p>Q. And if we go to the top of {L4/97.1/16}, we can see that we get to the "VerifySignature" function; do you see that?</p> <p>A. I do.</p> <p>Q. So, the verification of signatures was part of the AcceptBlock function, not the CheckBlock function; do you agree?</p> <p>A. I have not looked at the original code since about 2017, and the way that I would look at it would be in UML, etc. So the diagrams that I had up earlier, that myself and earlier staff and later staff worked on, are those. Do I recall every single thing from when I released the code back then? No. But what I can tell you is, if you give me my diagram, I can take you through it. Do I remember all of the functions in my code off by heart? No, not any more.</p> <p>Q. I think Satoshi Nakamoto would remember if there was a check of all the signatures of all the transactions in the CheckBlock function, Dr Wright, but you don't remember that, do you?</p>	<p>Dr Wright is shown that the verification of signatures in transactions was part of the AcceptBlock function, not the CheckBlock function as he had previously identified. In response, Dr Wright is claiming that he cannot recall functions in the code as he has not looked at it since about 2017. Dr Wright also appears to be stating that his "environment" impacts coding output.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. After 15 years, no. What I can tell you is, if you give me my -- my environment and my code, I can walk you through it.</p> <p>Q. Nothing to do with your environment.</p>	
<p>{Day8/131:9-17} {L8/250/16} Headers - based synchronization and parallel block download</p>	<p>Q. And if we go to {L8/250/16} and go to the bottom of the page, at line 2348, we can see a number of entries with green lines in the margin; do you see that?</p> <p>A. I do.</p> <p>Q. And the lines in green are -- show that it's new or moved code, right? You're not familiar with GitHub?</p> <p>A. I don't use GitHub, I used SPV.</p> <p>Q. Bitcoin SV is actually on GitHub, isn't it?</p> <p>A. My team run on GitHub, yes. I don't. I still use SVN.</p>	<p>Dr Wright is admitting that he does not use GitHub, despite BSV being on GitHub.</p>
<p>{L3/237} Statistics studies.doc</p>		
<p>{Day8/134:14} - {Day8/135:8}</p>	<p>Q. Then if we go to {L3/237/13}, do you see, at the bottom, it says this: "Each node verifies a block before it propagates it to the connected peer nodes. In this way only valid blocks are propagated, and any invalid blocks are quickly isolated. The Bitcoin Core client lists all of the validation requirements in the following functions." We've just established that the terminology of "Bitcoin Core client" didn't exist in 2008, right?</p> <p>A. No. You changed the operation of the core software. The term "Bitcoin Core" had been used multiple times. So the core software, the node software and the difference between client software, including SPV, with the patches released for that, were different things. So Bitcoin Core used the term. That wasn't the first time that was used. You adopted that name.</p> <p>Q. Nobody referred to the "Bitcoin Core client", as you do here, in 2008, did they?</p> <p>A. No, this is talking about the main versus SPV. So that was different to what you're talking about there.</p>	<p>Dr Wright is denying that the term "Bitcoin Core client" is anachronistic.</p>
<p>{Day8/135:22} - {Day8/136:24}</p>	<p>Q. There's no reference in the White Paper to CheckBlockHeader, is there?</p> <p>A. It has reference to SPV, which only checks Block Header. There is no reference to any of the coding terms in the Bitcoin White Paper.</p>	<p>Dr Wright is refusing to admit that the term "CheckBlockHeader" is anachronistic.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. When you say SPV checks -- "only checks Block Header", what do you mean by "SPV" there?</p> <p>A. Simplified Payment Verification.</p> <p>Q. Right.</p> <p>A. What that basically means is, like --</p> <p>Q. To assist in the payment of individual transactions?</p> <p>A. No, it's a -- basically what we're talking about is a light node. So a node where an individual doesn't need to download the entire blockchain. For instance, I can just have the block headers and then I can have a localised(?) path of where I'm checking an individual transaction. I can keep each of those.</p> <p>Q. Dr Wright, nobody referred to CheckBlockHeader until the change that I took you to, did they?</p> <p>A. No, that's wrong. That was actually part of building SPV systems, that was basically the function I was looking at at that time.</p> <p>Q. There isn't a single document in which anybody refers to CheckBlockHeader as a single function until Dr Weller introduced it through GitHub, right?</p> <p>A. I've no idea when he put it in that, but when I was discussing the introduction of SPV, these concepts were back there as well.</p>	
{Day8/137:3-6}	<p>Q. Dr Wright, we've got the patches that Satoshi Nakamoto sent to Mr Andresen; they do not include CheckBlockHeader.</p> <p>A. No, because I went off to develop things myself.</p>	<p>Dr Wright is evasive in response when asked to confirm that the patches that Satoshi sent to Mr Andresen did not include "CheckBlockHeader".</p>
{Day8/137:11} - {Day8/138:11}	<p>Q. Dr Wright, I know you want to talk about all of your latest things. I'm actually trying to ask you about things that Satoshi Nakamoto would know about, and that is the original --</p> <p>A. No, you're --</p> <p>Q. -- Bitcoin code, right, and there was no reference in the original Bitcoin code to CheckBlockHeader, was there?</p> <p>A. Again, difference between core, as in main nodes, and those that are doing less, SPV, and there is a reference to SPV. SPV nodes are those that only have to check the headers across the network. If you read the section, you will see that.</p>	<p>Dr Wright is evasive when asked to confirm that there was no reference in the original Bitcoin code to "CheckBlockHeader".</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Dr Wright, I am very confident that I can read any section of anything and I will not see a single reference to CheckBlockHeader.</p> <p>A. Because the code's not referenced in the White Paper at all.</p> <p>Q. And you're saying that -- when did you say then you invented this? Was it in 2010, you said, when you were talking to Mr Andresen?</p> <p>A. No, I started working on SPV before I even released Bitcoin. So, what I was doing is a combination of Timecoin, which was a separate product, and Bitcoin. Bitcoin was the main free product; Timecoin extended everything.</p>	
<p>{Day8/138:12} - {Day8/139:16}</p>	<p>Q. So, the second anachronism in this document is the reference to CheckBlockHeader, I would suggest. And if we go over the page {L3/237/14}, you won't be surprised to learn that we also see a third anachronism, which is that you've referred to UTXO addresses; do you see that?</p> <p>A. I do.</p> <p>Q. And those did not exist as an idea in 2008, did they?</p> <p>A. They did.</p> <p>Q. Satoshi Nakamoto never used the expression "UTXO" in any of his dealings, did he?</p> <p>A. Yes, I did, because it's me. So, what you're suggesting is that all of my work -- and none of this was actually in my dealings either, as Satoshi I didn't talk about epidemic modelling, even though that's the case, I didn't talk about a lot of the uses of Bitcoin. I said that they were there, but I went off and built them. Just because I didn't give them for free doesn't mean that I didn't create them.</p> <p>Q. And if we go to the top of page 15 {L3/237/15}, we can see that this document refers to "the UTXO pool".</p> <p>A. Mm-hm.</p> <p>Q. That only came into existence after the Ultraprune request was updated, right?</p> <p>A. No, that's incorrect. Once again, the models that I'd been building include this. So, what you're assuming is that code and ideas that I'd already got in iDaemon, and other such things, are the only place they exist. And what a UTXO pool is, in my system, is very different to yours.</p>	<p>Dr Wright is refusing to admit obvious truth that UTXO is an anachronism and that Satoshi never used this term, and is evasive and digressive in response. UTXO is discussed in Professor Meiklejohn's report at {G/2/16}.</p>
<p>{Day8/140:9-13}</p>	<p>Q. You've read -- and you chose to rely on it as a reliance document?</p> <p>A. I did.</p>	<p>Dr Wright is admitting that the document at {L3/237} is a reliance</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. And you didn't spot those three anachronisms?</p> <p>A. Again, they're not anachronisms.</p>	<p>document, refusing to admit the obvious truth that it contains three anachronisms (Bitcoin Core client, CheckBlockHeader, UTXO).</p>
<p>{PTR-F/39/1} - A Competing Transaction or Block Model.doc</p>		
<p>{Day8/140:20} - {Day8/141:22}</p>	<p>Q. If we then go to PTR-F, tab 39 {PTR-F/39/1}, we're going to come to another document, and this one's produced from the BDO image so it's meant to pre-date 2007, right -- the end of 2007? But again, it refers to the UTXO addresses and the UTXO pool, doesn't it?</p> <p>A. Yes, and as I said, I don't publish everything I write.</p> <p>Q. Dr Wright, this is very compelling evidence that you interfered with the content of the BDO Drive to incorporate documents that cannot have come from 2007, isn't it?</p> <p>A. It is not. Again, you're using a common sort of shortened form of a word and saying that because there's not a lot of evidence, that most of the logs aren't there, that that must be it. And this is the whole point, there are a few logs and 99% of everything sent at that time is gone --</p> <p>Q. My learned friend Mr --</p> <p>A. -- despite the fact that your clients run it, none of the private messages on any of the forums are available.</p> <p>Q. Do you think other people were familiar with the term "UTXO" before we saw etotheipi mention it?</p> <p>A. People working in companies I've been with, yes.</p> <p>Q. Do you think people who were involved in Bitcoin were aware of it?</p> <p>A. I didn't really talk that much to people in Bitcoin. If you look at the number of communications I had, even with those I had a lot of communications with, such as Gavin, it's very limited.</p>	<p>Dr Wright is refusing to admit obvious truth that UTXO is an anachronism to 2007, providing vague and evasive responses.</p>
<p>{Day8/142:11-24}</p>	<p>Q. You wrote this content, didn't you?</p> <p>A. Of course I wrote this content. This content was created by me, but not like you're saying. It was created by me in -- like, over 15 years ago.</p>	<p>Dr Wright is evasive regarding the anachronism in this document, referring to his patents.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Dr Wright, you forged these documents, didn't you?</p> <p>A. I did not. Again, what you're saying is that other terminology which I've used in multiple other things must have been shared with people. I create -- I've got several thousand documents, as in ones that are patented, and I have not discussed any of those terminologies outside of corporations where people have NDAs.</p> <p>Q. So nobody else could have forged these documents?</p> <p>A. They're not forged.</p>	
<p>{CSW/1/102} First Witness Statement of Dr Wright</p>		
<p>{Day8/143:19} - {Day8/145:1}</p> <p>{L9/247.1/1} bitcoin/src/script/s cript.h~L18 (Github)</p> <p>{L1/199/1}</p> <p>C++ for Dummies 5th Ed.</p>	<p>Q. It refers to a GitHub page; do you see that?</p> <p>A. I do.</p> <p>Q. And we can find that at {L9/247.1/1}. So that's the GitHub reference that you have given and it's taken us to the script.h file on GitHub; do you see that?</p> <p>A. That is correct.</p> <p>Q. And so we can see, at row 18, that is declaring a constant integer variable called "MAX_SCRIPT_ELEMENT_SIZE"; do you see that?</p> <p>A. I do.</p> <p>Q. Just out of curiosity, do you know what unsigned means in that?</p> <p>A. I do. Basically it's unsigned variable, it's not an integer with --</p> <p>Q. With what?</p> <p>A. It's larger. I'm not sure how -- I mean, on the stand here, I'm not sure how I'd say it, but --</p> <p>Q. Take a wild guess.</p> <p>A. How I would describe it, I'm not quite sure. I know what it is.</p> <p>Q. Okay.</p> <p>A. I'm not terribly good when I'm trying to do things like this. Writing it down would be different.</p> <p>Q. Well, do you recall you mentioned that you had a book by Professor Stroustrup?</p> <p>A. I do.</p>	<p>Dr Wright is struggling to explain the meaning of unsigned integer, a basic concept in C++ coding.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. You haven't disclosed that book, but you have disclosed three other books about C++, so I want to take you to one of those. It's {L1/199/1}, and could we go to page 47 {L1/199/47}. Do you see that it explains that "unsigned" means that it cannot be negative?</p> <p>A. Yes, I do understand that. Would I have thought of saying it in such a simple way? No.</p>	
<p>{Day8/145:20} - {Day8/146:10} {D1/28/2} - Replace 520 constant with MAX - SCRIPT - ELEMENT - SIZE (Github)</p>	<p>Q. Actually, no, we were looking at the script header file, I think, so we should go to page 2 {D1/28/2}, and do you see under script .h, that's where it's added? Do you see that?</p> <p>A. I do.</p> <p>Q. That identifies that max_script_element_size equals 520, right?</p> <p>A. No, it says minus on that and plus on the other one.</p> <p>Q. Sorry?</p> <p>A. Are we looking at 673?</p> <p>Q. No, we're looking at line 20 under the script header file, script.h?</p> <p>A. Oh, the constant unsigned - it's an unsigned int -</p> <p>Q. It's identifying that the value of max_script_element_size is 520; do you see that?</p> <p>A. I do.</p>	<p>Dr Wright is appearing unable to read basic Git commit logs.</p>
<p>{Day8/146:20--24}</p>	<p>Q. So what was happening in the change to the script header file was that a constant was being named as -- a variable was being named as max_script_element_size, which had a value of 520 bytes, right?</p> <p>A. Well, it's a constant, it's not really a variable.</p>	<p>Dr Wright is quibbling over the meaning of a constant variable, indicating that either he is being overly pedantic, or he does not understand what a "variable"/"constant" means in C++.</p>
<p>{Day8/147:13} - {Day8/148:5}</p>	<p>Q. So the essence of this commit was the replacement of a hard-coded size limit of 520 bytes with the constant maxed max_script_element_size, right?</p> <p>A. That's changing it, yes.</p> <p>Q. Which was defined as 520, right?</p> <p>A. Yes.</p>	<p>Dr Wright continues to be questioned on {CSW/1/102}, para 545(f), refusing to admit that his statement was incorrect in stating that the document</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. So in script.cpp here, we can see here that it previously said if vchPushValue.size is greater than 520, return false, and now it's saying if vchPushValue.size is greater than max_script_element_size, return false, right?</p> <p>A. Okay.</p> <p>Q. So the document that you referred to in your witness statement wasn't evidence of BTC imposing a 520 byte limit, was it?</p> <p>A. No, it's still being imposed. It's there with the max script size in the constant.</p> <p>Q. The limit already existed, didn't it?</p> <p>A. Yes, but the limit was meant to be updated, just like block size.</p> <p>Q. The change that you refer to in your witness statement was just giving a name to that limit, right?</p> <p>A. No. The limit was meant to be updated. Just like the remove script and other such things.</p>	<p>referenced (L9/247.1/1) was not evidence of BTC imposing a 520 byte limit as the limit already existed.</p>
<p>{Day6/159} - Day 6 transcript</p>		
<p>{Day8/148:16} - {Day8/150:2}</p>	<p>MR GUNNING: -- which is this. Dr Wright, I noticed, on Day 6 at page 159 {Day6/159}, that you read out a definition of "transaction". Do you recall doing that?</p> <p>A. I do.</p> <p>Q. And I looked at the words that you'd used in that and I noticed that the language you used came from a couple of websites, and it's very important you do not -- is that where you got that definition from?</p> <p>A. No, it's not.</p> <p>Q. Where did you get it from?</p> <p>A. That's something I've been using for a long time.</p> <p>MR JUSTICE MELLOR: But you were reading it from your notebook, weren't you?</p> <p>A. Yes, I wrote it down in here, my Lord. But a transaction being an atomic process is something that is something I've been saying for a long, long time.</p> <p>MR GUNNING: Well, what you said was: "A sequence of multiple operations performed on databases and served as a single logical unit of work." Which I found on</p>	<p>Dr Wright is not accepting obvious truth that his definition of "transaction" came from a couple of websites, fauna.com/blog/database-transactions and techtarget.com.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>fauna.com/blog/database-transactions. Then I heard you say: "A transaction is a set of related tasks as a single action." Which I found on techtarget.com.</p> <p>A. I'm sure it's on many other places as well.</p> <p>Q. Right.</p> <p>A. Each of those are common terms. I mean, it's a common definition. So ...</p> <p>Q. It's very important you do not, in this break, start looking at your mobile phone, all right?</p> <p>A. I don't have my mobile phone at the moment.</p> <p>Q. Good.</p> <p>A. And I won't be getting it back until the end of the day. So like the other day, I'm not looking at it in these breaks.</p>	
<p>{Day8/150:23} – {Day8/152:20} {D1/4/6} Commit 4bd188c4383d6e6 1 4e18f79dc337fbab e8464c82 (made by Satoshi on 15 August 2010)</p>	<p>Q. And if we go down to {D1/4/6}, at row 89, do you see that what we were looking at before, which is the vchPushValue.size was reduced by Satoshi from 5,000 bytes to 520 bytes; do you see that?</p> <p>A. I do. At the time, there was an attack against the network and a vulnerability, and the script was temporarily disabled, there were other limits put on. All of that was meant to be temporary. At the time, I also said block size could be increased, etc.</p> <p>Q. It was Satoshi Nakamoto that limited the ability to use script by setting a maximum size of 520 bytes, wasn't it?</p> <p>A. Not in the way that you're suggesting. There was a communication between multiple people, including Gavin and myself, and it was decided as a temporary measure. The script and other things were done as a temporary measure.</p> <p>Q. Well, you say a temporary measure, but of course this is 16 August 2010, but Satoshi didn't leave the scene for a little while after that, did he?</p> <p>A. I was building other systems.</p> <p>Q. If we could go back, if we might, to {CSW/1/102}, at (f), do you see you put: "BTC ... limited the ability to use script by placing a maximum size and enforcing this rigorously."</p> <p>A. Yes, they enforced it rigorously. Some of the people in BTC are the ones who suggested this, going right back to 2010. I had noted also with block size that you could increase this just by a simple –</p> <p>Q. Do you want to wait for my question?</p>	<p>Dr Wright is refusing to admit that it was Satoshi who placed a maximum size on the use of script, not BTC.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. I thought that was your question.</p> <p>Q. No. The question is that it wasn't BTC that placed a maximum size on the use of script, was it, it was Satoshi Nakamoto?</p> <p>A. No, it was BTC who enforced it rigorously.</p> <p>Q. And you didn't know that because you're not Satoshi Nakamoto, are you?</p> <p>A. Of course I knew that. I've got many debates where I've talked about this. I've said in public forums that while I implemented the 1MB limit, the idea was that it would be removed. I've said that the script – I've been on many, many sort of stages and things like that stating this , so you're misrepresenting what I've said, because I have stated publicly , multiple times, that this was implemented as a temporary fix because there was an attack on the network, and that attack on the network was one I discussed with Gavin and others at the time.</p>	
<p>{CSW/1/100} - Disabling OP codes</p>		
<p>{Day8/153:6-14}</p>	<p>Q. Again, are you saying that OP codes that are important to the functioning of the script have been disabled by BTC Core as you call them?</p> <p>A. The way that I'm answering this is, yes, because what I did was put a temporary block on them. They have been removed from the code all together and replaced. Some of the early scripts, where the functionality was there, have been completely replaced. This includes sort of actually changing and adding for SegWit, new ones.</p>	<p>Dr Wright is inconsistent in relation to the quality of his memory, now claiming to remember the details of the OP codes.</p>
<p>{Day8/154:7-14}</p>	<p>Q. Well, we can see the background to it if we go to -- and I know, because it was apparent the other day, that you've read Mr Andresen's emails over the weekend, right?</p> <p>A. No, I have not. I haven't been home.</p> <p>Q. If we go to L6 --</p> <p>A. Actually, I was home for the weekend, but I haven't read his emails over the weekend.</p>	<p>Dr Wright is changing his story on an aspect that he should easily remember (whether he was home for the weekend or not).</p>
<p>{Day8/157:10-25}</p>	<p>Q. And ... So a couple of things in relation, if we go back to your witness statement at {CSW1/100/1}, bottom of the page. You referred there to many OP codes that were important and the functioning of the scripts having been disabled, but you</p>	<p>Dr Wright is evasive when asked to confirm that he did not mention in his witness statement</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>didn't mention that they were disabled by Satoshi Nakamoto, did you?</p> <p>A. No, what I'm referring to is the fact that I pulled them temporarily, and in August/September, I discussed, not only with Gavin, but other people, the fact that a security code check needed to be done. So, to enable these again, we needed to have the code verified. So, it's not that the code for, like, LSHIFT was necessarily a problem, it's my implementation was a problem, and if it was written better so that checks would be made, that would be okay.</p>	<p>that OP codes had been disabled by Satoshi.</p>
<p>{Day8/158:18} - {Day8/161:1}</p>	<p>Q. Well, we can look at this section of your witness statement again if you like, but the gist of this witness statement was that the dastardly people that you regard as being at BTC Core had disabled all these OP codes, right?</p> <p>A. There is a distinction, and a very big one, between putting a temporary block in there, a few lines saying that if you see that for the moment, disable them, and actually rewriting the codes that they no longer exist, which is what's happened now. You're nodding and going, "Oh no", but the actual thing is, now there's no code. And in fact some of those areas have been overwritten with new OP codes that do completely different things.</p> <p>Q. Well, we can see, in relation to OP_2MUL, you take that as another example of an OP code that's been disabled, right?</p> <p>A. I do.</p> <p>Q. And you set out a series of reasons why you say that wasn't necessary, right?</p> <p>A. I agree.</p> <p>Q. And I think, in your evidence on Thursday last week, you said that it was very easy to turn it back on, right?</p> <p>A. It should be, yes.</p> <p>Q. Well, it's disabled in BSV, isn't it?</p> <p>A. It's not meant to be.</p> <p>Q. What do you mean "it's not meant to be"?</p> <p>A. It's in the thing that it should have been turned on already, so I will be rather upset if it's not, I haven't checked.</p> <p>Q. Right, well, if we go back to {S1/1.18/85}, we can see, at the bottom, that it says for "BSV Script OPCodes", "OP_2MUL DISABLED"; do you see that?</p>	<p>Dr Wright is claiming it is possible to put a "temporary block" on OP codes. When presented with the fact that the OP_2MUL code is disabled in BSV (even though he has stated this is not necessary in his eleventh witness statement), he appears surprised and states that it is "not meant to be".</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. That's something that needs to be fixed. It should be -- if it has -- if that's true, then I'll need to make sure that someone fixes that asap.</p> <p>Q. Well, it certainly seemed to be disabled to us when we looked this morning. Were you aware of that?</p> <p>A. I haven't looked this morning, no. But like I said, I'll be definitely checking and talking to people.</p> <p>Q. But this is -- if we go back to page 100 of your witness statement {CSW/1/100}, this is a classic example of you showing that you're not Satoshi Nakamoto because the disabling of OP_2MUL was undertaken by Satoshi Nakamoto, right?</p> <p>A. Yes, I implemented the code and I do know that. I have stated on stage saying that, yes, I implemented it.</p> <p>Q. Okay, so if we go to page {CSW/1/101}, you have this whole explanation as to why it may or may not have been done, but Satoshi Nakamoto would know why it had been done.</p> <p>A. I do know why it's been done. Like I just said, I told you about the overflow for left shift and people were actually complaining about this as well. Most of the things have been turned on one by one in BSV, as we checked the code, so we've been rigorous in that, because some of the people in your team like to ensure that we are by checking for bugs, and most of those have been turned on. That one I didn't realise had been missed.</p>	
<p>{G/6/50} - Fourth Expert Report of Mr Madden</p>		
<p>{Day8/163:3-14}</p>	<p>Q. And it has a key ID that we can see, which is CF1857E; do you see that?</p> <p>A. I do.</p> <p>Q. So there are two keys within this PGP key, right?</p> <p>A. I haven't worked on PGP for a long time, so I'll take your word for it.</p> <p>Q. Okay --</p> <p>A. I used to know it much better.</p> <p>Q. But there's a primary key and a sub key, right?</p> <p>A. Yes.</p> <p>Q. And that's not at all unusual, right?</p>	<p>Dr Wright does not appear to recall or understand Satoshi's public PGP keys.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	A. No.	
<p>{L2/202.1/27} - OpenPGP Message Format document {G/6/50} - Fourth Expert Report of Mr Madden</p>		
<p>{Day8/168:1} - {Day8/170:11}</p>	<p>Q. What it shows us is that Satoshi's PGP key, the primary key in his PGP key was designated as a signing key, right?</p> <p>A. No, it shows that it could be used as that. I noted that earlier. What I also said is you shouldn't be using the same keys.</p> <p>Q. It also identifies, doesn't it, that it couldn't be used -- the primary key could not be used as an encryption key, right?</p> <p>A. No, the algorithms are in there and it was used as an encryption key.</p> <p>Q. So --</p> <p>A. As you well know.</p> <p>Q. If we could go then, if you don't mind, we'd better go back to {G/6/50}. Do you see that the primary key -- do you see the algorithm number?</p> <p>A. I do.</p> <p>Q. So it says "algo 17"; do you see that?</p> <p>A. I do.</p> <p>Q. "Algo 17" is associated -- it means that it's a DSA algorithm, right?</p> <p>A. Correct.</p> <p>Q. So that is a signing key, isn't it?</p> <p>A. No, it's more for code signing. So if you do an encrypted packet, you would encrypt and sign.</p> <p>Q. We just agreed DSA is not for encryption, is it?</p> <p>A. Like I just said, you use the two keys. You encrypt and sign. So if you wanted to do an encrypted to someone else or validate or have something else, it's a process of encrypt and sign. So that's how you would use that.</p> <p>Q. Sorry, you're not right, Dr Wright. The primary key here is a signing key, the sub key, do you see the algorithm that's identified for that? It says "algo 16"?</p> <p>A. Yes.</p>	<p>Dr Wright is refusing to accept the obvious truth that the primary key in Satoshi's PGP key was designated as a signing key.</p> <p>Dr Wright is stating that he has not touched C++ since 2017, which is inconsistent with his first witness statement, paragraph 71 {E/1/15}, in which he states "... throughout my career, C++ has played a prominent role in various capacities. Although his current work primarily involves Python, because of its efficacy in higher level tasks, C++ continues to be an integral part of his coding knowledge and skills, underscoring its enduring relevance in his professional career."</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. That's an ElGamal algorithm, isn't it?</p> <p>A. I don't remember each of the names of these off the top of my head.</p> <p>Q. Which is -- which would make it an encryption key, wouldn't it?</p> <p>A. ElGamal, yes.</p> <p>Q. So there are two keys here, one of which is a signing key and one of which is an encryption key?</p> <p>A. That's correct.</p> <p>Q. And can we go then to {CSW/1/46}. We should have paragraph 243 of your witness statement. You said: "The PGP ... is not a signing key."</p> <p>A. It isn't a signing key, it was used for encryption. Data was encrypted both from Malmi and from Gavin Andresen.</p> <p>Q. Dr Wright, it was set up as a signing key. The primary key in the PGP key was set up as a signing key, wasn't it?</p> <p>A. No, it was constructed automatically and it was never set up as a signing key. Do I remember each of the numbers in PGP any more? No. It's just like I did a lot of work between 2005 and 2008 to get up to speed on C and C programming for when I did Bitcoin and I don't any more. I haven't touched C++ since 2017. I have staff now and they do. So, do I remember it all? No.</p>	
<p>{Day8/171:11} - {Day8/172:2}</p>	<p>Q. Come back to PGP, though. We've established that the primary key of this PGP key was a signing key, right?</p> <p>A. We've established that it's an automated system and that I didn't play around with a whole lot of settings. It was a key for encryption and that's what I used it for.</p> <p>Q. So had you signed with this PGP key, that would have been powerful evidence that you were Satoshi, wouldn't it?</p> <p>A. No.</p> <p>Q. You would have been able to sign with a key that was directly associated with him, wouldn't you?</p> <p>A. No. Once again, the server has been owned and re-owned from multiple people. A requirement for proving identity isn't that you hold a piece of data. If I was to have a key, I would have to have it in my possession and control the whole time.</p>	<p>Dr Wright is implausibly denying that signing with Satoshi's PGP key would have been powerful evidence that he was Satoshi.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{E/1/22} Dr Wright’s First Witness Statement		
{Day8/174:10} - {Day8/175:4}	<p>Q. -- that there were 69 computers. So that’s where you were spending the \$11,000, right?</p> <p>12 A. Something like that, yeah. I don’t have the exact amount. It was actually the -- there were -- the company paid for the three-phase power and I paid for the normal house power.</p> <p>Q. Okay. Because you haven’t actually disclosed any electricity bills, other than those that accompanied your 2008 and 2009 tax return, have you?</p> <p>A. I ’ve only got the personal ones. The records for Information Defense I don’t have any more.</p> <p>Q. Right. Why not?</p> <p>A. It’s been 15 years.</p> <p>Q. Right, well, why didn't you ask for them from the electricity providers earlier?</p> <p>A. They don't have them going back that far.</p> <p>Q. Did you ask?</p> <p>A. Yes.</p> <p>Q. Okay.</p> <p>A. At least my lawyers told me they did.</p>	Dr Wright is blaming third parties (his lawyers) for not requesting the electricity bill records for his computer systems.
{Day6/146} - Day 6 Transcript		
{Day8/176:2-18}	<p>Q. Could we go to {Day6/146:24} to {Day6/147:9}. You were accusing here Professor Meiklejohn of misrepresenting Bitcoin mining and nodes, and you said, because she was complaining about -- she was looking at the hash rate that would have been relevant in light of the target values that were applicable in the early days of Bitcoin, right? And you said: "The majority, at a low level like that, is actually validating ECDSA."</p> <p>A. I said one part.</p> <p>Q. You said "the majority".</p> <p>A. No, of Bitcoin. I also have noted, as I did in my witness statement, that I was running logging and collation systems and testing systems. So, one of the things that I was doing, as</p>	Dr Wright is refusing to accept obvious truth that he had stated that the “majority” of computer usage in the early days of Bitcoin would have been validating ECDSA.

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>well as Bitcoin, the way that you're talking about, I have been, since then, working at scaling solutions.</p>	
<p>{Day8/177:5} - {Day8/179:7}</p>	<p>A. There's no "yes" or "no", because there's a leading question here. My Bitcoin use included all of the test systems I was doing. So, if you're saying my Bitcoin use on the public network, then, no. My Bitcoin use on the public network included all of the test systems, all of the logging systems, etc.</p> <p>Q. Okay. Because how many transactions would have been being verified, per block, in the first year of Bitcoin?</p> <p>A. It varied, but not a lot.</p> <p>Q. Well, out the first 32,489 blocks which were created up to the end of 2009, there were just 219 transactions, weren't there?</p> <p>A. I haven't counted, but not many, no. Very few.</p> <p>Q. But, typically, there were zero transactions per block, weren't there?</p> <p>A. Yes. As I noted, there was a dead period in 2009.</p> <p>Q. Maybe one transaction per block, occasionally -- very occasionally two or three, and on only one occasion five, right?</p> <p>A. I'm actually surprised with five, but I haven't noticed that one.</p> <p>Q. So the majority of computer usage cannot have been validating ECDSA, Dr Wright.</p> <p>A. Like I said, I was doing testing as well. So, you're saying the public network was it.</p> <p>Q. Well, shall we read the rest of what you said? You said: "The majority, at a low level like that, is actually validating ECDSA. ECDSA is far more computationally intense process than hashing. So what we need to do is actually go through validation of blocks, checking, later running testnet as well, and ensuring that all that process happens before you distribute the block." Right?</p> <p>A. "On top of that, I had to run multiple systems", to quote myself. And then I said all of that "allowed me to have multiple systems, including the logging system~...", etc. Those logging systems were running that.</p> <p>Q. You were presenting to the court that the majority of your usage of your systems for Bitcoin was validating ECDSA, right?</p>	<p>Dr Wright is refusing to accept obvious truth that the "majority" of computer usage in the early days of Bitcoin could not have been validating ECDSA, provides evasive answer by reference to his patents.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Yes, but not the way that you're saying. What I was saying is, I was embedding transactions in block headers and doing calculations based on that, at the time.</p> <p>Q. And that assertion, I would suggest, is demonstrably false by reference to the blockchain.</p> <p>A. No, actually, it's not. I have a number of patents on how to do this. So, some of those have been implemented and there are companies now running the software, such as Certihash. Certihash has integrated with IBM and they're running it on clients. So, that's based on technology I developed in 2008.</p>	
<p>{Day8/179:8} - {Day8/180:11}</p> <p>{E/8/4} - Witness Statement of Danielle DeMorgan</p> <p>{L5/70/79} - Electricity Bill at home in Lisarow</p>	<p>Q. Can we go, if you don't mind just to go backwards for a moment, to {E/8/4}. This is Dani DeMorgan's witness statement, paragraph 11. You said that she was talking about 2002; do you recall that? She's actually talking about 2008, isn't she?</p> <p>A. No, when she saw it in a bedroom, it was 2002. I had multiple homes in the Central Coast, by the way, I had one in the Hawkesbury, so she'd obviously mixed the two up.</p> <p>Q. You see, the trouble is, we do actually have your electricity bills from Lisarow, don't we?</p> <p>A. You would have the personal ones.</p> <p>Q. Right.</p> <p>A. You wouldn't have the three-phase.</p> <p>Q. And the cost per month was closer to 800 -- well, for three months was closer to \$800 than \$11,000, wasn't it?</p> <p>A. No, like I said, I had a separate account for Information Defense.</p> <p>Q. Well, we can --</p> <p>A. I had three-phase power put into that area.</p> <p>Q. We can go to {L5/70/79}. This is the electricity bill at Lisarow, right? It's in your former wife's name, right?</p> <p>A. That is the house one. That is very limited, just my office, etc. As I stated, there was three-phase that was on a separate switch.</p> <p>Q. And you have no record of the electricity bill for that?</p> <p>A. I have no records of any of the accounting for Information Defense at that time.</p>	<p>Dr Wright is evasive when asked about the electricity bills in his house in Lisarow at {L5/70/79}, claiming these are personal bills, and that he has no record of the bills for Information Defense (presumably the larger bills as stated in his first witness statement).</p>
<p>{L19/49/2} - Capture of https://satoshi.nakamotoinstitute.org/posts/bitcointalk/threads/259/</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day8/183:16} - {Day8/184:6}</p>	<p>Q. Satoshi said this: “It would have been nice to get this attention in any other context. WikiLeaks has kicked the hornet’s nest and the swarm is headed towards us.” Right?</p> <p>A. Yes.</p> <p>Q. And it indicates that Satoshi did not want the negative attention that might come from being associated with WikiLeaks, right?</p> <p>A. I wanted a whole lot of other things first. As I said, it's money and it's legal, so whether I necessarily like something that is legal is irrelevant, but I didn't want it to be seen as a WikiLeaks thing.</p>	<p>Dr Wright is asked about Satoshi’s response about being associated with Wikileaks, he appears unable to answer the question.</p>
<p>{L7/391/1} - The Conversation Article by Craig S Wright LulzSec, Anonymous - freedom fighters or the new face of evil</p>		
<p>{Day8/184:15} - {Day8/185:10}</p>	<p>Q. Now, can we then turn to {L7/391/1}. This is an article that you, Craig S Wright, wrote on LulzSec and Anonymous, right?</p> <p>A. I wrote it, and it was published for me.</p> <p>Q. But you wrote it in August 2011, right?</p> <p>A. About then, yes.</p> <p>Q. So that’s less than a year after Satoshi’s “hornet’s nest” comment, right?</p> <p>A. Yes.</p> <p>Q. And you wrote it for an online publication called The Conversation?</p> <p>A. I did.</p> <p>Q. And it was the first article in which you, Craig S Wright, explicitly referred to Bitcoin, isn't it?</p> <p>A. No, it's not.</p> <p>Q. You say you have earlier writings, public writings, that relate to Bitcoin?</p> <p>A. Yes. Are they all available any more after 15 years? No.</p> <p>Q. Nobody’s pointed to one earlier, Dr Wright.</p>	<p>Dr Wright is admitting that he wrote the article at {L7/391/1}, denying that it was the first article in which he referred to Bitcoin, but stating that they are not “all available” after 15 years.</p>
<p>{Day8/186:16-23}</p>	<p>Q. Thirdly, you spelt "bit coins" as two words; right?</p> <p>A. No, autocorrect did that on me.</p> <p>Q. It never did it to Satoshi, did it?</p> <p>A. No, he never used that site.</p>	<p>Dr Wright refers to Satoshi in the third person: “he never used that site”.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Right, so you're saying it's the autocorrect on that site, are you?</p> <p>A. Autocorrect, on that site, does certain things, but it didn't on -- what do you call it -- the forum.</p>	
<p>{Day8/188:6} - {Day8/189:10}</p>	<p>And then you say this: "Bit Coin ..." This time capital "B", "Bit", capital "C", "Coin", then: "... ([capital B] Bit [capital C] Coin) is a digital currency. Bit Coin offers a full peer-to-peer currency solution." So, stopping there, you're still using two words to refer to Bitcoin, right?</p> <p>A. Still the same site. And, yes, I didn't check it that it had done that.</p> <p>Q. But now you're capitalising the first and second words?</p> <p>A. I'd done that multiple times as Satoshi as well. It's in the code as that.</p> <p>Q. Not as separate words, you have not.</p> <p>A. No, because I had the separate capital, that's why this site added the space.</p> <p>Q. I think that the only place that Satoshi ever used a capital "C" for "Coin" in "Bit Coin" was in the readme text that was issued with the code, right?</p> <p>A. No, also on some of the forums.</p> <p>Q. And he then removed it.</p> <p>A. No, I standardised after all that happened. So most of those changes that you're talking about I removed, I didn't do.</p> <p>Q. Dr Wright, the fact is that when you first emerged to talk about Bitcoin you were not familiar with it and you didn't even know how to spell it properly, right?</p> <p>A. That's totally incorrect, and I did. I already had a company extensively researching on that area.</p>	<p>Dr Wright's explanation for his inconsistent spelling of Bitcoin as two words is incoherent, and is inconsistent with his use of "FaceBook" as one word in the same post (see below).</p>
<p>{Day8/189:21-25}</p>	<p>Q. Well, if we just stick with this. PayPal, there's no space between "Pay" and "Pal". "Facebook", you've put it, I think, once with a capital "B" for the second word; it's always one word, right?</p> <p>A. Neither of those correct.</p>	<p>Dr Wright is not accepting obvious truth of the inconsistency in his spelling of Bitcoin.</p>
<p>QUESTIONS FROM MELLOR J FOR DR WRIGHT</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day8/190:13} - {Day8/191:8}</p>	<p>MR JUSTICE MELLOR: Could we bring up the transcript for Day 3 at page 161 {Day3/161}. Do you see, at line 15, you said you set the time in LaTeX, yes?</p> <p>A. Yes, my Lord.</p> <p>MR JUSTICE MELLOR: And that's in the context of questions about the creation date timestamp in LaTeX files.</p> <p>A. Yes.</p> <p>MR JUSTICE MELLOR: Do you have to set the time in LaTeX, or is there a default?</p> <p>A. You don't have to, and it depends on the system. So, generally, when you're doing metadata in the hypertext area, you could choose to or not. I generally do. Or you could put something like a date, and in the date it will automatically pull it up every time you do it. So if I'm doing something like assignments for uni, I just do the date reference and then the last one is it, and then I generally set it after I've done-... So as I'm doing drafts, I have it autose, and then when I have the final, I set it. And I keep it that way because, then, if I'm asked by the uni again, I have the same document.</p>	<p>Mellor J is asking about whether you have to set the time in LaTeX, or if there is a default. Dr Wright's response is incoherent.</p>
<p>{L5/16/1} – bitcoin</p>		
<p>{Day8/191:9} – {Day8/192:15}</p>	<p>MR JUSTICE MELLOR: Okay. Next can we go to {L5/16/1}. Now, this is document ID_000538.</p> <p>A. Yes.</p> <p>MR JUSTICE MELLOR: And you were asked some questions about this on Day 3.</p> <p>A. Yes.</p> <p>MR JUSTICE MELLOR: And in relation to this one, in your fourth witness statement you indicated that this document was made available to various staff and consultants.</p> <p>A. Yes. It was also loaded on SSRN. Nchain staff run SSRN and some of the other things for me, and I'd requested that one of the versions was loaded and it had to be reloaded for some reason, I'm not quite sure why.</p> <p>MR JUSTICE MELLOR: Now, there are certain formatting differences between this and the – what's been called the control copy of the Bitcoin White Paper. But apart from those, the only difference in the content, is instead of saying "Satoshi Nakamoto" at the top it says "Dr Craig S Wright".</p>	<p>Mellor J is querying with Dr Wright why his employees at nChain would access {L5/16/1} rather than the real Bitcoin White Paper.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. It does.</p> <p>MR JUSTICE MELLOR: Why would any of your employees or consultants access this document when they've got the real thing, the published document?</p> <p>A. They had not only this, but a lot of documents.</p> <p>MR JUSTICE MELLOR: Yes, why would they access this rather than the real thing?</p> <p>A. I had asked people to put the document up on SSRN. So. SSRN has a policy of no pseudonyms, so my only thing to think of is finding one to put up and load on SSRN. I'm not actually sure. I didn't ask anyone why, my Lord.</p>	
<p>{Day8/192:16} – {Day8/194:22}</p>	<p>MR JUSTICE MELLOR: Okay. The next point concerns the various trusts you set up.</p> <p>A. Yes.</p> <p>MR JUSTICE MELLOR: Because as I understand it, the purpose of these trusts was to keep your assets, and particularly the IP, as you stressed, but also the Bitcoin, away from your creditors, yes?</p> <p>A. Primarily the intellectual property.</p> <p>MR JUSTICE MELLOR: Yes. You wanted to keep it away from any bankruptcy or insolvency proceedings?</p> <p>A. Yes, my Lord.</p> <p>MR JUSTICE MELLOR: Yes. And as I understand it, you made it clear that the trusts meant you couldn't access any of the Bitcoin.</p> <p>A. That's correct.</p> <p>MR JUSTICE MELLOR: And did that also apply to the IP?</p> <p>A. I couldn't -- it's in my head, and most of my things I could probably recreate with a bit of time, but I don't -- from my understanding of the law, I don't think anyone can force me to create something if I can't get it. So my understanding is, if I was bankrupted, they can't force me to provide work that they can't access.</p> <p>MR JUSTICE MELLOR: Okay, but the IP that you're talking about, you stressed it was ideas, all those papers you'd written –</p> <p>A. Yes.</p> <p>MR JUSTICE MELLOR: -- right? So, you mentioned database rights, obviously copyright, quite a big body of confidential information –</p>	<p>Mellor J is questioning Dr Wright about his trust structure.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>sA. Yes.</p> <p>MR JUSTICE MELLOR: -- right? Now, was that body of IP put beyond the reach of your creditors or not, in the trusts?</p> <p>A. I think so. I was never properly challenged. I went bar the GAAR Panel in Australia, which is the General Anti-Avoidance and, like, Review Panel for tax, and that was brought up. The issue was, because I wasn't bankrupted – if I was bankrupted, they said that doing that would be illegal, because I was doing it to avoid bankruptcy. But because I wasn't bankrupted, they said: there's a technicality and we can't charge you for something you intended to do that didn't happen.</p> <p>MR JUSTICE MELLOR: But as I understand it, the IP was subject to the same trusts as the Bitcoin.</p> <p>A. The locking of information was “The Trust”, which is locked away. There is a lot of information I can't access. Then, the ownership was supposed to structure things so that the company owns these rights. One of the issues I had would be, if the Australian – like, the Tax Office technically owned database rights or anything like that, or could show it, I saw that as a major problem, so I tried to hide that away. If the Tax Office took over that, they could shut down my project, and I think some of them would have.</p>	
<p>{Day8/194:23} - {Day8/196:5}</p>	<p>MR JUSTICE MELLOR: You see, it seems to me there's a contradiction. The IP was the subject of these trusts, and yet you and your employees continued to work on all the information, file patents, etc.</p> <p>A. No, that happened afterwards, my Lord.</p> <p>MR JUSTICE MELLOR: What, after 2020?</p> <p>A. No, before that. I started redeveloping in 2013. So, in 2013, when I won in the tribunal, I had a settlement with Mr McArdle, so both of those issues went away. So I paid Mr McArdle for a settlement, that ended that bankruptcy, and because I won in the tribunal, in March 2013 that was handed down, and then I thought I could do something to get around all of this, but a few weeks later, Dave died. So then I started building most of it from scratch. I knew the ideas in my head, but I couldn't access my notes.</p> <p>MR JUSTICE MELLOR: So the trusts continued after March 2013?</p> <p>A. Yes. They're still continuing now.</p>	<p>Mellor J questioning Dr Wright about his trust structure, particularly why he and his employees continued to work on the IP that was the subject of these trusts.</p> <p>Dr Wright stating, implausibly, that he did not think a draft of the Bitcoin White Paper was valuable.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>MR JUSTICE MELLOR: So why was, for example, this draft of the Bitcoin White Paper, why was that accessible to your staff at all?</p> <p>A. I had some files. These weren't put in or locked away. So, there was information that I didn't think was as valuable. All my data, for instance, that I locked away, I still haven't got access to. Some of that we've recreated, but there are a lot of other files that I did have access to -</p> <p>MR JUSTICE MELLOR: So you didn't think --</p> <p>A. -- I just I didn't think they were valuable in that way.</p> <p>MR JUSTICE MELLOR: You didn't think a draft of the Bitcoin White Paper was valuable?</p> <p>A. No, I actually didn't, my Lord.</p>	
<p>{L3/237/13} - Statistics studies.doc</p>		
<p>{Day8/196:6} - {Day8/198:6}</p>	<p>MR JUSTICE MELLOR: Okay, thank you very much. Oh, one final question. Can we go back to {L3/237/1}, please, page 14 {L3/237/14}. Sorry, wrong reference. (Pause) Okay, the question is about the function CheckBlockHeader.</p> <p>A. Yes.</p> <p>MR JUSTICE MELLOR: Yes? So if I look at the original Bitcoin source code, on your evidence, I will find a function named CheckBlockHeader, will I?</p> <p>A. No, you won't.</p> <p>MR JUSTICE MELLOR: Why not?</p> <p>A. Because the SPV function hadn't been built. So, I talked about this in 2010 and I noted that it needed to be built, and that's the headless client. Now, the early version was just a mishmash of everything. The IP-to-IP functionality, which had a few problems and ended up being turned off, and the full node software and every -- and client software were all in one mashed-up UI that did everything. What I needed to do was build a standalone client that would allow users to transmit instantly, securely. So, by "IP-to-IP," my Lord, what I mean is IP address, your machine, sending to another machine. To make that work, not just to an IP that non-geeks don't use, I needed to build in some sort of secure DNS, a naming system, probably some sort of system like PKI, so that we could have a public key infrastructure, so that your name is against an IP address, something like WhatsApp has for finding names and addresses, and none of that was done. So, the Block Header</p>	<p>Mellor J is querying why the reference to CheckBlockHeader is in present tense, not future tense.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>function would then take only the block headers. It's explained in the White Paper. Not built, but it's explained. It's like the alert keys in the White -- mentioned in the White Paper that you can alert nodes, but I hadn't done it yet. So at this point I was, sort of, working on if you're doing block propagation or block header propagation.</p> <p>MR JUSTICE MELLOR: Somebody's very kindly found me the right reference, which is the previous page, of course {L3/237/13}. On page 13, on screen, counsel was asking you some questions about that sentence: "The BitCoin Core client lists all of the validation requirements in the following functions."</p> <p>A. Yes.</p> <p>MR JUSTICE MELLOR: "CheckBlockHeader". It's in the present tense, not in the future.</p> <p>A. I write a lot of things in weird ways. I know that sound strange, but I could show you some of my existing academic things where I mix tense all the time.</p>	

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
DAY 9		
CROSS - EXAMINATION OF DR IGNATIUS PANG BY JONATHAN HOUGH KC		
{Day9/7:5-20}	<p>Before I get into your evidence, may I just ask you this. Have you watched any of Dr Wright's evidence over the last week and a half? No criticism if you have.</p> <p>A. I have not watched the evidence, but I was very curious, so I have mainly watched, you know, recall on YouTube, like people talked about what they've seen, and someone from Gavin Mehl - M - E - H - L - in particular, and there that might be another person linked to CoinGeek, but I only saw, you know, one media of that, but mainly Gavin Mehl.</p> <p>Q. So you've been watching reports by Mr Gavin Mehl and other material -</p> <p>A. Yeah.</p> <p>Q. - through CoinGeek website, yes?</p> <p>A. CoinGeek website, yes, and, you know, some information from Forbes.com, bits and pieces.</p>	<p>Dr Pang is confirming that he watched videos about this trial from Gavin Mehl through the Coingeek website (the editorial line of which consistently supports BSV and Dr Wright).</p>
<p>First Witness Statement of Dr Ignatius Pang {E/10/4}</p> <p>Discussion with Dr Wright re Lego set</p>		
{Day9/25:3-21}	<p>Q. Now, at the end of paragraph 9, you say this about the discussion: “These facts were refreshed in my memory over time over several of the video conferences with the lawyers at Ontier LLP between 2021-2023.” Now, that’s a comment you make in respect of - in relation to this part of the statement, but not in relation to other parts of the statement; is that right?</p> <p>A. Yes, that is particularly for this part of the statement.</p> <p>Q. Is that because this part of the statement was particularly informed by the conversations that you had over that period with the lawyers?</p> <p>A. It was particularly informed in that I have very deep reflections about my interaction with Craig and those questions act as memory prompts for me to recall these interactions, which subsequently led me to try and hunt down that, you know, photos I've taken on that day or, you know, that receipt that I had on that day.</p>	<p>Dr Pang discusses his process of recollecting his conversation with Dr Wright regarding the Batman Lego set.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{Day9/26:9-13}	<p>Q. We'll come to that a moment. But you say that you first brought this conversation to mind while discussing Dr Wright's case and your evidence with him and his lawyers; is that right?</p> <p>A. Yes, with Ontier.</p>	<p>Dr Pang admits that he first recalled this conversation while discussing Dr Wright's case and evidence with him and his lawyers.</p>
{Day9/27:10} - {Day9/29:5}	<p>Q. And then you say he suggested that you should try to build a Lego blockchain and that he challenged you to build it as long as you could?</p> <p>A. Yes, that was very strange, because at the first impression, I thought it would be very easy, you just stack the blocks one after another, you know, that would be a tower, but then I thought, is a tower a chain?</p> <p>Q. You say he told you that you couldn't use Lego Technic bricks; is that right?</p> <p>A. Yes, that is right.</p> <p>Q. Lego Technic bricks, is this right, are bricks which can make more complicated formations?</p> <p>A. Yes, that has been used to make, you know, cars with gears, remote control cars. I had one of those remote control cars back when I was a kid, so I'm very well aware of what it is, though I don't often buy and build Technic sets at the time.</p> <p>Q. Then the last sentence of paragraph 10 you say: "I was reminded of the statement about Technic bricks while I was drafting this witness statement as I remember it would have been very easy to create interlocking bricks with Technic bricks ..."</p> <p>A. Yes.</p> <p>Q. Was that a memory that just popped into your mind or was that something somebody else reminded you of?</p> <p>A. It just popped into my mind. It has popped into my mind before, but I haven't - I might have talked to Ontier about it, but can I blame the fact that there has been a lawyer - change in lawyers, or change in firms, so that information may not have been passed across between the lawyers and therefore I did not know whether I mentioned it to Ontier, but that definitely came back to me when I was talking to the second set of lawyers - I think they were Travers Smith or something.</p> <p>Q. So it came to you, you say, during the course of the various discussions you had with the lawyers about what your memories were?</p> <p>A. Yes, and I was - especially when I was writing this document, I was remembered - I remembered it, and then the lawyers say, you know, "Why do you came up this in new</p>	<p>Dr Pang gives an account of his conversation with Dr Wright regarding the Lego set, and how he remembered it during the course of conversations with Dr Wright's solicitors.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>statement? Is it because you came up with it whilst you were writing the document? Whilst we were recalling it, you came up with it". He specifically want me to trace and mention that I have written it as a new statement, as a track change or something like that, in my thoughts.</p>	
<p>{Day9/31:5} - {Day9/32:4}</p>	<p>Q. So on your account, to summarise this interaction, you show your senior colleague a Lego set which you think might be a collectors item and he challenges you to do something you can't understand, right? That's the first stage?</p> <p>A. Yes.</p> <p>Q. And then you ask him to clarify, and he suggests you try to build a Chinese chain puzzle out of Lego, which I'd suggest is both incomprehensible and a hopeless task.</p> <p>A. To me, at that time, yes.</p> <p>Q. Now, if this conversation went as you suggest, it really would have made no sense at all, would it?</p> <p>A. It made no sense at all. It is one of these funny things that happens with Craig every now and then. He says things that are nonsensical or funny, like he ate Babe, the pig. From a movie called Babe. He said he ate it.</p> <p>Q. I'm aware of the movie, Dr Pang. Did you think that Dr Wright was being just incoherent or making fun of you?</p> <p>A. He was making fun of me. That's - you know, people do in offices. They banter with jokes to establish intelligence and higher ranking.</p> <p>Q. It's a very odd sort of joke, isn't it, Dr Pang?</p> <p>A. Yeah.</p>	<p>Dr Pang admits his conversation with Dr Wright made no sense at all, and that Dr Wright was making fun of him.</p>
<p>{Day9/32:5} - {Day9/33:4}</p>	<p>Q. Now, I have to put this to you, Dr Pang. Your account is so confused and confusing that it really just doesn't make much sense in this respect about this conversation.</p> <p>A. It didn't make sense at the time, it doesn't make sense to me at all why he would say it. But I can say a lot of things retrospectively, but these are all my own opinion, unless you specifically ask for it, I would not say those opinions for, you know, brevity sake.</p> <p>Q. All I'm suggesting to you, Dr Pang, is that this hazy recollection of a nonsensical conversation is not - if you're being fair to yourself, is not a reliable recollection.</p> <p>A. That is not a reliable recollection, but the date in which I bought the Lego set and the fact that he said the word "blockchain" was 100% clear in my mind to be true.</p>	<p>Dr Pang admits that his recollection/account of the conversation with Dr Wright regarding the Lego set is not a reliable recollection (other than Dr Wright saying the word "blockchain").</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Well, Dr Pang, in the context of this very strange and hazy recollection, I suggest to you that picking out one word and trying to remember it as absolutely what he said is not reliable.</p> <p>A. The receipt and the fact that I bought the Lego set is completely reliable. You have got a date -</p> <p>Q. I'm not disputing you bought the Lego, Dr Pang, just to be clear on that.</p> <p>A. Okay.</p>	
{Day9/33:5-12}	<p>Q. Now, just to be clear, you don't say that at the time any connection was drawn by Dr Wright or anybody else with Bitcoin or digital cash or anything like that?</p> <p>A. No, there was other witnesses with me when Craig mentioned the word "bitcoin", another colleague, Hector Mabborang, was right next to Craig when he said it and he mentioned the joke to Hector Mabborang as well.</p>	Dr Pang introduces new evidence, not in his witness statement, that Dr Wright used the word "Bitcoin".
{Day9/36:12} - {Day9/37:12}	<p>Q. Now, the questions you recall Dr Wright asking didn't say anything about an alias, they were just, "Has anyone heard of [a Japanese name]", yes?</p> <p>A. Yes.</p> <p>Q. Would you accept this, just as a matter of common sense. If a person had an alias which they used for privacy, it would be quite strange behaviour to go round an office canteen talking about it, or are you not able to say?</p> <p>A. I think that would be quite strange if, you know - do you know someone called Iron Man, do you know someone called Batman, do you know someone called Superman? You know, if Superman go around, you know, asking everyone, you know - if Clark Kent went around asking everyone, "Do you know someone called Superman", that would be quite weird.</p> <p>Q. Once again, Dr Pang, would you accept that this is another hazy recollection of 15 years ago that you haven't been asked to recollect more recently?</p> <p>A. It is a very hazy recollection. I did not know what exactly he said, but I knew it was, to me, a Japanese - sounding name. That is right, it is very hazy. But I tried to recollect it as best as I could and I think it is true and I'm being truthful here.</p> <p>Q. I'm not suggesting to you you're being dishonest, Dr Pang, just that this is a hazy and unreliable -</p> <p>A. It is hazy. Hazy.</p>	Dr Pang admits that his recollection of Dr Wright going around the office canteen talking about his alias is hazy.
Dr Wright's tax claims for C01N Pty Limited		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day9/37:21} - {Day9/38:22}</p>	<p>Q. Are you aware that Dr Wright's company, C01N Limited, made an R&D tax offset claim for the 2012/13 - year for work done by you as a contractor?</p> <p>A. I do not recollect that I was a contractor. I was being paid with an ABN, so I do not understand that. I thought - I always thought that I was an employee. And the - our whole R&D business was only made known to me at the time I was working with Craig and I know that ATO is - Australian Tax Office is investigating and there was two very high ranking data analysis expert visiting Craig, a whole team, and I was asked to be there and present to support Craig in his claims.</p>	<p>Dr Pang states that he does not remember being a contractor for Dr Wright's company C01N Limited (work done by Dr Pang as a contractor being one of the expenses falsely claimed in the ATO proceedings).</p>
<p>{Day9/38:21} - {Day9/42:7}</p> <p>{L11/363/29}</p> <p>Reasons for decision by ATO for C01N Pty Ltd</p>	<p>Q. Paragraph 136 says: "On 14 August 2014, the taxpayer ..." That's C01N Pty Ltd, also known as "Strasan": "... advised that it incurred \$5,000 of expenditure to Dr Pang for undertaking ... R&D activities on behalf of the taxpayer. The taxpayer referred to Dr Pang as a 'contractor'. The taxpayer advised that the payment was made by ..." First: "C01n Ltd as trustee for the Craig Wright R&D Trust, transferring licences to the taxpayer in exchange for shares in the taxpayer." And then: "The taxpayer assigning the licences to Dr Pang as consideration for services performed in respect of the R&D activities." Do you see that?</p> <p>A. I have no idea what those licences are. I do not own a copy of those licences, so I don't know what those licences are.</p> <p>Q. That was going to be my first question, whether you, to your knowledge, received an assignment of any licences.</p> <p>A. I - if you ask me for a copy of the licences, I would not be able to give it to you, unless it was some, you know, GNU, you know, Common - Creative Commons licences, but I don't even know which ones I have used if I have used them. I've - I've - I've taken money for what I believe to be employments that is taxable and declared with the ATO, but I do not know of any of those licences, and even if you ask me to give it to you. I don't know what they are, and if I give them to you, I would not know whether they're the right ones.</p> <p>Q. Paragraph 137, the ATO reported that in support of the claim C01N had provided an invoice for \$5,000 dated 1 June 2013, issued by Dr Wright to C01N, describing the consideration as being transfer of beneficial ownership of licences and assignment of computer hardware and the licences are described in the invoice as an "SPSS" licence. First of all -</p> <p>A. I don't even know how to use SPSS. I know what it exists. I would probably be able to figure out a few buttons after, you know, looking at it extensively, but I don't use SPSS in my work.</p>	<p>Dr Pang states that he is unaware of (i) Dr Wright assigning licenses to him in exchange for shares in C01N Pty Ltd and (ii) the licences themselves.</p> <p>Dr Pang confirms that he was still under the impression that he was working for Hotwire PE during the ATO investigation into C01N.</p> <p>Dr Pang's recollection conflicts with what Dr Wright told the ATO.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. So you don't think that you received an assignment of SPSS licences?</p> <p>A. I could have got SPSS licences from the University of New South Wales for my academic use, but I chose not to use them because my expertise in this is in R statistical programming languages, and I have not used SPSS at all in all my work, ever.</p> <p>Q. So you don't think you were assigned SPSS licences by C01N or Strasan?</p> <p>A. I have not used SPSS given by C01N or Strasan. Q. And then the ATO says, at paragraph 138, that the companies, C01N or Strasan, had advised that there was no formal services contract for the provision of your services, but that Dr Wright invoiced C01N as agent for you. Did you have an arrangement with C01N whereby you provided services without there being a formal contract in place?</p> <p>A. I would not be able to tell you, because I was under the impression that I was working for Hotwire PE when the ATO asked, and I worked my guts off to try and do what Craig asked me to do, which is to recreate the Homie and Aussie Girl data analysis, or reboot that analysis and show the ATO office what it looks like.</p> <p>Q. Did you, Dr Pang, sign any agreement or enter into any agreement so that Dr Wright should be your agent for invoicing purposes?</p> <p>A. I don't - can you repeat that, please, my Lord? Q. Well, the suggestion in the report - and please don't call me "my Lord" - the suggestion in the report is that the - is that you appointed Dr Wright as your agent to invoice C01N, his company, on your behalf. Do you recall any arrangement to that effect?</p> <p>A. It's too complicated for me and I don't recall anything like that. It is as wild as anything that I've heard today.</p> <p>Q. Paragraph -</p> <p>A. I - I am not given a copy of his statement before, so I cannot determine the truth on the top of my head, or on my feet -</p> <p>Q. Understood.</p> <p>A. - on - on immediate recalling, and I hope I don't put myself in jail for that.</p>	
<p>{Day9/43:1-11}</p>	<p>Q. Now, the way it was presented was that C01N had provided you with a computer and software, and Hotwire, with a printer, payment for hours worked and superannuation, all on an independent contractor basis, not on an employment basis; do you understand?</p>	<p>Dr Pang confirms that he believed he was working on an employment basis, not an independent contractor basis.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. I believe it was on an employment basis, as far as I understand. I received a printer, which I've got, I've received laptop, but I don't recall any software at all that I have got a physical or digital copy of. The only access to any software was the Xero accounting software that I use online.</p>	
<p>{Day9/43:17} - {Day9/44:3}</p>	<p>Q. Page 50, please {L11/363/50}, of the document - actually, page 49 {L11/363/49}. There is a whole section of the report concerned with R&D tax offsets in relation to you, and at paragraph 246, over the page {L11/363/50}, the ATO said that the taxpayer had provided - so that's C01N - had provided contradictory accounts about whether Dr Pang was a contractor or employee and how Dr Pang was paid, including from Dr Pang himself, and your position is that you were an employee and certainly didn't receive any licences in payment; correct?</p> <p>A. Correct.</p>	<p>Dr Pang again confirms that he believed he was an employee and that he did not receive any licences in payment.</p>
<p>CROSS - EXAMINATION OF MR ROBERT JENKINS BY JONATHAN MOSS</p>		
<p>{L2/102/3} Dr Wright's BDO CV dated 2 May 2007</p>		
<p>{Day9/49:20} - {Day9/50:2}</p>	<p>Q. Now, back at the beginning of paragraph 11, you use the phrased "genesis log entry", but there are no documents attached to your statement, nor any other documents that COPA can find in these - what has been disclosed in these proceedings that refer to this term being used. Do you accept there are no documents that record that specific term?</p> <p>A. That's correct.</p>	<p>Mr Jenkins accepts there are no documents with the term "genesis log entry" in these proceedings.</p>
<p>{E/6} First Witness Statement of Robert Jenkins</p>		
<p>{Day9/53:3} - {Day9/54:2}</p>	<p>Q. You last saw this firewall up close and personal, so to speak, I presume in June 2000, when you left Vodafone; is that right?</p> <p>A. That's correct, yes.</p> <p>Q. So your memory of the technical details is now nearly 24 years old; is that right?</p> <p>A. You could say that, yes.</p> <p>Q. Let's just unpick a little bit of what you say in that paragraph bearing in mind that considerable lapse of time. You say the entries each had their own identifier; is that right?</p> <p>A. That's correct, row number 1, row number 2, row number 3, etc.</p>	<p>Mr Jenkins provides a description of the log system created by Dr Wright, which appears very basic.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. You have taken my next question away from me, Mr Jenkins. So the first entry would have been, say, 1; the second entry, 2; the third, 3, so on and so on; is that right?</p> <p>A. That's correct, yes.</p> <p>Q. So what was being in effect created was a sequential database?</p> <p>A. Not really. You could - you could refer to it as a - like a text file rather than a database. A "database" has other connotations. But, yes, certainly a text file.</p>	
<p>{Day9/54:16} - {Day9/56:9}</p>	<p>Q. And then it's in paragraph 16 that you talk about "eGold" {E/6/5}, and you say this would have been in the period 2000 to 2001; is that right?</p> <p>A. Around 2000/2001/2, around that period; correct.</p> <p>Q. You say in your statement, in fairness to you: "This would have been in the period ... 2000-2002." Correct? That's the top -</p> <p>A. That's correct.</p> <p>Q. -- the top of paragraph 16. And then, if we just look at the second sentence of paragraph 16, you say it was before eBay and before PayPal - I'll read the entire two sentences out: "So when I was working at COMindico, I remember Craig and I talked about eGold. This would have been in the period ... 2000-2002. It was before eBay and before PayPal and buying stuff online and paying for it was incredibly difficult ..." So you say there that - and we're in the period 2000 to 2002, that this was before eBay and PayPal; correct?</p> <p>A. Before eBay and PayPal was readily available in Australia, that's correct.</p> <p>Q. Right. Now, eBay launched in 1995, didn't it, Mr Jenkins?</p> <p>A. It could well have launched in 1995. Whether it was ubiquitous and readily available in Australia is a different matter.</p> <p>Q. And PayPal launched in 1998, and indeed it had its IPO in February 2002, and eBay bought PayPal in October 2002. Your statement here says "this was before eBay and before PayPal", but that can't be correct, so what are you actually saying in this sentence, Mr Jenkins?</p> <p>A. What I'm saying here is that whilst eBay might have been available and other online platforms available to pay for something online, there wasn't an easy means of paying for things like what the service that PayPal provides, and the only option, and it goes on in that paragraph to say essentially there</p>	<p>When questioned about the availability of eBay and Paypal in Australia before 2000, Mr Jenkins clarifies that he meant before they were "readily" available, the wording of which is not reflected at paragraph 16 of his witness statement.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>is only at the time an escrow - like service that was available at that time in Australia.</p> <p>Q. Okay, well, that wasn't very clearly originally, but we understand now what your evidence is on that point.</p> <p>A. Apologies.</p>	
<p>{Day9/58:12} - {Day9/59:5}</p>	<p>Q. Mr Jenkins, could we please look at the tenth page of your statement now {E/6/10}. These are the four documents that are supported in your witness statement. These are the documents that you were shown when you prepared this statement and you will note that the first of those is the transcript that I've just taken you to. Do you accept that you read this transcript before giving - before this witness statement in these proceedings was finalised?</p> <p>A. Interesting you say that, because I was never sent that document that's referred to as ID_004531. So you showing me on the screen today is the first time I've seen that.</p> <p>Q. So that's the first time you've seen the transcript?</p> <p>A. Correct.</p> <p>Q. I should point out, there are a number of versions of the transcript. Were you shown any version of the transcript?</p> <p>A. I've not received any version of the transcript, no.</p>	<p>Mr Jenkins states that he was never sent one of the PD57AC documents listed in his witness statement (ID_004531, the transcript of his evidence in Granath) and this is the first time he has seen it and that he was never sent any version of his Granath transcripts.</p>
<p>{Day9/61:15} - {Day9/62:13}</p>	<p>Q. Now, if we can go back to your statement, page 5 {E/6/5}, paragraph 16, the very last sentence of paragraph 16, you say: "We didn't have ongoing conversations around other digital currencies, but the concept of trust was a relatively consistent feature of what we talked about over the next few years." So your evidence there is it wasn't something you were regularly talking about, digital currencies, it was something that was one of many topics that you touched upon over the years with Dr Wright; is that fair?</p> <p>A. I think it's fair to say that, during that time, we were talking more about the trust side of things rather than digital currencies per se. It was more to do with - I think it was in relation to - to paying for - for a lunch at one stage, but essentially, the trust that's placed in a piece of paper, a piece of paper being a, you know, £5 note, £10 note, whatever it is, and it was conversations around why you trust a piece of paper that you hold in your wallet rather than something else that could be proven to be something more than just a promissory note. But essentially, the conversations were on the trust rather than actual digital currencies at that time.</p>	<p>Mr Jenkins agrees that his discussions with Dr Wright were not about digital currencies, but about trust in the context of banking systems.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day9/63:8} - {Day9/64:2}</p>	<p>Q. And it was you that was interested in E - Gold, not Dr Wright; is that correct? You were the one that was actually invested in E - Gold?</p> <p>A. So when I say invested in E - Gold, don't misinterpret that. I was the one that initially used E - Gold in order to make an online purchase, so I wasn't an investor in E - Gold. I'm not an investor in anything. But in terms of E - Gold, that was a means to - in order to purchase something online and that was the mechanism available and that was the escrow service available in Australia at the time.</p> <p>Q. So you were the one at the time using E - Gold. There doesn't appear to be any record of Dr Wright using E - Gold. Do you know if Dr Wright was also using E - Gold or was it just yourself?</p> <p>A. I'm unsure. I know that Craig knew about E - Gold and knew, you know, about escrow services. E - Gold, I think, probably at the time had several other competitors as well, but E - Gold was the one that was quite prevalent in Australia.</p>	<p>Mr Jenkins admits that he was the one that initially used E-Gold to make an online purchase, and was unsure whether Dr Wright used E-Gold.</p>
<p>{Day9/64:11} - {Day9/65:24}</p>	<p>Q. But can you name - can you remember the details - I appreciate it's a long time ago, but can you remember the details or the specific names of any other providers at that time?</p> <p>A. Off the top of my head right now, no, I can't. Could I refer to them in my emails, as I - you know, for the previous court case, and refer to other such services that I was looking at at the time? Yes, I probably have that information. Do I have it right now and has it been refreshed in the last couple of years? No, it hasn't.</p> <p>Q. I do appreciate it is a long time ago, Mr Jenkins, and I make no criticism of that. So just to clarify -</p> <p>A. Yeah, but - but just to clarify that as well, if I - if I may. There were certain - from the court case in Norway, I was given permission and was asked to specifically search for information in my emails and SMSs and anything else. If there was nothing there, I was asked to look for in terms of alternative means of - of escrow services back then and I wouldn't have looked for it. So it's disappeared into the annals of time. Where my more recent knowledge and memory prevails is based on the fact that, you know, 18 months ago, I was searching through these emails and it refreshed my memory. So I wasn't asked specifically what other escrow - like services were available back then, so it's not as fresh in my memory as it was for other things.</p> <p>Q. Perfectly understandable, Mr Jenkins. Do you think then that you might have been able to give a more accurate reflection, or recollection, I should say, of what was happening</p>	<p>Mr Jenkins disclosing that in Granath, he was specifically asked to search for information in his emails and text messages, etc. Discloses later that he was specifically asked not to conduct such searches in these proceedings {Day9/69:19-22}.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>back in this time had you undertaken such searches in advance of giving this evidence in these proceedings?</p> <p>A. Absolutely. And it wouldn't just be recollection, it would be factual.</p> <p>Q. It would be backed up by contemporaneous documents?</p> <p>A. Correct</p>	
{Day9/66:9-13}	<p>Q. And in your statement you mention conversations with Dr Wright about topics you discussed that could relate, or may relate to some of the broad concepts relating to Bitcoin; correct?</p> <p>A. That's correct, yes.</p>	Mr Jenkins agrees that he had conversations with Dr Wright about topics that “could” or “may” relate to some of the broad concepts relating to Bitcoin.
{Day9/66:14} - {Day9/67:7}	<p>Q. But you say you also talked about other topics. What other non - financial topics did you discuss with Dr Wright in this period?</p> <p>A. So during my time at Commonwealth Bank, I was asked initially to look at the firewall set up at Commonwealth Bank and was involved in the RFP process, I looked into the design of the firewall architecture for the - for the Bank. So at the time, because Craig was - was doing this kind of work for lots of other companies, we were discussing, you know, what the prevailing patterns were for architectural solutions for - for the likes of financial institutions globally. Later on, we were talking about, for example - I think it's in this document around OPRA, we were talking about grid computers. So at the time, I was working with the - with the Commonwealth Bank and the CSRL around building an operational risk adviser, which was a grid computing capability to run Monte Carlo simulations. We'd be talking about that kind of capability.</p>	Mr Jenkins explains that he discussed standard IT security topics with Dr Wright.
{Day9/67:24} - {Day9/68:9}	<p>Q. So you might have discussed telephony stuff when you were at Vodafone and discussed banking stuff when you were at Commonwealth Bank of Australia; is that fair?</p> <p>A. And - and vice versa. So whilst at Commonwealth Bank then talking about what mobile capability in your hand and how it could be used to improve the - the - you know, the interactions as far as banking's concerned or anything else.</p> <p>Q. You don't mention anything about mobile banking in your statement here, do you, Mr Jenkins?</p> <p>A. No. No, I don't.</p>	Mr Jenkins admits that in his witness statement he does not mention any discussions with Dr Wright around mobile banking.

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day9/68:10} – {Day9/69:22}</p>	<p>Q. Now, in paragraph 17, that’s when you say that you first recall the word “blockchain” in 2008. That was a very precise year, Mr Jenkins. Is it your evidence that Dr Wright told you the word “blockchain” in 2008?</p> <p>A. That’s my recollection, that’s correct.</p> <p>Q. And then you give evidence to tie in your recollection and your discussions with Dr Wright to Bitcoin later, and indeed you note at the third line up from the bottom of para 17, at the end there, that you are looking back at all of this with the hindsight of what we now know; is that correct?</p> <p>A. That’s correct, yes. And the other hindsight being, you know, the - again, the research I did for the previous court case, where I was able to, again, whether there were emails exchanged or whether they were, you know, things that were being discussed at the time, around that time.</p> <p>Q. But there isn't a single document that you have included in your witness statement that mentions the word "blockchain" from this time period, is there?</p> <p>A. Is there a document where I've referenced blockchain? No, there isn't a necessary(?) document, no.</p> <p>Q. So we've only got your memory to go on this; is that correct?</p> <p>A. There may well be emails that I have that make reference to blockchain, but I was asked not to refer to any - any previous emails or any previous anything other than what was brought up at - in Norway. So I may well have evidence that - that explicitly references blockchain in emails.</p> <p>Q. So you think you may have emails from 2008 involving Dr Wright that would have the word "blockchain" in them; is that correct?</p> <p>A. It's quite possible, yes.</p> <p>Q. And you have just told us that you were told not to look for such; is that right?</p> <p>A. I was told for this court case not to look for such, that's correct.</p>	<p>Mr Jenkins admits that he was specifically asked not to refer to or look for any previous emails with Dr Wright from around 2008 that reference “blockchain” for the purposes of these proceedings.</p>
<p>{Day9/70:16} - {Day9/71:7}</p>	<p>Q. That - sorry, that is I was just pointing out that it was mentioned in that, but when you're talking about it in 2008, are you sure that your recollection is accurate bearing in mind the passing of time and bearing in mind that you don't have any documents to back up what you have just told us?</p> <p>A. Okay, as I stated previously, I may well have documents that are able to back it up, all right? They were, as part of this court case, I was asked explicitly not to refer or refresh my</p>	<p>Mr Jenkins admits again that he was specifically asked not to refer to or refresh his memory in any way for the purposes of these proceedings.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>memory in any way, shape or form, all right? But in terms of whether those emails do or don't exist, they may well exist.</p> <p>Q. Okay. Are you aware that the word "blockchain" doesn't actually appear in the Bitcoin White Paper, either as one or two words, Mr Jenkins?</p> <p>A. Yes, I am aware of that.</p>	
<p>{Day9/72:19} - {Day9/73:15}</p>	<p>Q. Mr Jenkins, it's very important that we're quite precise here, because what your evidence says in paragraph 18, and I'll read it out, it says: "For example, some of the conversations I was having with Craig in mid-2005 were around currency because of the specific nature of one of my projects with [Commonwealth Bank of Australia] at the time. "Now, Mr Jenkins, I'll put it to you that it must have been you that raised that topic, because Dr Wright cannot have known what project you were working on within Commonwealth Bank of Australia unless you told him. Do you accept that must be the position?</p> <p>A. That is a logical position you've raised, yes.</p> <p>Q. Thank you. What was the name of that project?</p> <p>A. The name I can't remember.</p> <p>Q. You can't remember the detail of the name of that project from 2005. Is that because of the passing of time?</p> <p>A. It could well be the passage of time. It isn't something I've been asked to recollect or asked to research in any way.</p>	<p>Mr Jenkins accepts that it must have been he who raised the topic of currency with Dr Wright during conversations in mid-2005.</p>
<p>{Day9/75:3-7}</p>	<p>Q. Then at paragraph 21, further down the page {E/6/6}, you say that you and Dr Wright were talking about the design of the OPRA system. Again, this discussion arose from your work, Mr Jenkins, not Dr Wright; isn't that fair?</p> <p>A. That's correct, yes.</p>	<p>Mr Jenkins again accepts that it must have been he who raised the topic of the design of the OPRA system with Dr Wright, because it arose from Mr Jenkins' work.</p>
<p>{Day9/78:8}- {Day9/79:4}</p>	<p>Q. And as I've put to you a number of times already, you are looking at these conversations through what you now have been told to be true, which is that Dr Wright is actually Satoshi Nakamoto; is that correct?</p> <p>A. At that time, if it had come out at that time, then, yes, it's the case, but in - in terms of Craig being Satoshi, that isn't something that I - that was realised until much later.</p> <p>Q. I accept that, but I'm saying you are looking back at events that happened in your own career history, but you're looking back at those events to try and see if anything of the things that</p>	<p>Mr Jenkins again confirms that in Granath, he searched for previous emails, but did not conduct such a search herein these proceedings, indicating that he found nothing helpful in his searches for the Granath proceedings.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>you discussed with Dr Wright support his claim to be Satoshi Nakamoto; correct?</p> <p>A. That wasn't the intent of looking back. The - the intent of looking back was, as I said, for that previous case, in terms of doing a search in previous emails and email correspondence that had taken place, and if there was mention of blockchain around that time, then that's why I would have that timeline on there.</p> <p>Q. And unfortunately, we have been totally deprived of that exercise of a search in these proceedings, haven't we?</p> <p>A. We have, correct.</p>	
<p>{Day9/82:5} {Day9/83:9}</p>	<p>Q. So are you saying here that this reference to mining was Dr Wright telling you to mine Bitcoin?</p> <p>A. It was to run some code on my computer system in order to - certainly as far as Bitcoin was concerned, where Bitcoin wasn't necessarily mentioned, it was certainly to run the code on a computer system so that it would effectively help secure the information that was being distributed between computer nodes, and that in order to secure that in - in a way that was trustworthy, it needed that computer computational task distributed across a number of nodes.</p> <p>Q. Now, details matter, Mr Jenkins, and we do need to be quite clear about this. You're talking about some mining here in this period, say early 2009, but are you or are you not saying that Dr Wright mentioned Bitcoin to you in that period?</p> <p>A. So I'm saying that Bitcoin wasn't mentioned to me explicitly around that time, as far as I can recollect.</p> <p>Q. So you're just saying that he asked you to do some mining -</p> <p>A. Correct.</p> <p>Q. -- but you don't have any real recollection beyond that?</p> <p>A. No, it was more an explanation of: okay, so tell me what - what mining is, and then when he explained it was the execution of some code on your own computer system. And then it was, why, for what purpose? It was in order to ... so we're getting into the technicalities of - of what mining was and what it would contribute to. In terms of Bitcoin explicitly, it wasn't necessarily a term that factored into the conversation.</p>	<p>Mr Jenkins explains that Dr Wright did not mention Bitcoin to him when discussing mining in early 2009. Implausible that Jenkins would give over control of his computer without even asking for an explanation of what the system was and what his computer was being used for.</p>
<p>Mr Jenkins' video evidence from Granath</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day9/83:20} - {Day9/86:18}</p>	<p>(Video footage played)</p> <p>So Mr Jenkins, your very clear evidence in Granath and I took you to the warning that you were given at the beginning of those proceedings, your very clear evidence in Granath, given under oath, was that it was early 2011 when you first heard the term "bitcoin"; that's correct, isn't it?</p> <p>A. Yeah, I'd say that was correct.</p> <p>Q. And you were quite specific about that memory, Mr Jenkins, indeed you mentioned it twice, and you tied that memory to you being at Westpac; correct?</p> <p>A. That's correct. Yes, I did.</p> <p>Q. And, of course, it was September 2010 when you started at Westpac?</p> <p>A. That's correct, yes.</p> <p>Q. Can we now please go back to your evidence, Mr Jenkins, page 8, paragraph 33 {E/6/8}, and I'll read out the beginning of that. You say:</p> <p>"I remember around 2009 or 2010 Craig asked me if I wanted to buy some Bitcoin. This was the first time I heard that word, but to my mind we had discussed the technology underpinning something like Bitcoin before I heard the word Bitcoin."</p> <p>Now, your evidence you've given under oath today, which you swore in not even an hour ago, said to be true, says that you first heard the term Bitcoin in 2009 or 2010. That cannot be correct, can it, Mr Jenkins?</p> <p>A. It could be correct insofar as, with the recording that was played back, I had the benefit of reference to materials at the time for that particular court case, so I could be quite specific with what the timing was around the reference to the term "bitcoin". For this particular court case, I haven't been given that luxury to clarify that and to look up any evidence or any emails or any kind of that other correspondence I have that could clarify that. So, yeah, there does appear to be a discrepancy, and it may well have been the coincidental around 2010, you could say for both of those it was around 2010, late 2010/early 2011, around that kind of time frame.</p> <p>Q. But Mr Jenkins, you were very clear in Granath, you were very clear to tie the memory of the first time you heard "bitcoin" to being at Westpac.</p> <p>A. Correct.</p> <p>Q. Now, that means it cannot have been before September 2010; correct?</p>	<p>Jenkins ultimately accepts that his evidence in these proceedings was wrong, and that he did not first hear the term Bitcoin until early 2011. This contradicts Mr Jenkins' evidence in the Granath proceedings and Dr Wright's statement in his RFI response (Fourth Witness Statement {E/4/21}), in which Dr Wright states that he provided a draft of the White Paper to individuals including Mr Jenkins, i.e. before 2011.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. That's correct, yes.</p> <p>Q. Which means it absolutely -</p> <p>A. But nonetheless 2010.</p> <p>Q. Which means it absolutely could not have been in 2009; correct?</p> <p>A. That's correct. That would seem to suggest that, yes. But my statement there says, "I remember around 2009 ...2010 [he] asked me if I wanted to buy Bitcoin".</p> <p>Q. Yes, but it can't have been 2009; do you accept that? A. Yeah, well, that's what "around" means, but, yes.</p> <p>Q. No, Mr Jenkins, the details matter in this, because of course, by 2011 Bitcoin was much more common; back in early 2009, after it was released, it's not so. And you tied it back, very specifically, to your time at Westpac. You said, in fact, not even late 2010, you said early first half of 2011. So, do you accept there's a quite clear inconsistency between the evidence you gave in Granath, which of course was closer in time to these events, and the evidence you've given in these proceedings? Do you accept that as correct?</p> <p>A. As I've said previously, I had the benefit of - of using reference material in the previous court case and I haven't here, so this has been more reliant on - on the longer term memory.</p> <p>Q. So, based on that, your evidence in Granath, you must accept, would be better because you had the benefit of these other documents; correct?</p> <p>A. I would suggest that's the case, yes.</p>	
<p>{L18/62/12} Transcript of evidence of Robert Jenkins - Granath v Wright</p>		
<p>{Day9/87:23} - {Day9/89:7}</p>	<p>Q. Then if we go - if we could please go to page 12 of the transcript {L18/62/12}, right at the top, you were asked:</p> <p>“Did Craig Wright ever show you or send you a White Paper related to Blockchain technology?”</p> <p>And you answered: “No, he didn’t, never sent me anything. There was one meeting, I have a recollection that he did mention to me that he had been working on documenting, you know, what we had been discussing over a number of years, and he pondered and thought, ‘You may get something in the post’, you know?”</p> <p>So your evidence in Granath, which you just accepted is more reliable than your evidence in these proceedings, you’re quite</p>	<p>Mr Jenkins confirms that Dr Wright never sent him a copy of the Bitcoin White Paper, contrary to Dr Wright’s evidence in his Fourth Witness Statement {E/4/21}.</p> <p>Mr Jenkins had accepted in Granath that he had not been sent a copy of the Bitcoin White Paper.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>clear there that you never received a copy of the Bitcoin White Paper; isn't that correct?</p> <p>A. No, that's not correct. I think, actually, if you - because this is a transcription of what I said, so there are a smattering of errors in the transcription in any case, and what I would more likely have said at that stage is that, no, he didn't send me anything.</p> <p>Q. So he didn't send you -</p> <p>A. And - he didn't send me anything. Right? So that - it doesn't say that he didn't show me anything, just that he didn't send me anything, just to be specific. So, could you go to the recording on that and play that to actually hear what I said, as to what's been transcribed? And this is the first time I've seen the transcription, so ...</p> <p>Q. We can look at the - we can look at the video ourselves later on. I just want to clarify with you whether you accept that, that he didn't send you a copy of the Bitcoin White Paper, or do you say -</p> <p>A. Correct.</p>	<p>Mr Jenkins was later re-examined on this exchange at {Day9/96:20} onwards, wherein Mr Jenkins then claimed he had been shown a paper mentioning "Timecoin" from Dr Wright.</p>
<p>{Day9/91:19} - {Day9/92:17}</p>	<p>Q. And the reality is you can only speculate on Dr Wright being Satoshi because you have now been told that Dr Wright was Satoshi and you're looking back at your events with him through the prism of hindsight. Do you accept that's correct?</p> <p>A. Yeah, that, laid with a couple of other things, and one - one in particular, getting to know Craig as a person over the years, over the long time that I've known Craig. I've have known him to be a very unique individual, and I know him to be, on the one hand, a very shy individual, where he shies away from any form of publicity, or any form of acknowledgement in some of the work that he does, and I see the flip side of Craig, where he is gregarious and is, you know, the - a person who is very passionate about what it is he's working on, or what he believes in. So, I - that, where someone like Craig would have some kind of pseudonym associated with the work that he is does and it being something like Satoshi, or anything else, doesn't surprise me. So there was that aspect to it as well.</p> <p>Q. But you don't actually know. You weren't in the room where it happened, so to speak, when he claims to have been writing the Bitcoin White Paper, were you?</p> <p>A. No, I wasn't.</p>	<p>Mr Jenkins admits that he can only speculate on Dr Wright being Satoshi and confirms that he does know, providing an answer with no factual basis.</p>
<p>{Day9/93:15-21}</p>	<p>Q. A common thread here, Mr Jenkins, is that when looked back at, all of these interactions on these topics arose because of stuff you were involved in. In fact, the story of your</p>	<p>Mr Jenkins admits that all of his interactions with Dr Wright reflect</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>interactions with Dr Wright, as given in your evidence, reflects your career, not his. Do you accept that's correct?</p> <p>A. I do.</p>	<p>his career, not that of Dr Wright.</p>
<p>RE - EXAMINATION OF MR ROBERT JENKINS BY LORD GRABINER KC</p>		
<p>{E/6/7} First Witness Statement of Robert Jenkins</p>		
<p>{Day9/95:1-19}</p>	<p>Q. - the suggestion was that your memory was hopeless and that this couldn't have - or did not take place in 2008 or 2009 and that your memory is poor. What do you say to that?</p> <p>A. Look, I wouldn't claim my memory to be any better or worse than anybody else's. What - what I can say is, as I've mentioned to your learned friend, in the previous court case, that took place just around 18 months ago, I was asked to go and scour through my emails and text messages and documentation, and as I've said, in that process, I've discovered that I've hoarded an enormous amount of data, and so running some search criteria across that, it did surface a lot of evidence I was able to re - read. So what would have been a recollection casting my mind back more than 20 years has essentially been a casting my mind back around months, so it's much more fresh in my mind. I ran those particular topics I was asked to investigate for the previous court case.</p>	<p>Mr Jenkins explains that in Granath, he conducted extensive searches of documents, which produced “a lot of evidence” that he was able to re-read, cf. these proceedings.</p>
<p>{CSW/31/1} Timecoin paper</p>		
<p>{Day9/96:1} - {Day9/97:25}</p>	<p>On line 4: “ ... your evidence in Granath, which you just accepted is more reliable than your evidence in these proceedings, you're quite clear that you never received a copy of the Bitcoin White Paper; isn't that correct?” Then you said:</p> <p>“Answer: No, that's not correct. I think, actually, if you - because this is a transcription of what I said ... there are a smattering of errors in the transcription in any case, and what I would more likely have said at that stage is that, no, he didn't send me anything.</p> <p>“Question: So he didn't send you -</p> <p>“Answer: And - he didn't send me anything. So it doesn't say that he didn't show me anything, just that he didn't send me anything ...” -</p> <p>A. That's correct.</p>	<p>Mr Jenkins is asked by Lord Grabiner KC whether Dr Wright <i>showed</i> him anything (despite not <i>sending</i> him a copy of the Bitcoin White Paper). Mr Jenkins provides new evidence, not previously mentioned in this case or in Granath, claiming that Dr Wright showed him a paper that mentioned “Timecoin” around 2009/2010. He was then taken to a</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. - "... just to be specific." Did he show you anything?</p> <p>A. I do. I do remember seeing a couple of things, besides what Craig drew on the napkin. At a - at a subsequent meeting, I was shown a paper. It didn't make mention of Bitcoin but it did make mention of - of something called Timecoin, and that was something that - as a White Paper that he - he showed me at that time.</p> <p>Q. You said a bit later. When was that?</p> <p>A. It would have been in that time window I was saying. It was before I joined Westpac and - and after those series of lunches where he drew on the - on the napkin. So, around, again, 2009/2010.</p> <p>Q. And could you describe a little bit more fully the context in which that conversation took place? Where were you, for example?</p> <p>A. It would have been in - in one of the many cafes or restaurants that - that Craig and I attended over the years, and it would have been just to, kind of, run through and to show the fact that the White Paper had been produced off the back of some of the conversations we'd been having, and the drawings were done on - on the napkins and this was the - the fruit of his labour.</p> <p>Q. I'm going to show you a document and I want to ask you if you recognise the document. Could you be shown - or could we look at {CSW/31/1}. That's a Timecoin paper, "A peer - to - peer electronic cash system", with Craig Wright's name at the top of it. Do you recognise that document?</p> <p>A. As far as I can recollect that far back, because this isn't something that was discussed in the - in the Granath court case, but, yes, it does look certainly similar to the document that I saw, yes.</p>	<p>document (at {CSW/31/1}) which he had not been shown previously in this litigation or Granath. It is one of a number of Dr Wright's documents that mentions Timecoin, so it is unclear why this document was chosen by Dr Wright's team. Mr Jenkins said that it looked similar to the one that Dr Wright showed him. It is unclear how he could be sure based on a few seconds of seeing a document on screen which he had, according to his story, only seen once before, some 15 years ago.</p> <p>In addition to this evidence not being contained in Mr Jenkins' witness statement, it is in any event inconsistent with the timeline in Dr Wright's evidence, in which he states that "Timecoin" predated Bitcoin {CSW/1/59}.</p>
CROSS - EXAMINATION OF MR ROBERT JENKINS BY JONATHAN MOSS		
{CSW/31/1} Timecoin paper		
{Day9/99:6} - {Day9/101:7}	<p>MR JUSTICE MELLOR: I'm going to allow it, because you've elicited some quite important new evidence.</p> <p>LORD GRABINER: Well, my Lord, but it arose directly out of the cross-examination.</p>	<p>Mr Jenkins admits that he does not mention "Timecoin" in his evidence in any proceedings (neither Granath nor in these</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>MR JUSTICE MELLOR: But it's surprising it hasn't been in any witness statement.</p> <p>LORD GRABINER: I totally agree.</p> <p>MR JUSTICE MELLOR: So I'm going to allow further cross-examination.</p> <p>Further cross-examination by MR MOSS</p> <p>MR MOSS: Very briefly, Mr Jenkins. How many times do you mention Timecoin in your witness statement?</p> <p>A. Not at all.</p> <p>Q. How many times do you mention Timecoin in your Granath evidence?</p> <p>A. Not at all.</p> <p>Q. When Timecoin was mentioned to you, I noticed that you looked down in front of you. Is "Timecoin" written on a piece of paper in front of you?</p> <p>A. Yes, it is.</p> <p>Q. Why is it written on a piece of paper in front of you?</p> <p>A. Because I have -- my Lord, I have "Nokia Check Point Firewall 1", I have "Timecoin", I have "eBay/PayPal". These are things that I need to make sure that -- that are clearly understood, as far as this particular evidence is concerned.</p> <p>Q. And who told you that those things need to be clearly understood?</p> <p>A. Myself.</p> <p>Q. Your son? What's your son's name?</p> <p>A. Myself.</p> <p>Q. Oh, sorry, yourself?</p> <p>A. By myself, yes.</p> <p>Q. I thought you said your son?</p> <p>A. No. I don't have a son, that I'm aware of.</p> <p>Q. What else? Could you read out everything else that's written on your notes in front of you, please?</p> <p>A. It has: "Questions being asked. "Usher. "My Lord. "Nokia Check Point FW-1."Timecoin. "[And] eBay/PayPal." That's it that's written on the paper (indicates).</p> <p>Q. So you wrote Timecoin down --</p> <p>A. If you can see that.</p> <p>Q. We can't see that. That's okay.</p>	<p>proceedings). Mr Jenkins admitting that the word "Timecoin" is written on a piece of paper in front of him, together with some other words, and confirms it was written down before his evidence started.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Yes, okay.</p> <p>Q. You wrote Timecoin down on that piece of paper before your evidence started?</p> <p>A. Yes, I did.</p>	
{Day9/101:8-19}	<p>Q. And who told you to write that down?</p> <p>A. Nobody told me to write it down.</p> <p>Q. But Mr Jenkins, you have not mentioned Timecoin in any evidence, either here or in Granath before. Where on earth did your recollection of Timecoin come from?</p> <p>A. The recollection of Timecoin came about when I was in preparation for this particular court case.</p> <p>Q. And what was it that brought --</p> <p>A. In terms of -- there's -- there's lots of reference to a Bitcoin White Paper and I remember never being shown in any way, shape or form a Bitcoin White Paper, purely and simply.</p>	<p>Mr Jenkins explains that his recollection of Timecoin came about when he was “in preparation” for this case. This is implausible given that, on his evidence, he prepared much more thoroughly for his Granath evidence, conducting several document searches, and yet did not mention Timecoin there.</p>
{Day9/102:5} - {Day9/103:11}	<p>Q. And just out of fairness, given what has happened, I need to put it to you, we will suggest that you have been prepared for your evidence and that you wrote Timecoin down in advance with the intention of slipping it in when it has never been mentioned in any evidence that you’ve given in either these proceedings or Granath. Do you accept that?</p> <p>A. No, these were notes that I took during the course of this particular interaction rather than anything I wrote before the interaction.</p> <p>Q. That's not what you said earlier when I asked you, Mr Jenkins. You said the note had been prepared before. What is the truth?</p> <p>A. The truth is that, "my Lord" was something that I wrote on there in reference to how I need to refer to the judge as part of this case. The other items in terms of “Nokia Check Point Firewall-1” was in relation to the firewall that was used as part of the interaction with -- with Vodafone. I wanted to make sure that I remembered that to that level of detail in case that was asked.</p> <p>In terms of anything to do with a White Paper, if there were any questions that were going to come up as far as the White Paper was concerned, as I’ve said quite clearly, I’ve never received or been sent anything in relation to a Bitcoin White Paper, and that’s unequivocal.</p>	<p>Mr Jenkins states that the notes in front of him were taken “during the course of this particular interaction” and not before his cross-examination, which is inconsistent with his evidence given a few minutes earlier (where he stated he wrote it down before his evidence).</p> <p>When pressed on this, Mr Jenkins changes his story again, stating that he recollected the phrase “Timecoin” during this cross-examination, rather than in preparation for his evidence.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>When it comes to "Timecoin", that is a term of phrase that I have been familiar with in the past, that I recollected during this conversation that we've been having. That is a White Paper that I did see and was never sent.</p>	
<p>{Day9/103:22} - {Day9/104:11}</p>	<p>Q. But you said earlier that you made the note before this evidence started; is that correct? Bearing in mind --</p> <p>A. As far as the "questions being asked", "usher" and "my Lord", that's correct.</p> <p>Q. Are you saying you wrote "Timecoin" down during the course of the evidence, bearing in mind, Mr Jenkins, that we've all been watching you this entire time and I don't think anybody saw you write anything during the course of your evidence. Are you saying that you wrote the word "Timecoin" down after I started questioning you, or was it written down before I started questioning you?</p> <p>A. "Timecoin", "Nokia Check Point Firewall-1" and "eBay/PayPal", were all written during the course of this interaction.</p>	<p>Mr Jenkins reiterates that he wrote "Timecoin" during the course of this interaction, despite nobody seeing him writing anything.</p>
<p>{Day9/105:4-12}</p>	<p>Q. Finally, my final question, Mr Jenkins, is it your position now that you first remembered Timecoin today in the course of me questioning you?</p> <p>A. I -- I've remembered that particular title of that document in the course of the conversation we've had today, yes.</p> <p>MR MOSS: I would suggest to you that is not true, Mr Jenkins, but I accept I've already put that to you and you deny it.</p>	<p>Mr Jenkins reiterates that he remembered "Timecoin" during the course of this interaction.</p>
<p>CROSS - EXAMINATION OF MR SHOAB YOUSUF BY JONATHAN MOSS</p>		
<p>{L11/361} ATO Reasons for Decision C01N Exch Pty Ltd</p>		
<p>{Day9/130:14} - {Day9/132:5}</p>	<p>So then, if we go to page 10 {L11/361/10}, at the very bottom of page 10, we're in the "Relevant Facts" section, and this is, "Purported R&D activity". And we can see there -- and I'll just read out paragraph 39, or part of it, it says:</p> <p>"On 7 October 2013, the taxpayer applied to register a project named 'Sukuriputo okane' under section 27A of the Industry Research and Development Act 1986 ... for 2012-13 [year]. The project is described as a software library for financial cryptography including a prototype server and high-Level client API able to process Bitcoin transactions and markets."</p> <p>Do you see that?</p> <p>A. I see that, my Lord.</p>	<p>Mr Yousuf confirms that he was not aware of the R&D project "Sukuriputo okane" allegedly occurring when he was a director of C01N.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. So this was a project -- this was R&D activity that was happening when you were a director; correct?</p> <p>A. That's correct, my Lord.</p> <p>Q. And you know about this project, do you?</p> <p>A. I was not aware of this project, my Lord.</p> <p>Q. You are not aware of that project at all?</p> <p>A. Not -- I -- I don't remember about this project, my Lord.</p> <p>Q. Before I go over the page, just so we understand what I'm now going to, if you look at the last sentence of paragraph 39, it says: "The three core activities are described in the AusIndustry application as follows." Then over the page, please, {L11/361/11}: "Scriptable money: exploring the ways to program a distributed contract using Bitcoin to form agreements with people via the blockchain." "BTC' agents: exploring currency agents. "Transaction signing: no information is provided about this activity." So you're saying you don't know anything about this project?</p> <p>A. I don't remember exactly about this project, my Lord. I remember when Craig provided me an update about the company, he did mention about the work he has been doing on Bitcoin, digital cash, Bitcoin wallet. So I'm aware of it, but I'm not aware of exact specific projects being carried out.</p>	
<p>{Day9/132:15} - {Day9/133:6}</p>	<p>Q. Then, again, in paragraph 41, there's a further comment by -- or further recorded by the ATO that:</p> <p>"The taxpayer provided additional information to AusIndustry on 7 October 2013. Much of this information is taken from internet sources, without acknowledgment."</p> <p>Again, I assume you would say you don't have any recollection of that. Was that done by Craig -- sorry, was that done by Dr Wright?</p> <p>A. I -- I don't remember. I was not involved, so I cannot say anything on this, my Lord.</p> <p>Q. Then below, at paragraph 46, we see that in February 2016, AusIndustry made a finding that: "... none of the activities registered by the taxpayer in ... 2012-13 ... met the requirements of a core of supporting R&D activity." Are you aware of that finding?</p> <p>A. I'm not aware of that finding, my Lord.</p>	<p>Mr Yousuf confirms that he was not aware of the information provided to AusIndustry on behalf of C01N in relation to the R&D project.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{Day9/134:2-21}	<p>Q. Now, you said earlier that you were involved around ten months. What were you actually doing in the ten months when you were involved with C01N?</p> <p>A. Yes, so my Lord, our -- our main reasons -- our involvement, our initial business plan was to leverage Dr Craig Wright, you know, research on developing a security operations centre using the, you know, distributed network over the cloud. So we worked on setting up the Strasan business, focusing on cybersecurity advisory, cybersecurity training and education, cybersecurity solutions, which were focusing on, as I said, security, monitoring, penetration testing, vulnerability assessments. So we developed a lot of our offerings around that domains. We also did, you know, work with Craig developing a product which will help enterprises, especially small/medium enterprises to monitor their network remotely for the cybersecurity threats. So these were work I was involved working with Craig to launch these products and services.</p>	<p>Mr Yousuf describes the type of work he and Dr Wright did when he was involved in C01N, which is in the area of IT security.</p>
{Day9/134:22} - {Day9/135:4}	<p>Q. So in this period in C01N, you and Dr Wright were seeking to launch a cybersecurity business; is that correct?</p> <p>A. The cybersecurity business around, you know -- that was our initial phase 1. That was our plan to start it, because we both come from cybersecurity background, and -- and this is where we felt how we should start our company.</p>	<p>Mr Yousuf confirms that he and Dr Wright were starting a cybersecurity business.</p>
{Day9/135:5-15}	<p>Q. And then those two deductions -- well, one deduction and one offset that I just took to you in paragraph 47, are not the only deductions. Do you see below, in paragraph 48, there was a deduction sought for over AU\$2 million for “materials and assistance acquired from Professor David Rees”? Do you have any knowledge about that?</p> <p>A. I have no knowledge about this, my Lord.</p> <p>Q. In your time as a director of C01N, did you ever hear the name David Rees mentioned?</p> <p>A. No, my Lord.</p>	<p>Mr Yousuf confirms that he had never heard Dr Wright mention David Rees and had no knowledge about the AU\$2 million deduction sought for materials and assistance from him, despite being a director of the company.</p>
{Day9/135:21} - {Day9/136:22}	<p>“The taxpayer purported to enter into a contract with W&K entitled ‘statement of work’ for the provision of IaaS services over a 12 month period. The statement of work is dated 30 June 2012, and it appears to have been digitally signed by Dr Wright and Mr Kleiman on 2 July 2012.”</p> <p>Again, this statement of work was carried out when you were one of only two directors; is that correct, Mr Yousuf?</p> <p>A. Seems like it, my Lord.</p> <p>Q. And were you involved in the creation of that statement of work?</p>	<p>Mr Yousuf confirms that he had no knowledge of a contract with W&K for the provision of IaaS services, and that appeared to have been digitally signed by Dr Wright and Mr Kleiman.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. No, my Lord.</p> <p>Q. Do you know anything about that statement of work?</p> <p>A. No, my Lord.</p> <p>Q. Down below, in paragraph 57, it records -- the ATO decision records:</p> <p>“The statement of work appears to have been adapted from a US government IaaS tender document obtained from the internet .”</p> <p>Again, do you have any idea of who might have taken that statement of work off of the internet?</p> <p>A. No, my Lord.</p> <p>Q. It can't have been you. Could it have been Dr Wright?</p> <p>A. I mean, Dr Wright had quite a few people supporting him, so perhaps Dr Wright might have leveraged some support or services from others.</p>	
<p>{Day9/139:3-5}</p>	<p>Q. And you've given evidence that you have no recollection of this project whatsoever; is that correct?</p> <p>A. I don't recall about this project, my Lord.</p>	<p>Mr Yousuf re-iterates that he has no recollection of the R&D project discussed in this part of his cross-examination.</p>
<p>{Day9/139:10} - {Day9/140:22}</p>	<p>Q. Now, there's a lot of detail in here, and I'm not going to go through all of it because we can make our points based on the documents as be, and you have already said you don't know anything about this, but if we can now jump to page 14, please {L11/361/14}, which is the next page, paragraph 61: "The statement of work provides that the service is for a 'fixed fee for the provision of systems over ... 12 [months] ... However, an appendix titled 'C01N Pricing' states that 'Cost base will be calculated as [numbers]. At the time the contract was purportedly executed, the taxpayer's name was Strasan ... The taxpayer contends that the name of the supercomputer was 'C01N' and that this is evidenced by its entry in the Top 500 list. However, C01N's first entry in the Top 500 list was not until November 2014." Do you have any knowledge of the supercomputer being named C01N, Mr Yousuf?</p> <p>A. I -- I remember Dr Craig Wright sharing a news about supercomputer, but I don't remember what was that super computer was called and when was it.</p> <p>Q. But Mr Yousuf, you were a director of a company that supposedly had a supercomputer. Are you saying you knew nothing about it?</p>	<p>Mr Yousuf states that he recalls Dr Wright sharing news about a supercomputer, but confirms that he does not remember anything about it, and has no recollection of it being called "C01N".</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. No, my Lord, I'm -- I don't remember anything about the supercomputer.</p> <p>Q. Mr Yousuf, was everything to do with the supercomputer simply a sham?</p> <p>A. But why would you say that, my Lord?</p> <p>Q. Well, I'm just putting it to you. You're saying you have no knowledge of it, but the recording here in the ATO of the inconsistencies showing that the namings don't match up, they seem to be -- well, they do say that they didn't think a supercomputer existed. That's what their view was. And I'm asking you, do you think there really was a supercomputer or was it all a sham?</p> <p>A. My Lord, I have not seen it. That doesn't mean I can say it was a sham.</p>	
<p>{Day9/145:15-23}</p>	<p>Q. Now can we please go to paragraph 216, which is on page{L11/361/43}. Now, up until now, Mr Yousuf, I've asked you about a wide range of things that C01N was involved in in the period when you were a director and you have said that you know nothing about any of them. Are you aware of anything that was going on in C01N in this tax year?</p> <p>A. I don't -- no, my Lord. I was not involved and I was not aware of, my Lord.</p>	<p>Mr Yousuf confirms that he was not involved or aware of anything going on with C01N during the period that he was a director.</p>
<p>{E/7/4} First Witness Statement of Shoaib Yousuf Mr Yousuf leaving Strasan</p>		
<p>{Day9/149:25} - {Day9/150:21}</p>	<p>Q. My apologies. When you departed ways with C01N, were you bought out in any way? Were you paid to leave your role with C01N?</p> <p>A. No, my Lord. I had an agreement with -- with Dr Craig Wright. I don't -- I was not paid, but we had an agreement of a certain value, I don't remember, that -- that Craig -- Dr Craig will purchase my shares in the company and will pay me certain value, or certain, you know, amount, but I was not paid, my Lord.</p> <p>Q. And how much was that?</p> <p>A. I don't remember exactly, my Lord, but it was around -- I mean, just under -- recollection of my knowledge, around 200 or \$300,000.</p> <p>Q. Okay, we'll come to that in a second. Now, there's no mention in your evidence of any payment, is there, Mr Yousuf?</p>	<p>Mr Yousuf confirms that there was an agreement that Dr Wright would purchase shares in C01N of a certain value when Mr Yousuf left Strasan, but this is not mentioned in his evidence and it was never paid to him.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Payment in relation to, my Lord?</p> <p>Q. There's no mention of any payment or any discussions between you and Dr Wright to have you paid out of your role in Strasan, is there?</p> <p>A. No, I've -- we -- I didn't get paid, my Lord.</p>	
{L9/422/23} Cranston Appendix 1		
{Day9/151:11-20}	<p>Q. If we go over the page {L9/422/23}, the response in this Cranston appendix is in the right column, it says: "The suggestion that the former shareholders do not expect payment is incorrect. Dr Wright expects payment and Mr Yousuf (Shoaib is his middle name) is in regular contact asking when he can expect payment." Is that correct, Mr Yousuf, were you in regular contact with Dr Wright seeking payment, back at this time?</p> <p>A. I don't remember. Not of my knowledge, my Lord.</p>	Mr Yousuf states that he does not remember being in contact with Dr Wright seeking payment for leaving Strasan.
{L17/403/19} Kleiman Exhibits		
{Day9/154:18} - {Day9/155:5}	<p>Q. Does it surprise you that he was trying to buy you out in this way?</p> <p>A. No, my Lord.</p> <p>Q. And you were in fact then paid out, weren't you, Mr Yousuf?</p> <p>A. No, my Lord, I was not paid anything.</p> <p>Q. So are you just saying you just walked away?</p> <p>A. That's correct, my Lord. We had an agreement, I don't remember exact amount, and -- and then I walked out.</p> <p>Q. So you just said you had an agreement, you don't remember the exact amount, so you were paid something to walk away?</p> <p>A. No, I was not paid. I was not paid.</p>	Mr Yousuf stating that he was not paid anything is in contradiction to the document at {L17/403/19}.
{L9/82/6} Australian R&D Activities email		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day9/164:2} - {Day9/165:6}</p>	<p>Q. But why are you being invoiced for work, because of course, you don't invoice a company for your shares, do you, you invoice for work or services provided to a company? So what were you invoicing here to C01N?</p> <p>A. I have not invoiced anything, my Lord, to C01N or -- or Strasan.</p> <p>Q. So, you have no idea why Dr Wright told Ms Aitken that there was £250,000 [sic] of work carried out by you in the period 1 July 2012 to 30 June 2013, do you?</p> <p>A. I -- I don't -- I have no idea, my Lord.</p> <p>Q. And your position is that you didn't carry out any work in that period; is that right?</p> <p>A. My Lord, I'm not sure what work year is being referred. It could be, like, contribution of the initial ten months of the build-out of the company.</p> <p>Q. Well, it can't be anything from 1 January, say, 2013, because of course your LinkedIn profile says it was January 2013. So, this would presumably be referring to a quarter-of-a-million pounds -- quarter-of-million Aussie dollars work in the six months, July 2012 to the end of that year, and you're saying that you did and invoiced for no such work; is that correct?</p> <p>A. Yes, my correct -- that's correct, my Lord. My agreement was the sale of my shares of -- of my -- of my-- of the company to Dr Craig Wright.</p> <p>Q. I accept that, but as I think you agree with me, there's a significant difference between an agreement to buy out somebody's shares and invoicing a company for work; that's correct, isn't it?</p> <p>A. I understand, my Lord.</p>	<p>Mr Yousuf is evasive in response when asked why the email at {L9/82/6} from Dr Wright to Ms Aitken refers to invoicing his work, denying he ever invoiced anything to C01N/Strasan and the agreement was only to sell his shares in the company to Dr Wright.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
DAY 10		
CROSS - EXAMINATION OF DANIELLE DEMORGAN		
{E/8/4} - First Witness Statement of Danielle DeMorgan		
{Day10/11:9-24}	<p>Q. And you say that you later heard the name Satoshi Nakamoto and about Bitcoin, and that Craig was involved, yes? A. Mm-hm. Yes, correct, yes. When -- on the 2008 and I knew he was working with Lasseters because of -- I have a connection with one of the gentlemen from Lasseters, he was one of my old customers, and that's how I knew and remembered it was -- that was probably one of the times I did remember, that he was working on the digital currency.</p> <p>Q. You don't say in your witness statement anything about a digital currency, do you?</p> <p>A No. Well, when I asked -- when I said to them about their connection with Lasseters, they said they already had witness statements from Lasseters, so they didn't take it.</p>	Danielle DeMorgan provides hearsay evidence about Wright's work with Lasseters, but accepts that her statement does not address digital currency.
{Day10/12:23} - {Day10/13:5}	<p>Q. Now, you're aware, aren't you, that many people have been identified in the media and cryptocurrency circles as possible candidates to be Satoshi; is that right?</p> <p>A. I am aware, yes.</p> <p>Q. Do you know about the extent to which any of those are interested in Japanese culture?</p> <p>A. I have no clue. I really don't look into the others all of that much, to be honest.</p>	Danielle DeMorgan accepts that she does not know whether any of the other Satoshi candidates also shared an interest in Japanese culture.
CROSS EXAMINATION OF MARK ARCHBOLD		
{E/11/3} - First Witness Statement of Mark Archbold		
{Day10/15:25} - {Day10/16:8}	<p>Q. And you mention in your statement that you're not a coder {E/11/3}, but what is your technical background?</p> <p>A. My technical background is I've been working in the IT industry since the mid-'80s when it first -- when computers</p>	Mark Archbold accepts that he does not have a technical background.

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>and, you know, Windows first started to arrive on the scene. I -- I hadn't had any formal training, but -- apart from the Sun Microsystems and things like that, but, yeah, that's my background.</p> <p>Q. Thank you.</p>	
<p>{L1/52/1} - Lasseters Tasks</p>		
<p>{Day10/16:25} - {Day10/17:8}</p>	<p>Q. This appears to be a task list of the services that DeMorgan would supply to Lasseters; is that correct?</p> <p>A. Yes. Yes.</p> <p>Q. Do you think you would have written this document, perhaps?</p> <p>A. I think, looking at that, that would have been a collaboration between myself and Craig as to what Craig was -- was proposing --</p> <p>Q. Okay.</p>	<p>Mr Archbold confirms that he and Craig would have set out the tasks list being discussed, which relates to IT security issues with no relevance to digital currency.</p>
<p>{Day10/18:18} - {Day10/19:4}</p>	<p>Q. So it was Lasseters that had the up to date network diagrams, and they were the ones that were going to supply them to DeMorgan; is that correct?</p> <p>A. That's correct. I mean, we -- you know, Craig didn't have sight on what else we were doing, Craig was concentrating on the Check Point firewalls, the Cisco routers, that were part of the overall network design that we'd put in place prior to Craig coming online, and we would modify those where -- where we saw fit and if -- if it wasn't something that Craig needed to look at, we never bothered him with it.</p> <p>Q. Thank you.</p>	<p>Mr Archbold confirms that Dr Wright's work was focussed on firewalls.</p>
<p>{L1/280/1} - 00034805.email</p>		
<p>{Day10/22:3-21}</p>	<p>Q. Yes. Can we now please go to {L5/51/1}. Again, we have another email from Dr Wright, this time April 2009, where you can see him emailing on Sunday 12th, asking: "So how is life in the distant isles?" And again your response above that, you can see: "Hi Craig "How the hell are you [doing], what have you been up to, is this your company or are you contracting." So, again, it looks from this email that in -- and we're jumping now towards 2009, the last email we looked at</p>	<p>Mark Archbold appears to confirm that he and Dr Wright were not in touch much in the early 2000s.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>was 2005 -- so again, is it fair to say in that period that you also were not that often in contact with Dr Wright?</p> <p>A. No, I -- I think that, you know, we'd had a couple of conversations over that, you know, long period of time regarding, you know, what he was up to and -- and things like that. I -- from memory. I mean, I can't be 100% sure.</p>	
<p>{E/11/5} - First Witness Statement of Mark Archbold</p>		
<p>{Day10/28:1-15}</p>	<p>Q. Thank you. Now, this conversation is nearly 20 years ago. You can't be sure of the precise date or words that were spoken, can you?</p> <p>A. No, but I do remember him talking to me, you know, I do remember a discussion regarding digital currency, because, you know, the fiat currencies were being blocked by the US, you know, the Mastercards, the PayPals, and things like that were being not specifically blocked, but they were basically given a message from the US Government, "Don't do it, otherwise you could be in trouble".</p> <p>Q. And, Mr Archbold, there's no mention of any of that in your statement, is there?</p> <p>A. No.</p>	<p>Mark Archbold produces a new account regarding a discussion of digital currency which is not mentioned in his witness statement.</p>
<p>{Day10//28:25} – {Day10/29:10}</p>	<p>Q. Mr Archbold, that wasn't quite my question. I said - and I'll break this down into stages -- you are aware now, are you not, that Dr Wright claims to be Satoshi Nakamoto?</p> <p>A. Yes.</p> <p>Q. Yes. So do you accept that you are looking back at recollection of events from 20 years ago primed with that knowledge? Do you accept that proposition?</p> <p>A. Yes.</p> <p>Q. Thank you.</p>	<p>Mark Archbold accepts that his position on Dr Wright's claim to be Satoshi has been impacted by hindsight.</p>
<p>CROSS - EXAMINATION OF CERIAN JONES</p>		
<p>{E/14/12} - First Witness Statement of Cerian Jones</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{Day10/37:1-6}	<p>Q. Is the majority of your time -- your work time working for nChain?</p> <p>A. Probably, yes.</p> <p>Q. So would you describe yourself as a consultant for nChain?</p> <p>A. Yes, I expect so, yes.</p>	<p>Dr Jones accepts that she works primarily for nChain and that she is a consultant to them.</p>
{Day10/37:15} - {Day10/38:10}	<p>Q. Now, just very quickly on your relationship with Dr Wright. How would you characterise your relationship with Dr Wright?</p> <p>A. Obviously I work with him, as he's associated with my client. I don't work for him, never have done. As I said, he's associated with my client, so he's not my client specifically, although, colloquially, we might say "my client", right? But I am also friends with him and I would like to point out that I am also friends with my other clients as well. As I said, I'm in a very lucky position in that I can work for who I want to and who -- not work for who I don't want to. So, for me, professionally, I only work for people who I think have cool tech and who I think I will enjoy working with. And I am friends with all my clients; I go for lunch, coffee, dinner with my clients, I have been to international rugby matches with them, I've been to nightclubs with them, I have a client coming down in a few weeks' time to go visit a castle together that we are interested in. So Craig Wright is not special in -- in that regard.</p>	<p>Dr Jones concedes that she is friends with Dr Wright.</p>
<p>{E/14/9} - First Witness Statement of Cerian Jones - Page 38</p>		
{Day10/39:9} - {Day10/40:8}	<p>Q. Now, you say you have no professional motivation for adopting the view that Dr Wright is Satoshi, but I would suggest that, given your high level of involvement with nChain and how clearly closely associated you are with them, that you do have a professional motivation that Dr Wright is found to be Satoshi Nakamoto. Would you accept that?</p> <p>A. No. Whatever my Lord decides at the end of this trial will not have an impact on my professional or personal life.</p> <p>Q. And indeed you have regularly appeared at CoinGeek events over the past few years, haven't you?</p> <p>A. What do you mean by "regular"? I mean, I have been at CoinGeek events because I have been required to be there with my work from -- you know, IP work with nChain. So I have been there, absolutely. I mean, regular? You know ...</p>	<p>Dr Jones is evasive, failing to answer the question being put directly to her when pressed on whether she has a high level of involvement with nChain and whether she has a professional motivation for Dr Wright to be found to be Satoshi.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. How many events would you say you've attended in the past few years, or how many nChain-related marketing events have you attended in the past few years, would you say? A. What do you mean by "few years"?</p> <p>Q. Two years.</p> <p>A. Two years? Oh, without my diary in front of me, I don't know. Four? Five? I don't know.</p>	
{L14/68/1} - “The future of BTC” event		
{Day10/40:20-25}	<p>A. I know which event that is, because it's written in the background there. That's the very, very first event that Craig Wright did after the BBC interview, so -- and that was in Arnhem in the Netherlands. So that would have been, I don't know, around about 2017, something like that.</p>	<p>The slide in the background of {L14/68} lists Mr Matonis as being from nChain (in 2017).</p>
{Day10/41:12-18}	<p>Q. You're referred to there as nChain's "lead patent attorney" in that tweet?</p> <p>A. That's probably -- yeah, that's -- that's probably a fair description at that time, because they didn't have in-house counsel at that time. So I -- I was the one that took the brunt of the work with -- with Craig, and the -- and the drafting.</p>	<p>Dr Jones accepts that she was nChain's lead patent attorney in 2017.</p>
{L20/252.37/1} – Capture of “blockchain connected presents in conversation with...”		
{Day10/43:13-22}	<p>Q. So, again, this was an event where Dr Wright's claims to being Satoshi and the basis of BSV being the true version of Bitcoin was being promoted. Do you accept that?</p> <p>A. That blurb will not have been provided by me. It won't even have been provided by UDL or by Technology Connected, it will have been provided by nChain, because all of the speakers will have been asked for a little bit of information to put on the promotional material, and then Technology Connected --</p>	<p>Dr Jones is evasive, failing to answer the question being put directly to her and seeking to distance herself from an event at which Dr Wright's claim to be Satoshi was being promoted.</p>
{L20/252.85/1} – C0003654 – CoinGeek Live 2020 shining a spotlight on intellectual property and blockchain		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{Day10/45:4-10}	<p>Q. And you are aware, are you not, that CoinGeek is an outlet backed by Calvin Ayre and which promotes Bitcoin SV, aren't you?</p> <p>A. I am aware of that.</p> <p>Q. Indeed, it is clear that people associate nChain with BSV from one of the questions below, if we go down the page a bit.</p>	<p>Dr Jones admits that Calvin Ayre promotes CoinGeek and Bitcoin SV.</p>
{O5/2/2} - Transcript of CoinGeek (IP blockchain video)		
{Day10/46:13} - {Day10/47:23}	<p>Q. So, Dr Jones, in this video, you were referred to as "of counsel" at nChain. "Of counsel" is normally the name given to somebody who has some level of internal role at a company. Would you accept that?</p> <p>A. No, I -- that's not my understanding of the term, and I have never been internal at nChain.</p> <p>Q. You're not described there as an external counsel, are you?</p> <p>A. I think that's a term that -- that Jimmy or someone at nChain at the time came up with. I think it was a term that was sort of being used generally to mean a counsel associated with an entity. I don't think there was ever any intention on anybody's part to describe me as being internal. I've never been internal.</p> <p>Q. But you accept that to anybody viewing that, and you didn't correct anybody, I should point out, in this video, do you accept that anybody viewing that would look at that and believe that your job, or your role is associated with nChain and there's nothing there to indicate that you work for anybody else?</p> <p>A. My Lord, when -- when a legal representative, solicitor, patent attorney, whatever, goes to an event and speaks and they're with a client, it's associated with a client's industry or patent portfolio or whatever, they don't say, "Oh, and by the way, my other client list is ...". So, no. You're correct in that, no, I hadn't said, "By the way, I'm external and I also work for lots of other clients", but then you wouldn't expect me to. That moves on very, very quickly, if you look at the video. It's -- that wouldn't be normal to do that.</p> <p>Q. Dr Jones, you're arguing back, but you didn't actually answer my question. My question was: do you accept that the way that was presented would look to somebody that you were a -- you were just working for nChain, or just associated with nChain? That's all I'm asking.</p>	<p>Dr Jones is evasive, failing to answer the question being put directly to her and seeking to argue the case.</p> <p>Her suggestions that she has never been internal at nChain contradict her earlier concession that she was nChain's lead patent attorney.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	A. I think some people could misinterpret that.	
{L20/252.38/3} - Capture of “private investors acquire company behind bitcoin creator Craig Wright”		
{Day10/49:13-24}	<p>Q. Then if we go to the third page {L20/252.38/3}, just above, "nChain's Future Plans", it says: "The patent program at nChain involves some of the most complex technologies we have ever seen, and stands at the forefront of blockchain innovation worldwide', said Cerian Jones, a partner at [UDL] and nChain's lead patent attorney." So, again, I would suggest that here, again, you were being very closely associated with nChain and their patents, and those are obviously very closely associated with Dr Wright. Do you accept that?</p> <p>A. Yes.</p>	Dr Jones accepts that she is very closely associated with nChain.
{L18/109/1} - Capture of CoinGeek (multicast with bitcoin IP expert Cerian Jones tells CoinGeek backstage)		
{Day10/51:7-10}	<p>Q. So it's quite clear, do you accept, that you are associated with nChain and Dr Wright and nChain is very closely associated with Dr Wright's patents?</p> <p>A. I accept that.</p>	Dr Jones accepts that she is very closely associated with Dr Wright, and nChain.
{Day10/53:12} - {Day10/54:8}	<p>Q. Dr Jones, I'm not saying that you have been involved in any inflation of numbers, I'm just trying to clarify, based on your expertise, you're a patent attorney and you're nChain's patent attorney, there's been a lot of comment about the number of patents in this case and I'm trying to establish what you believe is a more accurate way to refer to a measure of innovation; is it by counting patent families or by counting individual patents?</p> <p>A. Well, first of all, I would say that it's a more accurate way - - if you're talking about granted patents, then you give the number of patents. If you're talking about patent families, you talk about number of patent families. But I just want to correct you on something there. You just referred to me as nChain's patent attorney. That is not correct. I'm not Craig Wright's patent attorney, I'm not nChain's patent attorney. I have multiple clients. I am not -- I do not belong to nChain, I do not -- I'm not employed by nChain and I don't think it is -- I think</p>	Dr Jones agrees that Mr Moss' method for counting patents is accurate, but seeks to argue Dr Wright's case by asserting that she is not nChain or Dr Wright's patent attorney.

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>it's actually misleading to refer to me as nChain's patent attorney. I know that sometimes people do that, but it's not actually correct.</p>	
<p>{Day10/54:21} - {Day10/55:7}</p>	<p>Q. Now, of the nChain patents where you were the recorded representative when you were at UDL, how many granted patents were you involved in where Dr Wright was named as the sole inventor?</p> <p>A. Oh, gosh. Just so that I'm really clear what you're asking me, and bearing in mind, I don't have access to those -- to those figures. You know, because I'm not internal, I do not have access to nChain's internal systems and I don't have access to my previous firm's data either, so you are asking me something off the top of my head now, right? So I can have a go at answering it, but ...</p>	<p>Dr Jones claims not to know how many of nChain's granted patents (where she was the recorded representative at UDL) solely listed Dr Wright as the inventor.</p>
<p>{Day10/55:17} - {Day10/56:16}</p>	<p>Q. Again, according to our research, this is six and this is only -- this is all publicly available information. Now, every other patent that involves Dr Wright has another inventor on it ; isn't that correct? All the nChain ones I'm talking about here.</p> <p>A. That's correct. And -- yeah, that is correct. There are some names --I'm talking about right in the early days now, right? Because for the last -- what was it, since about 2018,I've really been quite at arm's length in the sense that, in about 2018, they brought Will Chelton on board, they had internal counsel, so I very much stepped back, my role completely stepped back from nChain, I'm much more of a contractor, external entity in the sense that, you know, there was -- there was much more going on internally, in terms of process and all the rest of it . But in the very early days, there were some researchers whose names were added. I think it was kind of an internal convention, and I don't know that this is unique to nChain, a lot of companies will add researchers and so on as named inventors, as -- as a sort of a kudos to them. But whether or not they are the original deviser of the inventive concept, you know, I don't know. But the convention was to name the researchers who'd worked on the White Paper originating from the original OI.</p>	<p>Dr Jones suggests, implausibly, that she is at 'arms length' from nChain despite her previous concession that was nChain's lead patent attorney and remains closely associated with nChain and Dr Wright.</p>
<p>{Day10/57:5-12}</p>	<p>Q. And it is not unusual for this to happen maybe once or twice, but based on your experience in the industry, would you accept that for it to happen over 60 times is unusual?</p> <p>A. It speaks of an internal policy change, or - or something that's gone on, but I can't - I can't speculate as to what did or did not happen internally at meetings, or whatever, that I was not party to.</p>	<p>Dr Jones is evasive, failing to answer directly the question that is being put to her about whether it is unusual for Dr Wright to be added to patents</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
		as a co-inventor after grant.
{E/14/4} - First Witness Statement of Cerian Jones		
{Day10/58:23} - {Day10/59:14}	<p>Q. Okay. Now, I want to put it to you that anyone that invents anything in relation to Bitcoin or the blockchain simply has no bearing on whether that person is Satoshi Nakamoto. Do you accept that?</p> <p>A. Sorry, are you - are you asking if somebody gets a patent granted for a blockchain-related technology, that doesn't mean that they're Satoshi?</p> <p>Q. Yes.</p> <p>A. Yeah, I would agree with that.</p> <p>Q. What I'm trying to establish is, there's a lot of evidence in your statement about these patents, and what I believe your evidence is, is that these patents are things that you think show that Dr Wright could be Satoshi Nakamoto. If that's not the case and they have no bearing on it, say so, but they're in your evidence.</p> <p>A. I think so, in my opinion.</p>	Dr Jones accepts that whether an individual has invented something in relation to Bitcoin or the blockchain has no bearing on whether that person is Satoshi Nakamoto, contradicting her position in her witness statement
{E/14/9} - First Witness Statement of Cerian Jones		
{Day10/60:2-8}	<p>Q. -- why it's in here.</p> <p>A. Yes, because I was trying to explain how his IP, in my opinion -- I was trying to tie his IP and his way of thinking to the Satoshi Nakamoto question, as -- as an indication that it's the sort of thing that I think is aligned with or chimes with someone who's thinking about Bitcoin and potentially the developer of it.</p>	Dr Jones demonstrates that she sought to present her witness evidence in order to support a pre-determined conclusion.
{E/14/5} - First Witness Statement of Cerian Jones		
{Day10/61:18} - {Day10/62:7}	Q. But just before we go there, I want to ask you, because you refer to the EPO written opinion in paragraph 15 of your	Dr Jones accepts that the quote included is

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>statement in relation to this {E/14/5}. Now, the EPO written opinion is a standard document that sets out the prior art; correct?</p> <p>A. Correct.</p> <p>Q. And you point out that the examiner regarded the invention as being "novel and inventive"; correct?</p> <p>A. Correct. Can I just point out that I didn't draft or prosecute this application.</p> <p>Q. I know that. Thank you. But you point out that the examiner regarded it as "novel and inventive", but of course novel and inventive is the case for all granted patents?</p> <p>A. Correct.</p>	<p>standard in patent documentation.</p>
<p>{L20/351/3} - EPO Written Opinion</p>		
<p>{Day10/63:9-21}</p>	<p>Q. You do, in paragraph 15. So, what you don't mention in your evidence, because you rely on this written opinion, but what you don't mention -- and we don't need to go there, but for everybody's reference, this is {L20/351/3} at paragraph 9, what you don't mention is that the EPO written opinion recorded that it does not meet the requirements of Article 6 of the patent, the PCT because claims 1, 16, 18, 20, 24, 39 and 40 are not clear, so there was a clarity objection to all of those claims. You don't mention that in your statement, do you?</p> <p>A. No, I think that's an omission on my part.</p>	<p>Dr Jones accepts that her statement omits important information about the validity of a patent that she has sought to rely on in her witness statement as evidence that Dr Wright is Satoshi.</p>
<p>{Day10/63:25} – {Day10/64:20}</p>	<p>Q. And as you're well aware, when patents come to being litigated, there are obviously much broader searches that can be carried out, because an EPO search is intrinsically limited by a certain amount of budgetary constraints; correct?</p> <p>LORD GRABINER: My Lord, again, I apologise for intervening. What is the relevance of this? We want to know about the identity of Satoshi Nakamoto, not about this witness's knowledge of patents or the detail of some particular patent application.</p> <p>MR JUSTICE MELLOR: You've led this evidence.</p> <p>LORD GRABINER: Well, I may have done, but --</p> <p>MR JUSTICE MELLOR: There's quite a lot of detail in here about number 42, for example, so I'm going to allow some questioning to continue.</p>	<p>Dr Wright's leading counsel suggests that Dr Jones' evidence is 'supremely irrelevant' to the identity issue.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>LORD GRABINER: My Lord, I completely agree that this is in the evidence, but it is supremely irrelevant to the issues that your Lordship is concerned with in the trial.</p> <p>MR MOSS: My Lord, with that last point from Lord Grabiner, I fully and wholeheartedly agree. However --</p>	
<p>{L2/6/1} 06102105 DeMorgan Patents Road Map</p>		
<p>{Day10/69:25} - {Day10/71:5}</p>	<p>Q. Now, I'm not going to go through it, but if we go through the rest of this schedule -- this can be a point for closings, but just so everyone understands the point -- if you go through the rest of this, Dr Wright is listed fewer times than Mr Savannah. Indeed, we believe there's 12 for Dr Wright -- one is "Craig + Tech" -- and 30 for Mr Savannah. So, on the internal records, it would suggest that Dr -- that Mr Savannah was the person involved in coming up with this invention; do you accept that?</p> <p>A. Again, I have -- I've never seen this document before. I don't know how, when, why, or who by this was created. I don't feel that I can comment on this. I don't know what -- what the authors were intending or trying to do at this time. This is completely unknown to me.</p> <p>Q. Just one last question then before lunch. You have relied on number 42 in your evidence --</p> <p>A. Mm-hm.</p> <p>Q. -- as being an example of something that you believe is evidence towards the fact of Dr Wright being Satoshi Nakamoto, but I've just shown you a number of documents, internal documents, that show that actually it was Mr Savannah that was involved. Do you accept that it's possible that actually the real inventor behind number 42 was Mr Savannah and not Dr Wright?</p> <p>A. "Possible" and actual fact are very different things, aren't they.</p> <p>Q. Do you accept it's possible?</p> <p>A. Lots of things are possible, but I don't know that they're -- that they're true, or even -- or even likely. It is possible. I agree with you that it is possible.</p>	<p>Dr Jones is evasive, failing to answer the question being put directly to her and seeking to argue the case. When pushed she concedes that it is possible that the real inventor behind number 42 was Mr Savannah and not Dr Wright.</p>
<p>{Day10/73:1-19}</p>	<p>MR MOSS: So just one last question in relation to the other patents you rely on. Do you know who the co-inventor is of the other two patents that you rely on in your evidence?</p> <p>A. Not off the top of my head.</p>	<p>Dr Jones accepts her evidence relates to patent drafting and filing, rather than who</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. So, it was Mr Savannah for 222, and Mr Jiménez Delgado</p> <p>A. My Lord, can I -- can I just point out -</p> <p>Q. -- for 32?</p> <p>A. -- we drafted and filed those patent applications. We would ask -- when we were going to file a patent application, we would ask, "Who are the named inventors going to be", and we filed based on clients' instructions. I have no -- no internal knowledge, no -- I have never had any access to any internal documents or systems at nChain, I wasn't party on, you know, management, or invention meetings, or policies, or any of that internal stuff. I worked with the inventor to -- to draft and file patent applications. It's -- it's as narrowly defined and constrained as that.</p>	<p>was behind the inventive concepts.</p>
<p>{Day10/74:4-16}</p>	<p>Q. -- suggested(?). So if I can just clarify what you've just said. You're accepting that you're taking the information about who invented this on face value from nChain; is that correct?</p> <p>A. That is correct. But can I just say that there were times when we were stood in front of a whiteboard with Craig, and he would step through the invention that was to be protected, and then we would draft and file it. So -- so there's a difference there between those inventions and the ones that you're talking about on lists that -- that were drawn up before I'd even met the chap.</p>	<p>Dr Jones agrees that she is accepting the information about who invented patents at face value from nChain.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
DAY 11		
CROSS-EXAMINATION OF DAVID BRIDGES BY JONATHAN HOUGH KC		
{L17/473/3} Transcript of David Bridges' evidence in Granath v Wright Proceedings		
<p>{Day11/3:16} – {Day11/4:18}</p>	<p>Q. Page 3, please {L17/473/3}, lines 48 and following, do you see you were asked by a lawyer what Dr Wright did to help the bank when he was with BDO, and --</p> <p>A. Yeah.</p> <p>Q. -- you're recorded as saying this at line 50: "Yeah, so initially . was with BDO I met auditors from a security perspective, so he did a full audit..of the bank in terms of where, I guess our vulnerabilities and weaknesses from a security perspective were. He also at a lighter stage ." I think that might be "later", somebody mistranscribing your Australian accent.</p> <p>A. (Inaudible).</p> <p>Q. ". he then started doing similar tests on our third parties -- I'm not sure of the parties .. to assess their security standard .. their vulnerabilities, weaknesses .. and such." Is that a fair summary of the work he did for the bank while he was at BDO?</p> <p>A. Yeah, that's -- that's pretty much spot on.</p> <p>Q. Now, you then say in your witness statement that after Craig Wright left BDO, your bank engaged him as a consultant to help --</p> <p>A. Correct.</p> <p>Q. -- to, as you put it {E/9/4}, "help us uplift.. security at the bank", working in your offices every week or two; is that right?</p> <p>A. Absolutely.</p>	<p>Mr Bridges describes Dr Wright's work at BDO, which was in the field of IT security.</p>
{E/9} Witness Statement of David Bridges		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day11/5:25} – {Day11/6:16}</p>	<p>Q. So that, just so we understand this correctly, the parallel you were drawing between the event logger system that Dr Wright worked on and blockchain --</p> <p>A. Yeah.</p> <p>Q. -- technology is that both systems keep a record of transactions and there is good traceability in both systems; is that right?</p> <p>A. Yeah, it would be the traceability and the immutability, right? So if you deleted something, you had a copy of the deletion, effectively.</p> <p>Q. So the parallel you're drawing is that conceptual one, you're not saying that the two shared code in common or specific forms of technical feature?</p> <p>A. Oh, I wouldn't know, mate. On that level, that's -- that's out of my realm, from that perspective. I can tell you how it worked and how we used it, but that's -- yeah, but if you're going that level, that's like next.</p>	<p>Mr Bridges accepts that he does not know anything about blockchain technology, demonstrating little technical understanding.</p>
<p>{Day11/6:22}- {Day11/7:9}</p>	<p>Q. Well, Dr Wright’s lawyers have identified nearly 100 documents representing emails he sent to you and their attachments, and for the lawyers –</p> <p>A. He did.</p> <p>Q. For the lawyers in the room, that’s ID_006367 straight through to ID_006463. Does that strike a cord with you, nearly 100 documents representing emails and their attachments?</p> <p>A. He – he – he certainly sent me a lot of things and gave me a lot of things. I didn’t read them all and even the ones I read, I probably didn’t quite understand, but he certainly put a lot of things on my table or emailed me and .. yeah.</p>	<p>Mr Bridges accepts that he had no technical ability to understand the documents that Dr Wright sent him, and that he had received so many attachments that he did not read them all.</p>
<p>{L6/170/1} ID_006373 Email from Dr Wright to David Bridges {L6/171} Attachment to the email – IWSEC 2010(5).docx</p>		
<p>{Day11/8:11} - {Day11/9:3}</p>	<p>Q. Then {L6/170/1}, 8 April 2010, an email offering you, charitably, a bit of "bed time reading to help you sleep"?</p> <p>A. Yeah, that's correct.</p> <p>Q. The attachment -- the attachment is at {L6/171/1}. If we see the introduction is at page 2 {L6/171/2}, examining the impacts of different approaches to enforcing software security in relation to bugs in software. Do you recall getting that through, or is that just another that you may have received but you're not sure?</p>	<p>Mr Bridges accepts that he cannot recall whether he received the emails as he does not have them anymore.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Yeah, it's -- it -- I'd definitely say it's most likely if you -- if you've got the emails there and that, I'd -- I'd say, yeah, there's a good chance that he sent that through. It seems very relevant to what we were doing at the time. But, again, I don't have -- I don't have those emails any more from the bank, so I couldn't give you the "hey, guarantee you".</p>	
<p>{Day11/9:12-19}</p>	<p>Q. Well, no, just focusing on the documents that we had, we know that we've had a lot of documents which are focused on IT security, document forensics and legal subjects.</p> <p>A. Yeah.</p> <p>Q. You're not able to dispute that those subjects were subject on which he sent you lots and lots of papers?</p> <p>A. Yeah, if you -- if you're talking about those subjects, yeah, absolutely, he -- he sent those.</p>	<p>Mr Bridges confirms that Dr Wright sent him many papers on the topics of IT security, document forensics and legal subjects.</p>
<p>{E/9} Witness Statement of David Bridges</p>		
<p>{Day11/11:5} – {Day11/12:19}</p>	<p>Q. Moving on from that subject, we're going to a matter discussed in your witness statement. You say this, that while Dr Wright was working as a consultant for the bank --</p> <p>A. Yes.</p> <p>Q. -- so after he'd left BDO --</p> <p>A. Yeah.</p> <p>Q. -- he suggested an idea to you concerning your inter bank payment system; is that right?</p> <p>A. That's correct.</p> <p>Q. And that was when he was a consultant, after he'd left BDO, right?</p> <p>A. Yeah, that's right.</p> <p>Q. Now, we're not aware of there being any documents relating to this idea being put to you and you don't refer to any in your witness statement. Is it right to say that you don't have any?</p> <p>A. I -- yeah, I don't have copies of any documents, I don't think. Did he give us one at the time? Again, it's possible, because I introduced him to the CEO and the CFO, so we would have probably went into that meeting with something</p> <p>Q. But in fairness to you, what you're now doing in relation to this interbank payment system idea is recalling something he discussed 15 years ago without any documents to help you recall; is that fair?</p>	<p>Mr Bridges is evasive; failing to answer directly the question that is being put to him. The question here was not about the document on the screen (which was still the LLM proposal at {L15/442/1}), but rather, it was about Dr Wright suggesting an idea to Mr Bridger about his inter-bank payment system (after Dr Wright left BDO, when he was a consultant). However, Mr Bridges answers by reference to the document on screen ("When I read this document").</p> <p>Mr Bridges also confirms that he does not have any documents relating to the inter-bank payment</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. We're discussing -- yeah, we had the chat about -- it would have been about 15 years ago. What -- sorry, what's the point you're trying to make, sorry?</p> <p>Q. Just this, that when you try to recall this in your witness statement, you're looking back on a conversation 15 years ago and you don't have any documents to help your recollection?</p> <p>A. When I read this document, I -- it certainly triggers things and I -- okay, yeah -- no, that sounds like the conversations we had with the CEO and the CFO, particularly, as I said, things around, like, removing the intermediary, being able to do the - - the payments in a quick and efficient way. So those things certainly triggered memories from -- from those meetings.</p>	<p>system idea from Dr Wright.</p>
<p>{Day11/14:4-16}</p>	<p>Q. And again, you're not saying that there were specific technical features of what was being proposed that were common to what the Bitcoin System has adopted, are you?</p> <p>A. There's not specific technical, as in .. like, a -- sorry, I'm not quite following what you mean in terms of "specific technical".</p> <p>Q. What you say it had in common was just that it had a secure ledger or record system that couldn't be broken --</p> <p>A. Yeah.</p> <p>Q. -- you're not referring to specific detailed technical IT features, are you?</p> <p>A. Yeah, no, that's beyond me.</p>	<p>Mr Bridges concedes that he has no technical knowledge of Bitcoin.</p>
<p>{Day11/15:9} – {Day11/17:13} {L17/473/8} Transcript of David Bridges’ evidence in Granath v Wright Proceedings</p>	<p>Q. -- moving on to another subject, you describe discussing Bitcoin with Dr Wright shortly after an event which is important to the -- those interested in cryptocurrencies, which was the --</p> <p>A. Yeah.</p> <p>Q. -- time a person offered an amount of money -- amount of Bitcoin for a pizza and somebody else accepted and pizza was duly delivered; do you remember that?</p> <p>A. Yeah, yeah, I remember that, yeah.</p> <p>Q. And as you say in your witness statement, that event took place in May 2010, didn't it?</p> <p>A. I believe so.</p> <p>Q. Now, based on the evidence you gave in the Oslo case, that was the first time you ever heard Dr Wright -- Craig Wright used the word "bitcoin"; is that right?</p> <p>A. Yeah, yeah, that would be right.</p>	<p>Mr Bridges agrees that May 2010 was the first time he had ever heard Dr Wright use the term Bitcoin. This is inconsistent with Dr Wright’s RFI response, in which he states that he provided a draft of the White Paper to individuals including David Bridges (Fourth Witness Statement of Dr Wright, {E/4/21}).</p> <p>Mr Bridges also concedes that he had no knowledge of Bitcoin or how cryptocurrencies worked before the conversation in May</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. May we have on screen {L17/473/8}. If we look at the bottom of the page, this is how you put it in the Norway proceedings: "So, I remember it quite well. So, we were in the office and Craig showed us how this guy had done .. a Bitcoin payment to a pizza place, we were like, okay .. what the hell is Bitcoin? And he explained everything and okay, well then, we're like how .. the hell does this work? And then .. [he] pulled up his laptop and he had this thing called a digital wallet. Everyone knows what a digital wallet is now, but I remember cause it wasn't on your phone, it was on the laptop. So, he showed us this digital wallet, this is -- this is different. How does it all work? And he took us to the process and said it was a little bit complicated obviously at the time, but he explained that yeah, you had this .. this digital cash and you can transfer it to somebody as a form of payment, I liked that. Okay, very interesting. That was probably yeah, the really the first time that we started talking about Bitcoin." Is that right?</p> <p>A. Absolutely.</p> <p>Q. So, based on what you said there, you had no knowledge of Bitcoin or how cryptocurrencies worked before that conversation; is that right?</p> <p>A. Yeah, I wasn't really interested, to be honest with you. I mean, it was like this thing happened, I was like oh yeah, it's pretty cool, bit of a novelty. Obviously the digital currency aspect piqued our interest, okay, yeah, it was quite -- quite fun, wasn't it, really? It hadn't been done before.</p> <p>Q. And that was the end of the conversation, yes?</p> <p>A. Yeah, he showed us the -- like we sat down and watched -- had a look on his -- his laptop, and then he showed us how a digital wallet worked and everything, and as I said, he -- it wasn't quite like your GUI style now, it was just on a laptop with basically green screen feel -- look and feel, effectively.</p>	<p>2010, and had little interest in the subject.</p>
<p>{Day11/19:21} – {Day11/21:6}</p>	<p>Q. Final topic. Towards the end of your statement, you say that you had a discussion with some other people about Craig and Satoshi Nakamoto when the topic was in the news. Do you recall that?</p> <p>A. Yeah. Yeah, we were blown away.</p> <p>Q. And you say that that was in December 2015, right?</p> <p>A. I believe so.</p> <p>Q. So that would have been after articles had been published on the subject; is that right?</p> <p>A. Yeah, it was -- there was a big news flash over here. It was on -- you know, you had every news channel had it. There was a lot of coverage and everyone's going wild, so we were in the</p>	<p>When asked whether Mr Bridges is aware of any other candidates for Satoshi, he displays little knowledge or interest.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>boardroom having conversations, "Is it him? Is it him? Oh, it's him, isn't it?".</p> <p>Q. And you say in your statement that what made you think it was him was his love of Japanese culture and his education. You say that in your statement, don't you?</p> <p>A. I believe so, yeah.</p> <p>Q. Now, are you aware that quite a lot of other people have been identified in the media and in cryptocurrency circles as possible candidates to be Satoshi? Are you aware of that or not?</p> <p>A. I don't really follow it, to be honest with you.</p> <p>Q. So presumably --</p> <p>A. Like I said, I could've bought -- I wish I'd bought it, maybe, back then would have been lovely, but I didn't do it and I haven't done it, and you know what, I --</p> <p>Q. So you don't --</p> <p>A. -- prefer to (loss of audio) that way.</p> <p>Q. So you don't know anything about any of those other people?</p> <p>A. Not really, to be honest with you, mate, and like .. I know the -- the other Russian fellow that does the other one, but otherwise, you know, I'm not -- I'm not a -- I'm not a -- I'm not a fanboy or anything like that.</p>	
<p>CROSS-EXAMINATION OF MAXWELL LYNAM BY JONATHAN HOUGH KC</p>		
<p>{L2/491/1} Email from Max Lynam to Craig Wright</p>		
<p>{Day11/25:14} – {Day11/26:2}</p>	<p>May I now discuss with you the two email communications we have between you and Craig in our disclosure from 2008, and the first will come up on the screen in front of you. It's {L2/491/1}. Now, we can't say whether this document is authentic ourselves, because it hasn't been forensically examined, but it's a document in Craig Wright's disclosure. This appears to be, in the bottom part, an email from Craig on 20 May 2008, tooting his horn, as he puts it, about his accomplishments. Do you remember receiving an email of this kind?</p>	<p>When asked whether he remembers receiving the email at {L2/491/1} regarding Dr Wright's accomplishments, Mr Lynam thinks he would have received something "along those lines", but is not able to give a definite answer.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Yeah, I would have received something along those lines, because Craig would update us with that sort of stuff every now and then.</p>	
<p>{L3/321/1} Email from Craig Wright to Don Lynam and Julie Laimer</p>		
<p>{Day11/27:4-24}</p>	<p>Q. -- {L3/321/1}. We're going to look at another email that we have in the disclosure. Again, we haven't positively authenticated it, but it appears to be, at the top of the page, an email from Craig Wright to family members, Don Lynam, his uncle, Julie Laimer, I think is his mother, and then you and his wife copied, dated 12 December 2008; do you see that?</p> <p>A. Yeah.</p> <p>Q. And he refers to going to present a paper at an academic conference in Hyderabad; do you see that?</p> <p>A. Mm-hm.</p> <p>Q. And then he refers --</p> <p>A. Yes.</p> <p>Q. -- further down, to starting a second doctorate, yes?</p> <p>A. Yeah.</p> <p>Q. And having sat a GSE malware exam in Las Vegas?</p> <p>A. Yeah.</p> <p>Q. Is it fair to say that from both those emails, what he was talking about were -- in terms of actual work and projects, were IT security and digital forensics?</p> <p>A. Yes.</p>	<p>Mr Lynam affirms that the emails at {L3/321/1} concerned IT security and digital forensics.</p>
<p>{O3/3/7} Transcript of Max Lynam's evidence in Granath, October 2022</p>		
<p>{Day11/30:3-7}</p>	<p>And you describe getting the code running. Now, you refer to that, at least when it was first presented to you, as an unknown bit of code you were running; is that right?</p> <p>A. Correct.</p>	<p>This refers to code that Dr Wright requested Mr Lynam to run and test in late 2008. Mr Lynam confirms that the details of the code were unknown to him.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{E/13} Witness Statement of Maxwell Lynam		
{Day11/32:7-25}	<p>Q. Then paragraph 21, at the bottom of the paragraph, you say this -- sorry, paragraph 21, at the top of the paragraph, you say this: "At the time, I understood the code to be validating transfers and validating cryptographic keys ..." Then you say this: "It was a little bit like the hacking stuff Craig had been doing and very much like the transactions he'd been doing for Lasseters .." Now, "the hacking stuff", was that a reference to White Hat or ethical hacking?</p> <p>A. Oh, and the stuff that we just used -- that people used to do to each other as well. You'd just send messages backwards and forwards and ping backwards and forwards and do authorisation or not authorisation, the same way it works now, just --</p> <p>Q. But the hacking stuff Craig had been doing was White Hat or ethical hacking --</p> <p>A. Yeah.</p>	Mr Lynam is asked about the "hacking stuff" Dr Wright had been doing but displays little knowledge of it.
{Day11/33:18} – {Day11/34:10}	<p>So all I was putting to you, Mr Lynam, was that in your witness statement, you draw a connection between the code that you were running and "the hacking stuff Craig had been doing", and I was suggesting to you that "the hacking stuff" was White Hat or ethical hacking to probe the IT security vulnerabilities of a system.</p> <p>A. So, yeah, it was authorisations. So, you know, whether you're – when you're trying to get into a system, you need to have passwords and stuff like that, so you need authorisations, and the keys need to go backwards and forwards, and that's the same thing for the cryptographic keys is exactly the same as well for when you're doing that as well. So it's all related to the same body of work and expertise that Craig had been working on.</p> <p>Q. Now --</p> <p>A. And so that's what the program was. It was working with something to do with that.</p>	Mr Lynam's answer seeks to argue the case; straining to draw parallels between his knowledge of Dr Wright's work in "hacking stuff" and cryptography.
{Day11/34:15} – {Day11/35:7}	<p>Q. And you didn't say in your evidence in Norway that you'd been sworn to secrecy about the running of that code, did you?</p> <p>A. No.</p> <p>Q. As far as you knew, you could tell anyone that you were running Craig for code or that your father was?</p> <p>A. I could, yeah.</p>	Mr Lynam confirms that Dr Wright did not give him or his father any instructions to treat the code that he was asked to run as confidential.

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. And as far as you and your father knew, anyone could look at the code that was being run?</p> <p>A. Well, I wouldn't have thought so, because Craig sent it to us, so Craig had it, we had it –</p> <p>Q. But in --</p> <p>A. -- it was -- I'm not sure who else had it. I don't think it was listed publicly anywhere, because it was still testing code.</p> <p>Q. But he didn't stress to you that it was confidential and nobody could come and look at it?</p> <p>A. No.</p>	
<p>{Day11/35:8} – {Day11/36:3}</p>	<p>Q. Now, we can take that off screen. In the course of making your witness statement, somebody showed you a copy of the Bitcoin White Paper, didn't they?</p> <p>A. Yeah.</p> <p>Q. And you said you couldn't recall Craig ever sending you that document?</p> <p>A. I said we had received numerous documents and bits of information from him. That could have been one of them.</p> <p>Q. But you couldn't --</p> <p>A. They were all pretty similar.</p> <p>Q. You couldn't single that out from many documents Craig had sent you?</p> <p>A. No, because it was all talking about the same things.</p> <p>Q. And you don't describe particular contents of that paper in your witness statement, do you?</p> <p>A. No. I wasn't asked about it.</p> <p>Q. You're not somebody yourself who have a detailed understanding of cryptocurrencies, are you, Mr Lynam?</p> <p>A. Detailed, no. Fundamental, from an IT systems perspective, yes.</p>	<p>Mr Lynam confirming that he could not single out the Bitcoin White Paper from the many documents Dr Wright sent him as they were “all pretty similar”, demonstrating that he appears unable to distinguish between basic IT security topics and the Bitcoin White Paper.</p> <p>Mr Lynam also confirms that he does not have a detailed understanding of cryptocurrencies, but does have a “fundamental” understanding from an IT systems perspective.</p>
<p>{Day11/36:12} - {Day11/37:9}</p>	<p>Q. You haven't retained any of Craig Wright's messages that he sent you over the years, the emails or messaging applications discussing particular ideas, have you?</p> <p>A. Well, it would be almost impossible to do so in that the companies that we used for messaging back then have been sold two or three times and not even any of the user names work any more, let alone a record of the messages. The email server and domain that we used during that period of time when we were on the farm was disposed of and the servers shut down, and the other methodologies that we used for messaging</p>	<p>Mr Lynam confirms that his evidence is based solely on his recollection, without any documents from the time to refresh his memory (other than what has been supplied by Dr Wright's counsel).</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>back then were IRC and other instant messaging that doesn't have a history available, it was just direct messaging. So there would be no way for us to be able to have that unless I purposely took back-ups for some reason, which at that point in time I didn't really think there was any reason to take back-ups of everything and keep it for the next, you know, 12/15 years or whatever it is.</p> <p>Q. Mr Lynam, I'm not criticising you for a moment. I'm just making this point: you have had to give your evidence, understandably, without any documents from the time to refresh your memory, haven't you?</p> <p>A. That's correct. Apart from what's been supplied.</p>	
<p>{Day11/37:15} – {Day11/38:4}</p>	<p>Q. May we move on then to another subject, which is a dinner you had with Craig and his new wife, Ramona, in 2013 {E/13/7}.</p> <p>A. Mm-hm.</p> <p>Q. In your statement, you say that you'd heard the term "bitcoin" before this dinner; is that right?</p> <p>A. Correct.</p> <p>Q. So, by that stage, had Bitcoin started to feature in the news that you were watching?</p> <p>A. Well, I was in the tech industry, so it was part of what people talked about in the tech industry.</p> <p>Q. But at that stage, you didn't understand that the code that you had been running had anything to do with Bitcoin, did you?</p> <p>A. Well, not directly, no, I guess.</p>	<p>Mr Lynam confirms that despite being aware of Bitcoin by 2013, he was still unaware that the code he had been running for Dr Wright had anything to do with Bitcoin.</p>
<p>{Day11/39:8} – {Day11/41:7}</p>	<p>Q. So based on that answer, you had no idea what mining Bitcoin was before you went to that dinner; that's right, isn't it?</p> <p>A. That's correct.</p> <p>Q. And up until that time, you didn't think your running of computers for Craig was earning rewards in digital currency, did you?</p> <p>A. That's correct.</p> <p>Q. And before that dinner, you didn't have any belief that Craig had invented Bitcoin? Because you didn't even know what Bitcoin mining was?</p> <p>A. Well, before the dinner, no.</p> <p>Q. Now, were you aware that around the time –</p>	<p>Mr Lynam confirms that he did not know what "mining Bitcoin" was before the dinner in 2013, and he did not have any belief that Dr Wright invented Bitcoin before then.</p> <p>Despite being asked about Bitcoin, Mr Lynam then discusses the difference between blockchain and Bitcoin (displaying confusion between the two), although his evidence does not suggest that</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Sorry, I think – I think it’s probably a difference between blockchain and Bitcoin. So, I knew he’d been doing stuff with blockchain, but I didn’t know that we’d been mining Bitcoin. So blockchain was – is – is different to Bitcoin’s like a – a currency, like, you know, all the other blockchain currencies and stuff like that.</p> <p>Q. Well, we’ve already established that at the time you were running the code, as far as you were concerned, it was an unknown bit of code, wasn’t it?</p> <p>A. So, it was code that was validating the cryptographic keys, like I said before. It was validating the cryptographic keys. I knew, by that stage, that it had had something to do with blockchain, because it was the stuff that was underlying Bitcoin and whatever else was around at that stage.</p> <p>Q. Now, Mr –</p> <p>A. And so the blockchain stuff, I was aware that Craig had had stuff to do with. Bitcoin itself, I didn’t know we were running a Bitcoin mining application on our computer, but for it to be doing the transaction authorisation and so forth, I was aware that it was doing that type of thing, but not mining Bitcoin, which is a different thing.</p> <p>Q. Mr Lynam, you don’t say in your witness statement, and you didn’t say in your evidence in Oslo, that you were aware of Craig having produced something called blockchain before 2013, do you?</p> <p>A. I would believe that in my statement in Oslo where I was talk – where I was asked specifically about the White Paper, I’d been specifically asked about the White Paper and what it was. I didn’t know that it was Bitcoin, but the concept around blockchain, whether it was called that at the time or whether it was called something else, that concept around that and what had been done with it, that had been something that I was aware Craig was doing.</p>	<p>Dr Wright mentioned the term blockchain to him before the White Paper.</p>
<p>{L7/210/2} WKID Memo</p>		
<p>{Day11/43:18} – {Day11/44:4}</p>	<p>Q. So you weren’t aware of David Kleiman having records of mining from machines owned by your father, were you?</p> <p>A. No.</p> <p>Q. Second page, please {L7/210/2}, one-third down: “DK ..” That’s an abbreviation for David Kleiman: “.. holds other assets and maintains a list of owners (including himself and</p>	<p>Mr Lynam confirms that he was not aware of David Kleiman having records of mining from machines owned by his father (Don Lyman), nor was he aware of an</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>esp. ..." Presumably "especially": "... Don Lynam)." Again, that wasn't an arrangement you knew about?</p> <p>A. No.</p>	<p>arrangement between David Kleiman and his father.</p>
<p>{L7/195/13} W&K Operating Agreement</p>		
<p>{Day11/44:15} – {Day11/45:11}</p>	<p>Q. Page 13, please {L7/195/13}. By letter B, there is a clause dealing with what happens if the company is wound up, and do you see at (i), halfway down the page that's on screen, it says that: "Assets, including all token assets held in trust by the members of W&K for the originating third parties will be distributed in accordance with the initial allocation of CPU power used in the creation of the system. These parties include: "Wright International Investments Limited "Lynn Wright "Don Lynam "Max Lynam "Julie Laimer [and] "Gareth Williams" We see you're named along with a British security services agent called Gareth Williams.</p> <p>A. Mm-hm.</p> <p>Q. Were you aware, or did you ever think that you might receive a distribution of a company's assets as a result of you running bits of code for Craig?</p> <p>A. No.</p>	<p>Despite being named in the W&K Operating Agreement as an originating third party, Mr Lynam states that he was not aware that he would be receiving a distribution of the company's assets.</p>
<p>{E/13} Witness Statement of Maxwell Lynam</p>		
<p>{Day11/45:12} – {Day11/46:11}</p>	<p>Q. We can take that off screen now. Now, you say that, in late 2015, you discovered that Craig had been publicly identified in some magazines as Satoshi Nakamoto, the --</p> <p>A. Mm-hm.</p> <p>Q. -- pseudonymous creator of Bitcoin. Do you recall saying that?</p> <p>A. Yeah.</p> <p>Q. And that was the first time you'd ever heard the name Satoshi Nakamoto, wasn't it?</p> <p>A. No, I would have heard the name Satoshi Nakamoto, because I was working in tech and computers and some of the people were doing Bitcoin stuff, so -- but with someone saying that it was Craig was Satoshi Nakamoto --</p>	<p>Mr Lynam is asked about when he heard the name Satoshi Nakamoto for the first time. His response is evasive, and he seeks to assert that he had heard the name earlier than Dr Wright's public outing (but not in connection with Dr Wright). When pressed, Mr Lynam accepts that his witness statement is correct, i.e. that he first heard the name when Dr Wright</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. May we have {E/13/7}, paragraph 27, first sentence: "I first heard the name Satoshi Nakamoto when Craig was outed by the media." Is that right or wrong?</p> <p>A. No, I probably read it's relating to Craig, yes.</p> <p>Q. No, you don't say, "I first heard the name Satoshi Nakamoto in connection with Craig when he was outed by the media", you say, "I first heard the name Satoshi Nakamoto when Craig was outed by the media". Is that written wrongly?</p> <p>A. I don't know. It's possibly right.</p>	<p>was outed by the media.</p>
<p>{Day11/46:12} – {Day11/47:2}</p>	<p>Q. And did you also become aware in late 2015 or early 2016 that his claim to be Satoshi Nakamoto had been challenged?</p> <p>A. I think it's Craig's -- so there's a creator of Bitcoin or the person who created Bitcoin, with that being Craig, as opposed to Satoshi Nakamoto. Satoshi Nakamoto is sort of, like, fairly irrelevant as a name.</p> <p>Q. Just -- can I just --</p> <p>A. To me.</p> <p>Q. Can I just repeat the question so that you're able to answer it. Did you become aware, in late 2015 or early 2016, that Craig's claim to be Satoshi had been challenged, had been disputed?</p> <p>A. I was aware that Craig's claim to be the primary creator of Bitcoin had been challenged.</p>	<p>Mr Lynam is evasive, failing to directly answer the question that is being put to him, and seeking to argue the case.</p>
<p>{L15/322/3} Email from Craig Wright to Max Lynam anors</p>		
<p>{Day11/49:3-18}</p>	<p>Q. Now, your father appears to be saying that he discussed your memories going back some years to a period of interest, and that your memories were even more vague than his. Do you recall saying something like that?</p> <p>A. Well, he said it, I didn't say it –</p> <p>Q. No, but do you recall – he's saying that he's called you to see what you've recalled and that your memories are even more vague than his. What I'm asking you is, was he right to say that you'd said that?</p> <p>A. Well, what – what was he asking me about?</p> <p>Q. Well, I don't know, Mr Lynam, I'm basing this on an email that your father sent where he said –</p> <p>A. Yes, so, he might have asked me something that I'm not aware of. I'm not sure what he's saying that my memories are</p>	<p>Mr Lynam is evasive with regard to his memory of events.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	more vague than his on. What's he talking about? What's the...	
CROSS-EXAMINATION OF STEFAN MATTHEWS BY JONATHAN HOUGH KC		
<p>{Day11/53:20} – {Day11/54:15}</p>	<p>Are you currently the executive chairman and CEO of the nChain Group?</p> <p>A. Yes, I am.</p> <p>Q. You're also, as you tell us in your statement, a shareholder in the group.</p> <p>A. I personally am not a shareholder. My family trust has shares.</p> <p>Q. You tell us that the shareholding that is held is less than 10%?</p> <p>A. That is correct.</p> <p>Q. Are you able to estimate its current value?</p> <p>A. Value?</p> <p>Q. Yes.</p> <p>A. No.</p> <p>Q. You have no idea what the value --</p> <p>A. It's a private company, so we don't have a share price.</p> <p>Q. Would you accept that nChain Group was originally established to acquire intellectual property rights of DeMorgan, Dr Wright's company, and to carry forward work of Dr Wright?</p> <p>A. Correct.</p>	<p>Mr Matthews is evasive when asked to estimate the current value of his shareholding in nChain and states that it does not have a share price.</p> <p>Later at {Day11/87:14} – {Day11/87:18}, Mr Matthews concedes that when Mr Ayre acquired his majority stake, a value must have been placed on the shares of nChain.</p>
{L19/210/4} Switzerland Global Enterprise website article		
<p>{Day11/56:10} – {Day11/57:22}</p>	<p>Q. Take that off-screen for the moment. Calvin Ayre. Is it right that you've worked with Calvin Ayre for many years, going back at least to 2011?</p> <p>A. That's technically incorrect. I worked for a company that operated under the brand Bodog. Calvin Ayre was not</p>	<p>Mr Matthews is evasive, failing to directly answer the questions being put to him regarding Mr Ayre's financial ties to nChain.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>operationally involved in that business; he had licensed the Bodog brand to that company.</p> <p>Q. For how long have you known Mr Ayre as a business colleague or associate?</p> <p>A. I would say I first met Mr Ayre in Manila in 2011.</p> <p>Q. Now, {L19/210/1}, another document on screen, please. This is an article on the Switzerland Global Enterprise website, and page 4, please {L19/210/4}, an article of 11 August 2023. It refers to: "Ayre Group based in London is investing up to 500 million Swiss francs in [the] nChain blockchain company from the Greater Zurich Area." Is it right that Mr Ayre's group of companies invested up to 500 million Swiss francs in the nChain parent company around that time?</p> <p>A. It depends on how you define "invested". Mr Ayre's companies acquired share -- shares that were held by another shareholder. Mr Ayre did not invest cash, liquidity, into the company.</p> <p>Q. Is Mr Ayre a person with significant control of the UK subsidiary of the nChain Group, the UK operating company?</p> <p>A. Could you repeat that question, please?</p> <p>Q. Sure. Is Mr Ayre a person with significant control of the UK operating company within the nChain Group?</p> <p>A. No. Mr Ayre is a significant shareholder in the holding company.</p> <p>Q. So if he's identified on Companies House -- or the Companies House website as a person with significant control of the UK company, that's an error, is it?</p> <p>A. No, it's under advice, when required to list a UBO, we were advised that we should list Mr Ayre because of his shareholding in a holding company.</p>	<p>Mr Matthews states that Mr Ayre is not a person with significant control of the UK operating company within the nChain Group, but that he is a significant shareholder in the holding company. When asked why Mr Ayre is listed as such on Companies House, Mr Matthews blames third parties (his advisors).</p>
<p>{Day11/58:6} – {Day11/59:4}</p>	<p>Q. So Mr Ayre, on that occasion, based on that quotation, was holding out nChain as essentially based on Dr Wright's work and his patent portfolio; is that right?</p> <p>A. I wouldn't agree with that.</p> <p>Q. Well, he was giving that as the principal selling point of the company, wasn't he?</p> <p>A. It's one facet of nChain, it's not the only facet of nChain.</p> <p>Q. We can take that off screen. Would you accept this, that since 2015, you have spent, yourself, a fair amount of time promoting Craig Wright's claim to be Satoshi Nakamoto?</p> <p>A. At various times, yes.</p>	<p>Mr Matthews accepts that, since 2015, he has spent a fair amount of time promoting Dr Wright's claim to be Satoshi, but denies that he "directed or managed" the period in 2016 leading up to the big reveal.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. And in particular, in early to mid-2016, you did quite a lot of work as part of preparing for his big reveal as Satoshi, didn't you?</p> <p>A. That period in 2016 was not -- was not directed or managed by me.</p> <p>Q. We'll come to who made decisions in that period, but it's fair to say that you spent a fair amount of your time in the preparations for the big reveal, didn't you?</p> <p>A. I spent most of my time dealing with the conflict between Dr Wright and Robert MacGregor.</p>	
{Day11/59:5-21}	<p>Q. We'll come to that. And more recently, you've spent time engaging with lawyers engaged by nTrust, including Zafar Ali KC and Ted Loveday, haven't you?</p> <p>A. I had only one -- one time I ever met Ted Loveday, and I wouldn't call that an engagement. I was introduced to Zafar by Christen Ager-Hanssen, and I, again, would hesitate in calling that an engagement.</p> <p>Q. How many meetings did you have with Zafar Ali?</p> <p>A. I would say maybe four or five.</p> <p>Q. Was Zafar Ali retained by and paid by the company nChain?</p> <p>A. No.</p> <p>Q. By whom was he engaged and paid?</p> <p>A. I believe he was engaged by Christen Ager-Hanssen, and he was introduced as a very, very close friend who could give advice.</p>	<p>Mr Matthews asserts that Zafar Ali KC was not retained by nChain, which is inconsistent with correspondence with Mr Ali's solicitors, Clyde & Co: this part of the transcript was put to them by Macfarlanes in their letter of 19 February 2024. Clyde & Co's response ({M1/2/214}) states that Zafar Ali KC and Ted Loveday were in fact retained by nChain (with the knowledge and approval of, among others, its CEO and in-house lawyers).</p>
{Day11/60:6-12}	<p>Q. And you've been involved with at least one other company seeking to profit from the work of Dr Wright, the company Squire Mining, haven't you?</p> <p>A. Craig Wright had nothing to do with Squire Mining -- oh, sorry, he did take a shareholding position in a -- a capital raise that occurred at one stage, yes, you are right.</p>	<p>Mr Matthews admits that Dr Wright took a shareholding position in Squire Mining, another company seeking to profit from his work.</p>
<p>{M1/1/707} Letter from Clyde & Co on behalf of Zafar Ali KC & Ted Loveday dated 10 November 2023</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{Day11/61:9-19}	<p>Q. -- their professional conduct, and then they instructed solicitors, Clyde & Co, who wrote this letter on their behalf. Is the context now clear?</p> <p>A. Yes.</p> <p>Q. And paragraph 2, they say -- Clyde & Co say on behalf of Mr Ali and Mr Loveday: ".. our clients were instructed by nChain UK Limited .." Pausing there, is it right that they were instructed by nChain UK Limited?</p> <p>A. No.</p>	<p>Mr Matthews refutes information provided by Clyde & Co, who would have no interest in providing false information, denying that Mr Ali and Mr Loveday were instructed by nChain UK Limited.</p>
{Day11/61:20} – {Day11/62:9}	<p>Q. It then says that -- it then describes nChain UK Limited as: ".. the funder and supporter of litigation involving Dr Wright .." Is that right or wrong?</p> <p>A. That is incorrect.</p> <p>Q. So, is it right or wrong that nChain has provided funding for Dr Wright's litigation, directly or indirectly?</p> <p>A. That is incorrect.</p> <p>Q. You're saying that nChain has never provided funding, even indirectly through loans or transfer of shares, or anything like that, to support Dr Wright in his litigation?</p> <p>A. Correct.</p>	<p>Mr Matthews' denying that nChain is providing funding for Dr Wright's litigation, either directly or indirectly, contrary to the letter from Clyde & Co.</p>
{Day11/62:13-18}	<p>Q. How do you say, to your knowledge, Dr Wright's litigation has been funded, including his costs in these proceedings?</p> <p>A. I've never been involved in -- in details of how Dr Wright has funded these proceedings. Anything I may have read would only be hearsay.</p>	<p>When asked about how Dr Wright's litigation has been funded, Mr Matthews does not answer the question.</p>
{Day11/63:3} – {Day11/64:9}	<p>Q. That document featured Dr Wright's claim to be Satoshi because it was thought to improve the appeal of the company in the market, right?</p> <p>A. No, I would disagree with that.</p> <p>Q. Why --</p> <p>A. We weren't going to market.</p> <p>Q. Why do you say that Dr Wright's claim to be Satoshi was prominently featured in the company's IM?</p> <p>A. Just for reference, because it's true.</p> <p>Q. And it's because nChain stands to benefit from Craig Wright being Satoshi that it went to the trouble and cost of retaining lawyers to work on this case; that's right, isn't it?</p> <p>A. NChain haven't retained lawyers to work on this case.</p> <p>Q. Would you accept this at least, that nChain, a company whose whole business is crypto technology, would benefit, or</p>	<p>Mr Matthews is asked about whether Dr Wright's claim to be Satoshi improved the appeal of nChain. Mr Matthews is evasive in response, failing to directly answer the question being put to him and answering a different question to that asked.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>stand to benefit if Dr Wright was found to be the founder of cryptocurrencies?</p> <p>A. NChain is not a crypto company. NChain is a blockchain software research company. It doesn't trade in cryptos, it doesn't create cryptos, it doesn't -- it doesn't have any connection with cryptos.</p> <p>Q. Would you accept that nChain, giving it the description you've given it, would stand to benefit if Dr Wright were found to be Satoshi Nakamoto, the creator of the Bitcoin technology and the blockchain?</p> <p>A. NChain's value is in its intellectual property and its products. Just because Dr Wright's name appears on a number of patent filings doesn't make those patent filings any more or less valuable. The patents are valued on their -- on their ability to be able to generate meaningful solutions.</p>	
<p>{Day11/64:10-18}</p>	<p>Q. So you don't think nChain, despite prominently touting Dr Wright's claim in its IM, would stand to benefit if that claim were found to be right?</p> <p>A. I don't think the value of nChain's patents change at all; it's the technology which is the value. The fact that it was created or partially created by Dr Wright and others within the research team I don't think adds any -- any -- or detracts any value one way or the other.</p>	<p>Mr Matthews is evasive, failing to directly answer the question being put to him. He refuses to accept the obvious truth that the value of nChain's assets will be impacted by the outcome of these proceedings. There are tweets by Calvin Ayre which contradict this at {L20/252.5/1}, {L20/252.7/1}, {L20/252.11/1}, {L20/252.4/1}, {L20/252.3/1}</p>
<p>{Day11/64:19} – {Day11/65:2}</p>	<p>Q. You don't think it would have any effect on nChain's value or its profitability as a business?</p> <p>A. Well, we've never -- we've never relied on that, despite what you've been asserting.</p> <p>Q. Well, it's a simple question, and I think you still haven't answered. You're saying, are you, that you don't think nChain's value or profitability would be improved by Dr Wright being found to be Satoshi?</p> <p>A. Not by any material value, no.</p>	<p>Mr Matthews continues to be evasive when pressed for an answer to the original question (whether Dr Wright's claim to be Satoshi would affect nChain's value/profitability), failing to directly answer the question being put to him. Mr Matthews finally</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
		answers by stating, implausibly, that nChain's value/profitability would not be improved "by any material value".
{E/5/25} First Witness Statement of Stefan Matthews		
{Day11/65:8-10}	<p>Q. Does Mr Ayre also have substantial holdings in BSV, either directly or indirectly?</p> <p>A. I have no idea. I'm not involved in Mr Ayre's business.</p>	Mr Matthews's answer is implausible. As Co-founder and Executive Chairman of nChain he would be expected to have knowledge of the majority shareholder's business interests. Calvin Ayre has been a vocal supporter of BSV for years, and it lacks credibility for Mr Matthews to state that he would have no knowledge of this.
{L20/252.3/1} Capture of Calvin Ayre X Post		
{Day11/65:19-25}	<p>Q. I'm just asking what you understand it to mean, reading it now.</p> <p>A. He's instructing his -- his banks to buy BSV slowly. What else am I to understand? I haven't discussed that with Mr Ayre and nor would I normally discuss those type of things with Mr Ayre. He has a family office that looks after his private business.</p>	Mr Matthews is evasive, failing to directly answer the question being put to him, to explain what he understands Mr Ayre's tweet to mean.
{Day11/66:12-17}	<p>Q. Are you telling the court you had no knowledge of Mr Ayre trading in BSV, as this tweet suggests, based upon the outcome of this litigation?</p> <p>A. No, I don't have any knowledge, and nor would I normally have any knowledge, because I'm not involved in Mr Ayre's personal business.</p>	Mr Matthews denies having any knowledge of Mr Ayre trading in BSV based on the outcome of these proceedings.

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day11/66:20} – {Day11/67:1}</p>	<p>Q. We can take that off screen. Would you accept that the tweet, on its face, suggests a link between the outcome of this litigation and the price of BSV?</p> <p>A. I don't know what Mr Ayre was trying to imply. I didn't discuss that tweet with him before or after, so you'd have to ask him, not me.</p>	<p>Mr Matthews is evasive, failing to directly answer the question being put to him about the meaning of Mr Ayre's tweet.</p>
<p>{Day11/67:8-15}</p>	<p>Q. This is a digital asset in which your family trust has holdings of \$400,000 to \$450,000 worth. You would have a particular interest in the price of this asset, wouldn't you?</p> <p>A. I am not a trader. I don't buy and sell cryptos. I acquired my BSV a long time ago, and I don't follow the price on a daily basis. My interest is in the technology of nChain, not the price of BSV.</p>	<p>Mr Matthews is evasive, failing to directly answer the question being put to him about whether he would have an interest in the price of BSV (given that his family trust has substantial holdings in this).</p>
<p>{Day11/67:16} – {Day11/68:14}</p>	<p>Q. Would you accept that, as Mr Ayre appears to think, the price of BSV may be influenced by a conclusion that Dr Wright is Satoshi Nakamoto or isn't in proceedings around the world?</p> <p>A. You'd have to ask Mr Ayre, not me.</p> <p>Q. You yourself don't draw any link, do you, between the price of BSV and the success or failure of Dr Wright's claims to be Satoshi?</p> <p>A. BSV was not and is not a crypto where it lives and dies on its price and its trading volumes. BSV is a token that is directly linked to the utility of the BSV blockchain. NChain's business is about developing applications that sit on the BSV blockchain and thus delivering utility to the chain. The price of the token -- if the price of the token were to be extremely high, that would be detrimental to some of the business applications on the BSV blockchain, and I say "business applications" because that's one of the things that clearly distinguishes BSV from other blockchains.</p> <p>Q. But if the price were to be very high, that would be beneficial for your family trust holdings, which could be sold at a high price, right?</p> <p>A. It would also be detrimental to the transactional price on BSV.</p>	<p>Mr Matthews is evasive, failing to directly answer the question being put to him, namely whether the price of BSV may be influenced by the outcome of proceedings concluding whether or not Dr Wright is Satoshi.</p>
<p>{L13/492/12} 2016-06-30 The Satoshi Affair</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day11/69:18} – {Day11/72:3}</p>	<p>Q. Page 12, please {L13/492/12}, bottom paragraph. This is describing the plan that existed at the time of the big reveal effort: “The plan was always clear to the men behind nCrypt. They would bring Wright to London and set up a research and development centre for him, with around thirty staff working under him. They would complete the work on his inventions and patent applications – he appeared to have hundreds of them – and the whole lot would be sold as the work of Satoshi Nakamoto, who would be unmasked as part of the project. Once packaged, Matthews and MacGregor planned to sell the intellectual property for upwards of a billion dollars. MacGregor later told me he was speaking to Google and Uber, as well as to a number of Swiss banks. ‘The plan was to package it all up and sell it’, Matthews told me. ‘The plan was never to operate it.’” The quote that Mr O’Hagan ascribes to you in that context, Mr Matthews, did you say that to him?</p> <p>A. That is about as accurate as Andrew reporting on the BBC and other interviews quoting me as making statements in those interviews when I wasn’t even in the building. I’ve been asked a number of times about O’Hagan’s piece and I’d say that 80/85% of it is relatively accurate. That is not true. MacGregor did say that he was talking to Google and Uber. I don’t remember him saying about Swiss banks, but I have no evidence that he ever spoke to anybody. Let me tell you about MacGregor and O’Hagan. I didn’t know that O’Hagan was engaged in any form until roughly the first week of January, when I came to London and was invited to a breakfast with Craig Wright, his wife, MacGregor and O’Hagan. That was when I was first introduced to O’Hagan. What was the plan back in May/June – June 2015 was to engage somebody to write the history – the company, not to write a –a book on Satoshi Nakamoto. It was the history of the company. And the way that–acgregor explained his thinking on that was that it’s always easier to have somebody following the history of the company, collecting the information as it grows and then obviously at some stage a book or material would be released. But it was not the intention to release a story about Satoshi Nakamoto. We knew that that would come at some stage in the future, but that wasn’t the intention when O’Hagan was originally hired. With O’Hagan’s hiring, MacGregor, an IP lawyer in his own right, hired a guy, told me about it around January – December/January, told me that there was a non-disclosure agreement in place, and there was an agreement to write a book for £200,000 on the history of the company. Well, actually, when we got to the £200,000, MacGregor had changed his story, because the WIRED and Gizmodo outing had occurred and MacGregor completely changed his strategy for everything that was going on. So, going back to this, no, that was not the plan. That was not the plan when we engaged</p>	<p>Mr Matthews is asked about an extract from journalist Mr O’Hagan’s book which discusses Mr Matthews’ plans to package Dr Wright’s work as the work of Satoshi. In response, Mr Matthews denies this and accuses Mr O’Hagan of inventing facts.</p> <p>Mr Matthews appears to be stating that he was not involved when Mr O’Hagan was hired, however in emails formalising the agreement with Mr O’Hagan, {L11/47}, {L11/54}, Mr Matthews is a recipient.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	with Craig Wright in June 2015. That might well have been what was going through MacGregor’s head in January/February 2016, but it was not something that I was heavily involved with.	
{Day11/72:4-17}	<p>Q. We can take that off the screen now. Drawing these threads together, Mr Matthews, it's right, isn't it, you anticipate benefit both to your company and to you personally if Dr Wright's claim to be Satoshi Nakamoto is found to be correct, don't you?</p> <p>A. No. I am going to say it again. I spent a number of years of my life working very hard to grow and expand the nChain Group and to get it focused on developing solutions for government and large enterprise in the blockchain space. If I benefit from my shareholding through the family trust, or if I benefit from my work with nChain, it will be because nChain has been successful in its own right, not because of Craig Wright.</p>	Mr Matthews continuing to deny that the outcome of these proceedings will not benefit nChain.
{L20/183/1} Screenshot of Whatsapp conversation between Christen Ager-Hanssen & Stefan Matthews		
{Day11/72:24} – {Day11/73:14}	<p>Q. {L20/183/1}, please. Now, this is an image of a WhatsApp exchange apparently between you and Mr Ager-Hanssen, which he dated, in a tweet, to Monday, 25 September 2023. The images of the computer -- the images in the photographs are of a computer with Dr Wright's browsing history, as Dr Wright has accepted. Would you agree with that?</p> <p>A. No. I don't know what those images are. I never read those images at the time, they were difficult to read on my phone. I really didn't care what they were.</p> <p>Q. Dr Wright has also exhibited a larger photograph of one of them, which shows him doing web searches in relation to some of the documents he's alleged to have forged, apparently with his BDO Drive contents also on screen. Were you aware of that?</p> <p>A. No.</p>	Mr Matthews is asked about whether the images are of a computer with Dr Wright’s browsing history. Mr Matthews denies this, claiming not to know what these images are and that he did not read the images “at the time” (suggesting that he has reviewed the images since then).
{Day11/73:22} – {Day11/74:6}	<p>Q. And your reply -- replies are: "Fuck. "WTF is wrong with him. "Well, we have NCH to focus on, that's not fake." In your second witness statement you accept, don't you, that this is a genuine WhatsApp exchange between you and Mr Ager-Hanssen, it's not been doctored or anything?</p> <p>A. I believe it's genuine. I haven't had it validated, but I -- I would accept it as being genuine.</p>	Mr Matthews accepts that the WhatsApp conversation between himself and Mr Ager-Hanssen, as displayed in the screenshot, is genuine (consistent with his Second

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
		Witness Statement at {E/27/8}).
<p>{Day11/75:12} – {Day11/76:18}</p>	<p>Q. Well, your message wasn't just limited to acknowledging that you'd received those messages, was it?</p> <p>A. No, but my message was: let's get on with nChain.</p> <p>Q. I'll come to that in a second.</p> <p>A. I'm not worried about Craig Wright and what may or may not be fake, or not fake, or asserted. It doesn't worry me at all. My -- my focus, my problem is nChain.</p> <p>Q. But you didn't just say that the two of you should focus on your work for nChain, did you? You didn't just say that?</p> <p>A. I think I did.</p> <p>Q. Well, first of all, you expressed surprise at what he'd sent you. That's what the first expletive, "Fuck", means, isn't it?</p> <p>A. You're taking this particular exchange completely out of context. Ager-Hanssen was, and is, a particular style of individual. I was fed up with his -- at that -- what date was this?</p> <p>Q. 25 September 2023.</p> <p>A. From the 22nd -- from 22 September until I fired him, he was consistently harassing me, threatening me, and insisting that I withdraw as a witness in this matter and making statements to me personally that he would destroy me if I didn't withdraw as a witness. He and Mr Ali called me late at night, around midnight, one day, and said, during this period, "We are arriving in Switzerland tomorrow morning and we have documents for you to sign to withdraw as a witness". I said, "No, I'm not available", "Then come to London and sign". I was told no less than 20 to 25 times that Ager-Hanssen would stop at nothing to destroy me if I came to this courtroom.</p>	<p>Mr Matthews makes serious accusations of witness tampering against Mr Ager-Hanssen and Mr Ali KC, alleging that they tried to make him withdraw as a witness in these proceedings.</p>
<p>{Day11/77:3-20}</p>	<p>Q. And the second message you wrote was: "WTF is wrong with him." Yes?</p> <p>A. Yes.</p> <p>Q. And "him" was Craig Wright, wasn't it?</p> <p>A. Yes.</p> <p>Q. And, again, the meaning was clear. You were agreeing that Craig Wright had done something stupid or wrong, weren't you?</p> <p>A. No, I wasn't. I wasn't agreeing to any such thing. I didn't care.</p>	<p>Mr Matthews refuses to accept the obvious truth of the words in the message thread, denying that he was agreeing that Dr Wright had done something stupid or wrong.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. I appreciate you say that now, but the plain meaning of that message is –</p> <p>A. Well, this is – this is the impersonal nature –</p> <p>Q. – what the fuck is wrong with Craig Wright?</p> <p>A. This is the impersonal nature of messages, you can't determine what the emotion of the person is that's sending them at the time.</p>	
<p>{Day11/78:3} – {Day11/79:15}</p>	<p>Q. What do you say is the other meaning of: “WTF is wrong with him.”</p> <p>A. Fuck. What the fuck is wrong with him? Forget about it, move on; let's go to nChain. That was where my thinking was at the time.</p> <p>Q. That's not – you didn't write, “Forget him; ignore him; don't think about Craig Wright”, you wrote, “WTF is wrong with him”, in response to these allegations that Mr Ager-Hanssen was making, didn't you?</p> <p>A. No, that's not true.</p> <p>Q. And the plain meaning of that was agreeing –</p> <p>A. You can –</p> <p>Q. – that he had done something wrong, wasn't it?</p> <p>A. You can interpret that way if you want, but I'm telling you that that's not what my intention was.</p> <p>Q. And then you write: “Well, we have NCH to focus on, that's not fake.” And I think we can agree “NCH” is nChain?</p> <p>A. Yes.</p> <p>Q. And the words added, “That's not fake”, bear the clear implication that Dr Wright was fake, don't they?</p> <p>A. Everything – everything that was coming out of Ager-Hanssen's mouth was fake.</p> <p>Q. This is not coming out of his mouth, Mr Matthews, this is coming out of your mouth.</p> <p>A. Well, “biggest fake ever” came out of his mouth.</p> <p>Q. But you say, “That's not fake”, in relation to nChain, and the clear implication is you're saying Dr Wright is, aren't you?</p> <p>A. No. Ager-Hanssen is saying Craig Wright is fake.</p> <p>Q. Adding those words, “That's not fake”, indicated agreement that he was a fake, didn't it?</p> <p>A. That was not my intention.</p>	<p>Mr Matthews continues to be pressed on the meaning of his words in the message thread, and continues to be evasive, refusing to accept the plain meaning of “WTF is wrong with him.” And “Well, we have NCH to focus on, that's not fake”.</p> <p>Mr Matthews refuses to admit that his message implied that he thought Dr Wright was fake.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. If we asked any objective observer who knew the background to read those messages and say what they meant, they would say you were agreeing that Dr Wright was a fake, wouldn't they?</p> <p>A. And that would be wrong.</p>	
<p>{E/27/8} Second Witness Statement of Stefan Matthews</p>		
<p>{Day11/79:21} – {Day11/80:15}</p>	<p>Q. You say that you were fed up with Mr Ager-Hanssen accusing Dr Wright of being a fraud and that you didn't believe that Dr Wright was a fraud?</p> <p>A. Correct.</p> <p>Q. Now, this message, as we've seen, did not just say, "Christen, forget all this nonsense, focus on nChain", did it?</p> <p>A. No, it didn't.</p> <p>Q. Your message indicated agreement with his view that Dr Wright was a fake, despite you now saying you strongly disagreed with that view.</p> <p>A. I was putting a position to Ager-Hanssen that would fit with his assertions so that we could move on.</p> <p>Q. So you say now that you were trying to indicate agreement with his view that Dr Wright was a fake in order just to fob him off; is that what you're saying?</p> <p>A. No, I wasn't agreeing with his view.</p> <p>Q. You say that's not what your messages indicated?</p> <p>A. No, that was not my intent. It was a message between he and I and nobody else, and I wanted to move on.</p>	<p>Mr Matthews refuses to accept the obvious truth. The story he presents contradicts itself – if, as Mr Matthews suggests, his messages were not intended to indicate agreement with Mr Ager-Hanssen, how did he think they would work to pacify Mr Ager-Hanssen?</p>
<p>{Day11/80:16} – {Day11/81:18}</p>	<p>Q. Now, this message – we can take the witness statement off screen. This exchange happened at a delicate time, didn't it, Mr Matthews?</p> <p>A. The 25th?</p> <p>Q. It was three days after the mock trial, wasn't it?</p> <p>A. It was.</p> <p>Q. It was two days –</p> <p>A. It was a delicate time, because, as I explained earlier, I was being bombarded with threats around what was going to happen to me and my family and my reputation. I was going to be destroyed. Destroyed. And when someone is screaming “destroyed” at you, and smashing their palm on the desk in</p>	<p>Mr Matthews is evasive, failing to directly answer the question that is being put to him and instead discussing the “threats” that he was subject to.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>front of you and their face is 12 inches away from yours, that’s pretty threatening, and that’s what I was – that was what I was subjected to over a period of three or four days.</p> <p>Q. This was three days after the mock trial in which Dr Wright was thought to have performed badly, wasn’t it?</p> <p>A. In all fairness, Dr Wright didn’t get a chance to perform anything at that mock trial. It wasn’t a mock trial, it was an ambush and a – and a one-way interrogation of Craig to – to, I think, force me, as a witness, to withdraw as a witness in this case.</p> <p>Q. And it took place, this exchange, two days after Calvin Ayre had sent his three-page email threatening to cut off funding for Dr Wright, didn’t it?</p> <p>A. I don't know.</p>	
<p>{Day11/82:24} – {Day11/83:8}</p>	<p>Q. Let’s take this in stages.</p> <p>A. Go slowly.</p> <p>Q. Your message indicated agreement that Dr Wright, unlike nChain, was a fake, yes?</p> <p>A. No.</p> <p>Q. And if that -- on the basis that that is the message, as I've put it to you, that's not a message you would have wanted to deliver to Mr Ager-Hanssen at this time if it wasn't true, yes?</p> <p>A. I'm -- I'm still not piecing this together.</p>	<p>Despite COPA’s counsel breaking the question down, Mr Matthews continues to claim to not understand the question.</p>
<p>{L19/240.3.1} Stefan Matthews and CAH Part 2 - Transcript {L19/240.4/1} Audio of Stefan Matthews and CAH recording</p>		
<p>{Day11/84:14} – {Day11/86:5}</p>	<p>Q. If we go to page 4, please {L19/240.3.1/4}.</p> <p>A. Oh, I know what this is. This is a transcript of the recording that he allegedly took in Spain, and I can say pieces of this resonate with me. I don't know whether that recording is a legitimate -- a recording in its entirety. I know that the man has a history of clipping things together so, the recording, as far as I'm concerned, hasn't been verified.</p> <p>Q. Page 2, please {L19/240.3.1/2}. Next page {L19/240.3.1/3}. There is a quotation at time counter 08.21: "Because we're heading into a fucking train wreck on the 15th of January." Did you say those words to Mr Ager-Hanssen, as far as you're aware?</p> <p>A. I may have. I don't have specific recollection, but I may have.</p>	<p>Mr Matthews anticipating questions from COPA’s counsel, immediately stating that he does not consider that the recording at {L19/240.4/1} is verified.</p> <p>When asked if he recalls saying those words to Mr Ager-Hanssen, Mr Matthews is evasive, stating that he “may have” and that</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. We can listen to the recording. It's at {L19/240.4/1}, and bring that up and start the tape counter at eight minutes precisely. This is C00003561. If we can go to eight minutes in, eight minutes precisely, and just pause before we start. We're going to listen for it at 8 minutes 21 seconds. Play on, please. We'll need the audio. We may need to turn the speaker on. (Audio played) Pause there. Listening to that, does that refresh your memory? Do you recall saying, "We're heading into a fucking train wreck on the 15th of January"?</p> <p>A. It definitely sounds like my voice.</p> <p>Q. Was 15 January the original start date for this trial?</p> <p>A. I don't know. I thought it was 5 February. No, you're right. You're right, yeah.</p> <p>Q. That's what you were referring to in that conversation by describing "heading into a fucking train wreck on the 15th of January", isn't it?</p> <p>A. Well, you've got to remember that Ager-Hanssen and Zafar Ali were both in Spain at the time, and they both spent two days telling me how uncooperative Craig was with the development of his strategy and plan. So, it didn't look good, the way that they were presenting things to me about preparations for the -- for the hearing.</p>	<p>it "sounds like [his] voice".</p> <p>When pressed on this, Mr Matthews acknowledges that things "didn't look good" based on what Mr Ager-Hanssen and Mr Ali had been telling him, so he appears to admit ultimately that he said the words on the recording.</p>
<p>{Day11/87:14} – {Day11/88:22}</p>	<p>Is it right that if Mr Ayre was acquiring a majority stake and making a payment for the acquisition of shares that somebody must have placed a value on the shares?</p> <p>A. Yes. I'm not privy to exactly what those negotiations were, they were between two shareholders. Remember, Mr Ayre, through one of his companies, had a small shareholding that he -- that he invested a few years ago and he added to that shareholding by acquiring from another shareholder.</p> <p>Q. So it's not the case, is it, that a fair market value couldn't be placed on your family trust's shareholding in nChain Holdings if you needed to?</p> <p>A. If I were to undertake a valuation, yes.</p> <p>Q. Is it your position that you just have no idea what that valuation would produce?</p> <p>A. Yeah, I mean, again, disclosing what my percentage is -- and it's single digit percentage -- I'd rather not do that in open court if you don't mind.</p> <p>Q. Just based upon Mr Ayre's investment, would you accept that even a single digit percentage shareholding in nChain would be a very valuable asset?</p>	<p>Mr Matthews admits that it is possible to place a value on his family trust's shareholding in nChain, contradicting his earlier evidence at {11/53/20}- {11/54/15} where he states that shares in nChain do not have a value due to it being a private company.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. I'm not -- I'm trying to calculate here. I mean, any shareholding in any company is a valuable asset depending on the success, the future success of that company, and I know that you're trying to tie this to Craig Wright being Satoshi, and I've said repeatedly this morning that that's not where nChain's value sits.</p> <p>Q. But I'm just trying to understand, Mr Matthews, whether your stake in nChain is a significant valuable asset in your personal portfolio. Can I ask the question in that way without putting you in any difficulties?</p> <p>A. Just remember, the stake isn't my stake, it's a stake that's owned by a family trust and I wasn't the -- I'm not a beneficiary of that trust.</p>	
<p>{E/5/6} First Witness Statement of Stefan Matthews</p>		
<p>{Day11/89:15-17}</p>	<p>Q. Can we agree that Centrebet didn't actually engage him to produce a digital currency project or system?</p> <p>A. That's correct.</p>	<p>Mr Matthews agrees that Centrebet did not engage Dr Wright for a digital currency project/system.</p>
<p>{Day11/90:11-21}</p>	<p>Q. Paragraph 25, you say that you printed the document on the private printer in your office, either that day or the next, and that you read the paper straight away, right?</p> <p>A. Or I read the paper after I'd printed it, yes.</p> <p>Q. You say you believe that was the same day as you printed it?</p> <p>A. Yes.</p> <p>Q. You became aware of the word "Bitcoin" when you read that paper?</p> <p>A. Yes.</p>	<p>Mr Matthews confirms that he became aware of the word "Bitcoin" when he read the White Paper from Dr Wright's USB stick. This contradicts the evidence of Dr Wright, who at {Day6/121:23-25} claims the document he gave to Mr Matthews did not use the term "Bitcoin", only "Timecoin".</p>
<p>{Day11/90:22} – {Day11/91:5}</p>	<p>Q. You say that the document didn't have a name on it but it had a placeholder, paragraph --</p> <p>A. Yes.</p> <p>Q. -- 27?</p> <p>A. I've -- I've been asked this question so many times I -- I say that, with certainty, it did not have the name Satoshi Nakamoto on it. It could have had the name Craig Wright on it, but I believe that it had no name on it at all.</p>	<p>Mr Matthews states that he believes the document had no name on it at all.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{Day11/91:6-23}	<p>Q. Over the page to paragraph 28 {E/5/7}. You say that when you next saw Dr Wright after you'd read it, he asked you about the paper and you said words to the effect that you had no interest in it, didn't want any involvement and it wouldn't amount to anything?</p> <p>A. Correct.</p> <p>Q. Now, Mr Matthews, you must be aware of the importance of this story to Dr Wright's claim to be Satoshi and the presentation of that claim, mustn't you?</p> <p>A. Yes, I am. The White Paper was not the only thing related to the history of this. Over a two-year period, I had countless numbers of meetings, discussions, sketchings on pieces of paper and whiteboards about various aspects of what Dr Wright was creating. That's why, when I received the White Paper, it was no surprise to me to see this assembly of many of the concepts that we'd discussed at various times over a couple of years appearing in this paper.</p>	<p>Mr Matthews states, implausibly, that he had no interest in the Bitcoin White Paper, despite having “countless numbers of meetings, discussions, sketchings on pieces of paper and whiteboards about various aspects of what Dr Wright was creating”, and that this document was the “assembly of many of the concepts” that they had discussed.</p>
{L15/70/1} 2019 Squire Mining Press Release		
{Day11/92:7-17}	<p>Q. And then {L15/70/1}, please. This is a press release, in 2019, by the company Squire Mining, of which you were chairman and about which you spoke earlier?</p> <p>A. Yes.</p> <p>Q. Do you see that Dr Wright is described, in the third sentence, as an advisory board member for the company?</p> <p>A. Yes.</p> <p>Q. So not just a shareholder of the company?</p> <p>A. No, he had been an adviser on -- on mining for probably a year or so.</p>	<p>Mr Matthews admits that Dr Wright was not just a shareholder of Squire Mining, but he was also an adviser on mining.</p>
{Day11/93:4-13}	<p>Q. So this story about you receiving a copy of the Bitcoin White Paper has been a significant part of the pitch from these companies to the market, hasn't it?</p> <p>A. In this case, it was highlighting to the market that Dr Wright was the author of the Bitcoin White Paper, yes.</p> <p>Q. So you have committed to this story very publicly as part of pitches to the market, haven't you?</p> <p>A. I'm not going to say "pitches to the market". It's a statement of fact.</p>	<p>Mr Matthews admits that his story about receiving a copy of the Bitcoin White Paper was highlighting to the market that Dr Wright was the author of this document, but is evasive when asked to confirm this story formed a part of the</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
		company's "pitches to the market".
{L10/338/1} Email ID_004276		
{Day11/95:1-15}	<p>Q. And then you respond, 10 September 2015: "What is really important here is .. Craig is now at a comfortable point and has accepted 'coming out'. No pushing needed now."</p> <p>A. Correct.</p> <p>Q. Was that the response you gave?</p> <p>A. Looking at this email, and I'm assuming the email is verified, yes.</p> <p>Q. You referred to that email as refreshing your memory.</p> <p>A. Yes.</p> <p>Q. It didn't strike you when you --</p> <p>A. It didn't strike me as unusual, no.</p> <p>Q. Your immediate impression was this was a genuine email chain in which you contributed?</p> <p>A. Yes.</p>	Mr Matthews admits that the email at {L10/338} is genuine, contrary to Dr Wright's evidence ({Day7/7:5-24})

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day11/95:16} – {Day11/97:5}</p>	<p>Q. Now, as we saw, the email, at the end, refers to Dr Wright having asked you to review the paper, it having been on your desk at one stage for months, but you never getting around to that?</p> <p>A. I don't believe the paper was on my desk for months. It was on my desk for some weeks. They're Craig's words, not mine.</p> <p>Q. Absolutely, but what I'm putting to you is that the account Dr Wright gives at the bottom of that email is very different from the account that you've given. He says it was on your desk for months and you never got round to reviewing it; you say that you printed it out and read it immediately. There's a big difference --</p> <p>A. He wasn't there when I printed it out and he wasn't there when I read it immediately.</p> <p>Q. Would you at least accept this, that what Dr Wright said, with some confidence, in that email was very different from the account you've given about what you did with the White Paper?</p> <p>A. My interpretation of this is that I didn't go back to Craig and have a detailed discussion about the White Paper.</p> <p>Q. Well, it says a bit more than that, doesn't it? It says that it was sitting on your desk for months without you reading it.</p> <p>A. Well, I read it. I read it when I printed it.</p> <p>Q. Well, I appreciate that's what you're saying, but it's very different from what Dr Wright said in this email, isn't it? Yes?</p> <p>A. I don't -- I don't know what Dr Wright knew at the time, but I can tell you that I printed it.</p> <p>Q. You didn't respond to this email by saying, "That detail at the end about me and the White Paper, that's wrong in some fairly significant respects", did you?</p> <p>A. No, I didn't. I saw no point.</p> <p>Q. Why did you see no point when you saw Dr Wright saying something that was so demonstrably wrong, on your recollection?</p> <p>A. That was his interpretation. It wasn't what actually occurred.</p>	<p>Mr Matthews is questioned on the differences between his account and Dr Wright's account of the draft paper on the USB stick. Mr Matthews states that Dr Wright's account is not what actually occurred.</p>
<p>{Day11/97:15} – {Day11/98:9}</p>	<p>Q. And you've never provided any emails or text messages with anyone from 2008 or 2009 mentioning this draft document?</p> <p>A. No.</p>	<p>When asked to confirm that he has not provided any emails/text messages from 2008/09 mentioning this draft paper, Mr Matthews</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. And you've never provided any emails or text messages with anyone from that period discussing Dr Wright's digital currency ideas more generally?</p> <p>A. Well, there were no discussions with other people. The discussions were between myself and Craig Wright and they occurred in person and verbally in my office. Now, having said that, there are at least three or four other people that were working in my office that I subsequently found out that Craig had some similar discussions but not to the level that he did with me with the White Paper. They contacted me over the years as -- as things have appeared in the media.</p> <p>Q. They're not people you mention in your witness statement, are they?</p> <p>A. No. They've asked me not to mention their names, but if I - if I need to, I will.</p>	<p>produces a new story and refers to hearsay evidence that “at least three or four other people” had similar discussions with Dr Wright, and that they have “contacted [him] over the years”. Mr Matthews confirms they are not mentioned in his first witness statement, because they asked him not to mention their names, but he provides no reason as to why this evidence was not included in his witness statement without specifying the names of these individuals.</p>
<p>{Day11/98:10-16}</p>	<p>Q. On this story of the foundational text of Bitcoin being shared with you, the only evidence we have is your account and Dr Wright's account, right?</p> <p>A. On the -- on the aspect of the White Paper that he gave me on the USB stick?</p> <p>Q. Yes.</p> <p>A. Correct.</p>	<p>Mr Matthews confirms that the only evidence of the draft White Paper being shared with him on a USB stick is his account and that of Dr Wright.</p>
<p>{Day11/98:22} – {Day11/99:9}</p>	<p>Q. Are you aware that he said in his first witness statement, very firmly, that he handed it to you in hard copy?</p> <p>A. No, he handed me the USB stick. He may well have had hard copy with him, but he didn't hand me a hard copy.</p> <p>Q. Because you have a detailed recall of receiving the USB, finding the one file on it, printing that file on your private printer and then handing back the USB. That's what you've told the court, isn't it?</p> <p>A. That's correct.</p> <p>Q. And so if Dr Wright says that he handed you a hard copy, then that must be wrong, mustn't it?</p> <p>A. He handed me a USB stick.</p>	<p>Mr Matthews' account contradicts Dr Wright's evidence at {E/1/19}: “Around October 2008, I handed over a draft of the White Paper to Stefan Matthews... If memory serves me right, I left a printed copy of the draft on his desk”. Dr Wright also affirms his memory that it was a hard copy he gave to Stefan at {Day6/118:2-4}.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
		Notably, this is a key part of Dr Wright's evidence that he is Satoshi.
{Day11/99:19-24}	<p>Q. Now, that might appear on its face to be a document fitting Dr Wright's story of giving you a hard copy of the Bitcoin White Paper and asking for your views, but may we take it from your evidence that it's a document that wasn't given to you in 2008?</p> <p>A. No, it was not.</p>	As above, Mr Matthews reiterates that he did not receive a hard copy of the Bitcoin White Paper.
{L13/491/10} The Satoshi Affair		
{Day11/99:25} – {Day11/101:12}	<p>Q. Next, please, {L13/491/2}, back to "The Satoshi Affair". Page 10, please {L13/491/10}. At the bottom of the page, Mr O'Hagan writes this: "The 'Stefan' who was hovering during the raid on Craig Wright's house and office is Stefan Matthews, an IT expert whom Wright had known for ten years, since they both worked for the online gambling site Centrebet. In those days, around 2007, Wright was often hired as a security analyst by such firms, deploying his skills as a computer scientist (and his experience as a hacker) to make life difficult for fraudsters. Wright was an eccentric guy, Stefan Matthews remembered, but known to be a reliable freelancer. Matthews said that Wright had given him a document to look at in 2008 written by someone called Satoshi Nakamoto, but Matthews had been busy at the time and didn't read it for a while." Now, based on what you've said very firmly here, the words Satoshi Nakamoto weren't attributed to the document you received, were they?</p> <p>A. That's correct.</p> <p>Q. And so the account which Mr O'Hagan ascribes to you of being given a document written by somebody called Satoshi Nakamoto must be wrong, mustn't it?</p> <p>A. I didn't tell Andrew O'Hagan that the 2008 document was - had the name Satoshi Nakamoto on it. O'Hagan is an author. I'm assuming -- and I can only assume -- that he's attributing the Nakamoto name to the paper because everybody knows that the White Paper was written by Nakamoto and that I saw that document, or a version of that document, prior to it being released in 2008.</p> <p>Q. Well, the way he puts it is: "Matthews said that Wright had given him a document to look at in 2008 written by someone called Satoshi Nakamoto .." On your evidence, you wouldn't have told him that, would you?</p>	Mr Matthews accepts that his account of being given the 2008 document in these proceedings is inconsistent with that as written by Mr O'Hagan (which was also written based on what Mr Matthews had said).

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	A. No.	
{Day11/102:7-20}	<p>Q. Mr Matthews, your narrative now of receiving the White Paper is at odds with the story Mr O'Hagan says you gave him and at odds with Dr Wright's story now, isn't it?</p> <p>A. O'Hagan's account of what he wrote here, as a story, is not accurate.</p> <p>Q. It's a story that's not corroborated by anyone else or any documents, isn't it?</p> <p>A. I'm going to say again, what O'Hagan has written here is not 100% accurate.</p> <p>Q. Your story is not only uncorroborated, it wasn't mentioned for years, until it happened to support the big reveal plan; that's right, isn't it?</p> <p>A. No.</p>	Mr Matthews asserts that Mr O'Hagan's account of his receiving the draft White Paper is inaccurate.
{Day11/103:3} – {Day11/104:13}	<p>Q. This story of you receiving the Bitcoin White Paper never saw the public light of day until late 2015 when the big reveal was being put together; correct?</p> <p>A. No, I discussed this with Dr Wright and also with Mr Ayre in -- and others in June 2015, including Dr Wright's lawyer from Clayton Utz.</p> <p>Q. There's nobody else who has come forward to give evidence?</p> <p>A. No.</p> <p>Q. Mr Matthews, I have to put it to you, this story of you receiving the Bitcoin White Paper before publication is just not true, is it?</p> <p>A. That is fundamentally incorrect. It is true. I lived through that period, I experienced what I experienced through that period and it is true.</p> <p>Q. It is a lie which has been used since 2015 to embellish and support --</p> <p>A. It is not a lie.</p> <p>Q. -- Dr Wright's claim?</p> <p>A. It is not a lie. I had to endure this sort of harassment from Ager-Hanssen, threatening me about coming to this court.</p> <p>Q. And your account –</p>	Mr Matthews denies that his account of receiving the White Paper in August 2008 is untrue, despite no corroborating evidence. He seeks to divert the questioning by repeating the serious allegations of witness tampering from Mr Ager-Hanssen.

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. I'm not going to sit here and lie. I'm telling the truth and the absolute truth on what I experienced at that time.</p> <p>Q. This is a lie to which you have committed over the years and which you couldn't get out of, isn't it, Mr Matthews?</p> <p>A. That is untrue.</p> <p>Q. And the idea that Dr Wright had elaborate digital currency plans in 2007/2008 is also a lie, isn't it?</p> <p>A. No, it's not. There are -- Dr Wright made a submission to Centrebet in early 2009 which, had I agreed to the funding proposition, would have been, in my opinion, the furthest application built on the back of Bitcoin.</p>	
{Day11/105:12-23}	<p>Q. Mr Matthews, it's a very odd story, isn't it, a colleague offering you something of entirely unknown value for \$500?</p> <p>A. That's why I wasn't interested in it. I remember the day vividly. I was sitting in my office, my right-hand credenza always had my printer, my personal printer and my briefcase on it. And when he asked for the money, I reached for my briefcase to get my cheque book, and that's while we were having the conversation about whether I can give you more or -- or 500. And as soon as he mentioned Bitcoin, I closed my briefcase. I was not interested.</p>	<p>Mr Matthews displays a particularly vivid memory of events that day, despite being unable to recall which month it was in his witness statement at {E/5/7}: "In around March or April 2009".</p> <p>Mr Matthews restates that he was not interested in Bitcoin during this discussion with Dr Wright.</p>
{Day11/107:14-25}	<p>Q. Can you agree with this: a honeypot system is a generic term for an IT security system that acts as a decoy for cyber criminals?</p> <p>A. Yes.</p> <p>Q. And it does that by mimicking a real system and attracting attacks, yes?</p> <p>A. Yes.</p> <p>Q. So the fact of Dr Wright proposing a honeypot system to Centrebet wouldn't of itself denote any special knowledge of the Bitcoin System or blockchain, would it?</p> <p>A. No, but the immutable log store and a timestamp server does.</p>	<p>Mr Matthews accepts that a honeypot system as proposed by Dr Wright does not denote special knowledge of Bitcoin or blockchain. However, he goes on to assert that other features of the system do (immutable log store and timestamp server).</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{Day11/108:1-15}	<p>Q. That's another pitch which nobody at Centrebet other than you has ever spoken about, right?</p> <p>A. I have seen, at some stage, and it might have been shown to me around the time of the Kleiman trial, a copy that the lawyers had of that proposal and it surprised me because I didn't know how they got it.</p> <p>Q. Well, the only copy of that proposal we have in these proceedings has been debunked as unreliable by forensic documents experts, Mr Matthews. Just to be clear so that it's not suggested I haven't put our case, while Dr Wright may have been discussing honeypot security systems with you in early 2009, we don't know, he certainly didn't propose anything to do with the blockchain at that stage.</p> <p>A. Timestamp servers, yes.</p>	<p>Mr Matthews was not a witness in the Kleiman trial, but states that he has seen a copy of this Centrebet proposal from lawyers “around the time of the Kleiman trial”. Mr Matthews therefore appears to have knowledge of the Kleiman proceedings despite claiming nChain has no involvement in Dr Wright’s litigation.</p> <p>Mr Matthews also appears to accept that Dr Wright did not propose anything to do with blockchain in early 2009.</p>
{Day11/108:23} – {Day11/109:11}	<p>Q. From late 2011 -- we can take the document off screen. From late 2011, you were living and working in the UK as chief technology officer of Tyche Consulting Limited; correct?</p> <p>A. Correct.</p> <p>Q. And is this right, that was an English online entertaining and gambling company?</p> <p>A. The company was a technology provider to online gambling, yeah.</p> <p>Q. And it traded as Bodog UK?</p> <p>A. At the time, yes.</p> <p>Q. Bodog is a brand founded and owned by Mr Ayre; is that right?</p> <p>A. Yes.</p>	<p>Mr Matthews confirms that Bodog is owned by Mr Ayre.</p>
{E/5/8} First Witness Statement of Stefan Matthews		
{Day11/109:18} – {Day11/110:17}	<p>Q. Now, in your witness statement at -- this is paragraph 38 {E/5/8} -- we don't need it on screen -- you say that one weekend in early 2012, you watched a programme in which</p>	<p>Again, Mr Matthews displays a particularly vivid memory for details that are not capable of being tested,</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>you saw that Bitcoin was being used by some people living in the USA; is that right?</p> <p>A. That's correct.</p> <p>Q. And you say you expressed some surprise, you say probably in some colourful language, that Bitcoin had taken off?</p> <p>A. Yes, I -- I was channel surfing on cable, we had not long been in -- in our house in Weybridge, my sons weren't in the room and I was just channel surfing and I heard the word "bitcoin", and I stopped on that channel and I remember quite vividly there were people in caravans and tents in a forest somewhere in the US and they were talking about Bitcoin and they were transferring Bitcoin between mobile phones. It was round about that time my sons came back into the room and they said, "Dad, What are you watching", and I said, "I'm just watching this, whatever it was, programme", and they said, "Can we turn it over and can we watch football". So I said, "Yeah, sure, we'll turn it over", I had no interest in watching any more, but it was fascinating for me that the Bitcoin name came up and it reaffirmed my memories of history.</p>	<p>and yet simultaneously he cannot place the date itself, stating it was "sometime between mid-January and the end of March 2012" at {E/5/8}.</p>
<p>{Day11/112:9} – {Day11/113:3}</p>	<p>Q. You say that you met him and his wife in Sydney on 2 January 2014, just to catch up?</p> <p>A. Correct.</p> <p>Q. You say that she mentioned Bitcoin in conversation, but you didn't take the conversational cue because you had no interest in it?</p> <p>A. Correct.</p> <p>Q. You say that the meeting had no particular point to it?</p> <p>A. Correct.</p> <p>Q. Now, as you tell us, on that occasion you didn't go into any discussion of this invention that Dr Wright had come up with and the fact that it was being used around the world?</p> <p>A. No.</p> <p>Q. Mr Matthews, you were one of the privileged few to know that he'd made this extraordinary invention which was in use around the world and you didn't even discuss it in this first meeting in years? Is that really what you say?</p> <p>A. I wasn't interested.</p>	<p>Mr Matthews reiterates, implausibly, that he had no interest in Bitcoin.</p>
<p>{Day11/113:14} – {Day11/114:8}</p>	<p>Q. And on your account, Dr Wright's wife had been openly talking in a restaurant in Sydney about him having invented Bitcoin?</p> <p>A. Sorry? Say that again?</p>	<p>Mr Matthews is evasive in response to questions about the conversation with Dr Wright's wife in Sydney. When pressed,</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. On what you tell us, Dr Wright's wife had been openly talking in a Sydney restaurant about him having --</p> <p>A. Oh, it wasn't a restaurant, it was the lobby of the hotel.</p> <p>Q. Okay. She had been openly talking in the lobby of a hotel about Dr Wright having invented Bitcoin, right?</p> <p>A. Between the three of us sitting on the sofa, yes -- oh, no, sorry, what did you just say, openly talking about him inventing Bitcoin?</p> <p>Q. Yes.</p> <p>A. No, she didn't. She talked about Bitcoin and had I been following Bitcoin, and I said no.</p> <p>Q. So she raised the subject of Bitcoin and had you been following it?</p> <p>A. And I said no.</p> <p>Q. And you said no.</p>	<p>he denies that she was openly talking about Dr Wright inventing Bitcoin, but just that she "talked about Bitcoin" and whether Mr Matthews had been following it.</p>
<p>{Day11/114:12} – {Day11/115:1}</p>	<p>Q. It didn't occur to you even to mention the connection between the discussion of Bitcoin --</p> <p>A. What, between three people --</p> <p>Q. -- and the fact that he'd been supposedly --</p> <p>A. Between two people that obviously knew the history of the two of us and the wife. By the way, I didn't know she was the wife at the time.</p> <p>Q. But here was a cue mentioning something that, by this stage, early 2014, was featuring in the news and you don't even pick up the cue so far as to say, "Craig, you came up with this"?</p> <p>A. I was unaware -- I was unaware of anything around Bitcoin in the news. The fact that Ramona mentioned it was a surprise to me and I had no interest in opening a dialogue about it.</p>	<p>Mr Matthews claims to be unaware of anything around Bitcoin in the news in early 2014.</p>
<p>{L8/340/1} ID_001304 00007681.email</p>		
<p>{Day11/117:8} – {Day11/118:24}</p>	<p>Q. Now, if your account of events of 2007 to 2009 had been true, then the best selling point to Mr MacGregor would be to tell him that Craig Wright was in fact the mysterious inventor of the entire Bitcoin System, wouldn't it?</p> <p>A. That was not the point of the introduction.</p> <p>Q. No, but if you're trying to connect Craig Wright and Rob MacGregor on a project to do with virtual currencies, surely it</p>	<p>Mr Matthews is evasive, he fails to provide a plausible reason as to why he did not mention Dr Wright was the inventor of Bitcoin in the introductory email to Mr MacGregor.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>would have been relevant to tell him that Craig Wright had special expertise as the inventor of Bitcoin and the blockchain?</p> <p>A. Well, I did say that Craig Wright, several times, had spoken to me about virtual currencies --</p> <p>Q. You did.</p> <p>A. -- in my time at Centrebet.</p> <p>Q. You did.</p> <p>A. It was up to MacGregor and Wright to decide whether there was any -- any connection that the two of them wanted to use for any purpose. I -- I had -- again, I was involved in other things. I wasn't brokering a deal here, I was just introducing two people.</p> <p>Q. But you were introducing two people in the context of a project about cryptocurrencies and you're saying it doesn't occur to you to mention that one of them is the inventor of the whole Bitcoin cryptocurrency blockchain system?</p> <p>A. I didn't want to go to that level of detail, I wanted to introduce two people and let them find out if they had a way of working together.</p> <p>Q. It's not a level of detail; it's one sentence on something which you've told us had not been a matter of secrecy.</p> <p>A. I did not disclose that at the time to MacGregor. Obviously MacGregor found out later.</p> <p>Q. I know you didn't disclose it at the time, and you didn't disclose it at the time because you did not regard Craig Wright at the time as the inventor of Bitcoin.</p> <p>A. No, that's not true.</p> <p>Q. Because it would have been an obvious and natural point to make in his favour.</p> <p>A. I disagree.</p>	
<p>{Day11/118:25} – {Day11/119:20}</p>	<p>Q. Now, you say in this email: ".. Craig talked to me several times about some work he was doing with virtual currencies." And you say that that happened "during my last year with Centrebet". Now, you refer there to work with "virtual currencies" plural, don't you, not invention of the principal virtual currency; correct?</p> <p>A. Correct.</p> <p>Q. And you say that that took place in your last year with Centrebet which, as we've established, was late 2010 --</p> <p>A. What I should have --</p>	<p>Mr Matthews is questioned about the inconsistency in the dates of his discussions with Dr Wright on "virtual currencies" in this email ("last year with Centrebet" – late 2010-2011), compared to his first witness statement (2007-2008, {E/5/5}). Mr Matthews is evasive and claims</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. -- and late 2011?</p> <p>A. If I was more accurate, I would have said "in my last years at Centrebet".</p> <p>Q. That's not what you wrote, though, is it, Mr Matthews?</p> <p>A. No, it's not what I wrote. It doesn't change the truth.</p> <p>Q. Mr Matthews, reading this email of how you actually introduced Craig Wright in February 2014 makes it perfectly clear that you did not regard him as the inventor of Bitcoin.</p> <p>A. I disagree with that totally.</p>	<p>that the wording of this email is inaccurate.</p>
<p>{E/5/11} – First Witness Statement of Stefan Raymond Matthews</p>		
<p>{Day11/124:10-24}</p>	<p>Q. When you reconnected with Dr Wright and met him in Sydney, he had serious business problems, didn't he?</p> <p>A. He did.</p> <p>Q. You put it in your CoinGeek interview that the staff numbers in his companies had been reduced to nil by the time you were on the scene, didn't you?</p> <p>A. When I arrived in Sydney, that trip, the -- there was no staff in the office at all. The -- the office looked like somebody had blown a whistle, everyone had dropped what they were working on and walked out.</p> <p>Q. And your impression --</p> <p>A. With the exception of two people, who were still doing a few things for him in the background, as close friends, Allan Pedersen and Dr Savannah, but they were not in the office when I went there.</p>	<p>Mr Matthews confirms that Dr Wright's businesses were struggling in mid-2015.</p>
<p>{L9/395/1} – 00006297.appointment</p>		
<p>{Day11/125:15} – {Day11/126:7}</p>	<p>A. It's possible, but the – the reality is that Mr Ayre did not invest in Craig's businesses.</p> <p>Q. But the discussion at that point, whether it was Mr Ayre or you and Mr MacGregor, was about investment in Dr Wright's businesses, wasn't it?</p> <p>A. Yes.</p> <p>Q. It wasn't, for example, Bitcoin trading; it was investment in the actual businesses?</p>	<p>Mr Matthews discusses the purpose of the meeting with Mr Ayre in April 2015, stating that it was not about a sale and purchase of Bitcoin, contrary to Dr</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Yeah, yeah. Yeah. It was, you know, analysing the business and whether there was a viable business opportunity to work with the technology.</p> <p>Q. So if somebody were to say that the only purpose of this meeting and these discussions at the time was a sale and purchase of Bitcoin, you would disagree with that, wouldn't you?</p> <p>A. Sale and purchase of Bitcoin?</p> <p>Q. Yes.</p> <p>A. No, that's not true.</p>	<p>Wright's evidence at {Day7/80:16-25}.</p>
<p>{L9/458/1} – Re: for 1:30 meeting</p>		
<p>{Day11/128:7-16}</p>	<p>Q. {L9/458/1}, please, 18 June, an email from Mr Ayre, at the bottom, discussing focusing on the "LoI". Is that letter of intent?</p> <p>A. Yes, that would be letter of intent.</p> <p>Q. And agreements to get Dr Wright going; do you see that?</p> <p>A. Mm-hm.</p> <p>Q. So by this -- at this point at any rate, Mr Ayre was actively involved in the prospective investment?</p> <p>A. He was actively involved in the discussions around a prospective investment.</p>	<p>Mr Matthews confirms that Mr Ayre was actively involved in discussions around a prospective investment in Dr Wright's company, DeMorgan.</p>
<p>{L9/489/1} – Re: Escrow Agreements</p>		
<p>{Day11/129:23} – {Day11/130:1}</p>	<p>Q. So, at that stage, Dr Wright's businesses were unable even to pay the lawyers who were working on the tax enquiries?</p> <p>A. That's correct.</p>	<p>Mr Matthews confirms that Dr Wright's businesses were in dire financial straits at this time.</p>
<p>{L10/33/2} – term sheet demorgan</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{Day11/131:15-24}	<p>Q. And then the fifth section, the new company was going to enter into a services agreement with Dr Wright for 3.5 million, consisting of a \$1 million initial rights payment, which included the rights to Dr Wright's life story; do you see that?</p> <p>A. Yes.</p> <p>Q. And do you see that referred to the exclusive rights to Dr Wright's life story as a person rather than a company's life story, didn't it?</p> <p>A. Yes, it did.</p>	<p>Mr Matthews confirms that the services agreement included the exclusive rights to Dr Wright's life story as a person rather than a company's life story, contradicting Dr Wright's evidence who said at {Day7/96:17} – {Day7/97:19} – “<i>What they said was they were going to document the growth of the company</i>”</p>
{L10/34/2} – term sheet a sommer		
{Day11/135:5-7}	<p>Q. So the effect of this deal was quite a substantial bail out for Dr Wright and his companies, wasn't it?</p> <p>A. Yes.</p>	<p>Mr Matthews agrees that this deal was a substantial bail out for Dr Wright and his companies.</p>
{Day11/136:2-25}	<p>Q. And as we saw, a part of this deal was that the new company was going to acquire, for significant sums, rights to Dr Wright's life story as well as those intellectual property rights?</p> <p>A. Yes. I go back to the concept of "story". I mean, it was always obvious to us that at some stage or another there would be, you know, public acknowledgement of Craig Wright's involvement in the creation of Bitcoin. But the story rights themselves initially was around being able to document what we were doing in real-time and what the development of nChain was all about. Things flipped after December '15 and - - and I'm sure you're probably going to ask me a lot more -- a lot of questions around that.</p> <p>Q. Absolutely. But the agreement was referring to Dr Wright's life story, wasn't it? We can go back to it.</p> <p>A. Correct, yes.</p> <p>Q. And without being flippant, the life story of Dr Wright, competent IT professional with lots of postgraduate degrees, was hardly going to fly off the shelves in the airport bookshops, was it?</p> <p>A. The life story rights were referring to Dr Wright's involvement in the creation of Bitcoin.</p>	<p>Mr Matthews accepts that the buyout of life story rights related to Dr Wright's involvement in the creation of Bitcoin. This contradicts Dr Wright's evidence at {Day 7/96:11}- {Day7/97:1}- “<i>all of the talks and negotiations were about having basically the new company recorded as it's growing building....it was the life story to do with all the building and the intellectual property</i>”</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{L10/66/1} – 2015-07-04 Watts to Wright		
<p>{Day11/139:2} – {Day11/141:3}</p>	<p>Q. So you're aware, aren't you, that Mr Sommer himself, writing a personal and without prejudice email, explained that he regarded the problems with the documents as extremely serious?</p> <p>A. This is an interesting topic because, in that private conversation that I had with Andrew Sommer, I asked him what evidence existed to suggest that there had been any form of access to the Tax Office system. The assertion was that somebody entered the Tax Office system, changed documents and left the system. There was no evidence of any security breach, there was no investigation around a security breach, and I asked Andrew Sommer, "If there's no evidence and there's no evidence of any attempted entry into that system, why are they pointing the finger at Craig Wright"? And he said, "They told me that if there's anybody in the world that could enter their system, make a change and exit without any footprint, any evidence at all, it would be Craig Wright". But they had no evidence at all.</p> <p>Q. You're aware, aren't you, Mr Matthews, that the ATO, in their decisions, found what they described as dozens of footprints of forgery by Dr Wright? Are you aware of that?</p> <p>A. No, I'm not aware of that. They asserted that it must have been Dr Wright, but there was no – there was no evidence of any breach of their systems whatsoever, from what I was told by Clayton Utz.</p> <p>Q. The email appears simply to be saying that versions of emails submitted by Dr Wright are different or do not correspond to emails on the ATO's systems.</p> <p>A. Yeah, this is a sad email. It came at a – it came at a difficult time and it came with Andrew's apologies, that, "I have to do this because the ATO are a large client of my firm and the other partners have put me in this position where I have no choice".</p> <p>Q. Well, all the indications in the personal email to Ramona Watts are that this is a matter which Andrew Sommer himself took seriously, aren't they?</p> <p>A. Andrew Sommer was protecting his own position.</p> <p>Q. You said a few moment ago that the ATO didn't issue negative decisions in relation to Dr Wright's companies' R&D offset claims; is that right?</p> <p>A. They didn't. They rejected the claims and issued penalties.</p>	<p>Mr Matthews produces a new story concerning a private conversation with Mr Sommer at Clayton Utz.</p> <p>Mr Matthews' new story is inconsistent with the text of the email from Mr Sommers: Mr Matthews states that the ATO was wrongly accusing Dr Wright of hacking their systems, but the email gives no hint of such an accusation and simply states that versions of emails submitted by Dr Wright (i.e., emails with the ATO officials) were different from the versions on the ATO's own systems.</p> <p>The accusation was not that Dr Wright hacked their systems, but that he forged emails; the letter and email from Mr Sommer make clear that Clayton Utz regarded the ATO's position on the forgeries as compelling.</p> <p>Mr Matthews also states that he is unaware of the ATO decisions issued in March & April 2016, rejecting Dr Wright's claims.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. You're not aware that in March and April of 2016, the ATO issued a series of very lengthy, detailed and well-reasoned decisions rejecting those claims?</p> <p>A. No, I'm not aware, I was out of –</p> <p>Q. You didn't receive any of –</p> <p>A. – out of the scene at that stage, I think.</p> <p>Q. March and April 2016 you weren't out of the scene.</p> <p>A. Then I'm not aware of them.</p>	
<p>{Day11/141:4} – {Day11/142:6}</p>	<p>Q. Are you aware that in the context of the ATO decisions, Dr Wright claimed that he made some payments to Professor David Rees for consultancy services?</p> <p>A. Repeat that, please?</p> <p>Q. Are you aware that in the context of those ATO dealings, Dr Wright claimed that he had made payments to Professor David Rees for consultancy services?</p> <p>A. I am aware that that was stated, yes.</p> <p>Q. Are you aware that the -- that Professor Rees' family told the ATO that they'd never heard of Dr Wright and Professor Rees had not done consultancy work and that he was in a nursing home in his last weeks of life when he supposedly engaged in transactions with Dr Wright?</p> <p>A. I'm not aware of any correspondence or communication between the ATO and the Rees family.</p> <p>Q. You don't yourself, do you, attest to these accounts of Dr Wright having dealings with Professor Rees? Do you?</p> <p>A. I don't have any first-hand knowledge or exposure to any dealings that Dr Wright had with Professor Rees.</p> <p>Q. Have you ever seen communications between Dr Wright and Professor Rees?</p> <p>A. I think I saw, in June 2015, what looked like a Bitcoin transfer to an address that was said to be associated with Professor Rees.</p> <p>Q. You're not aware whether that transfer was genuine or whether Dr Wright had genuine dealings with Professor Rees?</p> <p>A. No, I can't say.</p>	<p>Mr Matthews states he has no “first-hand knowledge” of Dr Wright’s dealings with Professor Rees, and yet makes an unsupported statement that he “think[s]” he saw what looked like a Bitcoin transfer to an address associated with Professor Rees, but cannot say if that was genuine or not.</p>
<p>{L10/338/1} – Email from Dr Wright, cwright@tyche.co.uk Re: The book</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{Day11/142:20-25}	<p>Q. So you and Mr Ayre were keen for Dr Wright to make his claim to be Satoshi publicly?</p> <p>A. We were, but there was no timing associated with that. It was not intended to be in 2016 in the way that things unfolded, as MacGregor took an active hand in orchestrating what occurred.</p>	<p>Mr Matthews confirms that he and Mr Ayre wanted Dr Wright to make his claim to be Satoshi publicly.</p>
{Day11/143:15} – {Day11/144:13}	<p>Q. He was, on any view, in this email that we see at the bottom of the page, if we move down, he was talking with no lack of enthusiasm about the contents of the book, wasn't he?</p> <p>A. Yes, he was. He was comfortable with the concept.</p> <p>Q. So by September 2015, he was comfortable with the concept and engaging with what the book would contain?</p> <p>A. No. No. If we're talking -- if you connect the book to the engagement of Andrew O'Hagan --</p> <p>Q. I'm not doing that at the moment. All I'm saying is that, at this stage, he is talking with no lack of enthusiasm about the contents of the book, including in that "PS" we looked at?</p> <p>A. Yeah, he was comfortable with the concept that a book would be written, but there had been no engagement with anyone at this point in time, and I'm talking about September 2015, about actively writing the book.</p> <p>Q. But he certainly wasn't saying in September 2015, "I definitely do not want to come out as Satoshi Nakamoto ever", was he?</p> <p>A. No, he wasn't. He knew that at some stage that would occur, but his wish was that it wasn't until after his children had finished school.</p>	<p>Mr Matthews' evidence about Dr Wright's desire to come out as Satoshi contradicts Dr Wright's position that he did not want to come out as Satoshi Nakamoto in September 2015.</p>
{Day11/144:19} – {Day11/145:24}	<p>Q. Well, if anyone was to say Dr Wright was never going to be revealed as Satoshi until the WIRED and Gizmodo outings made that essential, that would be wrong, wouldn't it? It was always the plan to reveal him as Satoshi.</p> <p>A. It was always understood that it would occur at some point in time, but there was no timeline associated with it.</p> <p>Q. Now, we see, at the top of this email, that Dr Wright was writing from an email address at Tyche.co.uk. Dr Wright was given a formal employment role at Tyche, wasn't he?</p> <p>A. Yes. I can give you the reasons for that.</p> <p>Q. Yes, please.</p> <p>A. When -- when we executed the heads of terms in -- on 29 June, it was always -- it was an understanding, following the signing of that, that the Wrights would move to London. For - for them to move to London and live in London and for Craig</p>	<p>Mr Matthews confirms that Dr Wright was given a formal employment role at Tyche, contrary to s Dr Wright's evidence during days 7 & 8:</p> <p>{Day7/109:14} "Tyche is a British company belonging to Rob that I never worked for"</p> <p>{Day7/110:2} "I'm not Tyche. Never have been.", which Dr Wright confirmed when questioned on this topic again at</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	to work with nChain in London required a visa, a work visa, and MacGregor's company, Tyche, at the time, had an allocation of foreign work permits on its books, and he said, "I'll get human resources to allocate one of those to Craig, we'll enter an employment agreement with Tyche, and then he will be issued with his UK permit and that will allow him to reside in the UK and work for -- for Tyche, and then we will transfer his employment and his visa to the nChain Group, or the NewCo group, once that's set up", and that's what occurred. It actually went, I think, a three step process. It went from Tyche to the workshop to nChain.	{Day8/5:12}- {Day8/7:21}.
{L10/358/1} – RE: Job title and salary for Craig {L11/285/1} – Implementation Deed 07 01 16 Final – Fully Executed		
{Day11/146:1-11}	<p>1 We see here an email chain in September 2015 between you and Kelly Connor of Tyche Consulting Limited, arranging a salary package and job title for Dr Wright with Tyche in connection with, as you say, the visa arrangements?</p> <p>A. Yes.</p> <p>Q. And then {L11/285/1}, please.</p> <p>A. I noticed -- I noticed on the 21 September email, he has a high salary.</p> <p>Q. If we go to the top of the page {L10/358/1}. Yes, £160,000.</p>	This contradicts Dr Wright’s evidence in relation to this email on day 8, where he stated “I don’t see anything about Tyche there. As noted, I was given the chief science officer role at nCrypt, now nChain, so my filing with HMRC for that year has me as chief science officer for nCrypt” ({Day8/9:24}- {Day8/10:11}).
{L11/285/10} - Implementation Deed 07 01 16 Final – Fully Executed {L10/426/1} – Craig Wright – signed contract		
{Day11/147:2-12}	<p>Q. Page 10 {L11/285/10}, paragraph 7.2(a). This records Craig Wright as having: ".. entered into an Employment Contract with Tyche Consulting Limited [with] a salary of £160,000 .. per annum." And that's correct, isn't it, that such an employment contract was entered into?</p> <p>A. I believe so, yes.</p> <p>Q. {L10/426/1}. That's the employment contract. As far as you're aware, that's a genuine document, isn't it?</p> <p>A. As far as I'm aware, yes.</p>	Mr Matthews confirms that Dr Wright entered into an employment contract with Tyche, and that the contract is a genuine document, contrary to Dr Wright’s evidence on Day 8 {Day8/8:1-25}, in which he denies that this document contains his signature.

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{Day11/148:5-24}	<p>Q. But certainly, when Dr Wright was employed by it, from October 2015, and his salary and package set up in the previous month, that was an entirely genuine employment relationship?</p> <p>A. Yes, it was.</p> <p>Q. And because it was in relation to his visa, you would have expected Dr Wright to know about that?</p> <p>A. Sorry, what?</p> <p>Q. Because it was to do with -- necessary for his visa --</p> <p>A. Yes.</p> <p>Q. -- you would expect Dr Wright to know about this employment relationship, wouldn't you?</p> <p>A. Well, he got paid under this -- under this contract, as far as I'm aware.</p> <p>Q. Now --</p> <p>A. Now, I'm looking at the cover page, I don't know what the rest of it is.</p> <p>Q. We can look at the next page to see his signature {L10/426/2}.</p> <p>A. That looks like his signature.</p>	<p>Mr Matthews states that the signature in the employment contract at {L10/426/1} does look like Dr Wright's signature, contrary to Dr Wright's evidence on this document, who at {Day8/7:22}- {Day8/9:2} states "That's actually not my signature" and "I've never once in my life signed without putting "Craig S Wright" individually".</p>
{L10/424/1} – Re: Publication		
{Day11/153:16} – {Day11/154:5}	<p>Q. Mr Matthews, the life story was part and parcel of every single one of these agreements from June 2015.</p> <p>A. A small part.</p> <p>Q. And Dr Wright was perfectly content to go along with the reveal, including providing details and engaging with what the book would contain?</p> <p>A. Dr Wright was content going along with the reveal of his involvement in the creation of Bitcoin, but at a time that suited him, and that time that suited him he repeatedly said was after his children had finished school. He had concerns for his family. He had deep concerns for his family.</p> <p>Q. None of the agreements stipulated that timescale, did they?</p> <p>A. No.</p>	<p>Mr Matthews admits that the "life story" (i.e., Dr Wright's involvement in the creation of Bitcoin) was part of all the agreements entered into from June 2015, and that Dr Wright was content to go along with this reveal.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{L11/25/2} – Re: Reported re: Satoshi		
{Day11/155:1-18}	<p>Q. So at that stage, at least Mr Ayre anticipated Dr Wright coming out within a matter of a few months, didn't he?</p> <p>A. At a -- I will repeat, at a time that was agreed with Craig, not at the time that he was going to be forced to.</p> <p>Q. Mr Ayre cannot have thought that the plan was to delay the reveal for years, could he, based on this email?</p> <p>A. We hadn't decided.</p> <p>Q. He thought that the reveal was going to take place in just "a few more months", didn't he --</p> <p>A. Well, that's not --</p> <p>Q. -- from this email?</p> <p>A. That's not true, because the reveal wasn't at that stage intended to occur at any particular time.</p> <p>Q. And the concern was not about whether the reveal happened but you all keeping control on it when it did happen in short order?</p> <p>A. Yes, it needed to be properly managed.</p>	<p>Mr Matthews accepts that the concern at the time was not whether the reveal was happening but that “it needed to be properly managed”.</p>
{L11/47/1} Email from Mr MacGregor Re: Bakers		
{Day11/155:25} - {Day11/156:24}	<p>Q. And he's setting out various items, including option agreements, an agreement with Mr O'Hagan, patent protection, a risk register and so on. Do you remember those being matters of discussion at this point, shortly before the WIRED and Gizmodo outings?</p> <p>A. No.</p> <p>Q. Item (5), he says: "We're going to need to create a 'proof packet' before too much longer. I've been thinking about this and have a couple of ideas. Activating the SN [Satoshi Nakamoto] wallets goes a long way, but all it really proves is that someone is in control of SN's private keys, which could .. have been transferred or acquired otherwise." And then he suggests documentation and support from a credible blockchain insider; do you see that?</p>	<p>Mr Matthews appears to be accepting that this email is genuine, in contrast to Dr Wright's evidence in Day 7 where he states that he cannot say whether it is genuine or not as it was sent “from someone else to an email address I don't control” ({Day7/107:23}-Day7/108:21}).</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. It was around about this time that MacGregor was starting to move more aggressively towards the outing and getting his thoughts around what that might mean.</p> <p>Q. So this email which you're reading now from 24 November 2015 with those ideas from Mr MacGregor chimes with your recollection of what he was saying around that time?</p> <p>A. Yes. He became far more aggressive and demanding on this after the events in December.</p>	
<p>{Day11/156:25} - {Day11/157:14}</p>	<p>Q. Then do you remember, as you say in your witness statement, that in early December 2015, Dr Wright was outed by WIRED and Gizmodo?</p> <p>A. Yes.</p> <p>Q. They cited as items of evidence some posts on Dr Wright's blog, for example, which were later found to have been modified. Do you remember that?</p> <p>A. No.</p> <p>Q. They cited other items of evidence which were later discredited; do you remember that?</p> <p>A. No.</p> <p>Q. Do you remember that shortly after the initial articles, some follow up pieces emerged suggesting that Dr Wright may be a hoax?</p> <p>A. I remember that.</p>	<p>Mr Matthews denies any recollection of evidence that had been modified/discredited on Dr Wright's blog post.</p>
<p>{L11/187/1} – 00000290_item_msg</p>		
<p>{Day11/161:2-7}</p>	<p>Q. {L11/285/1}, please. Shortly after the stories from WIRED and Gizmodo, Dr Wright and his family made their permanent relocation to the UK, didn't they?</p> <p>A. They had already secured a property in Wimbledon, I think as early as October 2015, but the family relocated shortly after the events of December '15, yes.</p>	<p>Mr Matthews stating that Dr Wright relocated to the UK shortly after the events in December 2015, which is inconsistent with Dr Wright's evidence at {Day7/126:3} – {Day/126:17} where he states that he moved before the articles were published.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{L11/342/2} – Life Story Rights and Services Agreement – 17 Feb 2016		
{Day11/163:8-20}	<p>Q. And do we see that it provided for Dr Wright to receive payments in stages, so 100,000 on signature, 150,000 on completion of a first draft of a manuscript of the story, 250,000 on publication of the first book, and 250,000 on the earlier of a public announcement by EITC of the identity of the creator of Bitcoin or 31 December 2016; do you see that?</p> <p>A. Correct. This agreement was discussed, finalised by Craig Wright, myself and Robert MacGregor in Antigua at the time.</p> <p>Q. So these were milestone payments to encourage Dr Wright in each stage of the process; correct?</p> <p>A. Yes, that's where we were at that point in time.</p>	<p>Mr Matthews admits that the payments to Dr Wright in the EITC Agreement were to “encourage” him at each stage of the process, in contrast to Dr Wright’s account on Day 7 in which he stated that he was very unhappy about entering into this agreement and that Mr MacGregor was using it as leverage ({Day7/132:5} onwards).</p>
{Day11/163:25} – {Day11/165:19}	<p>Q. Page 4 at the bottom {L11/342/4}, clause 4 was entitled "Services", and it's over on page 5 {L11/342/5}, Dr Wright agreed to provide a range of services including making himself available for interviews, provisions of subject materials and so on, didn't it?</p> <p>A. Yeah, there was a lot of discussion about this and it was agreed that MacGregor wouldn't enforce anything that Craig objected to at the time.</p> <p>Q. Any documents supporting that position?</p> <p>A. No, but it was discussed at the time that we were drafting this in Antigua, and there were handshakes and there were agreements as gentlemen as to what would occur.</p> <p>Q. Then page 16 {L11/342/16}, Annex</p> <p>A. If we look at the "Description of the Subject's Life Story" within that agreement, the only life story of any interest to you and Mr MacGregor was the creation of Bitcoin, right?</p> <p>A. Please say that again?</p> <p>Q. The only life story of any interest, based on this Annex A, was Dr Wright's life story supposedly as the creator of Bitcoin?</p> <p>A. Well, that's a significant event in his life story, but his life story's got a lot more interesting stuff in it as well.</p>	<p>Mr Matthews stating that Mr MacGregor would not enforce anything that Dr Wright objected to in the agreement, and that none of this would occur unless it was approved by Dr Wright (completely contrary to Dr Wright’s account on Day 7 {Day7/132:5} onwards).</p> <p>Mr Matthews accepts (after being pressed) that Dr Wright’s life story around the creation of Bitcoin is “an important and significant part of his life story”.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Once again, I have to suggest that Dr Wright's life story would not be a huge crowd-pleaser if it was simply his life story as an information technology security professional.</p> <p>A. It's an interesting career that he has, but, yes, I understand your point that -- that his life story around the creation of Bitcoin is an important and significant part of his life story.</p> <p>Q. So it was clear, as documented in this agreement, that there was going to be a big media process to sell this life story and there were going to be lots of publications about it?</p> <p>A. Yes.</p> <p>Q. And that was consistent with what had been discussed since September and earlier?</p> <p>A. Again, the -- the underlying agreement between us was that none of this would occur unless it was approved at a time that Craig was content with, and he kept saying over and over again that he wanted to ensure that his family and children were clear of school, and safe.</p>	
<p>{Day11/166:3} – {Day11/167:13}</p>	<p>Q. But it's wrong to say, isn't it, that the WIRED and Gizmodo outings led to Mr MacGregor becoming insistent about Dr Wright providing proof, he was --</p> <p>A. No, that's not --</p> <p>Q. -- making clear his desires before that?</p> <p>A. -- that's not wrong -- that's not correct. MacGregor became insistent, unreasonable, dictatorial, day by day, as January unfolded and the rest of the year unfolded. He was aggressive, he was arrogant, he threatened to send Craig back to Australia with not a penny in his pocket, he threatened to cancel his visa, and he did that again in May.</p> <p>Q. We'll look at the emails from May tomorrow, but you are trying to cast Robert MacGregor as the villain, aren't you, Mr Matthews, to provide an excuse for Dr Wright not providing proper proof?</p> <p>A. No, not at all.</p> <p>Q. And when we looked at the emails in September and October 2015 from Mr MacGregor and November 2015, he wasn't being aggressive or unreasonable, he was setting out plans for proof to be provided.</p> <p>A. I had -- during this period between February and May, I had several meetings with MacGregor's head of marketing, Catherine Kauchemann, who repeatedly told me that she was embarrassed by the way that MacGregor was conducting himself, and the pressure that he was putting on Craig and the way that he was putting that pressure on. She told me, late last</p>	<p>Mr Matthews attempts to place blame on Mr MacGregor to provide an excuse for Dr Wright's failure to provide proper proof.</p> <p>Mr Matthews refers to new hearsay evidence from Ms Kauchemann regarding Mr MacGregor's behaviour, a witness who has not been called in these proceedings.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>year, because I spoke to her, and she said, "If you want details of those meetings, you should talk to Victoria Brooks from the Milk agency", because Victoria kept detailed records in a diary. So, I can tell you that it was hostile. The environment was hostile. Every single meeting was hostile, with threats being made and raised voices. It was very, very unpleasant and it was not a good business environment.</p>	
<p>{L11/349/1} – 00000245.email</p>		
<p>{Day11/167:14} – {Day11/170:5}</p>	<p>Q. We'll come to the emails of March and April 2016 shortly, but the emails we've looked at so far don't show Mr MacGregor being hostile, or angry, or threatening, they show him suggesting, in a collaborative way, means of providing proof, don't they?</p> <p>A. Oh, MacGregor was hostile.</p> <p>Q. But answer the question. The emails we've looked at don't show Mr MacGregor being --</p> <p>A. Emails don't show emotion. You can write things in emails, but they don't show the emotion with which the message is being delivered.</p> <p>Q. Early March 2016. By that stage you were making plans for Dr Wright to engage in proof sessions, weren't you?</p> <p>A. What date?</p> <p>Q. By early March 2016.</p> <p>A. I'm going to amend that. MacGregor was making plans, I wasn't.</p> <p>Q. {L11/349/1}, please. This is an email, in the bottom part of the page, 8 March 2016, you forwarding to Dr Wright an email from Jon Matonis to you, to which Dr Wright replies, concerning means of proof; correct?</p> <p>A. Ah, if you're talk -- I need -- I need to know the context of that previous statement that you made to me. When you say I was engaged in organising proof sessions, if you're -- if you're talking about the Matonis and Andresen sessions; is that what you're talking about?</p> <p>Q. Well, that's what we're talking about at the moment.</p> <p>A. Okay, good, now I've got context. Thank you.</p> <p>Q. So you were involved in arranging those?</p> <p>A. Yes, I was. And the Matonis session, I told you that MacGregor, myself and Dr Wright were in Antigua and we were in the discussions around that life story rights agreement.</p>	<p>Mr Matthews confirms that he was involved in arranging the Matonis and Andresen proof sessions.</p> <p>Mr Matthews confirms that it was his suggestion that Jon Matonis could be a person that could participate in a private proof session.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>There was a lot of emotional debate and discussion around proof sessions, and eventually we got to a point where Craig agreed -- Dr Wright agreed that he would do a private proof session to one person to demonstrate to MacGregor that he had that capability. Now, it was -- it was myself that came up with the suggestion that Jon Matonis might be a person that could participate in a private proof session, and the reason I came up with Jon Matonis was because, back in October 2015, when Dr Wright and I were both in London and he was -- he and I were interviewing candidates for positions in the -- in the office in London and he did a -- he participated in an online conference from London in the US that he was asked not to, but he did, and I was having breakfast with him, because we were both staying at the Courthouse Hotel in Oxford Circus, and while we were having breakfast his phone rang, and he was talking to this guy and he says, "Jon, let me introduce you to Stefan", and he hands me the phone, so I had this short conversation with Jon Matonis, who I had never heard of before. So, when we were in Antigua, I said, "What about Jon Matonis, because he has a history in the -- in the ecosystem, and he's a well known person and obviously you have some sort of trust situation with him, Craig?", and he said, "Yes, Jon would be acceptable for a proof". Now, I reached out to Jon. I had no way of connecting with him, Craig didn't have his phone number. I reached out to Jon on LinkedIn, sent him a message and said, "I'd like to talk to you about something", and two days' later he replied, and ultimately I was back in London at that stage, and he and I met at the Boost Juice Bar in Mayfair and that's where it began.</p>	
<p>{Day11/170:12-17}</p>	<p>Q. You were, as we see, actively involved in arranging these proof sessions?</p> <p>A. Yes, I was.</p> <p>Q. And you say that the arranging of these proof sessions was a compromise that had been worked out, initially?</p> <p>A. That's correct.</p>	<p>Mr Matthews again confirms that he was actively involved in arranging the proof sessions for Dr Wright.</p>
<p>{L11/372/1} – 00000035.email</p>		
<p>{Day11/171:1-8}</p>	<p>Q. {L11/372/1}. You sent an email, after that, suggesting that Mr Matonis: “ ... make contact with either Gavin ...” That’s presumably Gavin Andresen, yes?</p> <p>A. Yes.</p> <p>Q. “.. or Mike.” Mike Hearn?</p> <p>A. Yes. Mike was never spoken to, as far as I know.</p>	<p>Mr Matthews confirms that they did not speak to Mr Hearn (in relation to a proof session), as far as he was aware.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{L11/367/1} – 00000032.email {L11/374/1} – 00000014.email</p>		
<p>{Day11/171:14} – {Day11/172:25}</p>	<p>Q. And he says in his third paragraph that he couldn't convince the creator, whom he wasn't naming at that point, to re-send signed emails as requested because there was a desire for no non-physical proof floating around; do you see that?</p> <p>A. Yes.</p> <p>Q. So, it wasn't only Mr MacGregor who was interested in obtaining further objective proof, was it?</p> <p>A. Are you suggesting me?</p> <p>Q. Mr Matonis was.</p> <p>A. Oh, well, Jon, at that stage, had already seen proof, right?</p> <p>Q. Yes, but he said he'd been unable to convince Dr Wright to provide objective proof that he was requesting in the form of two signed emails.</p> <p>A. Yes.</p> <p>Q. Then {L11/374/1}, bottom of the page, you emailed Mr Matonis in response referring to the actual reveal process being likely to: ".. entail a media session on 30 March .. with media releases on 22 April, a press conference on 25 April and the LSE panel event on 27 April."</p> <p>A. That's correct. They're the instructions I received from MacGregor, and they're the instructions that Dr Wright and MacGregor had very strong disagreement on for a week and never agreed to this. Dr Wright never agreed to this. I was instructed by MacGregor to proceed with getting people lined up for this event.</p> <p>Q. You weren't Mr MacGregor's underling, were you, Mr Matthews? You were a businessman in your own right, signatory to these agreements. You were a free agent, weren't you?</p> <p>A. As MacGregor put it, "As long as my money's on the table, you will take instructions from me".</p> <p>Q. You were actively running with this media reveal process with no lack of enthusiasm, weren't you?</p> <p>A. I was running with it. I wasn't enthusiastic about it.</p>	<p>Mr Matthews suggests that he acted solely upon Mr MacGregor's instructions in this media reveal process.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{L11/484/1} – 00000044.email		
{Day11/173:22} – {Day11/174:24}	<p>Q. This is an email that you've specifically referenced in your witness statement, among just 20 in total, 20 documents in total, and you reference it as refreshing your memory. As far as you can recall, this was a genuine exchange of emails?</p> <p>A. As far as I can recall, yes.</p> <p>Q. And we see that Dr Wright's email address is shown as "craig@ncrypt"; do you see that?</p> <p>A. It is.</p> <p>Q. Now, we saw other emails from him, craig@ncrypt, in mid-March 2016 earlier in your testimony; do you recall?</p> <p>A. Yes.</p> <p>Q. And we'll -- and there are further emails from that address going right through to early May 2016. Do you recall receiving emails at the time from Dr Wright at this address?</p> <p>A. No, I -- I wouldn't -- I wouldn't remember what email addresses I was receiving things from in 2016.</p> <p>Q. That's fair. Do you recall a time, any time in this period from mid-March to early May 2016, when it struck you that an email you'd received from Dr Wright didn't make sense, or didn't seem to accord with his views, or didn't seem to come from him?</p> <p>A. I often, even today, receive emails that I would put in that classification.</p> <p>Q. But specifically emails from Dr Wright around that time?</p> <p>A. No, I -- I -- that's an impossible question to answer.</p>	<p>Mr Matthews accepts that, as far as he can recall, the exchange of emails at {L11/484} is genuine, which involves an email sent from Dr Wright's "craig@ncrypt.com" address.</p>
{Day11/175:5-21}	<p>Q. And he says that one thing he would want was to verify, in his computer, either: "A message signed with the ... PGP key Satoshi Nakamoto used in 2010 ..." Or: "A message signed ... from early Bitcoin blocks ... "Yes?</p> <p>A. That's what he says.</p> <p>Q. And he said that he wants to verify this on his computer: "... because it would be easy to modify the pgp or bitcoin software to make it look like signed messages were verifying correctly." Yes?</p> <p>A. That's what he wrote.</p> <p>Q. And he never got to verify on his computer, did he?</p>	<p>Mr Matthews confirms that Mr Andresen never got to verify a message signed with (i) the PGP key Satoshi Nakamoto used in 2010, or (ii) from early Bitcoin blocks.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	A. No, he didn't.	
<p>{Day11/176:18} – {Day11/177:12}</p>	<p>Q. So Dr Wright was trying to manoeuvre the proof sessions away from objective proof, whether that was cryptographic proof or emails or forum posts, towards a technical conversation?</p> <p>A. I don't know what they spoke about. What I do know is that Mr Andresen and Dr Wright communicated with each other. I'm not sure that that was 100% by email, or whether they had telephone calls, I don't know, but I do know that I received an email, and you've probably got it, from Mr Andresen saying, "I'm ready to come to London".</p> <p>Q. The message being delivered in this email on 30 March 2016, can we agree on this, is precisely the message that Dr Wright was delivering to you, trying to avoid cryptographic proof or the provision of early emails or forum posts? That's entirely consistent with the line he was taking, isn't it?</p> <p>A. Well, he was prepared to do a signing with Mr Andresen, but it was under certain conditions, and those conditions were that it was private.</p>	<p>Mr Matthews accepts that Dr Wright was prepared to do a signing session with Andresen, albeit in private.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
DAY 12		
CROSS - EXAMINATION OF STEFAN MATTHEWS BY JONATHAN HOUGH KC		
{L9/467/2} - Emails with Dr Wright discussing ATO, cc Calvin Ayre, Clayton Utz, in June 2015		
<p>{Day12/2:12} - {Day12/3:4}</p>	<p>Q. Page 1, Dr Wright emails Calvin Ayre, copying Mr Philip, yourself and Mr Sommer of Clayton Utz, 20 June 2015: "Privilege and all that as Andrew Sommer is on this as well. "Stefan knows my history with Bitcoin from March 2009 on. "Calvin and Jim know late". That's June 2015, a few months before that email about the book. On your account, Mr Matthews, it's wrong that you first knew about Dr Wright's history with Bitcoin from March 2009, isn't it?</p> <p>A. No, that's incorrect. I have no idea why Craig wrote March 2009 because he'd been working closely with me since 2005 and we'd been discussing aspects of Bitcoin through 2007/2008 and into 2009.</p> <p>Q. An extraordinary mistake from him to make, isn't it?</p> <p>A. You'd have to ask him.</p>	<p>Mr Matthews provides no explanation as to why Dr Wright wrote the incorrect date as to when Mr Matthews first knew about Bitcoin.</p>
{L12/1} - Chain of emails re: Andresen proof		
<p>{Day12/3:12-17}</p>	<p>Q. And Dr Wright was pressing for him to provide proof by way of a conversation about technical stuff; do you remember that?</p> <p>A. I do. But Dr Wright's - that discussion about technical stuff was a precursor to Mr Andresen agreeing to come to London to do a private proof.</p>	<p>Indicator of Dr Wright/Mr Matthews' social engineering in advance of the Andresen signing.</p>
<p>{Day12/4:14} - {Day12/5:1}</p>	<p>Q. Yes. And that would make sense, because the emails are about Mr Andresen's requests. Then Mr MacGregor says: "Can we not split the difference? Can we let him examine a signed message on his computer, but in a controlled environment? Were you able to find, Craig, the original email or other messages you exchanged with Gavin? I know the challenges with the ATO and the control of the keys question, but there are ways to contain it." Now, just looking at this email, that</p>	<p>Mr Matthews concedes that in the email at {L12/1}, Mr MacGregor is seeking to achieve a compromise for Dr Wright.</p> <p>See also the email at {L12/262/1} from 20</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>doesn't show Mr MacGregor being nasty, but seeking to achieve a compromise, doesn't it?</p> <p>A. In this particular email, yes.</p>	<p>April 2016, wherein Mr MacGregor responds to Dr Wright's proposal of a compromise, and states "I think your proposal is utterly reasonable. This is 100% your decision, regardless of the PR team or anyone else's views. I'm behind this completely."</p>
<p>{L12/155} - Emails between Uyen Nguyen and Matthews around signing sessions</p>		
<p>{Day12/5:6-20}</p>	<p>Q. Do you recall that in advance of that signing session, you received some messages which appeared to be from Uyen Nguyen about the Tulip Trust and access to keys? Do you remember any of those?</p> <p>A. Not particularly, no.</p> <p>Q. {L12/155}, an email of 5 April 2016, so a couple of days before the signing session with Mr Andresen, from Uyen Nguyen, supposedly on behalf of the Denariuz Seychelles primary trustee, referring in the last main paragraph to the primary trustee having approved Dr Wright's request for signing of a message. Do you see that?</p> <p>A. I see it.</p> <p>Q. Do you recall receiving emails of that kind --</p> <p>A. Not particularly, no.</p>	<p>Mr Matthews has an inconsistent memory, stating that he has no recollection of the emails at {L12/155}, which are around the same date as the signing session.</p>
<p>{L12/154} Email from Uyen Nguyen to Mr Matthews around signing sessions {L12/153} Email from Uyen Nguyen and Mr Matthews around signing sessions</p>		
<p>{Day12/5:21} - {Day12/6:11}</p>	<p>Q. {L12/154}, this is another email to you, 6 April 2016, and this is also supposedly from Ms Nguyen. She writes here that the Tulip Trading Trust trustee had approved a request for: "... signing a message to be drafted by Dr Wright for the purposes of proving the authenticity of Dr Wright's actions." It then goes on to say: "Please advise within the next 24 hours to settle violations on Tulip Trust asset. Tulip Trading Trust will seek legal protection when trust asset is violated to protect</p>	<p>Mr Matthews accepts that the wording put to him in {L12/154} is very oddly phrased.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>beneficiaries." This is a somewhat oddly phrased email, isn't it?</p> <p>A. It's what, sorry?</p> <p>Q. It's an oddly phrased email?</p> <p>A. Very oddly phrased.</p>	
<p>{Day12/6:12} - {Day12/7:4}</p>	<p>Q. It suggests, doesn't it, that there's a permission, but also a violation in prospect?</p> <p>A. I dealt with Denis on a couple of occasions around this time to receive consent for the use of private keys for the purposes of this private proof session. I didn't deal with this person, I've never met this person. I have a vague idea as to who she is, but it's not someone that I dealt with personally or spoke to personally. Denis -- I can't recall Denis' surname, but Denis was, for my purposes, the trustee of the Tulip Trust and he provided specific approval for the keys to be used for a very specific purpose and only that purpose and only on that occasion. We received the letters from Denis giving that approval, it was either on the morning of the Matonis proof or the evening before, but I know that we were concerned that we might not be able to do the Matonis proof if those letters didn't arrive.</p>	<p>Mr Matthews describes Denis' (presumably Mayaka) alleged role in the Tulip Trading Trust. Mr Matthews states that he has not met Ms Nguyen and did not deal with her.</p>
<p>{Day12/7:14} - {Day12/8:8}</p>	<p>Q. Let's look at another one of these emails on these days. {L12/153}, this one dated from 7 April and yet another email apparently from her to you. This one refers to being concerned about the media event due for 8 April and describing that as "a serious breach in trust policy". Do you recall receiving these sorts of emails from Ms Nguyen at that time?</p> <p>A. I do recall receiving some communication from her and I pretty much ignored it because it was irrelevant to what my purpose was. I was dealing with Denis.</p> <p>Q. Did you ask Dr Wright about these very weird emails you were getting from Uyen Nguyen?</p> <p>A. Yes, I have a recollection of speaking to him about maybe not these emails in particular, but her, and his suggestion to me was to ignore her.</p> <p>Q. How do you think she knew or are you aware how she knew that these signing sessions, which were protected by NDAs and so on, were taking place, if not through Dr Wright?</p> <p>A. I don't know.</p>	<p>Mr Matthews is unable to provide an explanation as to why Uyen Nguyen was aware of the signing sessions.</p>
<p>{L12/225/1} Email chain discussing signing sessions with journalists</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day12/11:11} - {Day12/12:9}</p>	<p>Q. And do you recall you responding along these lines, that you needed to discuss the concept of coin movement, having had an interesting conversation with Rob, you thought there was a worthwhile discussion to be had?</p> <p>A. I don't specifically recall that, but I would concede that it was probably -- well, I wrote it, so, you know, I meant it.</p> <p>Q. So on that basis, looking back and being fair about this, Mr MacGregor had plainly convinced you that there was a discussion to be had and that he wasn't being outrageous or unreasonable?</p> <p>A. No, I wouldn't conclude that at all. My discussions with Mr MacGregor were quite heated at times and particularly through this period.</p> <p>Q. So when you wrote the words: "... I had an interesting conversation with Rob earlier and I think there is a worthwhile discussion to be had ..." What you really meant was, "I've had a heated conversation with Rob and I think he's being really unreasonable"?</p> <p>A. No, that's not what I said. What I meant was, if we sit down and discuss this further, we can possibly come to an arrangement that suits everybody.</p>	<p>Mr Matthews accepts that he wrote the email.</p> <p>Mr Matthews refuses to accept the obvious truth that Mr MacGregor was not being unreasonable, even where the emails from both of them are not confrontational.</p>
<p>{L12/363/2} - Emails and documents with Milk Publicity regarding signing sessions</p>		
<p>{Day12/15:8-19}</p>	<p>Q. So by that stage, there was a plan in place for Dr Wright to sign one or more messages on his blog, at the time of the media reveal?</p> <p>A. There might have been a plan in place because I see the action is for Alan and Nick and Victoria. I don't recall who Alan and Nick are, but Victoria is Victoria Brooks from Milk --</p> <p>Q. Milk Publicity.</p> <p>A. -- Publicity. And this is what I was referring to yesterday, that MacGregor was conceiving plans with Milk around this publicity with the media that was not 100% agreed by Craig Wright.</p>	<p>Mr Matthews accepts that there was a plan for Dr Wright to sign one or more messages on his blog, but that it was not "100%" agreed by Dr Wright.</p>
<p>{Day12/16:1-14}</p>	<p>Q. And these were actions -- these included actions for you, didn't they?</p> <p>A. Me, along with other people. Not me specifically, except the one to do with communicating with Jon and Gavin.</p> <p>Q. Yes, but the first one: "Action [CW, Stefan, Ramona, Kat]: Finalise the technical blog infrastructure, complete the security</p>	<p>Mr Matthews initially admits that the publicity plan included actions for him, but then rows back, stating he had no involvement</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>review and hack-testing, load-testing assessment and fail-over planning, complete the blog content." So you were one of those who were identified as responsible for the preparation for the blog?</p> <p>A. Regardless, I had no involvement in the preparation for the blog.</p>	<p>in the preparation for the blog.</p>
<p>{Day12/17:22} - {Day12/18:15}</p>	<p>Q. So by this stage at least, you were closely involved in the preparations for the big media reveal?</p> <p>A. I was involved in co-ordinating; I wasn't driving or directing.</p> <p>Q. And you certainly didn't respond to that email by taking issue with the central plan for a blog on which Dr Wright would sign messages?</p> <p>A. Not all communication was by email. There were a number of meetings and face to face discussions.</p> <p>Q. But in your in-line responses to that email, you didn't say, "What the hell is this plan about Dr Wright signing blog messages? I never thought that was part of the deal", did you?</p> <p>A. The blog message?</p> <p>Q. Well, if we go back to the --</p> <p>A. Yes, I know what you're talking about.</p> <p>Q. You didn't take issue with that plan which was set out so fully here, did you?</p> <p>A. No, I didn't at the time.</p>	<p>Mr Matthews accepts that he was involved in co-ordinating preparations for the media reveal. Mr Matthews also accepts that, in effect, signing was the plan.</p>
<p>{E/5/21} First Witness Statement of Mr Matthews</p>		
<p>{Day12/18:21} - {Day12/19:14}</p>	<p>Q. May we now go to your witness statement, {E/5/21}, paragraph 99 "I had no involvement in arranging the public proof sessions ..." Would you now qualify that by saying that you in fact had quite a number of significant roles to play in arranging the public proof sessions?</p> <p>A. No, I think the operative word here is "arranging". The public proof sessions were arranged by Milk and MacGregor's team, including Catherine, and I wasn't the person that was setting out the process of what was going to happen in those meetings.</p> <p>Q. So you don't think that ensuring staff were working to handle enquiries to do with them, helping with the blog infrastructure, getting Mr Matonis and Mr Andresen lined up</p>	<p>Mr Matthews refuses to accept the obvious truth that his witness statement is inconsistent with the plain words of the emails indicating that he was involved in arranging the proof sessions, and despite accepting above that he was "involved in co-ordinating"</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>to answer journalists' questions, you don't think that that work had anything to do with arranging the public proof sessions?</p> <p>A. I think those activities are peripheral to arranging.</p>	<p>preparations for the big media reveal.</p>
<p>{Day12/19:15} - {Day12/20:12}</p>	<p>Q. You then go on to paint this picture that you've been giving us in court today about Mr MacGregor bullying Dr Wright, constantly rejecting his ideas, having no concern for him. That's the picture you paint in paragraph 99, isn't it?</p> <p>A. Yes.</p> <p>Q. But the emails consistently tell a different story, don't they, of Mr MacGregor just looking for objective proof and seeking compromise where it could be found?</p> <p>A. If you just rely on the emails, you would be excused for forming a particular opinion, but the reality was that there's another side to this and that's the face to face discussions, the meetings. Of course MacGregor's not going to present a hostile position in emails, but I can assure you he did so, not once, not twice, dozens of times, face to face in meeting rooms.</p> <p>Q. But it goes further than that, doesn't it, Mr Matthews? Your responses to him show you working co-operatively and collaboratively with him, suggesting that his ideas are worth consideration, not treating him as a pariah?</p> <p>A. Yes, I tried to work constructively and collaboratively with him and to act as a bridge between he and Dr Wright.</p>	<p>Mr Matthews continues to assert that Mr MacGregor was very different in emails compared to face to face meetings, in which he was very hostile. This explanation is implausible in light of the contemporaneous emails that he has been shown above.</p>
<p>{L13/40/1} - Email from Ms Brooks at Milk Publicity</p>		
<p>{Day12/21:2-8}</p>	<p>Q. And she sets out in this email, on 29 April, a timeline for 2 May, including, at 07:59, Dr Wright's blog went live, and 07:59 Dr Wright signed block 9. So do you recall that, by this stage at any rate, there was a clear plan for the blog to go live with a message signed using the private key for block 9 on that blog?</p> <p>A. That was the requirement that was set out, yes.</p>	<p>Mr Matthews accepts that there was a plan for Dr Wright's blog to go live with a message signed using the private key for block 9.</p>
<p>{L13/88/1} email plus {L14/327/1} attachment "If I seeing myself Jean v.2"</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{Day12/22:5-8}	<p>Q. And, as you understood it at that time, that draft blog post was supposed to be providing a cryptographic proof, wasn't it?</p> <p>A. I believe that was the intent, yes.</p>	<p>Mr Matthews accepts that the draft blog post was intended to provide a cryptographic proof of Dr Wright being Satoshi.</p>
{L13/64} Emails with MacGregor re signing session		
{Day12/23:1-18}	<p>Q. You, at that point, were again cooperating with Mr MacGregor and taking his ideas perfectly seriously, weren't you?</p> <p>A. Trying to, yes. Trying to -- trying to bridge this conceptual divide that occurred -- that existed between MacGregor and Dr Wright.</p> <p>Q. But, if anything, your response suggests understanding of Mr MacGregor's position and that you have no idea why Dr Wright is taking his position?</p> <p>A. Well, I didn't go back to Mr MacGregor and say, "You're a fool because the genesis block doesn't have a key to sign with". I could have, and I probably should have, but I was more conciliatory than that.</p> <p>Q. But you also didn't suggest that he was being unreasonable to suggest signing with an additional block, did you?</p> <p>A. No, I wouldn't have thought that was unreasonable. Dr Wright didn't agree with me though.</p>	<p>Again, Mr Matthews seeks to place blame on Mr MacGregor.</p> <p>Mr Matthews seeks to explain his response by suggesting he was attempting to be conciliatory - this is, notably, an excuse he also deploys in respect of the Mr Ager Hanssen WhatsApps.</p>
{Day12/23:24} - {Day12/24:1}	<p>Q. Again, no suggestion of tension, difficulty or hostility, is there?</p> <p>A. Not in the email threads, no.</p>	<p>Mr Matthews accepts there is no hostility in the email threads.</p>
{L13/74 - "If I sign myself Jean v5" attachment}		
{Day12/24:23} - {Day12/25:10}	<p>Q. And he copies you, attaching "If I sign myself Jean v5", saying: "See attached input from Stefan and I."</p> <p>A. Yes.</p> <p>Q. And then at {L13/74/1} is "If I sign myself Jean [version] 5". If we can go through it, just briefly, we can see that there are some -- a few comments, but not many. So is it right that</p>	<p>Mr Matthews accepts that the blog post "went through [his] hands" but will not specify to what level he was involved in giving input.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>you, along with Mr Pederson, as his email suggests, had reviewed this blog post at that time and given some input?</p> <p>A. To what level it was reviewed, I couldn't state at this point in time, but it obviously went through our hands.</p>	
<p>{L13/72/1} Email from Mr Macgregor Re: 3, 2, 1...</p>		
<p>{Day12/25:11} - {Day12/26:3}</p>	<p>Q. At that stage, you understood that that blog provided the cryptographic proof which you were all expecting it to, yes?</p> <p>A. That was the intent.</p> <p>Q. {L13/72/1}, please, Mr MacGregor emails on the evening of May 1: "Best of luck to all tomorrow. I can't say how impressed and honoured I've been working with you all on this project." Do you see that?</p> <p>A. I see it.</p> <p>Q. Dr Wright, "Thank you" and Mr Ayre: "Ya ... this is going to be big news."</p> <p>A. Yes.</p> <p>Q. So, is it right that, as those emails suggest, the mood that evening was optimistic with Mr MacGregor and Dr Wright getting on just fine?</p> <p>A. Yes.</p>	<p>Mr Matthews accepts that the mood on the evening prior to the blog release was optimistic, with Mr MacGregor and Dr Wright getting on.</p>
<p>{L13/97/1} - Email exchange with MacGregor, Matthews, Ayre, Wright re blogpost</p>		
<p>{Day12/28:10-15}</p>	<p>Q. Then Dr Wright responds: "The wrong copy was uploaded." And Mr Ayre suggests fixing that. Do you recall Dr Wright's initial response or excuse being that the wrong blog post copy had been uploaded?</p> <p>A. Yes, I do.</p>	<p>Mr Matthews confirms that he recalls Dr Wright's initial excuse for the issue with the signature in the blog post was that the wrong copy had been uploaded.</p>
<p>{Day12/28:16} - {Day12/29:6} {L13/100/1} New Blog Post.docx</p>	<p>Q. Mr MacGregor suggested a new draft blog post, which we see at {L13/100/1}, which proposed a new message signed with private keys linked to the genesis block and block 9. Do you remember Mr MacGregor proposing a new blog post of that kind?</p> <p>A. I just need to study this for a second.</p>	<p>Mr Matthews asserts that he does not recall Mr MacGregor proposing a new blog as set out at {L13/100/1} in response to Dr</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Of course. Take your time.</p> <p>A. Which part do you want me to focus on?</p> <p>Q. Well, if you see simply that this was a blog post which was prepared by Mr MacGregor, according to our records, indicating that there would be a public signing with the genesis block address and the block 9 address. And all I'm asking you is whether you remember Mr MacGregor's response being to propose a new blog in these terms?</p> <p>A. No, I don't.</p>	<p>Wright's excuse regarding the blog post, showing that Mr Matthews has an inconsistent memory regarding these events.</p>
<p>{L13/168/1} Email exchange with Matthews, Wright and Andresen following big reveal</p>		
<p>{Day12/29:24} - {Day12/30:10}</p>	<p>Q. Yes. Is it right that, that day, after the Sartre blog had been discredited, you spoke to Dr Wright, presumably over the phone, while he was in Paris?</p> <p>A. I spoke to Dr Wright a dozen times that morning while he was in Paris.</p> <p>Q. And do you recall that in one or more of those dozen phone calls, he agreed, as you say here, to sign a new message with block 9 and block 1 keys?</p> <p>A. I don't remember it specifically, but I've written it in my email so I would suggest that that's probably what my understanding was at the time that I drafted the email.</p>	<p>Mr Matthews' answer is vague, however he does not deny that Dr Wright agreed to sign a new message with block 9 and block 1 keys.</p>
<p>{Day12/30:23} - {Day12/31:6}</p>	<p>Q. So quite apart from the emails, you recall him indicating that as his initial position at any rate?</p> <p>A. It was one of his positions on that day. It was an extraordinarily chaotic day, as you could appreciate.</p> <p>Q. Do you recall feeling sufficiently confident to tell Mr Andresen that that was his position?</p> <p>A. I felt that I needed to tell Gavin that that was his position. Whether I felt confident that that was what was going to happen was -- I was probably uncertain.</p>	<p>Mr Matthews admits that he felt uncertainty as to whether Dr Wright would sign.</p>
<p>{L13/213/1} Email exchange between Mr Matthews and Mr Matonis</p>		
<p>{Day12/31:22} - {Day12/32:4}</p>	<p>Q. Now, looking back and knowing what you do, the problem with the blog post wasn't incorrect versions of screenshots and code being loaded, was it?</p>	<p>Mr Matthews states that he did not know where the incorrect versions of screenshots/code on</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. No, I believe incorrect versions were loaded, but where the incorrect versions came from I'm unsure.</p> <p>Q. Dr --</p> <p>A. There were so many versions flying around that I couldn't keep track of them myself.</p>	<p>the blog post came from.</p>
<p>{Day12/32:5} - {Day12/33:2}</p>	<p>Q. Let's take this in stages. The Reddit-ers and the journalists discredited the Sartre blog because the key which was referred to in it was not -- or the -- rather the signed message that was referred to in it wasn't a new signed message but was an existing signed message on the blockchain; is that right?</p> <p>A. I believe that is correct, yes.</p> <p>Q. Now, as I think you have said and as certainly Dr Wright has said, it was Dr Wright's intention to put that message in the blog post?</p> <p>A. You'll need to put these questions to Dr Wright. It's my -- it was my understanding at the time, and it's still my understanding, that he deliberately provided incorrect information.</p> <p>Q. So --</p> <p>A. And I use the word "deliberately", not "inadvertently". But why? I don't know.</p> <p>Q. So at least looking at this now, this wasn't a "fuck up", as you put it, this was a deliberate act by Dr Wright, wasn't it?</p> <p>A. Well, I can't be certain because I don't stand in his shoes, but, from where I sat, I felt that incorrect information was provided.</p>	<p>Mr Matthews confirms that he thinks that Dr Wright "deliberately" provided incorrect information for the blog, but does not know why.</p>
<p>{Day12/33:8} - {Day12/34:19}</p>	<p>Q. Well, the court has been able to examine the difference between the blog post as Dr Wright approved it and the blog post as issued by Mr MacGregor, but they both contained, I suggest to you, the same flawed message which the Reddit-ers and which the journalists discredited?</p> <p>A. And I would say that, at that time, MacGregor, nor myself had the ability to be able to determine that.</p> <p>Q. No. No, I'm not suggesting you did. But when you wrote this message around lunchtime on 2 May 2016, did you understand from Dr Wright, from all those discussions, that the failure of the blog post was due to an error or a deliberate inclusion of information that -- or a message that wasn't a true cryptographic proof?</p> <p>A. I think it would be fair and accurate to say that, at that specific time, given the timing of events, I was inclined to understand that it was an error.</p>	<p>Mr Matthews appears to accept that Dr Wright was misleading him as well. Mr Matthews accepts that, at the time he thought it was an error, but now he believes the wrong material had been included deliberately by Dr Wright.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. And that's consistent with what Dr Wright wrote in that exchange with you and Mr Ayre, that the wrong copy had been uploaded, yes?</p> <p>A. It would be consistent with that.</p> <p>Q. So is this fair. Dr Wright was telling you that an error had been made in including the wrong material, when, in fact, what he's told us and I think what he's told you since is that he included precisely what he wanted to?</p> <p>A. That would be a fair statement I think.</p> <p>Q. So on that basis, on that day, Dr Wright was lying to you, wasn't he?</p> <p>A. I don't know. I can't say that. I'm not in a position to be able to determine that.</p> <p>Q. Well, he was telling you that incorrect material had been included in error, when he now tells us, and you understand based on your statement, that incorrect information had been included deliberately?</p> <p>A. At that point in time, he may have believed that incorrect material had been included. I don't know.</p>	
<p>{L13/166/1} Email from Mr Matthews to Mr Andresen following blog release</p>		
<p>{Day12/35:19} - {Day12/36:5}</p>	<p>Q. You've said in your witness statement that you believe that Dr Wright quite deliberately put in a message that wasn't true cryptographic proof?</p> <p>A. That's what I believe now. It's not what I understood on 2 May 2016.</p> <p>Q. I'm not suggesting that that was your understanding then. What I'm suggesting to you is that if Dr Wright told you that incorrect screenshots and code had been provided, and he told you that on 2 May, that was a lie, wasn't it?</p> <p>A. It could have been he -- I can't say whether he was lying or not, but that's what he told me.</p>	<p>Mr Matthews is pressed on whether Dr Wright lied to him on 2 May 2016 about incorrect screenshots/code being provided, Mr Matthews is evasive in response.</p>
<p>{Day12/36:14} - {Day12/37:3}</p>	<p>Q. So do you recall, at that stage, starting to suggest to Mr Andresen the idea of him sending Bitcoin to an address associated with block 9 and that being sent back as a further proof exercise?</p> <p>A. Yes, this was a process that was conceived by Robert MacGregor as a corrective step.</p> <p>Q. L13 --</p>	<p>Mr Matthews provides new evidence, presumably to bolster Dr Wright's reasons for why the information in the blog was incorrect and he was unable to provide proof.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Sorry, I want to add to that.</p> <p>Q. Of course.</p> <p>A. The issue that we discussed at the time is that that was, we believed, contrary to the approval that had previously been given by Denis on how the private keys may be used. And MacGregor was going to explore ways of dealing with that and he took that as his action item from the discussions we had.</p>	
{L13/208.6/1} Email from Andresen to Matthews		
{Day12/37:14-17}	<p>Q. Sorry, let’s keep this on screen.</p> <p>A. Gavin says to me in that email {L13/208.6/1}: “Tell Craig screwing up screenshots is exactly the kind of mistake I can imagine making myself ...”</p>	<p>Mr Matthews highlights additional material from the email that is helpful to Dr Wright.</p>
{L13/101/1} continuation of the chain of emails on 2 May 2016		
{Day12/37:24} - {Day12/38:7}	<p>Q. Mr MacGregor, that afternoon, writes: “It’s not a clerical error at all. “We posted a multi-page and convoluted way to validate a key, which could have been a paragraph, then tripped over that complexity.” So, at least by that stage, it was understood that this was an error of substance rather than just some copy not being included correctly?</p> <p>A. It would appear that way, yes.</p>	<p>Mr Matthews accepts that the error in the blog post was substantive, rather than a clerical error.</p>
{L13/104/1} - Mr Ayre / Mr Matthews emails		
{Day12/38:13- 21}	<p>Q. Then {L13/104/1} I’d like to ask you about. Mr Ayre says: “... lets fix this ASAP then.” And Mr MacGregor writes: “Craig and Stefan are both en route to Wimbledon now to get access to the computer Craig needs.” Do you recall, that afternoon, when Dr Wright came back from Paris, you going to Wimbledon with him to —</p> <p>A. No, I don’t.</p>	<p>Mr Matthews has inconsistent recollections, confirming he does not remember going to Wimbledon following Mr Ayre’s email.</p>
{L13/123/1} Emails between Ramona and Mr MacGregor		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day12/39:19} - {Day12/40:8}</p>	<p>At {L13/123/1}, we see, here, Ramona responding, in the middle of the page, that Dr Wright was working on the blog and triple checking to ensure no mistakes and that Craig could resign transactions on blocks 1 to 9 but nothing could be taken away as discussed. So, at that stage, do you recall, that evening, Dr Wright being positive about doing a further signing, but only being concerned not to have Bitcoin taken away from those early blocks?</p> <p>A. The Bitcoin taken away was the solution to the restriction that Denis put on the use of the private keys. That's how MacGregor conceived this process to fit within those boundaries. Would I say that Dr Wright was positive? No. He was reluctant and argumentative, but appeared to be going along with the process.</p>	<p>Mr Matthews mentions the restriction that Denis put on the use of the private keys, possibly a reference to L13/8, paragraph 2.4 (discussed below {12/45/5} onwards).</p>
<p>{L13/137/1} - 00001114_item.msg</p>		
<p>{Day12/40:17} - {Day12/41:2}</p>	<p>Q. Further up, Mr Andresen has sent an email, according to Mr MacGregor: "Saying 'what is with the funky proof'? Craig has not responded yet but is going to say, ' I [fucked] up but loaded the wrong post, will be reloading this asap.'" Yes?</p> <p>A. Yes.</p> <p>Q. So that's consistent with your recollection that Dr Wright was telling you that this was a simple error?</p> <p>A. Yes, at the time.</p>	<p>Mr Matthews accepts that, at the time, Dr Wright was telling him that the issue with the blog post was a simple error.</p>
<p>{E/5/22} - First Witness Statement of Stefan Raymond Matthews</p>		
<p>{Day12/41:7} - {Day12/42:1}</p>	<p>Q. May we now return to your witness statement before the break, {E/5/22}, paragraph 104. The fourth line down, after referring to the reveal taking place on 2 May, you say that: "... there was a blog post that was meant to occur ..." But you weren't really involved, "or only peripherally", in the discussions between Dr Wright and Mr MacGregor about the blog post.</p> <p>A. That's correct.</p> <p>Q. Would you now accept that you were fairly centrally involved in discussions about the blog post to the extent of reviewing it?</p> <p>A. No. I would still say that "peripherally" is the correct way of explaining what was occurring at the time.</p>	<p>Mr Matthews maintains that he was only "peripherally" involved in discussions about the blog post, not accepting the obvious truth of the contemporaneous emails.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Despite Mr Pederson's email saying that you and he had reviewed it and you were providing input on it?</p> <p>A. Well, there was very little input and the review was a peripheral process to the creation of the blog post.</p>	
<p>{Day12/42:23} - {Day12/44:5}</p>	<p>Q. -- but that isn't what anybody else was saying, is it?</p> <p>A. I don't know what you're referring to.</p> <p>Q. Well, the blog post, in reality, had been approved by Dr Wright and issued in broadly the terms that were planned, hadn't it?</p> <p>A. The blog post material was provided by Dr Wright.</p> <p>Q. Yes.</p> <p>A. There was -- the posting of that material was done by MacGregor. Posting occurred late at night, 11.00, 11.30, maybe even after midnight, I'm not 100% certain. I was staying in my apartment at the time in London in Piccadilly, and MacGregor was calling me every 10 or 15 minutes asking if I'd heard from Dr Wright. My answer was no. Dr Wright wasn't replying to MacGregor. MacGregor said to me, "We're getting to a point I have to post, I've made some edits to this post" -- I don't know what the edits were -- and the post was made.</p> <p>Q. But the part of the blog post that was unsatisfactory, the part of the blog post that was the problem was the message that wasn't a proof; correct?</p> <p>A. The signatory?</p> <p>Q. Yes.</p> <p>A. I doubt that MacGregor modified that, but I don't know.</p> <p>Q. We know he didn't, so on that basis, the problem with this post was not a combination of Mr MacGregor changing some things and Dr Wright sending accidentally any incorrect material; the problem with the post was Dr Wright sending Mr MacGregor a proof that wasn't a proof?</p> <p>A. Isn't that what I'm saying in paragraph 104?</p> <p>Q. Well, you suggest --</p> <p>A. My personal assumption is that it was deliberate sabotage by Dr Wright who did not want to do this.</p>	<p>Mr Matthews accepts that Mr MacGregor did not modify the part of the blog post that was the problem, i.e. that Mr MacGregor's edits were not likely to be consequential.</p> <p>Mr Matthews also states that he believes the blog post was deliberate sabotage by Dr Wright (who did not want to do it).</p>
<p>{Day12/44:6-18}</p>	<p>Q. What you don't say is that the information about the problem being due to incorrect material came only from Dr Wright; that's the case, isn't it?</p> <p>A. Restate that, because that sounded confusing to me.</p>	<p>Mr Matthews accepts that it was Dr Wright who gave the initial explanation that the problem with the blog post was that the wrong</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Okay. The only person who said the problem with this blog post is that the wrong material was uploaded in error, the only person who said that was Dr Wright?</p> <p>A. That was where that initial explanation came from. It came from Dr Wright.</p> <p>Q. And that was incorrect because the problem with the blog post was not an error, but that it quite deliberately did not include proper proof?</p> <p>A. That's what I said.</p>	<p>material had been uploaded.</p>
<p>{L13/8/2} - Limited Consent and Indemnity</p>		
<p>{Day12/46:21} - {Day12/47:12}</p>	<p>Q. If we go back to the second page, {L13/8/2}, do you recall receiving this document around that time, or a document of this kind, providing the consent required for the signing sessions in advance of the big reveal exercise?</p> <p>A. Big reveal exercise?</p> <p>Q. Well, the big reveal exercise on the days that followed, which we saw planned out in those Milk Publicity emails?</p> <p>A. No.</p> <p>Q. So you don't recall receiving a document of this kind?</p> <p>A. Of this kind, related to the Milk Publicity PR sessions that were held that I wasn't at?</p> <p>Q. We saw that you were an addressee of that email?</p> <p>A. Yes. But, no, I don't remember. This is consistent with the consent that was given prior to the Matonis and Andresen private proof sessions, but I can't say that what I saw was in this form.</p>	<p>Mr Matthews does not recall receiving the document at {L13/8/2}, although accepts it is consistent with the consent that was given prior to the private proof sessions.</p>
<p>{Day12/47:13} - {Day12/48:5}</p>	<p>Q. Let me ask you about one detail of it to see if it refreshes your memory. Paragraph 2.4 has a representation by Dr Wright: "The total amount of Bitcoin secured within these addresses ... shall not drop below the amounts so secured as of the date of this consent ... For the avoidance of doubt, this restriction would not prevent the receipt of Bitcoin to these addresses and the subsequent transfer out of these deposited amounts, provided however that the amount of Bitcoin within these addresses at no time drops below the Trust Asset Threshold."</p> <p>A. 2.4 would be consistent with the arrangements that were made to -- for BBC and, as I understand it, Matonis and Andresen to send a partial coin to one of those addresses and</p>	<p>Mr Matthews accepts that arrangements were made with the BBC to send Bitcoin.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	for Dr Wright to return that amount. That would be completely consistent with section 2.4 and the way it's described there.	
{Day12/48:13-18}	<p>Q. -- beforehand. But all I was asking you is that, would this document suggesting the groundwork being laid for that Bitcoin transfer exercise be consistent with your recollection of events, that such groundwork was laid?</p> <p>A. Yes.</p>	Mr Matthews admits that preparations for transfer of Bitcoin were made.
{L13/216/3} - 00001134_item.msg		
{Day12/49:7-22}	<p>Q. Sorry. Then over the page, page 3, {L13/216/3}, you were at that point understanding Dr Wright to be working on a blog update, weren't you?</p> <p>A. That's correct.</p> <p>Q. In fact, he worked on that, or was claiming to be working on that during the night, wasn't he? We can see that from page 1, {L13/216/1}, an email from Ramona, at 3.00 am on 3 May: "... getting closer to finishing Allan. But not yet there. A very long night ..."</p> <p>A. Yes, fair enough.</p> <p>Q. So does that accord with your recollection that Dr Wright was claiming to be working on this new blog through the night of 2 to 3 May?</p> <p>A. Yes.</p>	Mr Matthews recalls that Dr Wright was claiming to be working on the new blog through the night of 2-3 May 2016.
{L13/209/1} - 00001203_item.msg {L13/249/1} - 00001206_item.msg		
{Day12/52:1-24}	<p>Q. Because you say in your witness statement that on these days, Mr MacGregor was drafting blog posts for Dr Wright and trying to manipulate things?</p> <p>A. Yes, he was.</p> <p>Q. What I'm suggesting is that he was actually sharing blog posts at every stage with Dr Wright for his views?</p> <p>A. I can tell you he didn't share every blog post with Dr Wright for his views, because I sat with him in his boardroom and he wrote two blog posts, from memory, on his laptop and posted them in front of me.</p>	Mr Matthews asserts that Mr MacGregor did not share every blog post with Dr Wright for his views, and that he wrote two posts on his laptop and posted them in front of Mr Matthews. It is unclear which blogposts Mr Matthews is referring to, and it is not

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Well, this particular blog post, which has some importance in the case, the “Extraordinary Proof” blog post, that’s one which the emails suggest was approved by the Wrights. Are you able to disagree with that?</p> <p>A. I’m a bit confused, because I’m looking at this and the Ramona reply was “ramona@nCrypt” and I don’t know what Ramona was doing with an nCrypt email address.</p> <p>Q. Well, lots of the emails we’ve seen that you’ve accepted include Ramona with an nCrypt email address.</p> <p>A. It’s puzzling to me, but still ...</p> <p>Q. Mr Andresen and Mr Matonis were given nCrypt email addresses, weren't they, at various points?</p> <p>A. Mr Matonis was, he came to work at nChain after these events.</p>	<p>discussed in his witness statement.</p> <p>When asked if the “Extraordinary Proof” blog post was approved by the Wrights (as suggested by the emails), Mr Matthews is evasive and does not answer the question, instead diverting to a different topic, whether Ramona had an nCrypt email address.</p>
<p>{L13/250/1} - 00000224.email</p>		
<p>{Day12/53:7-25}</p>	<p>Q. {L13/250/1}, please, an email here from you to Mr Andresen on the afternoon of 3 May: "Hi Gavin, "CSW has committed to moving a coin associated with the block 9 address. "The intent is for you to send a coin to that address and then for CSW to return that coin to you." Now, on 3 May, were you in regular contact with Dr Wright again?</p> <p>A. Presumably so, yes.</p> <p>Q. Including over the phone?</p> <p>A. Yes.</p> <p>Q. Do you recall Dr Wright agreeing, at that stage, to move a coin associated with the block 9 address?</p> <p>A. Yes.</p> <p>Q. And in keeping with that, you were then making the arrangements which you understood Dr Wright had agreed to?</p> <p>A. Yes.</p>	<p>Mr Matthews accepts that Dr Wright did agree to move a coin associated with a block 9 address, in contrast to Dr Wright’s evidence on this point, e.g. {8/25/1} onwards, denying that the emails on this topic are genuine.</p>
<p>{E/5/22} - First Witness Statement of Stefan Raymond Matthews {L13/236/1} - 00001071_item.msg</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day12/54:17} - {Day12/57:13}</p>	<p>Q. May we look at your witness statement, {E/5/22}, 106: "In my exchange with Mr Andresen on 2 May 2016, I discussed another option to try to rectify the situation, which would involve Mr Andresen sending Bitcoin to an address associated with block 9 and then Dr Wright sending it back to Mr Andresen. Mr Andresen said he was happy to do that. The piece that is missing from that email is that Dr Wright never agreed to this." Do you now want to correct that -</p> <p>A. Sorry, what are you saying?</p> <p>Q. Fourth line, the sentence: "The piece that is missing from that email is that Dr Wright never agreed to this", namely a move of coin. Do you see that?</p> <p>A. Dr Wright refused, then agreed, then refused.</p> <p>Q. You say here that "Dr Wright never agreed to this". Do you now accept that that's wrong?</p> <p>A. Yes, I'll accept that, at one point in time, he did agree.</p> <p>Q. And he agreed long enough for you to be making arrangements for it on his behalf, didn't he?</p> <p>A. We were making arrangements on his behalf even before he 89 indicated he would do it.</p> <p>Q. So your confident assertion, "The piece that is missing from that email is that Dr Wright never agreed to this", is false?</p> <p>A. Yes, there was a point where he did agree before he retracted that again.</p> <p>Q. {L13/236/1}, we see a continuation of emails or a set of further emails about the PGP key and at least the final one is copied to you at the top of the page; do you see that?</p> <p>A. Yes.</p> <p>Q. Then, if we look at the bottom of the page, Mr MacGregor is recorded asking, that afternoon of 3 May, whether anyone ever signed anything publicly with the PGP key associated with Satoshi. Do you see that?</p> <p>A. Where are you reading?</p> <p>Q. Right at the bottom: "Did you ever sign anything publicly (or privately) with the PGP key associated with Satoshi?" Right at the bottom of the page.</p> <p>A. Yes, I see it.</p> <p>Q. Then there was a response by Dr Wright that there were no signed messages anywhere. Do you see that?</p> <p>A. Yes.</p>	<p>Mr Matthews concedes that his witness statement was incorrect when stating that Dr Wright "never agreed" to move Bitcoin to an address associated with block 9.</p> <p>Mr Matthews also admits the email chain at {L13/236}, which Dr Wright denied was authentic (see {8/34/12 onwards}).</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Then, after a further exchange, we see Mr MacGregor writing that: "We NEED this key today! It's getting late in Seychelles. "We have to get Denis to hunt this down NOW." Yes?</p> <p>A. Yes.</p> <p>Q. Then an email, at the top of the page from Dr Wright, apparently copied to you: "I need one more slice. "... I will be on it ASAP. I have sent a few emails. "It is a work day, so I hope to have it soon. "Uyen has the other one I can access, but I think that is dangerous." Do you remember this discussion taking place that afternoon about your trying to get access to key slices in order to gain access to the private Satoshi PGP key?</p> <p>A. Vaguely, yes. And that would be consistent with the approval that you showed me from Denis a few minutes ago.</p> <p>Q. Well, that approval was concerned with the private keys to the early blocks. This is about the PGP key.</p> <p>A. Oh, key slices. Yes, I must admit my memory around the PGP key is a little vague. I don't have much recollection of those discussions at all.</p>	
<p>{L13/325/1} - 00001120_item.msg</p>		
<p>{Day12/59:1} - {Day12/60:17}</p>	<p>Q. Then, moving to 4 May, {L13/325/1}, we see you, that morning of 4 May 2016, writing: "Update on; "... 'k' value calculation. "... Final required slice of the PGP key." Do you remember what the "'k' value calculation" referred to?</p> <p>A. It's one of the three variables in Bitcoin when you're generating an address.</p> <p>Q. Do you recall why you were asking about that on that morning?</p> <p>A. No, I don't.</p> <p>Q. Then you, according to this, your email referred to a "final required slice of the PGP key" --</p> <p>A. Let me just read this email.</p> <p>Q. Yes, please do. (Pause)</p> <p>A. Yes, I have a recollection of what this is about.</p> <p>Q. Can you tell us?</p> <p>A. Yes. I believe it was associated with a concern that Dr Wright had that in the early Bitcoin code there was some bug</p>	<p>Mr Matthews confirms that this is an email that he wrote, but cannot remember the details of the discussions regarding the PGP key.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>that he was concerned about and this was why he and I had a conversation with Gavin Andresen on the morning that those coins were meant to be sent and moved.</p> <p>Q. Is this right, that was a concern he claimed to have as a basis for not going through with the coin move transaction?</p> <p>A. Yes. Do you want me -- I mean, we have to put it in context so you understand it.</p> <p>Q. We'll come to that in a few minutes --</p> <p>A. Okay.</p> <p>Q. -- to put it in the right context, in fairness to you. But you recall writing this email on that subject, and we also see that it referred to obtaining a final required slice to gain access to the PGP key; is that right?</p> <p>A. Yes, well -- no, I don't remember that part, but I know what the k value is all about.</p> <p>Q. So you think this is an email you wrote, but you can't remember the detail of the discussions about the PGP key?</p> <p>A. Correct.</p>	
<p>{Day12/61:3-5}</p>	<p>Q. So Mr MacGregor was at least trying to deal with Dr Wright's express concerns?</p> <p>A. Yes.</p>	<p>Mr Matthews concedes that Mr MacGregor was trying to deal with Dr Wright's concerns in this email.</p>
<p>{L13/338/1} - 00001160_item.msg</p>		
<p>{Day12/62:21} - {Day12/63:25}</p>	<p>Q. Then Mr MacGregor refers to email communications between Mr Finney and Satoshi and suggests trying to dig those up and offers for himself or you to go to Wimbledon to sift through the email archives.</p> <p>A. Correct.</p> <p>Q. Do you recall on that day Mr MacGregor raising this as another option to provide some --</p> <p>A. I just want to go to the Craig email at 7.35, saying: "I can dig up pictures of the farm." I'm presuming that refers to the farm where he was mining Bitcoin in New South Wales?</p> <p>Q. Your guess is as good as mine.</p> <p>A. That would be my take on that, because it was around this time he asked me to call his ex-wife and ask her if she still had pictures of the server racks in the farm and in the garage, and</p>	<p>Mr Matthews confirms this email chain, and volunteers further detail regarding Dr Wright asking him to call Lynn to see if she still had photos of "server racks" and Dr Wright's equipment. There is no mention of this recollection in Mr Matthews' evidence.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>I did. And the reason he asked me to call her, because when he was contracted through Information Defense to nChain, it was Lynn Wright that used to contact me and send me invoices for payment. So he asked me to call her and, before she said anything, introduce myself and say "Remember me from nChain", which I did. I asked her about the pictures of the racks and she said, yes, she had, to her recollection, a number of pictures in shoe boxes in storage in the garage, which she would dig out for me at some stage, and went on to say that Craig cared more about the equipment in the garage and at the farm than what he did her. So it was interesting to see that reference to digging up pictures at the farm.</p>	
<p>{Day12/64:9-16}</p>	<p>Q. But do you have a recollection of the Finney emails being a subject of discussion around that time?</p> <p>A. Not a major subject of discussion, no.</p> <p>Q. Do you recall at all Mr MacGregor asking about early emails as a form of proof around that time?</p> <p>A. With Hal Finney?</p> <p>Q. With any early Satoshi correspondence?</p> <p>A. Not specifically, no.</p>	<p>Mr Matthews confirms that he does not recall Mr MacGregor asking about early emails with Hal Finney as a form of proof.</p>
<p>{L13/331/1} - 00001188_item.msg</p>		
<p>{Day12/64:17} – {Day12/65:6}</p>	<p>Q. {L13/331/1}, we see here an email from Dr Wright to yourself, Ramona and Robert MacGregor, “nCrypt_Craig”, 4 May 2016. This appears to be an entirely generic article about the genesis block. Do you see that?</p> <p>A. Yes. Looks like it’s a cut and paste from somewhere.</p> <p>Q. You and Mr MacGregor were trying to get Dr Wright to provide some kind of objective proof and here was he providing you with an article that proved nothing; is that right?</p> <p>A. I’m not sure of the context of this.</p> <p>Q. Do you remember getting this sort of infuriating email that provided you with no proof while you were hoping to get something of use?</p> <p>A. Not particularly, no. I would have had no interest in the Genesis block anyway.</p>	<p>Mr Matthews states, implausibly, that he would have had “no interest” in the Genesis block.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{L13/340/1} - 00001201_item.msg		
{Day12/65:12} - {Day12/66:17}	<p>Q. Further up the page, Mr MacGregor responds that it is lower priority, 07.48 email, do you see that?</p> <p>A. Yes ...</p> <p>Q. About a third of the way down the page or halfway down the image we see?</p> <p>A. From Ramona to Robert MacGregor: "But is it low priority?"</p> <p>Q. Just below that: "OK, this one is lower priority, but as soon as we get the transfer done, we need to start building technical credibility on the blog. Ignore for now."</p> <p>A. Yes.</p> <p>Q. Then, at the top of the page, after Ramona has asked whether it's really low priority because it's important for Craig: "If we don't get the transaction posted or something fundamental today, it'll not matter because no one will read it." So these emails suggest that Dr Wright was providing or wanting to discuss technical papers and the like, while you and Mr MacGregor were looking to obtain something in the way of objective proof; right?</p> <p>A. Yes.</p> <p>Q. That must have been infuriating for you?</p> <p>A. Dealing with Craig over the years, I've learnt to contend with him moving off in tangents all over the place.</p> <p>Q. But as we saw with his initial response to Mr Andresen's request for proof, he's trying desperately to pivot away from forms of objective proof, isn't he, at this stage?</p> <p>A. I'm not sure that I would agree with that.</p>	<p>Mr Matthews accepts that these emails show that Dr Wright was wanting to discuss technical papers, while he and Mr MacGregor wanted to obtain objective proof, and that Dr Wright "[moves] off in tangents all over the place".</p> <p>Mr Matthews does not accept the obvious truth that Dr Wright was trying to avoid providing forms of objective proof.</p>
{L13/344/1} - 00001168_item.msg		
{Day12/67:2-21}	<p>Q. If we go further up the page, Ramona is saying: "We are searching hard now." And then that: "Craig thinks he will be able to find them within the hour." And you're quoted in the email chain: "Any value in me going over to Wimbledon this morning and working from there?" Do you remember offering your services in that way?</p>	<p>Mr Matthews confirms that he went to Wimbledon to "make sure that the coins moved" and was trying</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. 4 May was the date that coins were meant to move, right?</p> <p>Q. Yes.</p> <p>A. Yes. I offered in that way, but I was instructed by MacGregor to go over there and make sure that the coins moved.</p> <p>Q. At that stage, as well as being involved in that exercise, you were trying to further the project of getting the Hal Finney emails, weren't you?</p> <p>A. It would look like it, yes.</p> <p>Q. And that would accord with your recollection?</p> <p>A. Yes.</p>	<p>to obtain the early Hal Finney emails.</p>
<p>{L13/277/1} - Signing From Block 9.docx</p>		
<p>{Day12/68:2-24}</p>	<p>Q. And if we look at the blog post, it's {L13/277/1}, "Signing From Block 9.docx". This blog text, if we look at it, envisages an arrangement where The Economist would send a sum in Bitcoin to the block 9 address and Dr Wright would send it back. Based on that email and this blog post, that was what was being proposed as an exercise at that point. Do you remember receiving and forwarding on a blog post of this kind?</p> <p>A. I don't remember it, but I see the email and I did.</p> <p>Q. And it's consistent with what you were doing at that time, laying the groundwork for the coin move with The Economist?</p> <p>A. That's correct.</p> <p>Q. At that stage, so we're now around lunchtime on the 4th, you still thought that Dr Wright was content with that exercise?</p> <p>A. Correct.</p> <p>Q. So right through from part way through 3 May, through to part way through 4 May, you thought that Dr Wright was prepared to go through with this exercise?</p> <p>A. I thought that he would go through with the exercise. It wasn't absolutely smooth waters, but he had agreed that he would.</p>	<p>Mr Matthews accepts that Dr Wright had agreed to do a transfer of Bitcoin from the block 9 address for the Economist, which contradicts Dr Wright's account.</p>
<p>{E/5/23} - First Witness Statement of Stefan Raymond Matthews</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{Day12/72:5-19}	<p>Q. But if Dr Wright was raising a problem with that, there were other forms of objective proof you could have put forward, weren't there?</p> <p>A. Probably, but you've got to put it in context around credibility and everything else that had occurred during that period of time. Moving the coins back and forth was felt to be the absolute --</p> <p>Q. Gold standard?</p> <p>A. Gold standard.</p> <p>Q. But Dr Wright, that day, wasn't offering any form of objective proof, was he?</p> <p>A. Well, at that stage, he'd refused to do it.</p> <p>Q. But he wasn't saying, "I won't do the coin transfer but I'll provide a new signed message to the world"?</p> <p>A. No, he provided no alternative.</p>	<p>Mr Matthews accepts that there were other forms of objective proof that Dr Wright could have put forward if moving coins was a problem, but Dr Wright was not offering any alternative.</p>
{L13/383/1} - 00000239.email		
{Day12/73:21} - {Day12/74:11}	<p>Q. Now, the person attempting to do the persuasion at that stage, shortly before that happened, was you, wasn't it?</p> <p>A. Unfortunately, yes.</p> <p>Q. {L13/383/1}, please, this is an email from you to Mr Andresen the following day. You say in your second paragraph that: "The situation that unfolded this week was horrific ..." You would say that: "... until 1 minute prior to Craig's actions there was no indication that he would default." Do you see that?</p> <p>A. That's correct. From the time that we terminated our conference call on my phone until he left the room there was no indication that he was not -- was going to default.</p>	<p>Mr Matthews confirms the words of the email at {L13/383/1}, and that there was no indication that Dr Wright was going to default.</p>
{Day12/74:20} - {Day12/75:6}	<p>Q. We can take that down. So drawing the threads together, between 2 and 4 May, both you and Mr MacGregor explored a range of ways that Dr Wright could provide some proof, didn't you?</p> <p>A. I guess we did. Did we explore all avenues and ranges? Probably not.</p> <p>Q. But you weren't insistent on just one way. You were, as we saw from the emails, you were canvassing a range of options?</p> <p>A. But we moved fairly quickly to focusing on this three-party movement and return of coins.</p>	<p>Mr Matthews admits that both he and Mr MacGregor worked to explore a range of ways for Dr Wright to provide proof.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day12/75:14} - {Day12/76:2}</p>	<p>Q. And you can't yourself say whether he defaulted because he wouldn't or couldn't provide proof?</p> <p>A. I can't say.</p> <p>Q. Moving then back to the signing sessions with Mr Matonis and Mr Andresen --</p> <p>A. Oh, sorry, I just need to correct what I just said. Given that I had seen him use the private keys in two private proof sessions, I assumed that he could use the private key again for block 9 in the way that this was proposed. So I would say wouldn't, rather than couldn't.</p> <p>Q. But you say that on the assumption that the signing sessions were genuine?</p> <p>A. I believe the signing sessions were genuine.</p>	<p>Mr Matthews initially states he cannot say whether Dr Wright defaulted because he would not, or could not provide proof, but then rows back, and clarifies he meant "wouldn't".</p> <p>Mr Matthews confirms that he believes the signing sessions were genuine.</p>
<p>{L11/367/1} - 00000032.email</p>		
<p>{Day12/76:7} - {Day12/77:24}</p>	<p>Q. Moving back then to the signing sessions, first of all, the one with Mr Matonis, you don't refer to there being any notes of either of those sessions, do you?</p> <p>A. Of the signing sessions? Notes?</p> <p>Q. Notes.</p> <p>A. No. There were no notes.</p> <p>Q. So you're working -- no criticism, but you're working from memory in relation to events of eight years ago?</p> <p>A. Yes.</p> <p>Q. And you weren't yourself involved in the technical exercises, the actual performance of the demonstration?</p> <p>A. No, I was sitting on the other side of the table.</p> <p>Q. Now, in relation to the session with Mr Matonis, you tell us in your witness statement that you recall that three keys were tested, those relating to blocks 1, 9 and either 5 or 7; do you recall saying that in your statement?</p> <p>A. Yes.</p> <p>Q. Dr Wright's recollection in his statement is that two keys were tested, those relating to blocks 9 and 11; are you aware of that?</p> <p>A. No.</p> <p>Q. Mr Matonis' recollection in an email we looked at yesterday, at {L11/367/1}, was that the key related to block 1</p>	<p>Mr Matthews is asked about the signing sessions, and confirms there are no notes of either of them.</p> <p>Mr Matthews confirms that he was in the room, but could not see the computer screen (as he was sitting on the other side of the table) and was not himself involved in the actual performance of the demonstration.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>had been tested and he didn't refer to any others. Are you confident that your recollection is the right one?</p> <p>A. Yes, I am. The reason I am is that I was surprised. Both gentlemen were given the option of selecting at random, without notice, three of the first 10 or 12 blocks and, to my surprise, both chose block 1 and 9 and the other two blocks were different choices, either 5 or 7.</p> <p>Q. You can't recall -- focusing on the Matonis session at the moment, you can't recall whether Dr Wright had the supposed private keys on a USB or hard drive, can you?</p> <p>A. No, I can't.</p> <p>Q. And you couldn't yourself see the computer screen?</p> <p>A. No.</p> <p>Q. But you do recall that the session was carried out on Dr Wright's laptop?</p> <p>A. It was carried out on Dr Wright's laptop with Mr Matonis viewing the screen.</p>	
<p>{Day12/78:17-24}</p>	<p>Q. Now, Mr Andresen recalls that the hotel WiFi was used to connect to the internet and that a WiFi hotspot may have been used. Do you recall that?</p> <p>A. The hotel WiFi was used because we called the business centre supervisor in to provide the connection details to Mr Andresen.</p> <p>Q. Do you recall that a WiFi hotspot may have been used?</p> <p>A. No, it was the hotel WiFi.</p>	<p>Mr Matthews confirms that the hotel WiFi was used to connect to the internet.</p>
<p>{Day12/78:25} - {Day12/79:12}</p>	<p>Q. In the Kleiman proceedings, Mr Andresen told the court that he didn't check that the laptop was factory sealed; is that right?</p> <p>A. Sorry, say that again?</p> <p>Q. In the Kleiman proceedings, Mr Andresen said that he didn't check that the laptop was factory sealed; is that right?</p> <p>A. I would say that's incorrect, because the laptop was brought in in a -- freshly purchased from Curry's in Regent Street -- sorry, Oxford Street, and then brought to the Covent Garden Hotel. It was in its original packaging with the invoice. It was handed to Mr Andresen and he unboxed it.</p>	<p>Mr Matthews asserts that Mr Andresen's evidence in the Kleiman proceedings, stating that he did not check that the laptop used for the demonstration was factory sealed, was incorrect.</p>
<p>{Day12/79:13} - {Day12/80:16}</p>	<p>Q. Now, Mr Andresen, again giving evidence in the Kleiman proceedings, was very clear that it was Dr Wright who had chosen and downloaded the software to be used including the wallet software; that's right, isn't it?</p>	<p>Mr Matthews states that, in relation to the software to be used at the demonstration, Dr Wright was asked what he preferred to</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Dr Wright was asked what he preferred to download and then Mr Andresen actually did the download.</p> <p>Q. Well, I'm going to suggest to you, based on Mr Andresen's evidence, that it was Dr Wright who did the download?</p> <p>A. No, the keyboard was in the control of Mr Andresen.</p> <p>Q. And, again, I'm going to suggest to you, based on -- given Mr Andresen's evidence, that the set-up and all the downloads were done by Dr Wright?</p> <p>A. That's incorrect.</p> <p>Q. You say in your statement that one of the verifications failed and you say that was because an "S" was missed from the message; is that right?</p> <p>A. That's correct.</p> <p>Q. Now, I'm going to put to you, based on the evidence of both Mr Andresen and actually Dr Wright, that what happened was that Dr Wright had asked for the letters "CSW" to be put at the end of the message and that was what was missed. Any recollection of that?</p> <p>A. No. My recollection is it was an "S". Whether it was an "S" in the "CSW" ... but it was an "S" was my recollection.</p> <p>Q. I'm going to put to you that the person who spotted the omission was not Mr Andresen, but Dr Wright?</p> <p>A. Yes, I think that's true.</p>	<p>download and then Mr Andresen did the download. This is different to the evidence of both Mr Andresen (in the Kleiman proceedings) and Dr Wright on this point in these proceedings.</p>
<p>{Day12/80:17-22}</p>	<p>Q. Is it fair to say that, beyond what we have covered, you aren't able to comment on the technical details of the signing sessions, both because you were on the other side of the table and because you're not a technical expert?</p> <p>A. Correct.</p>	<p>Mr Matthews accepts that he is not able to comment on the technical details of the signing sessions.</p>
<p>Dinner with Mike Hearn, July 2016</p>		
<p>{Day12/81:21} - {Day12/82:19}</p>	<p>Q. During the dinner, Mr Hearn, in his statement, describes having asked Dr Wright some technical questions to which he thought Satoshi would know the answers; do you remember that?</p> <p>A. Mike asked a lot of detailed technical stuff that was, in my opinion, heavily related to a number of the patent filing activity that nChain was currently undertaking and I told Craig not to answer them. And I explained to Mike why.</p>	<p>Mr Matthews raises new evidence that he had other contact with Mr Hearn after this dinner in July 2016. Mr Hearn is asked about this during his cross-examination on day 14.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Well, I'm going to put to you what Mr Hearn says because that's rather different. On his account, these were questions not about nChain's patents or new developments for Bitcoin, but about basic features of the original Bitcoin System?</p> <p>A. Well, this is rather interesting because that's not how I recall it. And, interestingly, after that dinner, Mike and I exchanged six/seven emails. I had lunch with him with Marco Bianchi at Marco Bianchi's favourite Italian restaurant in Zurich, and it was quite a lengthy lunch and discussion, and I had a follow-up coffee meeting with Mike Hearn at a coffee shop adjacent to the FIFA museum in Munich a couple of months later, and at no stage did Mike take any issue with the points that you're raising.</p>	
{Day12/83:2-11}	<p>Q. On his recollection, when Dr Wright was struggling with questions, that was when you cut him off, not in order to object to questions about nChain's new work?</p> <p>A. No. That's totally not true. It's kind of interesting because Mr Ager-Hanssen, whose name has come up before, was in Zurich with me not that long ago, back in September, and he asked me for Mike Hearn's contact details, and he and Mr Ali, after my dinner with the two of them, said that they were going to Mike Hearn's house.</p>	Mr Matthews appears to be implying that Mr Hearn is in cahoots with Mr Ager-Hanssen and Mr Ali. Mr Hearn addresses this during his cross-examination on day 14.
{Day12/83:18-21}	<p>Q. Well, you indicated that part of the objective was an opportunity to build support for Dr Wright's claims; you accepted that a few minutes ago?</p> <p>A. No, no, Mike Hearn asked if he could meet Dr Wright.</p>	This is contrary to Mr Hearn's recollection, he gives his account on day 14.
{Day12/84:2-6}	<p>Q. But the fact that, Mr Hearn, having asked these questions, didn't later support Dr Wright's claims rather bears out his position that he was unimpressed, doesn't it?</p> <p>A. I've never asked him to support Dr Wright's claims.</p>	Mr Matthews denies that he ever asked Mr Hearn to support Dr Wright's claims to be Satoshi. However, Mr Hearn was mooted as one of the people who could potentially attend a proof session in emails between Ramona, and Mr MacGregor (to which Mr Matthews is copied), e.g. {L12/111}.
<p>{L16/388/1} - CSW Life Story Rights Termination Release and Assignment - back Agreement 04.05.20.docx</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day12/85:18} - {Day12/86:7}</p>	<p>Q. I see. We can take that off screen now. So in May 2020, the idea of this contract being carried out was given up?</p> <p>A. Yes.</p> <p>Q. Why was it given up?</p> <p>A. We saw no nexus between that and nChain's focus and business.</p> <p>Q. But the -</p> <p>A. MacGregor was out of the scene. Verification of Dr Wright being Satoshi was not an important issue. The business had a completely different strategy and focus.</p> <p>Q. You had given up on a media exercise to prove to the world that Dr Wright was Satoshi in the way planned in mid-2016?</p> <p>A. Correct.</p>	<p>Mr Matthews confirms that he had given up on a media exercise to prove that Dr Wright was Satoshi as originally planned in mid-2016.</p>
<p>{Day12/86:14-18}</p>	<p>Q. Are you aware of Dr Wright also having made very hostile and aggressive posts about Bitcoin developers and people who pursue Bitcoin protocols different from his?</p> <p>A. I've seen a lot of posts that Dr Wright has made that I personally wouldn't have made and I wish he didn't.</p>	<p>Mr Matthews admits that he has seen a lot of Dr Wright's posts, which he wishes that Dr Wright had not made.</p>
<p>{E/27/1} - Second Witness Statement of Stefan Matthews</p>		
<p>{Day12/87:9} - {Day12/88:6}</p>	<p>Q. And you describe being told that the person playing the judge for the event would be a full-time judge but the event could not be recorded because the judge was doing a favour and couldn't be associated with the event?</p> <p>A. That is correct.</p> <p>Q. You don't happen to recall the judge's name, do you?</p> <p>A. No, I wasn't told the judge's name and we were not allowed to interact with the judge.</p> <p>Q. Were you at all troubled about that, a judge being involved but wanting his involvement kept secret?</p> <p>A. I didn't understand then what I understand now.</p> <p>Q. Now, in the course of that exercise, Dr Wright was cross-examined by Mr Ali on some of his reliance documents; is that right?</p> <p>A. A selection of his reliance documents.</p>	<p>Mr Matthews confirms that he was not told the name of the judge at the mock cross-examination, and that Mr Ayre was not present.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. In that mock cross-examination, the view of those watching, not just Mr Ager-Hanssen, but Mr Ali, Mr Ayre and yourself --</p> <p>A. No, Mr Ayre was not there.</p> <p>Q. Ah, he wasn't watching, was he?</p> <p>A. He was not there. When he was told about the event, he said he wanted nothing to do with it.</p>	
<p>{Day12/88:7-20}</p>	<p>Q. Did you not try to make arrangements for Mr Ayre to attend?</p> <p>A. Yes, I did.</p> <p>Q. But he didn't attend?</p> <p>A. I was -- Ali and Ager-Hanssen asked me not to disclose to Mr Ayre what the event was until the day of the event. However, Mr Ayre was already planning to arrive in London on the 21st and I organised to have dinner with him on the 21st, and when Mr Ager-Hanssen found out about that, he invited himself to dinner. So the three of us had dinner. And it was at that dinner that Mr Ager-Hanssen explained to Mr Ayre what was going to happen on the 22nd. And Mr Ayre said, "No, I'm not participating in this event".</p>	<p>Mr Matthews confirms that he tried to make arrangements for Mr Ayre to attend, but that Mr Ayre refused to participate.</p>
<p>{L19/212/6} - Mr Ayre email re: Mock Trial</p>		
<p>{Day12/89:9-15}</p>	<p>Q. {L19/212/1}, please, page 6, {L19/212/6}. Now, this is an email, the body of the email is from Calvin Ayre to Craig Wright, copied to you and others. The email at the top is you forwarding that email to Christen Ager-Hanssen. Mr Ayre has acknowledged this email. Did you receive it?</p> <p>A. Yes.</p>	<p>Mr Matthews confirms that he received the email at {L19/212/1}, contradicting Dr Wright's account that he does not know where this email came from and that it doesn't look like "any of the ones I've got" {8/101/8}.</p>
<p>{Day12/91:2-14}</p>	<p>It's right, isn't it, that Mr Ayre had funded a significant amount of Dr Wright's litigation expenses, isn't it ?</p> <p>A. I'm not quite sure what the relationship was between Dr Wright and Mr Ayre in return -- in association with loans. How that was constructed, I was never a party to it, so I really am not a person who can answer that question.</p>	<p>Mr Matthews admits that there are "loans in place" between Dr Wright and Mr Ayre, presumably to fund this litigation.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. But certainly the natural meaning of this email, which you received, is that Mr Ayre had spent significant sums funding Dr Wright's litigation?</p> <p>A. I don't have any first-hand knowledge but the understanding I had that there were loans in place.</p>	
{Day12/92:5-18}	<p>Q. Then he says, in the last three lines: "This is not how this would play out in the media if we spend toe to toe with COPA and they still win which is what is most likely ..." What do you understand him to mean by saying -- by referring to us "spending toe to toe with COPA"?</p> <p>A. I don't know what that means. I'm assuming he refers to himself and his family office.</p> <p>Q. And that must be a reference to spending within the context of this litigation?</p> <p>A. I don't know.</p> <p>Q. Well, spending "toe to toe with COPA" can only be within this litigation, yes?</p> <p>A. Not something that I've been a party to.</p>	<p>Mr Matthews is evasive when pressed on whether Mr Ayre is funding this litigation, not answering the question and stating that it is not something that he has been a party to.</p>
{Day12/93:10-19}	<p>Q. We can take that off screen now. Just a final couple of minutes, Mr Matthews. You're not aware, are you, how Mr Ayre knew so much about the mock trial exercise and its outcome, are you?</p> <p>A. Well, he was aware of it because he was briefed.</p> <p>Q. By whom?</p> <p>A. By Ager-Hanssen and Ali beforehand, not only on the 21st but at lunch on the 22nd, before the trial occurred.</p> <p>Q. And presumably briefed again afterwards?</p> <p>A. Presumably, yes.</p>	<p>Mr Matthews confirms that Mr Ayre was briefed (up to twice) about the mock trial, showing that Mr Ayre was taking a close interest in the outcome of these proceedings.</p>
{Day12/93:20} - {Day12/95:11}	<p>Q. Just a final minute or two. Mr Matthews, it's right, isn't it, that you have strong personal motivations to back up Dr Wright's claim to be Satoshi?</p> <p>A. What do you mean by that?</p> <p>Q. Well, your company, nChain, has, from the start, based its pitch to market on Dr Wright's supposed work and his claim to be Satoshi, hasn't it?</p> <p>A. There's never been a pitch to market. Nchain is a private company. Nchain benefited enormously in the early days from the acquisition of intellectual property from the DeMorgan Group. A number of white paper titles that came across to nChain through that transaction in 2015 was amazing and enormous. Something in excess of a thousand titles came in to</p>	<p>Mr Matthews denies that Dr Wright's claim to be Satoshi is nChain's pitch to market. Mr Matthews references nChain's many patent filings.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>the nChain business that we created here in London in Oxford Circus. In the first year, we triaged those and refined them to a group of 460 or 480 titles that we felt were the most important titles in the blockchain space, and that was what formed the backbone of the intellectual property filings. And our patent grant rate was remarkable in the first two or three years because of the quality of that intellectual property. We have filed, globally, over 3,000 patent claims and - to date, and 600 or 700 of those have been granted to date. So the nChain business today is what was intended when we set out on this journey in 2015. It is not reliant on Craig Wright. Craig is no longer an employee of nChain UK. He is a consultant to nChain Licensing in Switzerland and that was because Dr Wright was developing a whole raft of inventions that were not related to blockchain at all, and he has filed patent applications for things outside of blockchain, and we - because of how UK law works and employment law, we had to do a carve-out letter to say that nChain didn't have any claim on these things that weren't related to the nChain business. And I've been discussing with Dr Wright for over a year this change of moving him, after he received his UK citizenship and he no longer was reliant on the nChain-sponsored visa, and that occurred some time ago, and we finalised that 30 September last year, and he moved to a consulting agreement on 1 October.</p>	
<p>{Day12/95:12} - {Day12/96:9}</p>	<p>Q. BSV, Bitcoin Satoshi Vision, is also strongly linked to Dr Wright and his claim, isn't it?</p> <p>A. It's strongly linked to Dr Wright. I mean, he always maintained, and Satoshi Nakamoto always maintained that the Bitcoin protocol was able to scale unbounded.</p> <p>Q. Calling it Bitcoin Satoshi Vision and having it promoted by Dr Wright makes it centrally linked to his claim to be Satoshi, doesn't it?</p> <p>A. I'm not so sure that it's even important anymore to be honest.</p> <p>Q. Is it right that nChain is the only developer of BSV?</p> <p>A. No, that's not true.</p> <p>Q. Has nChain itself dealt in BSV and paid its software developers in BSV?</p> <p>A. There may have been a time when staff were offered the option of being able to take part of their salary in digital assets, but I wouldn't have imagined that more than a handful did, and it was only for staff in I think the UK jurisdiction, I'm not sure.</p>	<p>Mr Matthews agrees that BSV is strongly linked to Dr Wright, but when asked about whether it is linked to his claim to be Satoshi, he is evasive in response. Mr Matthews admits that staff at nChain have been offered the option of taking part of their salary in "digital assets" (potentially in BSV).</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. I've already put to you that the value of your family trust holdings in nChain shares and BSV can be expected to rise depending on Dr Wright's claim and its success?</p> <p>A. I honestly can't see it.</p>	
<p>{Day12/96:22} - {Day12/97:5}</p>	<p>NChain's value is based on its intellectual property. Thankfully, thankfully, from 2015, the foundations of that intellectual property came from the DeMorgan Group. Thankfully, in the years since, Craig has been a significant contributor and inspiration to the research team and, thankfully, he has contributed enormously to BSV in the design architecture of Teranode and overlay networks which guarantee the delivery of unbounded scaling on that network.</p>	<p>Mr Matthews is, in effect, accepting a connection between BSV and nChain.</p>
<p>MR JUSTICE MELLOR QUESTIONS FOR MR STEFAN MATTHEWS</p>		
<p>{Day12/97:11} - {Day12/98:11}</p>	<p>MR JUSTICE MELLOR: Mr Matthews, there are a couple of things you can help me with. First of all, in your witness statement, you talk about the USB stick --</p> <p>A. Yes</p> <p>MR JUSTICE MELLOR: -- provided to you in August 2008 and yet you give no detail as to how you date it to August 2008. Do you have any anchor points?</p> <p>A. Well, the anchor point, of course, is that the White Paper itself was released publicly 31 October. So I know that it was before that occurred.</p> <p>MR JUSTICE MELLOR: How do you know that?</p> <p>A. Because the White Paper didn't exist when I was looking at this thing.</p> <p>MR JUSTICE MELLOR: How do you know that?</p> <p>A. Because I would have known if the White Paper had been released.</p> <p>MR JUSTICE MELLOR: Why?</p> <p>A. It would have been public.</p> <p>MR JUSTICE MELLOR: You mean, as soon as it was released, it was well known?</p> <p>A. No, no, that's not the case.</p> <p>MR JUSTICE MELLOR: Okay.</p> <p>A. I think I understand what you're getting at. That was -- that's my best understanding of how to place it in the 2008 calendar.</p>	<p>Mellor J asks Mr Matthews how he recalls that the USB stick provided by Dr Wright is from August 2008. Mr Matthews provides an incoherent explanation, initially stating his "anchor point" was the public release of the White Paper, and he knows the USB stick is from before this. When pressed on how he knows this, he provides a circular and nonsensical explanation.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day12/98:12} - {Day12/99:22}</p>	<p>MR JUSTICE MELLOR: Okay. Yesterday, you talked quite vividly about Mr Ager-Hanssen threatening to destroy you, yes?</p> <p>A. Yes, I did.</p> <p>MR JUSTICE MELLOR: I was curious as to how you thought that that threat would be carried out?</p> <p>A. Online. Online attacks. He has a history -- I've now found out -- of this type of behaviour and in fact anyone with five minutes and a browser, now, can clearly see the type of activity that he's been involved in over the years. Unfortunately, we didn't realise that at the time that we hired him into the nChain Group. We did do -- we did ask for a background check to be done, but the background check didn't raise the things that are quite clearly able to be seen today.</p> <p>MR JUSTICE MELLOR: But what would be the nature of these online attacks?</p> <p>A. Posting personal information about me. Constructing allegations and posting online. He told me that I would never be able to work, my reputation would be destroyed. Frankly, the reason I'm here is because I'm 68 years old, I'm not somebody in my 20s or 30s who is looking to establish a career. I fully expect that Mr Ager-Hanssen -- who is currently in Norway, hanging out at his mother's house with a couple of his associates, who has left this country because of legal activity and there are contempt proceedings associated with his actions and activities at nChain, he has a £95,000 court order for costs against him which is overdue and unpaid, he has at least a dozen or 15 court orders that he has not complied with, so when he sits there in front of me and tells me, "Myself and Mr Ali are going to destroy your life and destroy the reputation of you and your family if you attend court" -- where two months earlier, he was saying exactly the opposite.</p>	<p>Mr Matthews explains the nature of the personal attacks that Mr Ager-Hanssen has been threatening to carry out on him, and states that there is a £95,000 court order for costs against Mr Ager-Hanssen that is unpaid, as well as "at least a dozen or 15 court orders" that he has not complied with.</p>
<p>{Day12/99:23} - {Day12/100:16}</p>	<p>MR JUSTICE MELLOR: Now, you fired him because you were chairman and he was CEO.</p> <p>A. I did fire him. I terminated his consulting agreement.</p> <p>MR JUSTICE MELLOR: Okay. I mean, that tells one something where the balance of power lay; correct?</p> <p>A. Well, he was terminated with cause --</p> <p>MR JUSTICE MELLOR: Mm-hm.</p> <p>A. -- and the details are quite substantial and are subject to other legal proceedings.</p> <p>MR JUSTICE MELLOR: Sure. But since you fired him, has he carried out any of these online attacks on you?</p>	<p>Mr Matthews agrees that he fired Mr Ager-Hanssen, by terminating his consulting agreement, indicating that the balance of power lay in Mr Matthews' favour.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Yes, he's posted recordings of me; he's posted caricatures of me; he's posted internal communications which are confidential with my name on them.</p> <p>MR JUSTICE MELLOR: Is that --</p> <p>A. Numerous.</p> <p>MR JUSTICE MELLOR: Sorry?</p> <p>A. Numerous.</p> <p>MR JUSTICE MELLOR: Right.</p>	
<p>{Day12/100:17} - {Day12/101:2}</p>	<p>A. There was an injunction that was granted, a temporary injunction that was granted. There has been two/three hearings on that and there was a hearing to turn it into a permanent injunction. It was through those processes that a number of orders were given by the court that he hasn't complied with.</p> <p>MR JUSTICE MELLOR: Were these injunctions to prevent him from disclosing information that was alleged by nChain to be confidential?</p> <p>A. Correct.</p> <p>MR JUSTICE MELLOR: Okay. Thank you very much.</p>	<p>Mr Matthews explains the nature of the injunctions granted against Mr Ager-Hanssen, namely to prevent him disclosing information alleged by nChain to be confidential.</p>
<p>RE-EXAMINATION OF MR STEFAN MATTHEWS BY LORD GRABINER KC</p>		
<p>{Day12/101:6} - {Day12/102:11}</p>	<p>LORD GRABINER: Mr Matthews, just a few moments ago, in response to my Lord, you said that Mr Ager-Hanssen had been terminated for cause. What was the cause?</p> <p>A. We're getting into areas of confidentiality again. These matters are for another court, but it started with me receiving a communication from our desktop support team on the 26 or 27 September, alerting me to the fact that Mr Ager-Hanssen had instructed the desktop support team to open up nChain email boxes for eight people, for him to personally have access and review emails. One of those email boxes was mine. The system support team thought that this was an unusual and improper request so they referred it to me. I wrote an email back immediately, copying Mr Ager-Hanssen, saying that this was not authorised, that I felt there were legal issues involved and that the support team could only provide access to somebody's email box if it had board approval to do so. And the board wouldn't give that approval without taking some sort of advice in relation to it anyway. That triggered a series of events on that day where Mr Ager-Hanssen and some security people that he hired took over the nChain office in London and escorted a number of our people out of the office. They taped</p>	<p>Mr Matthews explains the cause of Mr Ager-Hanssen's termination.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>up the cameras of the CCTV footage, they shredded documents in the legal office, they physically broke into the server room and removed CCTV footage equipment from the server room. He was terminated that night.</p> <p>Q. Is there litigation flowing from that?</p> <p>A. There is.</p> <p>LORD GRABINER: Thank you very much indeed.</p>	
<p>CROSS - EXAMINATION OF MR STEVE LEE BY LORD GRABINER KC</p>		
<p>{C/12} - First witness statement of Steve Lee</p>		
<p>{Day12/110:12-24}</p>	<p>Q. In paragraph 8 and again I think in paragraph 12 {C/12/3}, you might just like to refresh your memory by looking at those two paragraphs, you talk about reaching out to a number of "independent people". Why are you so enthusiastic about independence? Why is independence so critical to what you're telling us?</p> <p>A. So, in paragraph 8, the reference to "independent" is kind of tied to what I just said: COPA is not exclusively for Block or any one company; it's intended for -- anyone can join, individuals or any organisation. So the independent people in companies that I reached out to were just other start-ups and other companies that are in the cryptocurrency space.</p>	<p>Mr Lee explains the nature of COPA's independence.</p>
<p>{X/20/2} - Blogpost on case</p>		
<p>{Day12/115:17} - {Day12/116:22}</p>	<p>Q. I think you said a little earlier that the fund funds the developers in their litigation. Do you know if they are funding the developers in this litigation?</p> <p>A. Can you repeat the question, please?</p> <p>Q. Yes. You said a little earlier on the transcript -- we can go back to it if you like, but you talked about the function of the fund being to support financially people in litigation if they're developers; that's right, isn't it?</p> <p>Q. This litigation. You're sitting in the courtroom where this litigation is being conducted.</p>	<p>Mr Lee is questioned on whether he knows if the Bitcoin Legal Defense Fund is funding the developers in this litigation, and Mr Lee is clear in response that he does not know the facts, as this relates to a separate case involving different parties</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Well, I only ask because it's a joint trial with other cases that have been joined. So I don't know the facts, but I would guess it's helping fund legal defence for developers -</p> <p>Q. Yes.</p> <p>A. -- in at least some of the cases that are joined to this.</p> <p>Q. I mean, I ask you because Mr Gunning, who acts for the developers, was pleading poverty at a much earlier stage in this litigation, but you seem to think, rightly or wrongly, that his clients are being funded out of this fund. You think that's quite likely, do you?</p> <p>A. Again, I don't know it to be a fact, but I would guess that's true.</p>	<p>(subsequently joined to the COPA case).</p> <p>Lord Grabiner KC then presses Mr Lee on this question, asking him to speculate on a matter on which he has no factual knowledge.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
DAY 13		
CROSS-EXAMINATION OF MR MARTTI MALMI BY CRAIG ORR KC		
{C/24/1} MM 2nd Witness Statement		
<p>{Day13/6:19} – {Day13/6:24}</p>	<p>Q. And you say there that you did not first approach Dr Wright in February, but only on 1 May 2009; do you see that?</p> <p>A. Yes. Yes, I see that. And I was talking about Satoshi Nakamoto, who I think is a different person than Dr Wright.</p>	<p>Mr Malmi confirming that he does not think Dr Wright is Satoshi Nakamoto.</p>
{L5/53/1} Email sent to Satoshi beginning of May 2009		
<p>{Day13/8:6} – {Day13/8:24}</p>	<p>Q. Now, you're aware of what Dr Wright says, aren't you, in his witness statement, which is that he had in fact contacted you, prior to this email, on forums where Bitcoin had been promoted? You understand that's what he says?</p> <p>A. Yes.</p> <p>Q. And that is in fact correct, isn't it? Your communications was Satoshi before 1 May weren't confined to a single discussion on the anti-state.com forum, were they?</p> <p>A. No, I haven't had a contact -- I have -- I don't consider having been in contact with Satoshi before sending that email, and I didn't discover Bitcoin in February 2009, but in April. That's probably when I started the forum threads also.</p> <p>Q. And how can you be so sure that you only discovered Bitcoin in April?</p> <p>A. I remember that it was not long after -- it was not long after I had discovered Bitcoin that I contacted Satoshi.</p>	<p>Mr Orr KC unsuccessfully attempting to establish that Mr Malmi had other discussions with Satoshi Nakamoto on forums, on the basis of Dr Wright's allegations. Notably, there is no evidence to support this allegation.</p> <p>Mr Orr KC is unsuccessful at undermining Mr Malmi's evidence that Dr Wright was wrong to say the first contact was in February 2009, as Mr Malmi ties his discovery of Bitcoin to the email, recalling that he sent the email not long after he discovered it.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{E/1/26} - Dr Wright's First Witness Statement		
{Day13/19:1} – {Day13/19:15}	<p>Q. And you agree, don't you, that at this time, the bitcoin.org forum was migrated to bitcointalk.org on a different server?</p> <p>A. No, I don't recall the server arrangements, the domain name thing can be changed independently of the servers and I do not recall the timeline of the server migrations in 2011. I think, at some point in 2011, the forum hosting moved to Tibanne, which is the company of Mark Karpelès, behind Mt Gox, was providing us with free hosting at that time. But again, I do not recall the exact timeline.</p> <p>Q. Putting on one side the exact timeline, it's right, isn't it, that the bitcoin.org forum was moved to a new server?</p> <p>A. At some point, yes, and also the domain name changed.</p>	Mr Malmi clarifying that the change of domain name occurred independently of the server migration.
{CSW/1/47} Dr Wright's Eleventh Witness Statement		
{Day13/21:22} – {Day13/22:7}	<p>Q. And it is right to say, isn't it, that the result of moving the bitcoin.org forum to a new server --</p> <p>A. Yes.</p> <p>Q. -- without transferring the original administrator privileges was to remove Satoshi's access?</p> <p>A. No, that was not the purpose.</p> <p>Q. It may not have been the purpose, but it was the effect, wasn't it?</p> <p>A. Yes. It was -- it was the effect, but I have always had great respect for Mr Nakamoto and he would only need to ask to get those credentials if he ever wanted.</p>	Mr Malmi denying that there was any intention to remove Satoshi's access as part of the server migration, and confirming that he could have requested access if he wanted.
{L5/54/15} Q&A Discussions between Satoshi and Mr Malmi		
{Day13/25:18} – {Day13/26:10}	<p>Q. Now, do you recall discussing the concepts of data security and timestamp servers with Satoshi?</p> <p>A. No, I do not recall that.</p>	Mr Orr KC attempting to establish that Dr Wright's IT security expertise is sufficient to demonstrate he has

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Okay. But it's clear, isn't it, that what this post is doing is drawing a connection between the securing of data and Bitcoin's timestamp server?</p> <p>A. That's a lot of text to digest, but, yes, fundamentally, the -- describing the blockchain way of timestamping with proof-of-work.</p> <p>Q. Exactly. And by "blockchain", you mean the timestamp server process that secured the ledger of transactions?</p> <p>A. Yes, and with proof-of-work, to be more specific.</p> <p>Q. And it's right to say, isn't it, that the object of the timestamp server underlying Bitcoin was to maintain a tamper proof record of transactions that was both transparent and verifiable by all participants?</p> <p>A. Yes.</p>	<p>the necessary expertise of Satoshi Nakamoto. Mr Malmi insisting on the importance of cryptographic proof of work.</p>
<p>{Day13/27:22} – {Day13/28:15}</p>	<p>Q. Can you explain what technical steps would be involved in adding a command to the Bitcoin protocol to timestamp a file?</p> <p>A. It would -- you would need to make a hash – a cryptographic hash of the file that you are timestamping and somehow embed it into a transaction, one of the transaction fields.</p> <p>Q. And that would be perfectly technically possible?</p> <p>A. Yes. I think, in fact, there are existing services that let you do this.</p> <p>Q. And indeed, it's right to say, isn't it, that Bitcoin itself has sparked widespread interest in the use of distributed timestamp server technology for purposes other than digital currency transactions?</p> <p>A. Well, I think digital currency is by far the biggest application, but, yes.</p> <p>Q. The concept of distributed timestamp servers is now used beyond digital currency transactions?</p> <p>A. Yes, to some extent, sure.</p>	<p>Mr Orr KC attempting to establish that Dr Wright's IT security expertise is sufficient to demonstrate he has the expertise that is sufficient to be Satoshi Nakamoto.</p>
<p>{C/2/3} First Witness Statement of Martti Malmi</p>		
<p>{Day13/28:24} – {Day13/30:12}</p>	<p>Q. Now, it's right, isn't it that, you also communicated with Satoshi by other means?</p> <p>A. No. He has sent me one private message on the BitcoinTalk forum, but I don't recall ever communicating with Satoshi over other means than email.</p>	<p>Mr Orr KC challenging Mr Malmi's evidence that Satoshi Nakamoto did not communicate with him by direct messages on the</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Are you sure about your recollection, Mr Malmi? Isn't it right that Satoshi did communicate with you by direct messages on the SourceForge forum?</p> <p>A. No, I don't ever recall communicating with him.</p> <p>Q. Well, Dr Wright doesn't accept that, but I've put his position to you. Now, so far as the direct messages on the forum are concerned, do those -- do records of those direct messages still exist?</p> <p>A. Yes, actually, I checked my direct messages on bitcointalk.org and I see that Satoshi has sent me one -- one message, I think in 2010. I haven't sent him any messages over there. I did not see the content of the message, because old messages are archived on BitcoinTalk for security reasons. I have requested unarchival, but I haven't received it yet.</p> <p>Q. And who have you requested that security access from?</p> <p>A. On BitcoinTalk forums there's a function for requesting unarchival of your old messages --</p> <p>Q. And --</p> <p>A. -- so ...</p> <p>Q. -- who currently controls access to that archive.</p> <p>A. I'm not up to date on the current management of the BitcoinTalk forum.</p> <p>Q. Who do you think it is?</p> <p>A. I don't want to speculate on that.</p> <p>Q. Please speculate.</p> <p>A. Well, Theymos -- Theymos was the other server admin who continued after I left.</p> <p>Q. And do you --</p> <p>A. The forum, I mean.</p> <p>Q. Do you know who are the individuals behind Theymos?</p> <p>A. I think Theymos has publicly gone by the name Michael Marquardt, but -- but I have never met him.</p>	<p>SourceForge forum, but with no evidentiary support.</p>
<p>QUESTION FROM MR JUSTICE MELLOR TO MR MARTTI MALMI</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day13/31:1} – {Day13/31:11}</p>	<p>MR JUSTICE MELLOR: Yes, just one question.</p> <p>Questions from MR JUSTICE MELLOR: Mr Malmi, you were asked about the removal of Satoshi’s access.</p> <p>A. Yes.</p> <p>MR JUSTICE MELLOR: And you said he would only need to ask to get credentials if he wanted.</p> <p>A. Yes.</p> <p>MR JUSTICE MELLOR: I assume he never asked; is that right?</p> <p>A. No.</p> <p>MR JUSTICE MELLOR: Okay, thank you very much.</p>	<p>Mellor J querying whether Satoshi Nakamoto ever asked for credentials to the bitcointalk.org forum; Mr Malmi confirming he did not.</p>
<p>CROSS-EXAMINATION OF DR ADAM BACK BY CRAIG ORR KC</p>		
<p>{C/6/2} Mr Wilcox-O’Hearn’s Witness Statement</p>		
<p>{Day13/34:21} – {Day13/35:25}</p>	<p>Q. Could I take you to Mr Wilcox-O'Hearn's witness statement, which is at {C/6/2}. In paragraph 3, he says: "I was involved in cryptography for many years before the development of Bitcoin ... I was good friends with others like Hal Finney, Nick Szabo, Adam Back and Greg Maxwell, and used to hang out on IRC ... channels and chat about open source projects, cryptography, and similar things." Do you see that?</p> <p>A. I see that.</p> <p>Q. Do you agree with it?</p> <p>A. Well, I wasn't using IRC at the time of the cypherpunks forum activity we're talking about, and I did not know Greg Maxwell at that time either. I knew Hal Finney, of course, from interacting on the forums, and Nick Szabo. I knew Zooko was involved with DigiCash, but, you know, I'd never met any of these people in person.</p> <p>Q. So is Mr Wilcox-O'Hearn overstating the connection between you?</p> <p>A. I mean, I wouldn't put a strong kind of feeling on that. You know, maybe some people feel differently about online conversations to in-person friendships, for example.</p> <p>Q. And are you still friendly with Mr Wilcox-O'Hearn?</p>	<p>Mr Orr KC questioning Dr Back on the statements about him in Mr Wilcox-O’Hearn’s witness statement. Dr Back confirming that he is not on good terms with Mr Wilcox-O’Hearn, thereby reinforcing the independence of COPA’s witnesses of fact.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Actually, he blocked me on Twitter some time ago, so evidently not.</p> <p>Q. And what was the cause of that?</p> <p>A. Well, he started Milk(?) Coin and I had some things to say about that which he didn't like.</p>	
<p>{H/182/6} -{H/182/7} – Exhibit SM-10 – Bitcoin’s Academic Pedigree by Arvind Narayanan & Jeremy Clark</p>		
<p>{Day13/43:8} – {Day13/44:24}</p>	<p>Q. Is that a fair description of the kind of research that was being undertaken on proof-of-work in the late 1990s and early 2000s?</p> <p>A. Yes, I mean, there seemed to be multiple people inventing similar things over time. For example, Juels and Brainard's client puzzles, they were unaware of Hashcash and their system is superficially similar. Like, in hindsight, being aware of Hashcash, you could see how to modify Juels and Brainard's later proposal to be as -- to work as Hashcash does, but they do it in an interactive setting, so -- and there are multiple threads like this. The -- I think, one thing to be aware of is the -- even though I have a PhD academic background, I was operating in a more applied sphere here where I was trying to -- interested in designing things that would be secure in practice and there's a bit of a kind of two silos in this kind of research, where the academic silos were interested in publication track records and the sort of applied people are interested in building things, and in this part of my career I was more interested in building things. So there are certainly cases where the academics were unaware of the applied and also where the applied, ie myself, aren't fully aware of the publication records stretching back years.</p> <p>Q. Now, at the beginning of that answer, you said, "there seemed to be multiple people inventing similar things over time"?</p> <p>A. Yes.</p> <p>Q. And it's fair to say that, by the early 2000s, there was a rich source of academic materials on proof-of-work systems?</p> <p>A. Yes, I mean, there was a track on memory hard proof-of-work, which proved to create a lot of papers, and when you get a new idea that enters people's consciousness, sort of the buzz at the moment, you get a lot of sort of derivative papers that think of applications of it or ways to incorporate it into other systems, so there's quite a bit of activity arising from that. And I think there were many more applied people familiar with</p>	<p>Mr Orr KC asking about the research being undertaken on proof-of-work in the late 1990s-early 2000s.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	Hashcash than would have been familiar with the academic history as well.	
<p>{CSW/169/5} – DOS- Resistant Authentication with Client Puzzles by Pekka Nikander & Tuomas Aura</p> <p>{L3/231/3} – Bitcoin White Paper Section 4 – Proof of Work</p>		
<p>{Day13/47:16} – {Day13/50:24}</p>	<p>Q. Now, in Bitcoin, the proof-of-work involves scanning for a value that, when hashed, the hash begins with a specified number of zero bits; that's right, isn't it?</p> <p>A. It's a simplification. It's because the -- this paper and the Hashcash paper is concerning itself with a very coarse-grained type of work where the difficulty can only adjust by a factor of two, then it's leading zeros, but in the Bitcoin case, the precision is much higher, so that it's technically to find a hash which is less than a target. Now, because that is a small – small number relatively, it will have a lot of leading zeros, but technically it's a little more than that, which is, you know, the first digit of the -- that isn't zero has to be below the target and so on, as a kind of floating point number.</p> <p>Q. Now -- well -- so I'm not quite sure what you're saying in that answer, because what I've put to you is precisely how the proof-of-work is described in the Bitcoin White Paper; do you follow?</p> <p>A. Yeah. I'm saying that the -- the way that Bitcoin uses the proof-of-work is a little different. So, when I designed Hashcash, I was -- I considered the case for that difficulty to vary by smaller increments than a factor of two. This paper appears to also use the factor of two simplification, but Bitcoin doesn't, and so Bitcoin is not just looking for leading zeros; it's looking for, you know, one number treated as a floating point to be less than another. And so leading zeros could result -- you know, the specification is not a number of leading zeros in Bitcoin, the specification is a difficulty which is the floating point number. But, you know, still at high level, you can see that there's a lot of work done and you're within a factor of, you know, a small distance of it having the right amount of work, but just in the fine detail, there could be, and there frequently are, Bitcoin proofs of work that have, you know, superficially the right number of zeros, but they're incorrect in the first digit or something. So really it's less than a target. Now I would say this is a fairly obvious optimisation and something I considered in the original Hashcash paper. This paper seems to take the same simplification that I did for the email use case.</p> <p>Q. Can I try to deal with this this way. Can we go to the Bitcoin White Paper in {L3/231/3}. Under the heading "Proof-of-</p>	<p>Dr Back explaining why the proof-of-work in the Bitcoin White Paper is similar to that in Hashcash, rather than that in the Tuomas Aura paper as asserted by Dr Wright.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Work", the second sentence: "The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits." Do you see that?</p> <p>A. I do.</p> <p>Q. Now, are you saying that that is an inaccurate description of the Bitcoin protocol?</p> <p>A. I am. It's a simplification.</p> <p>Q. Dr Back, I suggest to you it's accurate and that you are seeking to escape from what is clear, which is that the proof-of-work methodology in the Bitcoin Paper is similar, in the sense I have put to you, to the proposal devised by Tuomas Aura and others.</p> <p>A. No. I mean, if you -- if you look at it from that point of view, the Aura paper also simplifies to use leading zero bits, as Hashcash is, but the Bitcoin paper -- while the Bitcoin paper is expressed in that way, if you actually look into the details and the code and how it works, the difficulty is a floating point number, so it's a little more nuanced than leading zeros. So Satoshi effectively has simplified his explanation, and this is, I believe, also why Satoshi said that he used a system like Hashcash, which I think is like a small exaggeration, personally, in that he has introduced this floating point concept into it, which, you know, it's something I considered, it may have been discussed on forum lists or not, I don't recall, but it's certainly an obvious optimisation. So I'm just saying that the -- in summary, that the Aura paper and the Hashcash paper are both dealing leading zero bits, but the Bitcoin protocol is actually doing something more fine-grained than leading zero bits which is it has to adjust its difficulty, you know, within a tiny percentage when it -- when it adjusts, otherwise, you know, things will be gyrating on the network.</p>	
<p>{H/184/2} – Exhibit SM-12 – Wei Dai b-money</p> <p>{H/182/6} - {H/182/7} – Exhibit SM-10 – Bitcoin’s Academic Pedigree by Arvind Narayanan & Jeremy Clark</p>		
<p>{Day13/56:17} – {Day13/59:9}</p>	<p>Q. So it's right, isn't it, that in this process -- or in this proposal, solving a computational puzzle was the method by which the money was created?</p> <p>A. That's right.</p> <p>Q. Now, in Bitcoin, proof-of-work is used to secure the ledger and thereby prevent double spending rather than itself representing the money?</p>	<p>Mr Orr KC attempting to get Dr Back to distance Bitcoin from Wei Dai’s b-money proposal, Dr Back responding by explaining the similarities.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. I mean, I would say in Bitcoin that the proof-of-work is satisfying multiple purposes. So it's doing what you said, which is making the ledger immutable over time, but it is also the work that is used to bring new coins into creation.</p> <p>Q. It is, but the creation of the new coins is removed by a number of steps from the solving of the computational puzzle itself?</p> <p>A. I mean, I think only in the extent that multiple coins are produced during the work on a block. You know, originally 50, then 25, that people familiar with Bitcoin would know about that parameter changing over the years. So I think only superficially different in the sense that, you know, there are some formats involved, the coins are inside the format, the person who mines the block puts a public key at which they would be able to spend the coins they mine. So there's some necessary formatting to make that work in a Bitcoin context, but I would say the -- the proof-of-work is creating the coins and that's a critical part of Bitcoin's kind of economic gain theory that makes it robust.</p> <p>Q. It is used in the process which leads to the creation of the coins, but it is not itself the process by which the coins are created?</p> <p>24 A. I mean, I would say it's -- it's cryptographically bound together as an atomic action really. So I don't think -- you know, it's not as if you could do some work and have a certificate and then use the certificate to go and claim the coins. The work commits to the coins, so that it's a kind of atomic operation where you're sort of forced by the effort and the fact that everything is hashed together to decide, you know, which coins, which address, which set of transactions you're going to do the work on. So I think it's bound together, so it's all one thing.</p> <p>Q. I agree it is bound together, but Bitcoin does contrast with the b-money proposal where the solving of the computational puzzle itself led directly to the creation of money?</p> <p>A. I mean, I suppose another way to say it which would square the difference is that in b-money, the work is just creating the coins, whereas in Bitcoin, the work is creating the coins and committing to the ledger history.</p> <p>Q. Let me follow this through by reference to the same article we were looking at. If we can go to {H/182/8}. And if we can look at how the authors put what we are discussing. Under the heading, "Putting it all together", in the second line, they say: "In bitcoin, for the first time, puzzle solutions don't constitute cash by themselves. Instead, they are merely used to secure the ledger." Now, that's correct, isn't it?</p>	

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. I'm not sure really. I mean, it has the same form that we were just discussing, which is it's true that the puzzles are not solely the cash, but it's also -- but it's -- nevertheless it's not true that the -- the work is merely to secure the ledger, because, you know, then you would have two -- two sets of work: one to create the coins and another one to secure the ledger. So it's actually the same work doing both.</p>	
<p>{Day13/59:19} - {Day13/60:18}</p>	<p>Q. Dr Back, I'm well aware that your position is that essentially Bitcoin is a mere development of Hashcash; is that right?</p> <p>A. No.</p> <p>Q. Well, if we can follow what the authors say. If we drop down a paragraph: "Bitcoin neatly avoids the double-spending problem plaguing proof-of-work-as-cash schemes because it eschews puzzle solutions themselves having value. In fact, puzzle solutions are twice decoupled from economic value: the amount of work required to produce a block is a floating parameter (proportional to the global mining power), and further, the number of bitcoin's issued per block is not fixed either." Do you see that?</p> <p>A. I do.</p> <p>Q. And do you agree with it?</p> <p>A. No, for the same reason as before. But I think we are probably just focusing on the way that people express themselves, or the things that seem novel to them in their sort of after the fact description of the system, and you know, it's viable for different people who have an accurate understanding of how the system works to hold slightly different emphasis about, you know, the design, or how it holds together.</p>	<p>Dr Back explaining his position on the article at {H/182}, demonstrating that it is on a topic on which he has a genuine understanding.</p>
<p>{Day13/61:18} - {Day13/62:9}</p>	<p>Q. I don't think there's any controversy that Nick Szabo's proposal also was one of the foundations of Bitcoin. Let me just see whether you would agree with what the authors say at the beginning of this article {H/182/2}. In the second paragraph they say: "This article challenges that view by showing that nearly all of the technical components of bitcoin originated in the academic literature of the 1980s and '90s ... This is not to diminish Nakamoto's achievement but to point out that he stood on the shoulders of giants." Do you see that?</p> <p>A. I do.</p> <p>Q. And one of those giants would have been Nick Szabo?</p> <p>A. It didn't seem that Satoshi knew about Nick Szabo, and I had referred Satoshi to b-money and not Bit Gold for some reason.</p>	<p>Dr Back stating that he does not think Satoshi Nakamoto knew about Nick Szabo.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{L3/192/1} – Dr Back/Satoshi emails		
<p>{Day13/63:22} – {Day13/68:2}</p>	<p>Q. Now, in that final sentence there, you are drawing Satoshi's attention to Wei Dai's web page, aren't you?</p> <p>A. Yes, I'm giving him instructions on how to find it.</p> <p>Q. Yes. And then if we go to his response, he says: "Thanks, I wasn't aware of the b-money page ..." Do you see that?</p> <p>A. Yes.</p> <p>Q. And so, I mean, we can all interpret this email and the court will interpret it, but it is right to say, isn't it, that it's a fair interpretation of this exchange that what Satoshi was saying is that he wasn't aware of the page to which you had referred?</p> <p>A. I mean, the -- he had posted it on the cypherpunks list before, so I was just recounting what I'd seen on the cypherpunks list. And shortly after this, Satoshi did in fact contact Wei Dai and ask exactly what he said here, which is how it to credit b-money, and in his email to Wei Dai, which is public and was published on Gwern's blog, it starts out in the same way, that he wasn't aware of b-money and, I forget the exact wording, but it sort of confirms my interpretation, which is that he wasn't aware of b-money.</p> <p>Q. Well, I suggest to you that what Satoshi said to you is that he wasn't aware of the b-money page. He did not say to you that he was not aware of the concept or the idea of b-money; that's right, isn't it?</p> <p>A. No. I mean, reading Wei Dai's -- the email that Satoshi sent to Wei Dai, it seems to further confirm that Satoshi wasn't aware of b-money. And you know, the -- as I recall, the Bitcoin paper draft at this time didn't cite b-money, and it was only after this exchange with Wei Dai that he added the citation, and I felt slightly remiss in also not pointing him to Bit Gold because I feel Nick Szabo did as much work, if not more, than Wei Dai in developing the idea, but for some reason it didn't -- you know, it wasn't top of mind and so I'd just pointed him to b-money. But in any case, it seemed -- seems to me that, taken together, the email that Satoshi sent to Wei Dai and the email here, that Satoshi wasn't aware of b-money and, you know, when I was asked about this type of thing, probably in 2013 or 2014 on pod casts and so on, so that became relevant, you know, because this was just a, you know, looked at once email thread back then, right, that -- that was my interpretation, and I explain that while I think that he wasn't aware and another</p>	<p>Mr Orr KC questioning Dr Back on his interpretation of his emails with Satoshi Nakamoto directing him to Wei Dai's b-money page.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>question that commonly arises is: was Satoshi on the cypherpunks list? And so I was looking at it in that context.</p> <p>Q. And you agree that this is just your interpretation?</p> <p>A. It was Wei Dai's interpretation as well, and he actually wrote about it. Because I think people like to sort of inveil(?) themselves in the history, because it's -- you know, it's exciting and it's a, you know, portentous thing, and so there were people that tried to push on Wei Dai that he was instrumental in developing Bitcoin, or there are other people who have written about being involved in Bitcoin where it doesn't seem that initially they were, on forums and so on. And so it's a -- Wei Dai, you know, took the step to say that, well, he definitely wasn't involved in sort of design discussions with Satoshi and in fact retorted, well, as far as he was aware, Satoshi didn't even know about b-money so there was no way he could have been instrumental in the design of it, like interactively interacting with Satoshi.</p> <p>Q. No one except Satoshi can know exactly what he was and wasn't aware of, isn't -- that's obviously fair?</p> <p>A. That's a fair comment.</p> <p>Q. And it's also right, isn't it, that in reality, it would be surprising if the creator of Bitcoin was not aware of both the b-money idea and Nick Szabo's idea?</p> <p>A. I'm not sure. So, my supposition, in fact -- and this is speculation -- is that Satoshi, you know, posted the original proposal not on the cypherpunks list but on the cryptography list, and as far as I'm aware, he didn't actually put it on the cypherpunks list at all. And if you look at it, you know, in terms of the knowledge required, it seems plausible that he could have, sort of, had the idea to build an electronic cash system and started from Hashcash, and on some of Satoshi's forum posts he mentions that he had actually implemented Bitcoin before he wrote the White Paper, spent a few years implementing it before writing the paper. So, clearly, the details had been worked out before, because the implementation is -- you know, the specification and the paper actually misses a lot of key points. So, my working thesis is that he -- he was aware of Hashcash because it was more widely known in -- you know, anybody in IT, anybody dealing with spam, people developing internet protocols knew about that in the applied space, though evidently not as much in the academic space, right? And so, you know, that -- that could be a building block. And another reason I might think that is, even before b-money and Bit Gold, after I posted the Hashcash post that we had up on screen, the email from '97, it seemed to spark, independently, in multiple people, the idea that this was somehow like digital gold. I think Rick Solls(?) Had commented there, and a few people had</p>	

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>commented there, and then sort of got stuck on how to adjust the difficulty, ie, if the computers get faster, you would suffer hyperinflation at the rate of Moore's law, this kind of discussion. So -- yeah, so that -- that was my speculation, but that's all it is.</p>	
<p>Communications with Dr Wright</p>		
<p>{Day13/69:10} – {Day13/70:11}</p>	<p>Q. And you're aware that Dr Wright used the handle of "Professor Faustus" on Twitter?</p> <p>A. I -- I know he was on Twitter. I couldn't tell you the handle. He seemed to get banned a few times and create new handles.</p> <p>Q. And you communicated with him on Twitter between around 2012 and 2014?</p> <p>A. I actually interacted with him very little. Somebody I know called Ian Grigg, who I was following, was re-tweeting his -- his discussions about Bitcoin, and I found them annoying and incorrect and so I unfollowed Ian Grigg as a way to mute that conversation. So, following that, I had less, kind of, exposure to the things he was saying, yeah.</p> <p>Q. So far as your forum discussions and chat are concerned, you haven't disclosed any of that material in this case, have you?</p> <p>A. I just provided the emails with Satoshi. I do also get emails, quite a few of them over the years, from various people claiming to be Satoshi Nakamoto, and I stopped reading them because they -- some of them seem, I don't know, sort of like an Elvis impersonator or something, there's something wrong going on with them. And so they're writing a lot and I'm not reading it, and some other people in the Bitcoin development circles are cc'd on these, so I didn't submit any of those, because I didn't assume they were authentic in any way.</p>	<p>Dr Back confirming that he receives quite a few emails from people claiming to be Satoshi, but he has not disclosed them in this case – to which he is not a party.</p>
<p>Bitcoin SV</p>		
<p>{Day13/74:3} {Day13/76:1}</p>	<p>Q. Well, there is a fundamental dispute between you and Dr Wright and BSV, on the one hand, as to what is the appropriate future direction of the Bitcoin System?</p> <p>A. Well, I mean, I think you have to bear in mind that Bitcoin is open technology, and, you know, if I had strong views about some feature that I would like to get into Bitcoin, the chances</p>	<p>Dr Back providing his view on the people who have spun off from Bitcoin, suggesting they are like people who couldn't "change</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>are that I wouldn't succeed at getting into Bitcoin, because it's kind of like trying to propose to modify the rules of the game of chess: you're not going to succeed to modify them unless there's widespread acceptance of that change. And so, people who adopt that kind of enlightened view about how open source projects and a system like Bitcoin with, you know, a vast array of, sort of, financial interest of different parties that hold and invest and develop in it is that you need consensus, and consensus of decision-making process. Thinking back hundreds of years, that is very slow to change and can only achieve change with widespread approval. And so I put it to you that the -- the various forks that have spun off from Bitcoin, Bitcoin Cash, which later split into Bitcoin SV, and a few other forks, were by people who didn't -- you know, didn't accept that they couldn't change the rules of chess and so, you know, set up their own chess game with a niche to one side, and that's, you know -- and that's the economic reality as well, you know, the -- the sum total value of the market value of the forks is sub 1%, right?</p> <p>Q. There is a contrary view, as you know, which is that, in fact, the direction that you and others have taken Bitcoin is it is fundamentally contrary to the original protocol and Satoshi's original vision.</p> <p>A. I mean, I think it's dangerous to, sort of, do kind of biblical interpretations of scripture from Satoshi's writings and try to, sort of, retrofit your views into what he has said on the forums. But I do think that the market is, you know, fairly unanimous in view of Bitcoin as it is today and how it evolved. Now, of course, there are lots of people vying for improvements and optimisations in different directions, but the only changes that go forward are ones that have widespread approval. And so some people, when faced with the change that they want not being accepted, are going to move on and say, well, you know, maybe it will get accepted in the future, and others get, you know, disillusioned, or start their own chains, or start forks, and that is what some people have done, which – and BSV is a fork of a fork at this point.</p>	<p>the rules of chess” and set up “their own chess game”.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
DAY 14		
CROSS-EXAMINATION OF MICHAEL CHRISTOPHER HEARN BY LORD GRABINER KC		
<p>{Day14/2:18} – {Day14/3:1}</p>	<p>Q. I understand. Would we be right in thinking that R3 is a competitor of nChain?</p> <p>A. Well, I'll be honest, I don't really know what nChain does. I'm not really familiar with nChain at all. I could tell you that Corda is not a competitor to Bitcoin. R3 is presumably -- and I think nChain's a Bitcoin-focused company, that's about all I know. So I think they're not really competitors in my view.</p>	<p>Mr Hearn comments that he is not familiar with what nChain does.</p>
<p>{Day14/4:1-13}</p>	<p>Q. And you tell us that you refreshed your memory of what happened on that occasion from the email exchanges about the dinner?</p> <p>A. Yes.</p> <p>Q. So, understandably, you couldn't remember the detail of what happened that far back; is that fair?</p> <p>A. Well, I think I remember most of it, yeah. Actually, when we talked about the refreshing the detail, it was things like the name of the restaurant, or the exact date on which it happened. So, those details I had forgotten, indeed, but the actual discussions that happened during the dinner, I feel I remember pretty well.</p>	<p>Mr Hearn discusses his general recollection of the dinner with Dr Wright in July 2016.</p>
<p>{Day14/6:1} – {Day14/8:1}</p> <p>{D/507/2} Email from Jon Matonis to Mike Christopher Hearn</p>	<p>Q. So, according to that email, Jon Matonis is saying that it was you –</p> <p>A. Yeah.</p> <p>Q. – who asked if he, Jon, could introduce you to Dr Wright. That's not really according with your –</p> <p>A. That's not how I – that's not how I recall it, no.</p> <p>Q. No, I understand that, but it's – of course, the way you now recall it is not consistent either with the contemporaneous email, is it?</p> <p>A. Well, he – I didn't write that, he did.</p> <p>Q. I appreciate that, but did you ever respond to the email?</p> <p>A. No. My understanding is that Jon wanted me to meet Craig Wright and I was like, "Okay, fine, whatever", and then Jon translated this acquiescence into me wanting to meet him, but I didn't really care either way, to be honest, so ...</p> <p>Q. Well, I'm assuming you're being honest, obviously.</p>	<p>Mr Hearn discusses the background to his dinner with Dr Wright.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Well, yeah.</p> <p>Q. You see, when somebody tells a story about events happening eight years earlier and there's a contemporaneous record which is not consistent with it, it does perhaps –</p> <p>A. Yes, I understand.</p> <p>Q. – suggest that the memory may not be quite accurate. Is that a fair point?</p> <p>A. Well, I think the parts I remember are the important parts, which are what happened during the dinner and what Craig Wright said.</p> <p>Q. Well, we'll come to that.</p> <p>A. Yeah, the exact details of, you know, what Jon said at a conference, or who asked to meet who, I don't believe I asked to meet him myself.</p> <p>Q. So I –</p> <p>A. I would not have reached out, right? I did not email Craig directly, for example. This has all be done –</p> <p>Q. No, that's why –</p> <p>A. – through Jon.</p> <p>Q. – you wanted to use – to get to him through Jon Matonis, didn't you?</p> <p>A. No. I didn't particularly want to get to him at all.</p> <p>Q. I see. Anyway, what I suggest is that it was you who wanted to meet Dr Wright.</p> <p>A. Well, I reject that claim.</p> <p>Q. So you didn't want to meet him at all?</p> <p>A. No, no, no, I didn't particularly –</p> <p>Q. You were happy to meet him?</p> <p>A. I was happy to meet him because Jon asked me to, yeah, as far as I recall. And I don't particularly argue with people like that on threads about minor details.</p>	
<p>{Day14/11:2-6}</p>	<p>Q. Did you sign a non-disclosure agreement before that dinner?</p> <p>A. No, not that I recall.</p> <p>Q. Were you asked to sign one?</p> <p>A. No, I don't think so.</p>	<p>Mr Hearn confirms that he did not sign an NDA before the dinner with Dr Wright and that he was also not asked to sign one.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day14/11:13} - {Day14/12:8}</p>	<p>Q. No, I understand. But, I mean, you're saying you know nothing about nChain's business?</p> <p>A. I think -- so I'll tell you what -- everything I know, if that's okay? So I believe nChain is a company that does Bitcoin-related things that Craig Wright is involved in. It's focused exclusively on Bitcoin, as far as I understand, and I believe they've funded Bitcoin-related software.</p> <p>Q. Well, one area of competition between the two entities concerned the scalability of blockchain transactions. Did you know that?</p> <p>A. Well, I know that Craig Wright has been concerned with Bitcoin scalability and scalability is a general concern for all such systems.</p> <p>Q. Including R3?</p> <p>A. Any company that makes software, like database software, has to be concerned with scalability, yeah, that's not something --</p> <p>Q. That's an area of common interest, so to speak, between those businesses?</p> <p>A. Yeah, I guess.</p>	<p>Mr Hearn confirms that scalability is a concern for many companies, so not a basis for inferring that R3 competes with nChain.</p>
<p>{Day14/12:9} - {Day14/13:4}</p>	<p>Q. You suggest in your witness statement that Stefan Matthews played -- I mean, it's my word, but you may not disagree with it -- some sort of minder role at the dinner, particularly expressing concern that Dr Wright should not be discussing intellectual property information. Is that a -- that's a fair view of your view of your understanding of what was happening at that dinner?</p> <p>A. Well, I was asking questions that didn't -- didn't appear to me to involve any IP. I was asking questions about the core Bitcoin System, which of course is not patented. But, yeah, that was the justification I recall him giving for not answering any of my questions, yeah.</p> <p>Q. But is that right? You saw Mr Matthews as sitting there as some kind of minder --</p> <p>A. Yeah, I didn't know who he was at the time, yeah. So, yeah.</p> <p>Q. But was that your sense the relationship between him and Dr Wright?</p> <p>A. Yes</p>	<p>Mr Hearn comments on Mr Matthews' role at the dinner with Dr Wright.</p>
<p>{Day14/18:11} - {Day14/20:18}</p>	<p>MR JUSTICE MELLOR: Which bit?</p> <p>LORD GRABINER: That answer at line 25: "Mike asked ..."</p> <p>Mike, that's you: "Mike asked a lot of detailed technical stuff</p>	<p>Mr Hearn discusses his very limited interactions with Mr</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>that was, in my opinion, heavily related to a number of the patent filing activity ..." Etc.</p> <p>A. Well, from my perspective, it was about Bitcoin. From his perspective, perhaps he felt it was related to patents they were filing, but I could not have known that at the time, so I think this is just a difference of opinion.</p> <p>Q. Did he, at any stage in that conversation, say to Craig that he didn't want Craig to answer the questions you were raising?</p> <p>A. Yes.</p> <p>Q. Can you remember what it was that triggered him intervening and saying that?</p> <p>A. Well, Craig seemed to be stuttering, or struggling to answer and then he looked at Stefan, and Stefan was sort of like, "No, don't answer", and then I believe they -- they said this thing about the patents. "Patents", sorry.</p> <p>Q. Then MR HOUGH puts in effect your statement to the witness. He says: "Well, I'm going to put to you what Mr Hearn says because that's rather different. On his account, these were questions not about nChain's patents or new developments for Bitcoin, but about basic features of the original Bitcoin System?" And then Mr Matthews responds: "Well, this is rather interesting because that's not how I recall it ... interestingly, after that dinner, Mike and I exchanged six/seven emails. I had lunch with Marco Bianchi at Marco Bianchi's favourite Italian restaurant in Zurich ... quite a lengthy lunch and discussion ... I had a follow-up coffee meeting with Mike Hearn at a coffee shop adjacent to the FIFA museum ... a couple of months later ... at no stage did Mike take any issue with the points you're raising." Now, first of all, did that meeting take place as described there?</p> <p>A. Well, I honestly don't remember any of these meetings after this dinner at Wild Honey. After I was sent this transcript, I checked my mail from -- to find mails from Stefan, which I hadn't looked for before because I was only searching for emails from Craig Wright. And when he says we exchanged six or seven emails, what he means is that he -- he emailed me a bunch of times asking me to meet up. At some point he -- the last email in that -- in that thread says, "I'll text you", so quite possibly we did meet up. The FIFA museum, I think this a typo, or a "thinko". But there is a FIFA museum in Zurich; I don't think we would've met in Munich. These meetings could have happened. If so, I really don't remember anything about them.</p>	<p>Matthews, after the dinner with Dr Wright.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{Day14/26:20-25}	<p>MR HOUGH: Mr Hearn, one question in re-examination. You've expressed the views which are set out in this Medium article about block sizes and so on, yes?</p> <p>A. Yes.</p> <p>Q. Are you Satoshi Nakamoto?</p> <p>A. No.</p>	<p>Mr Hearn confirms that he is not Satoshi Nakamoto.</p>
CROSS-EXAMINATION OF DR HOWARD HINNANT BY CRAIG ORR KC		
{C/18} First Witness Statement of Howard Hinnant		
{Day14/30:9-19}	<p>Q. Now, not all libraries are standardised by the Standards Committee, are they?</p> <p>A. No. No, that's correct.</p> <p>Q. The Standards Committee doesn't have a monopoly on creating libraries?</p> <p>A. No, but it does have a monopoly on where the -- what namespaces those libraries use.</p> <p>Q. A monopoly or a practice?</p> <p>A. A practice that is specified in the standard, that if one puts a non-standard library into the standard namespace, the behaviour is undefined.</p>	<p>Dr Hinnant confirms that the Standards Committee specifies what namespaces libraries use.</p>
{Day14/31:1-5}	<p>Q. Project Chrono is an example of a library developed by third party programmers?</p> <p>A. Yes.</p> <p>Q. It's a physics simulation engine?</p> <p>A. That's my understanding.</p>	<p>Dr Hinnant confirms that Project Chrono is a physics simulation engine.</p>
{Day14/31:18-25}	<p>Q. And, secondly, he says that he set up his system so that use of the line "[hash] include <chrono>" in his code would lead to the inclusion of his own library. You understand that is what he is saying?</p> <p>A. Yes.</p> <p>Q. Now, from a technical perspective, it would have been possible for a C++ programmer to do, and I'm going to put to you, four steps.</p>	<p>This question and those which follow were put on the premise that they are things which it would be possible for a C++ programmer to do.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{Day14/34:4-19}	<p>Q. And so in summary, it is right, isn't it, that from a technical perspective, there was nothing to prevent a C++ programmer doing what Dr Wright says he did?</p> <p>A. It is possible. It is -- does result in undefined behaviour, and it is highly, highly unlikely.</p> <p>Q. You say it's highly unlikely because it's something that you regard as unconventional?</p> <p>A. I say it's highly unlikely because telling me that you started with Project Chrono and ended up with std::chrono is -- is absurd from a technical perspective. It's like saying I started with a P5 Mustang fighter plane to create a Ford Mustang car.</p> <p>Q. Mr Hinnant, that, with respect, is an opinion from you about the likelihood of Dr Wright acting in the way he says he acted.</p> <p>A. That is correct. That is my professional opinion.</p>	<p>Dr Hinnant describes an analogy for why it would be “highly, highly unlikely” to start with Project Chrono and end with std:chrono, from a technical perspective.</p>
{Day14/40:12} - {Day14/41:9}	<p>Q. And so if I take you to 2007, if we're thinking about the period 2006 to 2007, there was nothing at that point in time to prevent a C++ programmer developing their own random number library and calling it "random"?</p> <p>A. And putting it in namespace std?</p> <p>Q. If they wanted to, yes.</p> <p>A. The standard says that's undefined behaviour.</p> <p>Q. Again, we've already debated that.</p> <p>A. Yes. And the Boost library from which the standard random library derives is in namespace Boost and many people were using it gathering field experience. A programmer, in 2007, will have used Boost random, not standard random.</p> <p>Q. Well, you can't speak for all programmers, can you?</p> <p>A. Of course not.</p> <p>Q. And again, from a technical perspective, there would have been nothing to stop a C++ programmer modifying the Boost library and setting their own environment so that the random number generator that was within the Boost library is, for that programmer, within the std::namespace?</p> <p>A. Nothing except for the standard saying that that's undefined behaviour.</p>	<p>Mr Orr KC questions Dr Hinnant on the possibility of programmers developing and using standard random prior to 2007.</p>
<p>RE-EXAMINATION OF DR HINNANT - JONATHAN HOUGH KC</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day14/43:2} – {Day14/44:10}</p>	<p>MR HOUGH: Mr Hinnant, first of all, chrono and Project Chrono. Mr Orr put to you a series of steps which would be technically possible for a C++ programmer; do you remember?</p> <p>A. Yes.</p> <p>Q. You gave various answers that steps were technically possible; do you remember that?</p> <p>A. Yes.</p> <p>Q. You then said that it was highly unlikely that somebody would start with Project Chrono and end with std::chrono. Do you recall saying that?</p> <p>A. Yes.</p> <p>Q. You agreed that that was your opinion; do you recall that?</p> <p>A. Yes.</p> <p>Q. What facts or considerations is that opinion based on?</p> <p>A. That opinion is based on the knowledge that Project Chrono has no similarity whatsoever to std::chrono besides the name "chrono". It's -- it's a statement that is technically so outrageous that it's -- it's literally unbelievable. I cannot believe it. The -- the mere fact that somebody says that they derived a date time library from a physics library indicates to me that they don't have the technical expertise to even write chrono from scratch, because it would actually take more work to write chrono from scratch than to derive it from a completely unrelated piece of software. Chrono did in fact derive from other libraries. It derived from the Boost.DateTime authored by Jeff Garland. And Jeff Garland and I worked on chrono together in the 2007/2008 time frame -- well, in the 2008 time frame, I'm sorry. In 2007, we were working together, but it wasn't called chrono at that point, it was called Boost.DateTime.</p>	<p>Dr Hinnant provides clarification as to why his opinion is that it is “highly unlikely” that somebody would start with Project Chrono and end with std::chrono.</p> <p>His view is that Dr Wright’s claim is “so outrageous that it’s literally unbelievable”.</p>
<p>{Day14/44:12} – {Day14/45:1}</p>	<p>Now, in response to a number of questions, you said that something that was being put to you would be "undefined behaviour". Do you recall that?</p> <p>A. Yes.</p> <p>Q. What is the practical effect on the code and its functioning, if any, of something being undefined behaviour?</p> <p>A. When a compiler encounters undefined behaviour, it is not required to admit a diagnostic, it may admit a diagnostic or it may not. It may take the code and do exactly as the programmer intends, or it may take the code and completely modify it so that it does something completely different and unrelated. Literally anything can happen when the compiler comes upon undefined behaviour.</p>	<p>Dr Hinnant explains the practical effect of “undefined behaviour” on the code and its functioning.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{X/39/4} – Limitate speed of a socket-based date transferring – Python		
{Day14/45:15} – {Day14/46:7}	<p>MR JUSTICE MELLOR: Yes, I did have one question. Mr Hinnant, can you be shown page 42 of the [draft] transcript. Perhaps we can bring that up on screen. A recent answer you gave to MR HOUGH is at line 10 -- starts at line 10. If you can just show the whole of that answer, starting at line 10. Mr Hinnant, you will probably remember this answer. You see, at line 18, you say: "... it would actually take more work to write chrono from scratch than to derive it from a completely unrelated piece of software." I think the sense of your answer was the other way round; is that correct?</p> <p>A. You're correct. I -- I mis-spoke.</p> <p>MR JUSTICE MELLOR: Don't worry.</p> <p>A. It would take more work to derive it from a completely unrelated piece of software than to write it from scratch. My apologies.</p>	<p>Clarificatory question from Mellor J regarding Dr Hinnant's response in which he meant to state that it would take more work to derive chrono from a completely unrelated piece of software than to write it from scratch (not the other way round).</p>
CROSS-EXAMINATION OF ZOOKO WILCOX-O'HEARN		
{C/6} – Witness Statement of Zooko Wilcox-O'Hearn		
{Day14/60:8–13}	<p>Q. And it's fair to say that these events that we're discussing are a long time ago.</p> <p>A. Mm-hm, yes.</p> <p>Q. So remembering precise details when you don't have written records can be difficult.</p> <p>A. Yes.</p>	<p>Mr Wilcox O'Hearn discusses his recollection of interactions with Adam Back.</p>
{L3/278/1} – Metzdowd post Bitcoin P2P e-cash paper (Satoshi's announcement to the cryptography mailing list on 31 October 2008)		
{Day14/63:1–20}	<p>Q. If I refresh your memory with a document. If we can go to {L3/278/1}. Now, this, as I understand it, is the announcement to the cryptography mailing list by Satoshi Nakamoto on 31 October 2008, and he says: "I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted</p>	<p>Mr Wilcox-O'Hearn discusses his recollection of communications with Satoshi.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>third party." And gives a link to the paper. 8 Presumably that is what you first became aware of some time in 2008?</p> <p>A. Presumably. I don't remember if Satoshi also emailed me about it or not.</p> <p>Q. And does that mean that you and Satoshi had communicated with each other possibly even before the announcement of Bitcoin?</p> <p>A. No, definitely not, except he might have emailed me about the paper, but if so, that would have been the only time I communicated with him. It's possible he never -- it's possible I just saw it on the mailing list.</p> <p>Q. All right, well, I'll come back to that.</p>	
<p>{L18/310/2} – Exhibit Z-2</p>		
<p>{Day14/71:24} – {Day14/72:11}</p>	<p>Q. And presumably you did download the software? You wanted to see whether it was viable? You've said that you thought it had a flaw.</p> <p>A. I didn't download it at that time.</p> <p>Q. Why not?</p> <p>A. Well, for one reason, I didn't have Windows at that time and the initial release, I was just reminded by looking at that document, was only for Windows. But in general, I'm lazy and put things off.</p> <p>Q. So how did you conclude that the design had a flaw?</p> <p>A. Oh, just from reading the original White Paper, before the software was released. And I'm embarrassed about it. I was wrong to think that it was flawed.</p>	<p>Mr Wilcox-O'Hearn explains why he did not download the Bitcoin source code initially.</p>
<p>{X/43/12} – I'm Zooko Wilcox. Ask me Anything! – The Bitcoin Forum</p>		
<p>{Day14/74:7} – {Day14/75:7}</p>	<p>Q. And then your answer is: "I love this question ... I was entranced and sucked in by Bitcoin pretty early. A post about it on my blog is probably one of the earliest posts about Bitcoin ..." And then you give the URL: "I used Bitcoin a lot ..." Do you see that?</p> <p>A. Yes.</p> <p>Q. And that's all correct?</p>	<p>Mr Wilcox O'Hearn explains that he did not use Bitcoin in 2009.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Yes, but I didn't use it in 2009.</p> <p>Q. Well, that's --</p> <p>A. I was definitely entranced by it.</p> <p>Q. So that's what I'm just exploring with you, Mr Wilcox-O'Hearn, because here you are saying, in answer to a question that is focused on 2009, you are saying that you were "entranced and sucked in ... pretty early"?</p> <p>A. Yeah.</p> <p>Q. And I suggest you had in mind 2009 in that answer.</p> <p>A. Well, I don't remember what I had in mind, but I know that I wrote that blogpost in early 2009, I know that I contributed of some security auditing of Bitcoin, but that was a few years later. I know that I didn't really use Bitcoin, actually, until later, you know, probably because I've looked some of my records in preparation for this testimony.</p>	
<p>{C/6} – Witness Statement of Zooko Wilcox-O’Hearn</p>		
<p>{Day14/80:4} – {Day14/81:2}</p>	<p>Q. Right. You see, what I suggest is that you're in fact mistaken about that, and given what you've accepted is your very keen interest in Bitcoin, your perception that it was a revelation, that you were entranced and sucked in pretty early, that the reality is that you did in fact get more involved than you now remember: you downloaded, you ran the software and you were sent some Bitcoin by Satoshi.</p> <p>A. No way, by the time of -- like I mentioned earlier, Bitcoin had gone from a curiosity to a breakthrough in my mind at some point, and Satoshi was totally my hero. Still is. I love what Satoshi means to me and to people. So if I had ever gotten bitcoins from Satoshi, I would definitely remember that. But again, my earliest use of Bitcoin was OTC trading. You know, "OTC" means "over the counter". I forget what it was called, but there was this thing where people could post, if they wanted to buy or sell bitcoins, and then they could get each other's contact from it. That's my earliest memory of using Bitcoin for anything myself.</p> <p>Q. So, again, I suggest that the fact that you regarded Satoshi as your hero, it beggars belief that you didn't get more involved at the very earliest stage.</p> <p>A. You underestimate my laziness and procrastination.</p>	<p>Mr Wilcox-O’Hearn explains that he did not download or run the Bitcoin software, and never received Bitcoins from Satoshi.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day14/84:7-25}</p>	<p>Q. One final question, Mr Wilcox-O'Hearn. Now, you've referred to not having Windows in 2009. Did you ever develop solutions for Python in 2009 using Windows as well as Linux?</p> <p>A. I don't remember. I have had Windows off and on over the years. I do remember that when I did run Bitcoin, I ran it on Linux.</p> <p>Q. And --</p> <p>A. But I don't remember for sure. And I -- I did develop -- I did work on Python and some other things, Tahoe-LAFS especially, but I don't remember if I had Windows then. All I remember is that when I did run Bitcoin I ran it on Linux, and that it was later than 2009.</p> <p>Q. So you were able to run it on Linux when you first used it?</p> <p>A. Yeah.</p> <p>Q. And you were running Linux in 2009?</p> <p>A. Yes.</p>	<p>Mr Wilcox-O'Hearn confirms that he ran Bitcoin on Linux. The Linux version of Bitcoin was not available until after 2009.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
DAY 15		
CROSS-EXAMINATION OF DR WRIGHT BY JONATHAN HOUGH KC		
Mr Madden’s findings regarding the MYOB records / screenshots		
<p>{Day15/11:9} {Day15/12:6} (records {L5/150})</p> <p style="text-align: center;">at</p>	<p>Q. You're aware that Mr Madden and Dr Placks agreed that this and related screenshots weren't authentic to their stated dates and were backdated?</p> <p>A. No, I --</p> <p>Q. Are you aware of that?</p> <p>A. What I saw is a lack of understanding of MYOB, no testing, and basically statements without any supposition to support what they said. Whereas they could have actually run up MYOB, they could have had old versions and they could have tested their suppositions. Instead, each chose not to.</p> <p>Q. Let's try the answering the question trick, Dr Wright.</p> <p>A. I believe I just did.</p> <p>Q. They agreed these were not authentic to their stated dates and had been backdated. Do you understand and are you aware that that is the finding they made?</p> <p>A. I understand what they wrote and I also understand that they had no methodology and no test method. They just said, "I've looked at this, I've never seen anything, I've never had any training in MYOB, I've never read anything about MYOB, I looked at a blog and someone on a blog said something that differs from the MYOB official statement and I'm going to assume it's true".</p>	<p>Dr Wright questioning the competence of both experts for not approaching their analysis correctly.</p>
<p>{Day15/13:20-24}</p>	<p>Q. But it shows that transaction, doesn't it?</p> <p>A. It shows the date of the copy I made, yes, not the date of the transaction, no. Again, what you're saying is that this shows the date of the transaction. No, it shows the date when I made the copy.</p>	<p>Dr Wright not accepting the obvious truth, that the security audit clearly shows the transaction date.</p>
<p>{Day15/14:3-12}</p>	<p>A. MYOB Live was provided to AlixPartners first. That was done in 2019. And then to other solicitors in 2019.</p> <p>Q. We can go back to the transcript, but your story was that those screenshots were taken by Ontier using a live log-in to the MYOB system, wasn't it?</p>	<p>Dr Wright blaming third parties (Alix Partners) for failing to use “live” version of MYOB.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. That's not the way I said. The live log-in was provided to them. I wasn't involved in the process they used. I provided a live log-in directly to the solicitors and AlixPartners, and then they did whatever they did, and I'm not going to talk about what my solicitors did.</p>	
<p>{Day15/16:12} - {Day15/17:12}</p>	<p>Q. And so your story was, in relation to the entries on the journal security audit, that those showed transactions being added on 6 March, because in the context of the Kleiman litigation, you got somebody to extract information from the online version of MYOB into a QIF file, yes?</p> <p>A. Along those lines, yes.</p> <p>Q. And you then laboriously, item by item, entered the transactions into a local version of MYOB, yes?</p> <p>A. No, it's not laboriously. There's an automated process. You click a button.</p> <p>Q. Okay --</p> <p>A. So where you actually select everything, I wouldn't call that laborious.</p> <p>Q. Okay, you entered the transactions into a local version of MYOB?</p> <p>A. I did.</p> <p>Q. Your story was that you did that inputting of entries on 6 March 20And that had nothing to do with the screenshots, even though they happen to show the same entries; correct?</p> <p>A. They don't show the same entries, they're slightly different.</p> <p>Q. Well, even though they show, focusing on that one, that entry for 795,000, right?</p> <p>A. No, it's slightly different.</p>	<p>Dr Wright is evasive regarding what the MYOB entries show.</p>
<p>{Day15/17:12-25} {M/2/1000} - Ontier's account of the MYOB files</p>	<p>Q: Now, do you recall that Ontier informed us during your original evidence that they were first provided with log-in details to produce the screenshots on 9 March 2020? Do you recall them providing that information? I can go to the letter, if necessary.</p> <p>A. I recall what Oliver said.</p> <p>Q. And you recall that they informed us that they had subsequently produced the screenshots on or after 9 March 2020, including the one that we saw earlier, yes?</p> <p>A. All I know is what I was told by my solicitors at the time.</p>	<p>Dr Wright blaming a third party, stating that he only knows what his solicitors told him at the time regarding the creation of the screenshots.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{Day15/18:1-18}	<p>Q. Let's look at the letter then {M/2/1000}. A letter from your solicitors, passing on information from Ontier. Under paragraph 2: "Dr Wright first provided this firm with log-in details for the MYOB accounting software on 9 March 2020 and we first accessed the software on that same date. We did not have access to MYOB in 'late 2019' ... "We created a series of screenshots from that system on 9 and 10 March 2020, including screenshots that correlate with the screenshots which appear at Doc IDs ... 4076 ... 4077 ... 4078; and ... 4079." Just for your information, that includes the one at {L5/150/1} that we looked at. So, it's right, isn't it, that Ontier did not receive the log-in details in late 2019 you said, but on 9 March 2020?</p> <p>A. No, because AlixPartners received them from the US case in 2019 Ontier were involved.</p>	<p>Dr Wright not accepting the obvious truth of what Ontier said in their letter on his behalf regarding the MYOB files.</p>
{Day15/18:19} - {Day15/19:3}	<p>Q. And it's also wrong to say that Ontier captured the screenshots before 6 March 2020, as you told the court, isn't it?</p> <p>A. No, I was informed by them that it was.</p> <p>Q. Dr Wright, that's a lie, isn't it?</p> <p>A. From Ontier, it may be, but not from me.</p> <p>Q. Dr Wright, the difference between you and Ontier is that Ontier have no reason to lie while you do; that's correct, isn't it?</p> <p>A. Well, that's totally incorrect.</p>	<p>Dr Wright blaming a third party (Ontier) and accuses them of lying. Lord Grabiner later accepts the documents (including Ontier's letter) can be taken at face value {Day18/19:7-11}</p>
{Day15/19:14} - {Day15/20:15}	<p>Well, let me just draw the threads together then. Ontier were given the means to produce the screenshots just three days after you had made the entries relating to those very transactions, as shown in the journal security audit, right?</p> <p>A. No, they never had the screenshots, they actually made everything themselves, and the MYOB log shows that it was given to Ontier in 2019.</p> <p>Q. A document that hasn't been disclosed; is that right?</p> <p>A. No, actually it was available, so when the log-in was given to Mr Placks, that was information that he could have downloaded, and did.</p> <p>Q. Dr Wright, it was no coincidence that Ontier captured the screenshots -- were given the access to capture the screenshots and did so just three days after you had made the entries reflecting those, is it?</p> <p>A. I don't believe they did it at that date, because that had already been submitted to the US court.</p>	<p>Dr Wright continuing to blame others after Lord Grabiner's intervention.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. The obvious explanation is that the transactions in the screenshots were added by you to the MYOB system as an act of forgery on 6 March 2020.</p> <p>A. Seeing as screenshots had already been given to the US court, that makes it difficult to believe.</p> <p>Q. And another assertion by you without anything to back it up, isn't it, Dr Wright?</p> <p>A. Not at all.</p> <p>Q. Let's see if your team can.</p>	
The Substitute MYOB files		
<p>{Day15/20:24}- {Day15/21:13}</p>	<p>Q. You gave access to Dr Placks for the purposes of these proceedings, didn't you?</p> <p>A. No, I did not. I wasn't involved in any of the access, I didn't have any admin access, etc, so I don't know what the communication between the administration of MYOB and my solicitors was. I wasn't involved in that process at all.</p> <p>Q. So if Dr Placks identifies you as the inviting individual, that's wrong, is it?</p> <p>A. Correctly. It is absolutely wrong. What I have is my name on the system as the owner for founding the company. Now, that doesn't mean that I'm the person; craig@panopticopt isn't my email any more, for instance, and the other ones are just the payment emails.</p>	<p>Dr Wright blaming third party, stating that he was not involved in giving Dr Placks access to the MYOB files.</p>
<p>{Day15/21:14} - {Day15/22:14}</p>	<p>Q. So who do you say at the company gave him access to this material?</p> <p>A. Ramona, most likely.</p> <p>Q. So your wife gave access?</p> <p>A. I wasn't involved.</p> <p>Q. You know that your wife was giving access to this material?</p> <p>A. I wasn't involved.</p> <p>Q. Did you know that your wife was giving access to this material?</p> <p>A. I wasn't involved.</p> <p>MR JUSTICE MELLOR: Answer the question, please, Dr Wright. Do you know --</p> <p>A. I suspect.</p> <p>MR JUSTICE MELLOR: -- or not? Sorry?</p>	<p>Dr Wright giving a long and evasive answer, and subsequently blaming third parties (Dr Placks, Ms Watts) regarding his export of the MYOX file.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. I suspect, but that's not know. I mean, if I'm not involved, my Lord, making a supposition isn't knowledge.</p> <p>MR HOUGH: Now, Dr Wright, can we agree that these records to which access were given were database files in the MYOX format?</p> <p>A. No, they weren't. They were a live log-in. What then happened was, an MYOX was exported by Dr Placks. So once again, it wasn't actually any live testing. We requested that he did live testing on the online database, but instead he downloaded the MYOX and ran it on a local machine.</p>	
<p>{Day15/22:23} - {Day15/23:4}</p>	<p>Q. And are you aware, just as a point of fact, that both Mr Madden and Dr Placks concluded that these were created after 10 May 2023 on computing equipment with its clock setback to dates between 2007 2013?</p> <p>A. Again, as I demonstrated, they didn't understand the process that was published on MYOB for a forced update.</p>	<p>Dr Wright claiming greater knowledge than both experts.</p>
<p>{H/209/10} - Appendix PM 42</p>		
<p>{Day15/23:24} - {Day15/24:6}</p>	<p>Q. I'm just going to ask the question again. Do you accept that he found that there was a log-in and log out entry in relation to the same session user ID separated by 12 years?</p> <p>A. No, I'm telling you I don't accept his findings. They're completely wrong. They have nothing to do with how MYOB works and they are contrary to the actual stated positions of the company.</p>	<p>Dr Wright claiming greater knowledge than both experts, and introducing vague hearsay evidence.</p>
<p>{G/9} Fifth Expert Report of Patrick Madden</p>		
<p>{Day15/25:10} - {Day15/26:2}</p> <p>MYOB Session Security Log - ins</p>	<p>Q. Page 7 -- we'll come to why you say he's wrong in a second {G/9/7}. And in the table, he found a series of dates out of order with entries dated 6 June 2023 among the entries dated 2010; do you see that?</p> <p>A. I do.</p> <p>Q. And that export simply showed the entries in the order they were recorded in the database, didn't it?</p> <p>A. No, actually, it doesn't. This is related to changes in the schema, etc, so none of this existed in that format back in 2009/10, etc. Over the years, MYOB have changed their - their thing and moved into live. The use of live didn't exist until 2017 or '18. Before that, they had a different online package. So all of this references each of the schema updates that have been done by the company. Where there's something that doesn't match a schema and it's been updated, that gets</p>	<p>Dr Wright not accepting the obvious truth regarding Mr Madden's findings on date export.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	recorded. If you look on the web page for MYOB, it explains this.	
{Day15/26:3-20}	<p>Q. No, Dr Wright, it is quite simply false that as a result of updating, the user audit export puts the entries which have been made normally in an order out of date sequence. That's just false, isn't it, Dr Wright?</p> <p>A. No. The record IDs get updated. So once again, as it explains on MYOB, in some of their technical sites, this happens.</p> <p>Q. So Dr Wright, you're saying that this accounting software has a feature which produces these entirely misleading extracts; correct?</p> <p>A. No, what I'm saying is, rather than using MYOB Live, they've extracted a MYOX database. The statement I said was that we use and trust the live version of the database, not the extractions. The extractions are updated and the schemas change.</p> <p>Q. Dr Wright, Mr Madden's clear evidence - and it is correct - is that this simply shows the entries in the order that they were recorded in the database.</p>	Dr Wright providing an implausible explanation that record IDs get updated.
{Day15/27/3-16} (MYOB Session Security Log - ins)	<p>Q. Dr Wright, I just have to put to you again, it is simply false that this accounting software, the auditability of which is no doubt important, would produce records that are entirely misleading in the way that you suggest. That's just a lie, isn't it?</p> <p>A. No. Once again, I stated the live version. Live is run on the secure government version of AWS. Now, the live server has a separate log to the extracted one. The MYOB statement is that live, the online database, is secure. They also state that the file integrity changes as they update schemas. There were a number of schema changes done in 2020, 2021, 2022 and 2023, some of which were to do with security vulnerabilities that were being addressed.</p>	Dr Wright failing to accept the obvious truth and providing an explanation as to the way accounting software works without supporting evidence.
{Day15/28:14-23} {H/209} – Appendix PM42 (New MYOB files)	<p>Q. Page 18, please {H/209/18}. We see that table for Wright International Investments, and do you see that it those the first entry, dated 1 August 2009, corresponding – which corresponded to the first recorded log-in to the file being shown made with product version 2023.4.1.6, yes?</p> <p>A. No, that's the schema update version. Again, if he had done a real experiment and created a file and uploaded it, which I've now done, by the way, you would now see this.</p>	Dr Wright providing evidence in the form of hearsay / experiments without permission.

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day15/32:3-24} {H/209} – Appendix PM42 (New MYOB files)</p>	<p>Q. You say that that accounts for Mr Madden’s extract of raw data showing a 2009 entry associated with a May 2023 software version; correct?</p> <p>A. Not in the way that you’re implying. The note there is the version of schema being used. So what happens is, as they update anything, like they said in that page you showed from MYOB where they’re fixing errors with certain things, that applies.</p> <p>Q. Mr Madden’s extract showed a 2009 entry associated with a May 2023 software version and this is your explanation, right?</p> <p>A. No, what his thing shows is the schema applied to that record. So when you download the MYOX, it applies the schema, and then it says what schema version is being used on that record.</p> <p>Q. Well, first of all, that’s disputed, but before we get to Mr Madden’s latest findings, your position is that the entry which gives the 2023 software version in that table is accounted for by this upgrade process; correct?</p> <p>A. Yes, as it notes on the MYOB site and as, when you look at their technical details, or you do their technical training, it will tell you.</p>	<p>Dr Wright providing an implausible explanation for how the 2023 software version appears in the metadata for a 2009 entry.</p>
<p>{Day15/33:5-20}</p>	<p>Q. {G/9/9}, please. Mr Madden downloaded the installation file for all the versions of the MYOB software currently available on the website, paragraph 22; do you see that?</p> <p>A. No, he didn’t. There were far more. In fact, I can give you versions of MYOB based on my licences, which he could have used, going back to 1997. All of those are actually still available and downloadable.</p> <p>Q. Do you dispute that he downloaded the program versions which are shown in the table under paragraph 22?</p> <p>A. He – they’re not program versions, they’re schema update versions. So he’s downloaded the version and then put – and these are patches. So, what he’s saying is incorrect.</p> <p>Q. Well, that’s another point that’s disputed.</p> <p>A. Not by MYOB. It’s on their website.</p>	<p>Dr Wright seeking to rely on evidence that is not before the court.</p>
<p>{Day15/35:7-20}</p>	<p>Q. Dr Wright, the reality is simple. The log records a 2023 software version against an entry because the entry was made with that version of the software.</p> <p>A. No, actually, it doesn’t. And once again, what he’s doing is doing all of this offline. So at no point did he then load that onto MYOB Live. Now, the comments on schema changes</p>	<p>Dr Wright questioning the experts’ approach to analysing MYOB because they did not use MYOB Live.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>that are forced are MYOB Live. I've emphasised the whole time, we use MYOB Live, the database that is held on an AWS secure web server, and we do it that way.</p> <p>Q. Dr Wright –</p> <p>A. None of those logs were analysed –</p> <p>Q. Dr Wright –</p> <p>A. – and non-of those were tested.</p>	
<p>{Day15/35:21} – {Day15/36:14}</p>	<p>Q. Dr Wright, it would be a pretty serious flaw in this accounting system if ordinary upgrades had the bizarre effect of altering past activity records to show them as thoroughly misleading, wouldn't it?</p> <p>A. No, these are not misleading. This shows the schema record on the local version. As I keep saying, the live version of the database is the one that needs to be trusted and that's the one that he just refused to check for some reason. Despite being able to download from AWS the records, despite having a secure version with the log-in, no one would check that.</p> <p>Q. Dr Wright, this is accounting software used for business records, it's supposed to be reliable and auditable, isn't it?</p> <p>A. Yes, MYOB Live. The statement by the site is the live version is secure. So, downloading and doing the other, this is a schema record on your local machine. MYOB state categorically that you give the accountants an access to the Live system.</p>	<p>Dr Wright deliberately conflating "secure" and "accurate".</p>
<p>{Day15/36:15} – {Day15/37:14}</p>	<p>Q. You do not say anywhere and there is nothing in any public information to suggest that when you extract data in the way that Mr Madden did, it will record the wrong version of software against the entry which was identified for a particular date?</p> <p>A. No, what it's recording is the schema update. Again, if you go to the MYOB Live version, that for some reason Mr Madden seemed to avoid, then you get different information.</p> <p>Q. Dr Wright, these are lies without any support, aren't they?</p> <p>A. Maybe on the other side, but I'm telling you categorically, I gave you, as was demonstrated in the evidence you just provided, a log-in, which I believe came from my wife, to the live version of the database.</p> <p>Q. You gave that –</p> <p>A. Rather than using the live version –</p> <p>Q. She gave that to Dr Placks, didn't she? Gave that to Dr Placks?</p>	<p>Dr Wright blaming third parties (Ms Watts, Dr Placks) for failing to provide / use access, disclaiming his own involvement</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. I'm not involved, so I don't actually know, but the live version was available. And if Mr Placks has it, then Mr Madden can ask for it, I believe, as far as I'm concerned. I've been told that anything that my expert gets, the other expert gets, too.</p>	
<p>{Day15/40:4-20}</p>	<p>Q. And before the MYOX format was introduced in April 2016, the software didn't record a session ID, a universal unique identifier reference in the logs, did it?</p> <p>A. I'm not actually sure, but the web integrates all of that.</p> <p>Q. I'll come to that. Mr Madden's researches indicated that the software in the MYO format, so before April 2016, did not record a session ID reference in the logs for entries. Are you able to dispute that?</p> <p>A. Oh, totally. What you do is you have an MYO – I've got actual records that are in the disclosure platform going back to 1997. Now, those MYO files, when you load them into a Live database, and I checked this, adds the session ID of the user. So, the system actually adds it. So the session ID, when it's blank, is filled in.</p>	<p>Dr Wright referring to further documents that have not been disclosed, as well as providing a technical answer without any evidence to support it beyond hearsay experiments.</p>
<p>{Day15/41:13-21}</p>	<p>Q. Dr Wright, that's, first of all, not in evidence, and, secondly, false. The fact is that when the content is imported from a previous MYO file into the MYOX format, it just brings across the information which is already in the MYO file format; that's right, isn't it?</p> <p>A. Utterly wrong. Again, you've got to go to the live system. Again, you're sitting there going, "We refuse to do an actual experiment of the actual environment Craig had because we might get the data that he says".</p>	<p>Dr Wright blaming his experts for not performing relevant experiments; he could have instructed his expert to do this.</p>
<p>{Day15/42:9} – {Day15/43:8}</p>	<p>Q. So Dr Wright, we have three independent reasons why these records have been backdated. First of all, we have the log-in sessions out of time order, yes?</p> <p>A. No. I explained that.</p> <p>Q. Secondly, we have 2023 software versions recorded for 2009 and '10 entries, right?</p> <p>A. No, we have schema versions, when, on the MYOB website, there is a notice saying that the schema update occurred on those dates.</p> <p>Q. I'm not disputing updates, Dr Wright.</p> <p>A. No, you're disputing the fact that MYOB, on their website, states that these schema changes will occur.</p>	<p>Dr Wright refusing to accept obvious truths.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Dr Wright, we've been round the houses on this. I'm disputing that the system creates misleading entries?</p> <p>A. Oh, it's totally not misleading –</p> <p>Q. Third –</p> <p>A. – because the live system has the data</p> <p>Q. Thirdly, we have session ID numbers recorded which would not have been recorded for the filetype in use in 2009?</p> <p>A. No, because it's not using the files. As I noted, when you load, which would have been back in 2016/17 into the new format of Live and MYOX was there, you have to do the update. So you can't keep using an MYO file, it just doesn't allow you. MYOB forces you to upgrade. You don't have a choice.</p>	
<p>{Day15/43:9-25}</p>	<p>Q. Well, Dr Wright, I put to you that that is – your explanation for these anomalies is false, as both the independent experts found.</p> <p>A. No, I'll actually put to you that neither of them tested. Both of them seemed to refuse to check my environment. Despite writing pages and pages about using MYOB Live, both of them refused to ever log-in and check the live system.</p> <p>Q. So you, the person who completely lacks independence, are the only person who's right in this?</p> <p>A. No, actually, I had a chartered accountant analyse it, I had a third party accountant analyse it, went to MYOB experts and spoke to them, have an accountant who works for me, verified all of this. I also went and spoke to people who work at MYOB. I went through their web pages and that's why I pulled those pages stating exactly what I said.</p>	<p>Dr Wright providing an incorrect version of how the experts approached the MYOB analysis and relying on hearsay evidence of an accountant who supposedly analysed it, as well as MYOB experts and people at MYOB.</p>
<p>Papa Neema emails and attachments</p>		
<p>{Day15/49:6-12}</p>	<p>Q. And do you see that the author of this email has written, in the last paragraph: “You know, I have been loyal and I am always going to be. I have worked for you for 14 years and I know to be loyal.” Do you see that?</p> <p>A. I do.</p>	<p>Dr Wright accepting Papa Neema says this, yet he was not called to give evidence.</p>
<p>{Day15/49:13} – {Day15/50:17} {CSW/25/1} - Papa Neema email</p>	<p>Q. Now, back to the email at {CSW/25/1}, please. Just to be clear, you say that the signature block would depend upon the place from which you log in?</p> <p>A. Correct.</p> <p>Q. Well, just to point out, that's not accepted, that's disputed. But you maintain that?</p>	<p>Hearsay: Dr Wright provides an incredible explanation that Denis Mayaka sets his clock to London time, without explaining how he knows this.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. You can actually set signatures in your machine, so they're -- I mean, I have a lot of default ones, but you just go into the user settings, you go to signatures. If you want, I can talk you how to do it.</p> <p>Q. No, that's fine, I have disputed it. Top of the first page {CSW/25/1}, would you accept the recorded time zone offset for this email and the others, including both those on 10 September and those on 29 September was GMT plus one hour?</p> <p>A. Yes, Denis works on London time. Most of his clients are English.</p> <p>Q. So you say that he had his system set to be at that time, although he worked in Kenya?</p> <p>A. Yes, because most of his clients are English. The majority of clients he sets up companies in the Seychelles, Panama and everything like that, happen to be British. Most of them related to large British companies as well. British seem to like having these sort of companies.</p> <p>Q. But the time zone is certainly consistent with somebody writing from the UK as well, isn't it?</p> <p>A. No, it's consistent with someone doing work in the UK. I used to have my time zone set to America when I was doing American work.</p>	
<p>{Day15/52:17} {Day15/53:9} {CSW/31/1} TimeDoc2.pdf</p>	<p>- MR JUSTICE MELLOR: I'm not sure that was counsel's suggestion. What his question was: it would have been perfectly possible to write this document today and backdate its timestamp? It's a pretty simple question.</p> <p>- A. I don't think it would be feasible, my Lord. I think it would actually lead to changes. The software available online isn't the same versions. The ones that are downloaded are the patched ones with no security problems. This means that I would have to have a version of the software that isn't the one downloaded, that it would just be sitting in my drawer waiting for me to do it on a version of Windows, including all the old patches, then zipped with an old ZIPX thing that doesn't exist any more. I don't think it's feasible. I think the reason that no one's showing you could do this is I don't believe it's feasible. The difference would be the versioning would be the new versions that are downloadable, not the patched versions that weren't.</p>	<p>Mellor J intervenes to make Dr Wright answer the question. Dr Wright then suggests, implausibly, that it would not have been possible to backdate the document's timestamp.</p>
<p>{Day15/53:18} {Day15/54:6}</p>	<p>- Q. Well, Dr Wright, just before our break, this point, so that it's been put to you. As Mr Madden's found, it would just be a matter of downloading the software available today and</p>	<p>Dr Wright attempting to explain that the forgery would have been technically</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>rewriting this document to produce a forgery. That's all it would involve, isn't it?</p> <p>A. No. As you note, it's a version that is an unpatched version. So you would have to actually download the source code, remove the patching, go back to a vulnerable version of OpenOffice that was patched intentionally and removed. You could probably find that if you talk to the right developers -- which I haven't done, most of them are associated with COPA -- and then build a version, but that would be a huge effort. I'm talking a month of work for a document.</p>	<p>advanced to produce, and therefore it is less likely to have been done. To the contrary, Mr Madden's expert evidence indicates that to produce such forgery would have been simple.</p>
<p>{Day15/54:14-22} {CSW/31/2} TimeDoc2</p>	<p>MR HOUGH: May we have on screen {CSW/31/2}. Continuing with the TimeDoc 2 document and looking now at an example of the images in the document, Dr Wright, Mr Madden found that those were embedded picture images of low resolution and pixelated by comparison with those in the Bitcoin White Paper. Do you agree with that finding?</p> <p>A. Yes, they weren't coded using the LaTeX in the same way. I was experimenting with different things at the time.</p>	<p>Dr Wright is unable to provide an actual explanation for what he did to create the images in the document, just that he experimented with 'different things'.</p>
<p>Comparison between Wright's TimeDoc2 document and the actual Bitcoin White Paper</p>		
<p>{Day15/55:1-15}</p>	<p>A. Yes, and the White Paper, as I've shown, was done in LaTeX, and the creation in LaTeX of the image leads to differences when you export it as an SVN.</p> <p>Q. We obviously dispute that the White Paper was created in LaTeX, Dr Wright, but the pixelated images in your document are consistent with them having been screenshots from the Bitcoin White Paper images simply inserted into the document; that's right, isn't it?</p> <p>A. No, completely different. If they were screenshots, they wouldn't have the -- the same sort of depth. It's actually darker. What they relate to are other versions of the image file that I've played with where I was experimenting with converting from the images rather than in, like, the native LaTeX output into image files that I could use on a website, etc.</p> <p>Q. So you -- in this later document, you produced worse quality images through experimentation, Dr Wright?</p> <p>A. Yes. I was looking at putting them on the website at one stage, and the information in the LaTeX export needs to be converted into, well, common images for people to be able to download.</p>	<p>Dr Wright implausibly suggesting that the worse quality images found in his document were because he deliberately made them worse quality to be able to put them on a website.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day15/56:17} - {Day15/57:15}</p>	<p>Q. Dr Wright, I've put to you that some of your documents contain positive indicia of forgery. But it's right to say, isn't it, that it is possible to create a document with more or fewer indicia of forgery; correct? Can you at least accept that?</p> <p>A. Not the way you're putting it, no. I mean, the words I'd use probably aren't the ones I should use in court, but, no, I disagree. And you already know that I have image files in LaTeX I could -- and they go back to this sort of time frame. I could have easily had different levels now created. I could have had them high resolution.</p> <p>Q. This -- this --</p> <p>A. And if I took a screenshot, by the way, I could do a screenshot -- I've got an 8K card that would be way better than the existing White Paper.</p> <p>Q. Dr Wright, I am not interested in your boasts about cards that you possess that would allow you to forge it even better. Focusing upon the document. Mr Madden found that this document, TimeDoc 2.zip, which contained the PDF, was hash identical to a file on the Samsung Drive in a folder entitled "BDO". Would you accept that finding?</p> <p>A. Possibly.</p>	<p>Dr Wright not accepting of the obvious truth, and a simple proposition, that it is possible to produce documents with more or fewer indicia of forgery.</p>
<p>{Day15/57:25} - {Day15/59:12}</p>	<p>Q. Dr Wright, this document, TimeDoc 2.pdf, is not a document which was in your original disclosure; would you accept that?</p> <p>A. I would, because the Samsung Drive wasn't imaged correctly.</p> <p>Q. So this was a document that you didn't have until September 2023, and then suddenly, in the space of five days, you get it from two independent sources, Mr Mayaka and the handily rediscovered drive; is that right?</p> <p>A. Well, yes, I had my drive discovered. It should have been imaged earlier, like the other machines that were failed to be imaged, and it's probably on those, too.</p> <p>Q. Well, as you know, all that's disputed, but I'm just focusing on the coincidence at the moment. This document, which you don't have access to at all until mid-September 2023, then just happens to come to you within five days, from Mr Mayaka and from you happily discovering the Samsung Drive? Is that your evidence?</p> <p>A. No, I knew that Denis would have had it. I had been attempting to get people to contact Denis for three years.</p> <p>Q. And you say that in response to a request for invoices and other documents relating to your Seychelles companies from</p>	<p>Dr Wright blaming third parties, claiming to have tried to "get people to contact" Mr Mayaka in the intervening period.</p> <p>Dr Wright is evasive, producing a brand new assertion that he had his drive discovered and that he knew Mr Mayaka would have the TimeDoc2 document.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>2009 to 2012, Mr Mayaka sends you the four Abacus invoices and this one other document right?</p> <p>A. He did.</p> <p>Q. He doesn't send you any other company forms or records for the Seychelles companies, not company acquisition forms, articles of association, corporate returns, anything like that?</p> <p>A. No. Denis is not always good that way.</p> <p>Q. So just to be clear, he sends you four invoices and a document produced by Information Defense; correct?</p> <p>A. No, it's produced by the group. I mean, it's named Information Defense, but it wasn't produced by Information Defense.</p>	
{Day15/64:18-22}	<p>So that's the abstract of the Bitcoin White Paper as issued in March 2009; correct?</p> <p>A. That's one of the versions, yes.</p> <p>Q. Well, the one issued publicly in March 2009?</p> <p>A. It's one of the versions, yes.</p>	<p>Dr Wright cannot even accept that he is being shown the March 2009 version of the White Paper.</p>
{L2/441/1} - TimeCoin paper		
{Day15/69:9-24}	<p>Q. -- {CSW/31/1}, it's, "Timecoin: A Peer-to-Peer Electronic Cash System", whereas the one you claim to have produced in May 2008 had the same title minus the indefinite article, yes?</p> <p>A. Well, they're not related documents.</p> <p>Q. But they have the same title, don't they?</p> <p>A. I have -- my assignment I just submitted last night, actually for -- before my --</p> <p>MR JUSTICE MELLOR: Try and stick to the question, please.</p> <p>A. What I'm saying is, I have the same title in 25 versions of my doctorate and they're all different. I've gone through differences, I've produced different papers with the same title. So --</p> <p>MR HOUGH: But it has the same title as the May 2008 version; correct?</p> <p>A. They're both part of the same project.</p>	<p>Dr Wright refusing to accept the obvious truth regarding his own apparent case on the relationship between Timecoin and Bitcoin.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day15/71:24} - {Day15/72:5}</p>	<p>Q: What you have done here is to include the contents of the abstract from the Bitcoin White Paper from March with some changes of language and added some references to secure logging; is that right?</p> <p>A. No. I wrote this earlier. This wouldn't be the final version either, because there's -- it hasn't been proof checked properly, but it's one of them.</p>	<p>Dr Wright attempting to suggest that the spelling mistakes present in the non-Bitcoin White Paper text are because it wasn't a final version of the paper. However, this does not explain why the spelling mistakes only appear in the non-Bitcoin White Paper text.</p>
<p>{CSW/31} TimeDoc2 compared to Bitcoin White Paper</p>		
<p>{Day15/74:11} - {Day15/75:4}</p>	<p>Q. Well, if we -- can we bring up the entire introduction on the left so that they can both be seen alongside each other. The entire introduction to the CSW/31 paper. Well, if we put page 1 on {CSW/31/1} {L5/26/1}. If you read down, just to yourself, the introduction of each document, and what I'm going to ask you to do is to tell me what substantive difference there is between the two. Not differences of phraseology, but what substantive difference there is between the two.</p> <p>A. They're the same system, so I'm not going to do a compare, unless you want me to go word by word while we're sitting here.</p> <p>Q. Well, I'm simply asking you to look at each one alongside each other and tell me if there is any substantive difference, or whether, as I put it to you, the one is a direct paraphrase of the other?</p> <p>A. They're both my documents, they're both related on the same work, so have I written basically the same things in multiple documents? Yes.</p>	<p>Dr Wright is evasive on the alleged relationship between Timecoin and Bitcoin.</p>
<p>{Day15/77:9-21}</p>	<p>Q. Sections Against each other, please {CSW/31/2} {L5/26/2}. Can we have sections Against each other, so far as possible. Again, what I'm going to put to you is that the section above the image is a paraphrase of the Bitcoin White Paper but just with tokens referred to rather than coins. Do you accept that?</p> <p>A. Not the way you're saying. I mean, what we're talking about in tokens are what I explained in 2009 to people like Martti, etc. And you'll notice that from their emails. I wasn't talking about digital value. The digital value was the underlying</p>	<p>Dr Wright refusing to accept the obvious truth about the presence or otherwise of text from the Bitcoin White Paper.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	system that economically incentivises the nodes to operate and allows for micropayments --	
<p>{Day15/77:22} - {Day15/78:5}</p>	<p>Q. And then in the section below the image, that's another paraphrase of the Bitcoin White Paper but with a short paragraph added referring to data being included in transactions; is that right?</p> <p>A. Like I said, and as you now know, I said to Martti in 2009, as I have been saying the whole time, all you need do is a simple change that is noted in here and suddenly Bitcoin becomes a Tripwire server. Like I explained in the emails that I didn't have.</p>	<p>Dr Wright appearing to accept that he did not have the emails with Mr Malmi until Mr Malmi produced them in his witness statement during these proceedings.</p>
<p>{Day15/79:3-10}</p>	<p>Q. It doesn't add anything to the substance of the project, does it?</p> <p>A. No, actually, it does. The vigilance bit, ironically, that all of the laser-eyed BTC guys run around, is actually my trademark from 2009. So the main thing about "don't trust Verify", etc, that all of the BTC guys now take out of context, are parts of my 2009 trademark from Information Defense.</p>	<p>Dr Wright's answer demonstrates that he will attempt to use any IP rights he can to control others.</p>
<p>{Day15/79:23} - {Day15/80:15}</p>	<p>Q. It omits the section on proof-of-work. Now, you've accepted that hash based proof-of-work was a critical feature of the system, yes?</p> <p>A. Not the way you're putting it. What I'm saying is proof-of-work was. I used the system that Adam incorrectly noted to be, like he said, floating point, which was actually N(?) bits, so number of zeros in the code, as a way of determining a cost function and structuring economic cost.</p> <p>Q. Dr Wright, it's a simple point. The -- your Timecoin document, having advertised hash-based proof-of-work as a central feature of the system, then doesn't include a section on it, doesn't describe it.</p> <p>A. It's not about running nodes. The Bitcoin White Paper was a node document. That was for people to go out there, mine, earn and be part of the network. The structure here is for clients, SPV, the sort of use of writing information into the blockchain.</p>	<p>Dr Wright not accepting the obvious truth.</p>
<p>{Day15/85:12-17}</p>	<p>Q. Dr Wright, what I'm suggesting to you is that you've been busily paraphrasing, whether with your thesaurus or your ChatGPT, and you've unthinkingly used the wrong word.</p> <p>A. First of all, you've got my ChatGPT history and it has no such thing.</p>	<p>Dr Wright referring again to documents he alleges are in disclosure which are not (ChatGPT history).</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day15/86:7-18} {CSW/31/6} {L5/26/5}</p>	<p>Q. Sorry, that was a false point, Dr Wright. It was "Combining and Splitting Value", on the right, that's what's been missed out here, isn't it?</p> <p>A. Possibly, because that's not part of the Timecoin solution.</p> <p>Q. I see. So, you've got your electronic cash system, but it doesn't involve the facility to split and combine transactions with multiple inputs and outputs?</p> <p>A. No, no, no, that's actually part of the script. I've noted that. But the purpose here isn't digital cash, the purpose is actually for the HMAC authentication of files and the embedding of file timestamp information.</p>	<p>Dr Wright appearing to suggest that Bitcoin was the implementation of IT security features.</p>
<p>Papa Neema attachments "C Wright.zipx" invoices</p>		
<p>{Day15/92:12} - {Day15/93:19}</p>	<p>Q. And we can see if we look at page {G/9/44}, at the top, that the templates used for these four documents differ as between them: "Normal.dotm", "Abacus Inv.dotx", "Normal.dotm", and then "0 ABACUS SEYCHELLES LTD.dotx"; do you see that?</p> <p>A. I do.</p> <p>Q. That's the column for "Template". So is it right, on your account, that each file contains the same spelling mistake, "Invoice", for "Invoice", yes?</p> <p>A. I believe so. I -- my understanding from Denis is that he just used other files and copied and pasted them.</p> <p>Q. Well, it would be pretty surprising, wouldn't it, if each year Mr Mayaka creates a new document using a new template but he misspells "Invoice" in the same way in the title for each file?</p> <p>A. No, what that shows is that there's an invoice used and there's two different ones. So, you've got Wright International and Tulip, which are different. So you're confounding the Normal.dotm and Normal.dotm and the Abacus and the other one, so they're separate. But did he basically reuse documents? Yes.</p> <p>Q. But this isn't just a reuse of documents, this is creating a file from year to year using different templates and making the same spelling mistake.</p> <p>A. No, it's not using different templates the way that you're saying. You have a new template if you have updated default templates on your system. So, what you're showing is that at</p>	<p>Dr Wright providing hearsay evidence about Mr Mayaka's document creation process. The inference is that Dr Wright is Papa Neema (otherwise, how would he know this).</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>some point Denis has had a template update, which would be expected, and over time, even though he's using the base doc file, or docx file, that he has different templates associated with them.</p>	
<p>{Day15/94:19} - {Day15/95:12}</p>	<p>Q. Again, it would have been straightforward to just forge these invoices today, wouldn't it?</p> <p>A. No, it wouldn't. And the digital signature is Mr Mayaka's, and despite your saying he doesn't exist, some of the Ontier solicitors actually went and physically visited him for a month.</p> <p>Q. Well, there's no evidence of that and I'm not going - I'm going to warn you against going into privileged matters, Dr Wright. The logo on each one matches a web archive snapshot for the Abacus Offshore website from 2015 which could easily be obtained, doesn't it?</p> <p>A. No, it matches the web archive from 2009. But, no, they're different resolution.</p> <p>Q. Well, that's disputed, and you know that Mr Madden's finding is that it matches a web archive snapshot that's readily available now?</p> <p>A. The Wayback Machine goes right back to 2002 for them, I think.</p>	<p>Dr Wright providing more unsubstantiated evidence about what investigations his lawyers have supposedly conducted</p>
<p>{Day15/96:3-15}</p>	<p>Q. One straightforward way for you to support this story would have been to call Mr Mayaka as a witness, wouldn't it?</p> <p>A. I requested that that happened, but people don't like putting solicitors on as evidence.</p> <p>Q. Well, this is a man whose job, as you put it, was to produce these corporate documents for you and to carry out those corporate services for you. What would have been the difficulty in him coming forward and giving evidence on these matters?</p> <p>LORD GRABINER: My Lord, I object again. My learned friend is entitled to comment in due course about the absence of Mr Mayaka as a witness, end of.</p>	<p>Dr Wright claiming he wanted to call Mr Mayaka as a witness. Lord Grabiner accepts adverse inferences can be drawn from his absence.</p>
<p>Other documents relating to Tulip Trading / Denis Mayaka - supposedly from 2014 - that were put to Wright on Day 4</p>		
<p>{Day15/97:24} - {Day15/98:18}</p>	<p>Q. You claimed that they were forgeries planted on you and used by Ira Kleiman in his case against you in Florida; is that right?</p>	<p>Dr Wright blaming third parties, suggesting a conspiracy of documents being</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. No, they weren't planted on me, they were, my Lord, on a third party computer that was introduced as part of the Kleiman proceedings. These were machines that were imaged because of the wide-ranging long arm provisions of US law that includes anyone that I've ever had any association with, it would seem, because they weren't my staff at the time.</p> <p>Q. And you even claimed that both the 2011 and October 2014 Abacus incorporation forms for Tulip Trading were forgeries?</p> <p>A. I said that the emails on that were compromised.</p> <p>Q. No, you said that the incorporation --</p> <p>A. I said everything on that was compromised.</p> <p>Q. So that they were forgeries?</p> <p>A. Yes, I said the entire machine was basically my wife's, other people's, mine, emails that no one was allowed to access that were illegally accessed and altered.</p>	<p>planted on him (supposedly for use by Ira Kleiman).</p>
<p>{Day15/98:19} - {Day15/99:9}</p>	<p>Q. And it would have been pretty odd for somebody to forge a July 2011 Abacus incorporation form for Tulip Trading given that you say that Tulip Trading was in fact acquired by you in 2011 -- July 2011? That would be really strange, wouldn't it?</p> <p>A. No, it would be perfectly consistent, the reason being is that there were two separate sets of emails sent, one initially sent to the ATO, and then a third party associated with Ira, I believe, sent the other ones. So, what happened was the ATO received something saying, "These are Craig doing it", under official letterhead, that I didn't send, and then a third party said, "Craig made it up", and sent them to the ATO. Both of those had nothing to do with me. Third parties sent both to the ATO and then they were put into the Kleiman proceedings.</p>	<p>Dr Wright blaming third parties, in this case he suggests that two separate people created two separate versions of the forged documents in question.</p>
<p>Mr Madden's findings on DNS Records and Registrar details relating to domain service provider</p>		
<p>{Day15/100:3-24}</p>	<p>Q. We see that there's an entry for Abacus Offshore and its domain not relating to Google for the period 20 July 2009 to 25 November 2010; do you see that?</p> <p>A. I do.</p> <p>Q. And then a gap, yes?</p> <p>A. No. The way DNS works, it's not -- it's hierarchical. It is very different to the web. So where you have dark websites because you haven't, like, gone and Googled them and spidered them, DNS works from a top-down domain structure. What happens is you have the root domain, the com domain</p>	<p>Dr Wright refusing to accept the obvious truth that there is a gap in the DNS records.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>and then sub-domains. Now, before you can actually get on and have a domain registered, you have to actually propagate it. So, no, there can't be a gap. No, you can't have a gap. Google then verifies whether the record is propagated before they will allow you to do it. So what you're saying here, that's not a gap, that's actually, basically, that is the SOA number has changed but the information hasn't.</p> <p>Q. The next time record is from April 2015 to that same date, April 2015; correct?</p> <p>A. No. You're doing it completely wrong. This is an SOA update record.</p>	
{Day15/101:5-22}	<p>MR JUSTICE MELLOR: There's a gap in the data set out in this table.</p> <p>A. No, there is not, my Lord. The DNS works by recording entries, it doesn't have gaps, it doesn't do the time the way that they're saying. That references OA records for the times. The additions are additions to the site. So, there is no such thing as a gap in a whois record. It doesn't exist. I have two forensic books on this topic, I have published papers on this topic going back to the 90s. The reason people use whois in criminal records, of which I've been involved from a prosecution point of view in numerous expert testimony, is that there are no such things as gaps in DNS records. DNS must propagate. If it doesn't -- it's not like the web, it's not distributed. There is no such thing as a gap in a whois record of this type. It doesn't exist. And the reason they're not going out there and finding one is it doesn't exist.</p>	<p>Dr Wright continuing to deny the gap in records, despite intervention by Mellor J.</p>
{Day15/104:19} – {Day15/105:1}	<p>Q. {G/9/19}, please. Mr Madden conducted his own researches using available records and he found, as we see here, that up to 13 June 2014, the domain registrar was given as PDR Limited; do you see that?</p> <p>A. What he's recording is a PDR – like the record of the name service. I didn't look at name service changes</p>	<p>Dr Wright demonstrating that he is unfamiliar with basic IT terminology, he does not appear to know it stands for Name Server.</p>
{Day15/108:6-21}	<p>Q. The receiving server can verify the message against a public key from the originating mail server?</p> <p>A. Yes.</p> <p>Q. Common benefits of this are to prevent others spoofing your domain, yes?</p> <p>A. It's a domain spoofing -- yes.</p> <p>Q. And to prevent your emails being identified as spam?</p> <p>A. Correct, although it doesn't always work.</p>	<p>Dr Wright not accepting the obvious truth. Again, Dr Wright demonstrates his inability to say “yes” to a basic factual question, and insists on putting everything in his own words.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. So the primary use of DKIM authentication is to verify at the point of receipt the email is from its stated domain?</p> <p>A. If you have it set up. Probably only 30% of domains run DKIM properly; the majority don't right now.</p> <p>Q. But that's the purpose and use of it, yes?</p> <p>A. It's used by a lot of corporations, etc, to validate the source of their servers.</p>	
<p>CROSS-EXAMINATION OF DR WRIGHT BY MR GUNNING KC</p>		
<p>{E/33} - Fourteenth Witness Statement of Dr Wright The Bitcoin White Paper Latex Files</p>		
<p>{Day15/112:23} - {Day15/113:25}</p>	<p>Q. If your story about how these were created and how you maintained them over this period were true, they would be the sort of DNA of the Bitcoin White Paper, right?</p> <p>A. No, they're files that I've used and updated over time, so they're not the DNA of the White Paper, they're the papers that I have had for my work.</p> <p>Q. You say the White Paper was produced from LaTeX, right?</p> <p>A. It was.</p> <p>Q. And so if you had the White Paper in its native LaTeX form, that would be very important, wouldn't it?</p> <p>A. It's part of the evidence, like many other things. There's no, you sign or anything like that. The point I'm making is it's about work and effort and everything I've been doing. I've always stated this. So, your comment is that am I going to get a slam dunk or do I think this is a slam dunk because I go there's a LaTeX file? No. Nor did I ever say that.</p> <p>Q. Okay, I'm not sure I referred to slam dunks, but you surely would have understood the importance of preserving the documents?</p> <p>A. No, I've copied and pasted them. That's why they were never put in in the first place. I explained, multiple times, that these are files that I use in my ongoing research, and so that's why they're ignored back in Kleiman, etc.</p> <p>Q. You have held yourself out as a forensic examiner, right?</p> <p>A. I have been in the past, yes.</p>	<p>Despite claiming to be a forensics document examiner, Dr Wright is unable to explain why he never preserved or previously presented as evidence his LaTeX files.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{L1/470/8} - Document retention paper by Craig Wright		
<p>{Day15/115:3} - {Day15/118:9}</p>	<p>Q. And in the second paragraph: "It is usually when things go wrong that current documents are of the greatest significance." Right?</p> <p>A. That's correct.</p> <p>Q. And a little at the end of that paragraph: "Oral testimony without evidentiary support is not reliable. Documents may be used to trace records and their absence often says more than their existence, but not in a good way." Right?</p> <p>A. Yes, but we're talking over decades, so, again, this is part of why I've been trying to build Bitcoin, because there isn't an existing system, so --</p> <p>Q. Dr Wright, I'm going to cut you off, because the response that you've given to me suggests that you've changed your view about this --</p> <p>A. No, it doesn't.</p> <p>Q. Right.</p> <p>A. No, my view --</p> <p>Q. So you understand that grave consideration has to be given to the destruction of any document?</p> <p>A. No. If you go further in this document, you will see that while I say that there, you have to have a policy, and the policy then sets times. Now, in this document there's a table going into the expected life span of documents. None of those are the length of this course -- this court case away from when we did it. So if you go back to my table, you will see that seven years is generally considered more than enough time for any document retention.</p> <p>Q. I'm not interested really, Dr Wright, in what you've been doing in the last -- over seven years ago, I'm interested in what you've been doing in the last four months, right?</p> <p>A. Oh --</p> <p>Q. If we go to page 9 of this document {L1/470/9}: "If a dispute has previously arisen or is considered likely, it is very</p>	<p>Dr Wright provides an unconvincing explanation when cross-examined about the destruction of documents during the course of these proceedings.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>hazardous to destroy any documents." Right? You would agree with that?</p> <p>A. Yes.</p> <p>Q. "Cases where provisions for litigation had been included in audit reports are a definite example. In instances where it is probable that a dispute may arise or after a dispute has begun, a conscious choice to destroy documents could make one liable under the criminal offence of obstructing or perverting the course of justice." That's what you said?</p> <p>A. I did.</p> <p>Q. And then a couple of paragraphs down: "The destruction of documents can adversely influence a case through interference." Right?</p> <p>A. I do. I said that, yes.</p> <p>Q. And you accept that all of those things are correct?</p> <p>A. Yes, they are.</p> <p>Q. And it's not something that was a view of yours back in 2007 and 2008 that you had forgotten in November 2023, is it?</p> <p>A. No, because the documents aren't the originals. So what you're implying is that documents related to companies that were bought by companies, that were bought by companies, that were bought by companies, that were bought by companies, that were bought by companies. Exceeding the time frame that I put in my table, 20 times in some cases, where I said, "You need a policy", exceeding the policy that was formally stated and given, even the seven-year policy by three times, yes. I mean, I -- I don't believe that companies should keep records forever.</p> <p>Q. You were presumably told to preserve documents for the purposes of these proceedings?</p> <p>A. Yes.</p> <p>Q. You've had an Overleaf account associated with your craig@rcjbr.org email address since at least August 2023, right?</p> <p>A. Somewhere around there, yes.</p> <p>Q. We can tell it's that date because your -- the details for that account contain a Unix timestamp which gives a time and date on August 2023.</p> <p>A. That's fine. I don't recall the exact date, but yes.</p>	

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>{M1/2/157} - Chart plotting Dr Wright's work on the compiled BWP, based on Maths (OLD)_chunks file</p> <p>{L21/12/1} - Animation showing changes to BitcoinSN.tex and main.tex</p>	
<p>{Day15/122:4} - {Day15/123:17}</p>	<p>Q. So you worked for about three hours on 17 November; do you see that?</p> <p>A. I wouldn't say I worked for three hours. I wrote a sort of a CookBook and demonstration guide.</p> <p>Q. Well, we can actually literally see row by row, and I'm not going to take you through it, the changes that you're making in the chunks spreadsheet, right?</p> <p>A. Like I said, I was demonstrating what a no sort of spaceskip, etc, file was and what one was. So part of actually doing that file, the SN file, was to demonstrate the complete difference on how the files are created.</p> <p>Q. You then -- after you'd worked for about three hours, you then posted a Slack post, which we see at page {M1/2/156}. You'll see a couple of Slack posts there about watermarking. The timestamp on those is at Eastern Standard Time, so you posted about having put watermarking in, right?</p> <p>A. No, I believe that's to do with other posts I do. As I've noted before, I'm not the only person who runs these accounts and I do ask people to post things on certain topics.</p> <p>Q. Well, it's a pretty incredible coincidence, Dr Wright, because you post on your Slack post some stuff about watermarking, and then at the end, one of the final operations you do on the BitcoinSN.tex file is to slap in some comment about watermarking. It was you that posted this, wasn't it?</p> <p>A. No, I don't believe it was.</p> <p>Q. Who else was it?</p> <p>A. As I said, my Twitter --</p> <p>Q. (Overspeaking - inaudible) --</p> <p>A. -- my -- I'm not sure. Other people at nChain do. But I'd asked for a number of posts to be put out, so ...</p> <p>Q. Who was it?</p> <p>A. I don't actually know.</p> <p>Q. Was it the tall guy?</p> <p>A. Like I said, I don't actually run all my social media.</p> <p>Q. You did this.</p>	<p>Dr Wright is evasive, disavowing posts on his social media channels, whilst also blaming third parties for posting the Slack posts referred to.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{Day15/124:15-18}	<p>Q. This is 22 hours of working on the BitcoinSN.tex file in the Maths (OLD) folder, Dr Wright, isn't it?</p> <p>A. No, it's the occasional going back and forwards as I'm doing other things.</p>	<p>Dr Wright not accepting the obvious truth regarding the length of time spent on the BitcoinSN.tex file.</p>
<p>{Day15/125:9} - {Day15/128:1}</p>	<p>Q. We're going to come to the changes in a minute and we're going to come to the demonstrations in a minute, but the changes that you made to the BitcoinSN.tex file of the Maths (OLD) project and then to the main tex file of the Bitcoin project included changes which were designed to make the text of your LaTeX file more closely resemble the formatting of the Bitcoin White Paper; correct?</p> <p>A. No, not at all. The demonstrations were to show how the differences were. I'd actually already told my solicitors about it going back to October.</p> <p>Q. We can see, and we're going to go through some of this but hopefully fairly briskly, that you were adjusting the size of the spaceskip commands; do you agree?</p> <p>A. Yes. Like I was saying, you demonstrate how the thing works and I put them in and out.</p> <p>Q. And then you were adding and moving "/:"s, right?</p> <p>A. Yes.</p> <p>Q. And that was to try to enable you to try to replicate the line breaks and the spaces between words in the Bitcoin White Paper, wasn't it?</p> <p>A. Not at all. It was actually putting things back to demonstrate what it is without it and how these things work.</p> <p>Q. Now, we've prepared an animation which shows the changes that you made to those two files, BitcoinSN.tex and main.tex. It's at {L21/12/1} is the first format. And just before we play this, once it's open -- right, if we pause it -- we can see that the pages go from pages 1 to At the top and 6 to At the bottom, right?</p> <p>A. Mm-hm.</p> <p>Q. And the video identifies the row from the chunks spreadsheet that you had produced and the time of the change that is made in relation to all changes. So if we could press play on that. It takes about a minute, so there will be a period of silence.</p> <p>(Animation played)</p> <p>Now, if we stop there, do you remember -- as you were seeing that, do you remember a little bit flashed up in red towards the end?</p>	<p>Dr Wright (implausibly) suggesting that he was demonstrating to his solicitors how editing the Bitcoin White Paper might be done.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. I saw a quick flash, yes.</p> <p>Q. That's the period when you were on a conference call with Shoosmiths, right?</p> <p>A. I don't recall the exact date. I had multiple calls.</p> <p>Q. Well, rest assured, they've told us when it was and we've factored that into that animation. Now, what that animation shows is that you were moving and adjusting text, right?</p> <p>A. Yes, that was part of capturing and what I was demonstrating. The original was demonstrated to my solicitors at my home before any of this happened.</p> <p>Q. And we can see that, generally, the changes started on page And continued down the document, right?</p> <p>A. Oh, as I made each of the change, it's not the whole document changes. To demonstrate what the different commands do, I had to actually put them in.</p> <p>Q. There's a second form of the video, which we can see at {L21/13/1}, and this time the text that you were working on is overlain on the control copy of the 24 March 2009 Bitcoin White Paper, right? If we just look at that first slide, we can see that on 17 November 2023, the only page that bore a resemblance, but it wasn't a very good one, to the Bitcoin White Paper was the first page, right?</p> <p>A. No, as I said, what I did was actually had the first one and that's different as well. So I started doing a process to demonstrate how you actually create these things. So that was part of the demonstration.</p>	
<p>{L21/5/1} - Document prepared by Stroz based on the JSON file CSW had produced{L5/26/1} - Control version of the March 2009 publication of the Bitcoin White Paper</p>		
<p>{Day15/131:8-22}</p>	<p>Q. And so we have "Abstract" and then a space and then we have: "A purely peer-to-peer version of electronic cash would allow online ..." Right?</p> <p>A. Correct.</p> <p>Q. Just before the words "A purely peer-to-peer", you inserted the spaceskip command that we just looked at, right?</p> <p>A. I reinserted it. Basically, like I did, the BitcoinSN file was downloaded from one that Shoosmiths had already seen and I had multiple other files and I did this to demonstrate how the Bitcoin White Paper was created and the use of these things to do the spacing.</p>	<p>Dr Wright is evasive, referring to "multiple other" files, and implausibly suggesting that edits were done to demonstrate how the Bitcoin White Paper was created.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{L21/29.1/4} - Bitcoin SN Timecoin file		
{Day15/132:5} - {Day15/132:14}	<p>Q. So you used a base parameter of 0.3em, right?</p> <p>A. Yes, and I changed that to demonstrate the differences.</p> <p>Q. Do you know what 0.3em means?</p> <p>A. Yes, I do. It has to do with the character spacing and 0.3 of the standard space. I'm not sure exactly what they call it in LaTeX, but it's a standard marker space.</p> <p>Q. Were you very familiar with LaTeX before you were doing this?</p> <p>A. I know LaTeX. I don't -- I'm not an academic, I don't teach it, so I don't know all the terminology.</p>	<p>Dr Wright demonstrating his unfamiliarity with LaTeX terminology, despite claiming to be experienced in its use.</p>
{Day15/133:5} - {Day15/135:4}	<p>Q: And we can see from what you've put in there that you've put 0.3em plus 3.4em, right?</p> <p>A. Mm-hm.</p> <p>Q. So that would take it up to a maximum stretch of 3.7em?</p> <p>A. It gives a -- for the whole line, a minimum and maximum between characters, between words, etc, and a stretch factor</p> <p>Q. Well, you say to the whole line, it's actually for the passage to which this -- this -- this --</p> <p>A. Well, between --</p> <p>Q. -- command is being applied, because you had to put in lots of other spaceskip commands later, didn't you?</p> <p>A. No, I gave examples of how I did it. So this was showing the differences.</p> <p>Q. But in any event, it's 0.3, so the margin, it allows you to go up to 3.7 because it's plus 3.4, right?</p> <p>A. Effectively, yes, but it won't generally actually do that.</p> <p>Q. And it will allow you to go down by 0.1, so you could go down to 0.2em right?</p> <p>A. Fairly much.</p> <p>Q. So, now, you made a number of changes to those parameters over the next few versions of BitcoinSX file, right?</p> <p>A. Yes, it was to demonstrate how complex this was. So, you can't just set these values. Because it has an automatically</p>	<p>Dr Wright providing a vague answer, uncharacteristic of someone with the relevant technical expertise.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>generated range, if you change one, it means everything else varies significantly.</p> <p>Q. When you muck around with the spacing between words, you muck around with where the line breaks are going to appear in the paragraph, don't you?</p> <p>A. That was the idea of what I was demonstrating, and just how difficult it is to do these things and get correct -- for something correct.</p> <p>Q. And without the spaceskip command, you couldn't get the words to fit their position in the Bitcoin White Paper itself?</p> <p>A. No, actually it would be simpler. If you went for each space, what you could do is have, like, a set value between everything. So, instead of the "%%" type stuff, I could actually say a specified in millimetres distance. So the simple way to do this would be I would download a PDF file, if I wanted to copy it, and then I would have a Python script, and there are some available, and the Python script would then give the distances between words, measured exactly in the White Paper to the tenth of a millimetre.</p> <p>Q. That's if you wanted -- if you were forging the White Paper, that's what you would do it, is it?</p> <p>A. That's how you would do it, yes. And then --</p>	
<p>{Day15/136:23} - {Day15/137:16}</p>	<p>Q. And you then increased it to 0.6em, right?</p> <p>A. I did.</p> <p>Q. And you then reduced it to 0.2em in a bit below that?</p> <p>A. Yes, the best way of demonstrating how it works is to make a large change.</p> <p>Q. Yes, but none of this is being done on one of your demonstrations to Shoosmiths?</p> <p>A. This was actually part of what I was documenting at the time.</p> <p>Q. How were you documenting it?</p> <p>A. I had files.</p> <p>Q. What files?</p> <p>A. I had screenshots, etc, for some of the --</p> <p>Q. Sorry, you were taking screenshots every time you made a change to your Overleaf files?</p> <p>A. Some of these, yes. Not every single time, but when I was making differences. I also had other conversations even before this. Shoosmiths were at my house --</p>	<p>Dr Wright referring to more supposed files that he had, which he has not disclosed.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day15/139:7} - {Day15/139:25}</p>	<p>Q. You're not showing it to anybody, Dr Wright. We know the times when you're showing it to Shoosmiths. This can only be something that you're doing for yourself?</p> <p>A. No, actually, it's not, because I also created documents and I also documented the changes I was doing in what they wanted.</p> <p>Q. We're going to come to the documents that were produced, but standing back from this, we don't see that you were making adjustments to reintroduce known parameters from the Bitcoin White Paper, do we? That's not what you're doing?</p> <p>A. No, I'm actually adjusting it to show how different it can be.</p> <p>Q. What you're doing is tweaking parameters to try to get them to fit the layout of the Bitcoin White Paper, aren't you?</p> <p>A. No, actually, you wouldn't do that. And what you're actually -- you're saying --</p> <p>Q. It's not a question of what I would do --</p>	<p>Dr Wright not accepting the obvious truth, that it is possible to determine when he was amending the LaTeX files and that they do not corroborate his story that he was doing it as part of a demonstration to Shoosmiths.</p>
<p>{E/20/31} - Dr Wright's Sixth Witness Statement, paragraph 4</p>		
<p>{Day15/143:14} - {Day15/144:6}</p>	<p>Q. You referred to them as the White Paper LaTeX files and then you said this: "This applies --" You said: "I confirm ... the facts and matters stated in Field 1 are true, to the best of my information and belief." And then you confirm the facts and matters stated in Field 1 as to the nature and significance of these documents. You said: "This applies in particular to the facts and matters stated in ..." And then you identify specific paragraphs of Ms Field's witness statement, right?</p> <p>A. When I'm talking about the LaTeX papers, I was -- and the image files, I was particularly noting those that go back to 2007 the ones on the drive more than anything else.</p>	<p>Dr Wright seeking to reinterpret clear written evidence that he had given.</p>
<p>{E/24} - Hannah Field's First Witness Statement</p>		
<p>{Day15/144:13} - {Day15/145:3}</p>	<p>Q. Okay, well, let me take you then to the letter that we were sent on 27 November by Shoosmiths. It is at -- actually, no, instead of that, let's go to Ms Field's witness statement, which you're confirming here. It's {E/24/1}. Do you see, if we go to page 7 {E/24/7}, at paragraph 19.2, she says: "There are also</p>	<p>Dr Wright is evasive, and fails to accept the obvious truth in relation to what his own solicitors (Shoosmiths) have said</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>a number of LaTeX documents in Dr Wright's control, in addition to those found on the Hard Drives ..." Right?</p> <p>A. Yes.</p> <p>Q. And those are what have been called by everybody so far the White Paper LaTeX files, aren't they?</p> <p>A. No, but I'm not always clear and my solicitors had probably pulled out a lot of hair talking to me in my descriptions.</p>	<p>about what the White Paper LaTeX files actually are.</p>
<p>{Day15/145:16} - {Day15/146:12}</p>	<p>Q. Well, read paragraph 19.2.6.</p> <p>A. Like it says there, I recognise, in 5, that it's important and the Bitcoin folder contains LaTeX files which compiles into the Bitcoin White Paper.</p> <p>Q. Right. It says: "... when the code contained on them is compiled in Overleaf ... produce a copy of the Bitcoin White Paper ..." Right? The "White Paper LaTeX Files", right?</p> <p>A. Yes. But -</p> <p>Q. So those --</p> <p>A. -- the solicitors didn't understand what I was trying to explain when I was saying that LaTeX has moved from different packages, etc.</p> <p>Q. So why did you not clarify that in your witness statement in which you confirmed on oath that this was true?</p> <p>A. I still think it's true. I mean, it contains files that are compiled into the White Paper, that is my White Paper. Are there any differences? Yes, because it's on Overleaf and not the original MiKTeX. I don't see anything that's wrong with that sentence.</p>	<p>Dr Wright is evasive, and fails to accept the obvious truth in relation to what his own solicitors (Shoosmiths) have said about what the White Paper LaTeX files actually are.</p>
<p>{Day15/151:17} - {Day15/154:6}</p>	<p>Q. So earlier, on 17 November, you had the so-called White Paper LaTeX files in a different folder to Maths (OLD) or the Bitcoin folder, right?</p> <p>A. I copied it into my R drive and then uploaded into multiple places for the demonstrations.</p> <p>Q. And you have failed to produce the folder that held those earlier files, haven't you?</p> <p>A. Because I copied back and forwards between the others.</p> <p>Q. You deleted it?</p> <p>A. No, I did not. I moved it.</p> <p>Q. Can we go to {M1/2/210}. This a letter from Shoosmiths, dated 20 February 2024, so very recently, and we can see in paragraph 2.1:</p>	<p>Dr Wright appearing to confirm that he deleted documents that should have been retained as relevant to these proceedings.</p> <p>Dr Wright claiming that he did not want an adjournment of the trial, despite his production of new documents and a witness statement in support of the adjournment.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>"As you note in Your Letter, the Maths (OLD) project was created on 17 November 2023 at 16:26 [pm] ..."</p> <p>As I just put to you: "Dr Wright instructs us that this project was created by merging and/or copying files into Maths (OLD) from previous Overleaf project folders. Dr Wright tells us that he cannot remember what those previous project folders were called or whether he copied them directly within Overleaf or copied them from local copies he had previously downloaded from Overleaf. In any event, Dr Wright says that he deleted the previous projects folders after copying their contents ..." Why have you lied to me about that basic point, Dr Wright?</p> <p>A. I didn't. If you're talking about the previous things, then, yes, I've deleted them multiple times. Overleaf goes back quite a while, including multiple accounts. And have I kept them? No. I've copied between different Overleaf folders.</p> <p>Q. I said specifically to you that you had deleted those previous folders, and you said, "No, I did not, I moved it", is what you said.</p> <p>A. When you're moving, it actually changes the folder structure. So, we're talking about different things. I'm talking about the earlier stuff that I had in Overleaf here; you're talking about what I did on the 17th. So, they're different things.</p> <p>Q. Dr Wright, you deleted relevant and disclosable material just a couple of weeks before your application for an adjournment, didn't you?</p> <p>A. No. I didn't want an adjournment, for a start. But what I did was copy and paste these into different areas for demonstrations. The files in total were kept.</p> <p>Q. You must have known, Dr Wright, that that was improper?</p> <p>A. No, at that stage, everyone was telling me that there was no purpose of these and we wouldn't get them in. That's why I did the demonstrations. I did the demonstrations to show how little teeny weeny changes and how important it was, so I structured a whole lot of demonstrations to show just how critical these little tiny tweaks were and that you couldn't guess them.</p> <p>Q. We're not fools, Dr Wright. We can see the changes that you made; they were not tiny tweaks.</p> <p>A. No, they were tiny tweaks, and they were there to make the thing go back and forwards to show how it breaks ends, sometimes it actually breaks the whole file, etc. So the only way that I got the December stuff was to basically go through a series of exercises where I finally convinced my solicitors that this would actually be important.</p>	

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day15/155:14} - {Day15/160:8}</p>	<p>Q. You filed a witness statement which you knew was going to be served on us and that would be presented to the court to justify your application for an adjournment, didn't you?</p> <p>A. No, one, I didn't want an adjournment, my solicitors and barristers did. They said they needed time.</p> <p>Q. I'm not interested in that excuse, Dr Wright.</p> <p>A. No. No. No, that's --</p> <p>Q. We can see your witness statement. You did not tell us in that witness statement that you had been adjusting the White Paper LaTeX files --</p> <p>A. I demonstrated to my solicitors and my solicitors said --</p> <p>Q. I'm not interested in what you told your solicitors. Do you understand that?</p> <p>A. I know that you're saying that, but you're not listening to me either. Would you like me to answer?</p> <p>Q. I'm not going to allow you to answer a question about what you, Dr Wright, told the court by fobbing it off with an explanation about what you told your solicitors?</p> <p>A. So basically what you're saying is I can't answer because you're not going to let me answer.</p> <p>Q. You can confirm, because it's true, that you did not tell the court --</p> <p>A. So what you are saying, I can answer as long as I lie and perjure myself, both in this court and to god, which ain't going to happen. I had already shown all of this to my solicitors, they went through this process. So, very simply, why is no comments about what I did with my solicitors in there? Because they keep jumping up and down and going, "You can't mention anything we did".</p> <p>Q. Right.</p> <p>MR JUSTICE MELLOR: Dr Wright, just before we break, can I just get one thing clear, because --</p> <p>A. Yes, my Lord.</p> <p>MR JUSTICE MELLOR: -- I think you're now explaining that all those changes to the LaTeX files that are in that diagram, they're all done for demonstration purposes, and yet what was disclosed to COPA and the developers was the end product of all of that.</p> <p>A. I actually already had --</p> <p>MR JUSTICE MELLOR: Just wait.</p>	<p>Dr Wright not accepting the obvious truth when questioned by the Mellor J. His version of events (that he was adjusting the White Paper LaTeX files for his solicitors) is new, and is not supported by his witness evidence at the time.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Sorry.</p> <p>MR JUSTICE MELLOR: What you're now telling us is that we shouldn't be looking at that end product, we should be looking at the starting point, so all the analysis of chunks, what you're now saying, is a total waste of time; is that right?</p> <p>A. The analysis of chunks was a waste of time, yes, my Lord.</p> <p>MR JUSTICE MELLOR: Right, so --</p> <p>A. What I was saying --</p> <p>MR JUSTICE MELLOR: -- where -- why didn't you disclose the starting point as being the genuine LaTeX file of the Bitcoin White Paper?</p> <p>A. I did, my Lord. What I did was --</p> <p>MR JUSTICE MELLOR: Hang on, where was that produced?</p> <p>A. That's part of the files that were downloaded. I actually started with the original and then did the modifications to change and show all of this process.</p> <p>MR JUSTICE MELLOR: At which point did you say, "Don't worry about all the chunks, because that's all me just demonstrating to the solicitors"? When did you first make that clear?</p> <p>A. I actually had them over to my house --</p> <p>MR JUSTICE MELLOR: Okay, again, we're not interested in what you told them. I'm just --</p> <p>A. No, I showed them. I showed them Overleaf at my house and said, "This file is there", and explained it and compiled the Bitcoin White Paper while they were at my house. But they didn't think it was important. So the only reason I believe I got them to understand was I did a whole lot of exercises showing how little teeny weeny tweaks create big differences, can even break the file, etc, so none of the solicitors wanted to put it in.</p> <p>MR JUSTICE MELLOR: Why didn't you just show them a LaTeX file that looks materially identical to the Bitcoin White Paper?</p> <p>A. I did.</p> <p>MR JUSTICE MELLOR: Why did you need to do any demonstration?</p> <p>A. I did, my Lord.</p> <p>MR JUSTICE MELLOR: No, answer the question. Why didn't you just show them a Bitcoin White Paper that is materially identical to the published version?</p>	

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Overleaf has changes in OpenSymbol, etc, which I explained. So I explained those differences, and then I said, "This is the file I have now, I've migrated away from the old tools and it's been uploaded onto Overleaf". I then printed a paper that was, well, basically the same as the same one now, and then showed them that, and at that point they didn't think it was important.</p> <p>MR JUSTICE MELLOR: So now your case is you had to reconstruct a LaTeX Bitcoin White Paper file that looked materially identical to the original published Bitcoin White Paper? Is that what you're saying?</p> <p>A. No, I deconstructed the paper to show differences, removed all of those bits, then added them back to get to the original one. So I worked, basically, with a copy there, took everything out, and then added them back to show -- and made some tweaks along the way to show just how even a small difference radically changes it.</p> <p>MR JUSTICE MELLOR: Okay. Let's --</p> <p>MR GUNNING: Dr Wright, we're going to have to move on to a different topic, but I have to say it's absurd and obviously factually incorrect to say that you made the changes and then you undid all of the changes that you made. We can see that that isn't true by looking at the chunks file.</p> <p>A. No, you can't, because the file that I downloaded and ran in UltraEdit from my R drive, which was the original, basically it takes moments to strip all this information out. It's very simple to run a Python script and script all that out, basically take it all out, and then you add it back in from the original, show some changes, show that it won't work, etc.</p>	
<p>{E/23} - Dr Wright's Eighth Witness Statement</p>		
<p>{Day15/165:2} - {Day15/166:12}</p>	<p>Q. And you made no reference in that statement at all to your manipulation of the White Paper LaTeX files in November and December 2023, did you?</p> <p>A. There's no manipulation. As I noted, Matt and others from Shoosmiths had come out in October, so I'd already given it to them.</p> <p>Q. On 12 January 2024, you served your 11th witness statement, right?</p> <p>A. Around that date.</p>	<p>Dr Wright is evasive and not accepting of the obvious truth regarding when he first referred to the changes he made to the White Paper LaTeX files.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. And again, in that you made no reference to the adjustments that you had made between 17 and 24 November 2023, did you?</p> <p>A. I'll emphasise again, solicitors already came out and seen it in October of '23.</p> <p>Q. We have seen that you had said that you were going to identify for us the corrections that you had made in your reply witness statement; do you recall that?</p> <p>A. Yes.</p> <p>Q. And you didn't do it, did you? You didn't refer to those changes in your 11th witness statement, did you?</p> <p>A. Some things got cut, but I actually had even more rambling, longer witness statements at this stage.</p> <p>Q. It's not rambling. That would not have been rambling.</p> <p>A. Well, you guys confirmed that it was rambling earlier in what I put.</p> <p>Q. Well, lots of your statement is rambling, but it wouldn't have been rambling to admit that you had been manipulating the White Paper LaTeX files between 17 November and 24 -- in fact -- and, you know, 24 November, right?</p> <p>A. I didn't manipulate the LaTeX files at that date. As I noted, I'd already, in October, demonstrated, I'd copied that and downloaded it so that I could actually do the demonstrations. In October, they still didn't see that it would have any value, so the only way I could do it was to do the demonstrations.</p>	
<p>{H/20/11} - Madden Appendix PM3 - BWP, 6 hr time zone</p>		
<p>{Day15/168:15} - {Day15/173:3}</p>	<p>Q. We can see it at {H/20/11}.</p> <p>A. Minus seven goes to minus six when you add summer time.</p> <p>Q. Dr Wright, we can see here that the creation date was 20090324113315 minus 6, right?</p> <p>A. Minus 7, in the statement, when you add summer time becomes minus 6, plus one hour, so minus 7 plus one is minus 6.</p> <p>Q. Dr Wright, I perfectly well understand that if you were trying to state the relevant time at a minus seven-hour time zone that you would have put 103315, but actually, Satoshi didn't use a minus 7-hour time zone for this version of the White Paper, did he?</p>	<p>Dr Wright providing an unconvincing answer regarding the creation dates / time zones.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. No, you're incorrect once again. Time zones. If you compile it and you change, like, that not to be that part of the year, it will be different.</p> <p>Q. Dr Wright, the whole point of this section of your witness statement is for you to describe the -- is to describe what you were saying was the way in which you could configure the metadata properties, right?</p> <p>A. Yes.</p> <p>Q. But you put in duff metadata properties in your 11th witness statement, didn't you?</p> <p>A. Again, time zones. I know you seem not to understand it on purpose, but when you have a plus one on a time zone, it changes. So time zone plus one means negative 7 plus one, which comes out on the final document as negative 6.</p> <p>Q. If you're manually configuring the Bitcoin White Paper to identify -- and you're doing it in LaTeX, which Satoshi did not do, if that's what he had done, he would have had to put minus 6 to get the output that we're seeing here as the creation --</p> <p>A. No, if you did it on minus 6, because of plus 1, you'll actually get negative 5. So again, it's like London time. We keep adding an hour, subtracting an hour, making people change clocks -</p> <p>MR JUSTICE MELLOR: Hang on, Dr Wright. As I understand your evidence, in LaTeX, it's nothing to do with any clock, you put in these numbers.</p> <p>A. Ah, but the system will still use the timestamp information. So you put in those numbers --</p> <p>MR JUSTICE MELLOR: How? Which bit of this creation date field does the system change then?</p> <p>A. You still have to put in the time zone information if you want it not to change naturally on the system clock, my Lord. So the system clock, when it compiles, will recognise if it's a plus one and add that and modify it. So, when you do this, unless you do something like specify GMT, or Eastern Standard Time specifically, then it's going to take the natural sort of changes and drifts.</p> <p>MR JUSTICE MELLOR: Mm. I think I've previously asked you about whether there was a default or whether you had to put all this in manually.</p> <p>A. If --</p> <p>MR JUSTICE MELLOR: And I recall you answered it's manual.</p>	

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Yes, but what I'm saying here is the difference between the negative And the time zone information, my Lord. They're actually two different settings.</p> <p>MR JUSTICE MELLOR: Yes, I mean, I'm afraid, Dr Wright, I simply don't understand that answer. So if you want me to understand it, you're going to have to explain precisely how this works.</p> <p>MR JUSTICE MELLOR: Okay, but I don't understand why you would be worrying about summer time, plus 1, minus 1, etc.</p> <p>A. That's why it comes out, if you put 7 in --</p> <p>MR JUSTICE MELLOR: No, no, no, why wouldn't -- okay, we'll ssume Satoshi is putting in the creation date.</p> <p>A. Yes.</p> <p>MR JUSTICE MELLOR: Why would he worry about whether it was summer time or not?</p> <p>A. No, it's a time zone negative 7. At the time, I was doing a lot of work with American and Caribbean companies, so my default when I printed things was negative 7. The reason for that is, in Antigua, various other islands, a lot of gaming happens. So when I was doing, you know, documents, etc, I used standards for either South American or Caribbean time. Now, that comes with certain plus 1 minus or plus 10 type adjustments. Now --</p> <p>MR JUSTICE MELLOR: Adjustments from when?</p> <p>A. I'm not exactly sure when summer time does or doesn't start.</p> <p>MR JUSTICE MELLOR: No, no, no, but if you're talking about Antigua and Caribbean saying plus 1/minus 1, that's adjusting relative to which time zone?</p> <p>A. To the negative 7. So it will take negative And add one. So when it compiles, it becomes negative 6. So, he document here says that date, but then it becomes negative 6 in the PDF, because the PDF will display plus summer time, etc.</p> <p>MR GUNNING: Dr Wright, the last time I looked, the time zone difference in the Caribbean was minus 5 hours, but ...</p> <p>A. As I said, also Belize, other places. I did South American and the others.</p> <p>Q. You had a sort of travelling time zone then, did you?</p> <p>A. I did. I had dealings with a variety of Central American and Caribbean areas. I still do.</p>	

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{CSW/1/69} - para 365 - PDF Creation Date in Maths (Old) project		
<p>{Day15/173:19} - {Day15/174:9}</p>	<p>Q. I'm not going to waste time going into it, but it isn't. And we know how you came to put this command into the White Paper LaTeX files; it was something that you did not do until 1 December 2023.</p> <p>A. No, that's incorrect. I'd already demonstrated files set in the future, set in the past, and I've done that multiple times.</p> <p>Q. It's a matter of record. There is no PDF creation date command in the Maths (OLD) project, right?</p> <p>A. I've no idea.</p> <p>Q. It's the PDF creation date that's entered in the Bitcoin project up to 24 November is not the -- doesn't include the time and time zone that you've provided there.</p> <p>A. The one that I demonstrated when they were over at my house in October had all this, and when I demonstrated, I demonstrated how that worked.</p>	<p>Dr Wright claiming his "demonstration" documents had more metadata than that which was disclosed in these proceedings.</p>
{L5/26/4} - original BWP versus {M3/10/4} - Dr Wright's compiled version {L1/6/13} - Merkle's original tree		
<p>{Day15/177:5} - {Day15/179:4}</p>	<p>Q. And that's obviously an error, isn't it?</p> <p>A. Yes, in this version.</p> <p>Q. Any other comments on that?</p> <p>A. Not off the top of my head, no.</p> <p>Q. Isn't there something rather strikingly obvious?</p> <p>A. I don't memorise every part of my diagram, no.</p> <p>Q. Okay, well, let's go back to the Bitcoin White Paper. It's at {L5/26/1}. Let's go to page 4 of that {L5/26/4}. Perhaps we could put that up alongside -- yeah, sorry. So, do you see, if we look at those two things, in the original Bitcoin White Paper, which is on the left, the error isn't one of overflowing the bounding box, the mistake is that in your image, you've identified the hash of transaction 0 as "Hash01", right?</p> <p>A. Yes. There's a typo in it, yes.</p>	<p>Dr Wright demonstrating his inability to identify basic errors in an image of a Merkle Tree, despite their centrality to Bitcoin.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. And that is an error in your LaTeX code, right?</p> <p>A. No, it's not an error in the LaTeX code, it's an error in the diagram that's been introduced at some point.</p> <p>Q. It's an error in your code. If we go to {L21/11.2/7}. This is the code for image 4. Do you see, about ten lines down from the top, it says, "put(154.8, -548.3)"?</p> <p>A. Yes, and I've typed in "Hash01" instead of "Hash0".</p> <p>Q. Right. Because it doesn't make any sense to describe the hash of transaction 0 as Hash01, does it?</p> <p>A. It does in certain other versions of the document.</p> <p>Q. No, no, no.</p> <p>A. Well, yes, it does in other versions. This isn't the only time I've used that.</p> <p>Q. As a hash of transaction 0?</p> <p>A. As I said, this diagram has been used in multiple things, so where it says "Hash01", others were 00011, etc.</p> <p>Q. Oh dear. Shall we go back to {L5/26/4}. You understand how Merkle trees work, right?</p> <p>A. Of course I do.</p> <p>Q. Right. So the way that they work is that you take a hash of each of the transactions at the bottom, right?</p> <p>A. Mm-hm.</p> <p>Q. And a hash of transaction 0 is going to be hash 0, right?</p> <p>A. That's one way of naming. In a binary tree structure, you could also do other structures and names. Now, in my diagram, I've noticed I've put "Hash01" there and I've got an error in one of the versions, yes.</p> <p>Q. Because it doesn't make any sense to refer to the hash of transaction 0 as hash 0, because hash 01 is the hash of both hash 0 and hash 1, right?</p>	
<p>{Day15/179:19} - {Day15/184:3}</p>	<p>MR GUNNING: Well, Dr Wright, I'm not going to take up time asking you about Merkle trees, save to -- just this one point. You've referred to Merkle trees as being a type of binary search tree, right?</p> <p>A. Yes.</p> <p>Q. I have to suggest to you that somebody who was doing their first year undergraduate degree in computer science would know that a Merkle tree is not a form of binary search tree.</p> <p>A. No, that's actually incorrect. The reason --</p>	<p>As above, Dr Wright demonstrates his lack of technical knowledge when questioned over basic facts concerning Merkle trees.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Dr Wright --</p> <p>A. The reason they're actually used for SPV, they allow a structured search, they are completely ordered. The description given by Professor Meiklejohn is utterly wrong. Now, what you have is the ability now to have ordered transactions and this allows SPV to work.</p> <p>Q. Right, okay. Dr Wright, let's just go through this quickly. I hoped I wouldn't have to. But the point of a Merkle tree is that, as we can see here in this diagram, or indeed in Merkle's original diagram, that you take a hash of the datasets at the bottom, right?</p> <p>A. You take a hash of the transaction and you combine them.</p> <p>Q. Then you combine those hashes, right?</p> <p>A. And basically make an ordered tree structure. That's a balanced tree, as I've said, because it --</p> <p>Q. Let's just go through it slowly. So the next row up, we can see that a further hash is taken of the hashes in the row beneath, right?</p> <p>A. Yes, you -- you basically combine two at a time. Then it makes a binary structure, 01, so that basically you can go through and, if you have a number search, 01110, you can actually take the position in the tree and then follow it through.</p> <p>Q. Let's go --</p> <p>A. That's a key part of SPV.</p> <p>Q. Let's go to {L1/6/5} where we can see Merkle's original tree, I think.</p> <p>A. Merkle's original tree was used as a signature system. The use --</p> <p>Q. (Overspeaking - inaudible) -- wait for the question --</p> <p>A. -- of a binary tree structure in Bitcoin isn't.</p> <p>Q. Wait for the question, all right? I think, if we go to -- I think it's the final page of this. Sorry, I gave you a duff reference. 13 {L1/6/13}. So, do you see, we have there a Merkle tree structure, right?</p> <p>A. We do.</p> <p>Q. And what we can see is that we have what he describes as public files Y1, Y2, Y3, Y4, Y5, Y6, Y7, Y8, right?</p> <p>A. Not in the way you're actually describing. What he has is a hash based signature scheme so that you can have a signature based on something other than public/private key pairs.</p>	

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Okay, Dr Wright, take it from me that he refers to Y1 through to Y8 as public files, all right?</p> <p>A. Yes --</p> <p>Q. (Overspeaking) --</p> <p>A. -- to do with signatures.</p> <p>Q. Let's --</p> <p>A. No, what you're saying is incorrect. If you want to go through the document, we'll go into the signature section.</p> <p>Q. Dr Wright, a hash is then taken of each of those things, right?</p> <p>A. Again, if you go up -- can you scroll to the next page?</p> <p>Q. Let's stick. A hash is taken of each of those bottom --</p> <p>A. My Lord, this document describes signatures just above this diagram. Can we go to the page before and show?</p> <p>MR JUSTICE MELLOR: Why don't you just answer the questions and then you can add whatever qualification you want.</p> <p>MR GUNNING: I'm sure you can be brought back to all of that in re-examination, right? But what we have is a hash of the bottom -- of the public file at the bottom that's taken, right?</p> <p>A. You have a hash, a hash of the two files --</p> <p>Q. And then -- then, at the next row up, we see that a hash is taken of the combination of both of those hashes, right?</p> <p>A. You have a hash, a hash of the two hashes, etc, in a binary structure.</p> <p>Q. So, at that point, you've got a hash of the combination of Y1 and Y2, and a hash of the combination of Y3 and Y4, and a hash of a combination of Y5 and Y6, and a hash of a combination of Y7 and Y8, right? Quite straightforward.</p> <p>A. In this structure, yes, but it's a little bit different in Bitcoin.</p> <p>Q. It's --</p> <p>A. Where he's going hash 1,1,Y, hash 2,2,Y, etc, that's actually a different structure to actually how it is implemented in Bitcoin. Bitcoin is not designed as a signature system.</p> <p>Q. The next row up still, we can see that a further hash is taken of the combination of hashes in the row below, right?</p> <p>A. You hash sort of -- well, hash the files, hash them together, hash them together, etc.</p> <p>Q. Right, so at that point --</p>	

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. It allows searching. So, instead of having a list structure as a block, which would be far more easy and small BTC level stuff, you have a search --</p> <p>Q. Right, you're running away from my questions. I'm trying to take it very simply and slowly so the judge can understand what the picture is that we're seeing. So the second row down -</p> <p>A. What you're seeing is not to do with Bitcoin. This is the signature structure used by Merkle, which is different to what Bitcoin does.</p>	
<p>{Day15/188:10} - {Day15/189:20}</p>	<p>Q. When did you make that error?</p> <p>A. Oh, probably back years and years ago.</p> <p>Q. You can't have made it before the Bitcoin White Paper, because the Bitcoin White Paper doesn't contain it.</p> <p>A. No, that's incorrect. I could have made it, but not copied it across. I had -- some of these files go back into other documents I had from BDO that have nothing to do with Bitcoin, some have -- I mean, again, you're assuming that I've got one copy. I have 20-something copies of my last dissertation or thesis that I only did my viva for this week.</p> <p>Q. Right. Now --</p> <p>A. So that means I don't have just a copy and sometimes I don't copy the folder correctly.</p> <p>Q. On 22 January, so ten days after your 11th witness statement, your solicitors produced to us a redacted export of the Bitcoin folder's project history that had been obtained by you from Overleaf, right?</p> <p>A. Yes.</p> <p>Q. And --</p> <p>A. Well, actually, Stroz came out, or KLD, one of the people, and I downloaded it with them.</p> <p>Q. Two separate things happened. One is that Stroz and Shoosmiths came to your house and downloaded something and the other was that Overleaf were produced and emailed you something, right?</p> <p>A. Well, I got emailed a link and then, with KLD, we clicked the link and downloaded it.</p> <p>Q. Fine. Now, when that was produced to us, when the Bitcoin folder project history was produced to us, or before it, you, Dr Wright, had inadvertently put a json file associated with the Maths (OLD) project into that ZIP file, hadn't you?</p>	<p>Dr Wright blaming third parties - KLD - for disclosure failures.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	A. No. I downloaded that with the KLD people, clicked the link at one stage and things got sent.	
{AB-A/5/58} Letter from Macfarlanes to Court Paragraph 15		
<p>{Day15/193:3} - {Day15/194:15}</p>	<p>Q. Dr Wright, we have established, because we did it right at the very beginning of the cross-examination, that you copied the BitcoinSN.tex file into the main.tex file as described there, right?</p> <p>A. Yes.</p> <p>Q. Right. And the BitcoinSN.tex file was from the Maths (OLD) project, right?</p> <p>A. As this says --</p> <p>Q. Yes.</p> <p>A. -- it comes from -- no, as it says, it comes from another project. That was copied, like 20 existing files, into a similar structure. So --</p> <p>Q. Dr Wright, the content of the first full version of main.tex in the Bitcoin folder is identical, it's not just hash identical, it's identical to the final version of the BitcoinSN.tex file in the Maths (OLD) project.</p> <p>A. That's because that's where I started. You're getting it, again, the wrong way round. I downloaded these, I removed some of the stuff; the download stayed the same, that was in my R drive. That was then loaded up for the demonstrations where I compiled basically multiple versions to show the differences, and then I loaded the original one that I'd downloaded, which is talking here about the existing files of similar structure.</p> <p>Q. Dr Wright, the inference that was drawn by us when we saw this was that you had copied material from the Maths (OLD) project into the new Bitcoin project, and that was true, right?</p> <p>A. No, it's actually the other way round. I copied down. That's where these files are. I then copied those into the demonstration drive and then I copied later back into the other.</p> <p>Q. No, the Bitcoin project didn't exist until 19 November.</p> <p>A. No, but I had other folders, and like it says here, "20 existing files". The problem is that it doesn't have any information from previous --</p>	<p>Dr Wright not accepting the obvious truth regarding copying the BitcoinSN.tex file into the Maths (OLD) project.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{E/33/5} - Fourteenth Witness Statement (on Chain of Custody)		
{Day15/196:13} - {Day15/196:25}	<p>Q. Dr Wright, I have been now through each of the witness statements in which you purported to touch on the White Paper LaTeX files and you did not describe in any of those witness statements the changes that we saw in the animations, right?</p> <p>A. Because none of those were actually part of the files we're talking about. The files we're talking about are the ones that I demonstrated in October, that I downloaded to make sure they didn't change, that I re-uploaded afterwards, hence why, in the evidence, it says "existing files".</p> <p>Q. Can we --</p> <p>A. Existing files were loaded to create this.</p>	<p>Dr Wright claiming that he did not talk about the changes in the LaTeX files in his witness statement as those were different files, which is completely implausible.</p>
{M/3/15}, para 8 - Letter from Shoosmiths to B&B/Macfarlanes		
{Day15/199:25} - {Day15/201:5}	<p>Q. Can we go to {M/3/16}, paragraph 14. Let's just read that. It says this: "Importantly, Dr Wright's case in relation to the White Paper LaTeX Files does not depend on the proposition that he has not edited the ... code in those files since publication of the Bitcoin White Paper, or that the files are a time capsule that can be dated to any particular point in time. Our instructions are that Dr Wright did edit the code in the intervening years for personal experimentation and to make corrections and improvements, and for the purposes of the demonstrations referred to above, and that Dr Wright then sought to undo the changes to the LaTeX code he had made since publication of the Bitcoin White Paper in order to put the code into the form that would compile [to] the Bitcoin White Paper." Right?</p> <p>A. No, because that's the other changes. You're, again, confusing the maths folder and what I did in October. There were some changes I made in October when I was demonstrating to Matt and others, and those were basically -- I demonstrated these were changes and I undid some of those changes.</p> <p>Q. They were producing two us at this point the unredacted versions of both the Maths (OLD) project and the Bitcoin project, Dr Wright, so they're talking about both of them.</p>	<p>Dr Wright giving an evasive answer where he again refers to different material used in the demonstrations to Shoosmiths to that which was then disclosed in these proceedings.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. This is before that. As you demonstrated already, the Maths (OLD) was loaded from existing files. So those existing files were loaded into that structure.</p>	
<p>{L21/18.1} - Blob file that existed in the Maths (OLD) project on 17 November 2023 {L21/22.2/3} - image2.tex from Dr Wright's White Paper LaTeX files (earliest one in disclosure)</p>		
<p>{Day15/211:18} - {Day15/214:2}</p>	<p>Q. But you have remembered that you needed to convert the individual placing of letters into a full word, right?</p> <p>A. No.</p> <p>Q. Because if you had placed each letter individually, it would have screamed out that it was a forgery, right?</p> <p>A. Again, it would show that an automated tool had created it. But, no, I didn't do that.</p> <p>Q. If we then go to page 3 {L21/22.2/3} and go to {L21/18.1/64} on the left-hand side and let's go to the word "item". You forgot to change the word "item" from its Aspose encoding, didn't you, Dr Wright?</p> <p>A. I did not.</p> <p>Q. Every letter of that word has been positioned in exactly the same position as your Aspose output, right?</p> <p>A. Where is this document from?</p> <p>Q. The document on the right is image 2.tex from your White Paper LaTeX files.</p> <p>A. Which particular?</p> <p>Q. All of them, actually.</p> <p>A. That's not --</p> <p>Q. It doesn't change from 17 November, the earliest one that we've got.</p> <p>A. That's not how mine was, so ...</p> <p>Q. This is down to 0.035 of a micron, right?</p> <p>A. Possibly.</p> <p>Q. Which is about the length of a short segment of DNA, Dr Wright. It is tiny, right?</p> <p>A. A digital file will do it, but mine -- none of mine have that error, the originals.</p> <p>Q. That is your LaTeX file, Dr Wright, on the right. That is it.</p>	<p>Dr Wright not accepting of the obvious truth and blaming third parties - Christen Ager-Hanssen – who was in fact sacked two months before the LaTeX documents were put forward.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Not necessarily. As I said, I had someone on my computer the whole time.</p> <p>Q. Dr Wright, you cannot and would not have placed those letters to that level of accuracy if you were composing the Bitcoin White Paper in LaTeX from scratch.</p> <p>A. No, I would, because what you do is you use a tool. So the tool is a graphic tablet, and when you draw on a graphic tablet it records, right down to the --</p> <p>Q. Dr Wright, it's absurd to suppose that using a graphic tablet you're going to get exactly the same level of accuracy, down to 0.035 nanometres -- so 0.035 of a micron, actually -- get it right -- sorry.</p> <p>MR JUSTICE MELLOR: A schoolboy error. MR GUNNING: Down to 0.035 of a micron, using your tablet.</p> <p>A. No, actually, the other way round. What you're saying is if you take a digital document and then analyse it. But what I suspect, if this in my Overleaf, unfortunately, Mr Ager-Hanssen already demonstrated that he had access to all my things.</p> <p>Q. That's not going to do either, because the syntax of the code for your images is identical to the syntax of this Aspose output, right?</p> <p>A. It's similar in parts, yes.</p> <p>Q. Every line break in the code is in the same place, every command is in the same order, every line is in the same order. You used Aspose, Dr Wright.</p> <p>A. No, I did not. What I had done before this is I'd said how important this was to Mr Ager-Hanssen and Ali Zafar.</p>	
<p>{CSW/1/64} - Dr Wright's Eleventh Witness Statement</p>		
<p>{Day15/215:11} - {Day15/215:15}</p>	<p>Q. Any fool looking at that file would have realised that the word "item" had not been placed by a human, right?</p> <p>A. No, that's incorrect. I used a Wacom graphics tablet -- a high end one -- at one point, and that's how I drew these things.</p>	<p>Dr Wright contradicts his own witness statement as it is being presented to him, see paragraph 339 of Dr Wright's Eleventh Witness Statement. {CSW/1/64}</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
{CSW/2/27: Dr Wright's Appendix B to his Eleventh Witness Statement		
<p>{Day15/216:7} - {Day15/217:13}</p>	<p>Q. Well, unfortunately for you, the sequence of creation was retained, right?</p> <p>A. No.</p> <p>Q. And it was created in Aspose?</p> <p>A. No, it was not.</p> <p>Q. And we see that with all of your other images, right?</p> <p>A. No.</p> <p>Q. The only exception is image 1, where, for reasons I'm not going to take up time exploring, Aspose doesn't deal with slanted text correctly, does it?</p> <p>A. I have no idea.</p> <p>Q. You do, because you had to change the words "verify" and "sign" out of the Aspose and code for them separately, right?</p> <p>A. No.</p> <p>Q. Dr Wright, so what we are seeing in your LaTeX files is the DNA of Aspose, isn't it?</p> <p>A. I can't actually say. What I do know is that when I first mentioned all of this Mr Ager-Hanssen and Ali Zafar were a bit upset.</p> <p>Q. We do not see the DNA of Satoshi Nakamoto in your White Paper LaTeX files, do we?</p> <p>A. You do, but you also see that people have been on my system, which your own evidence has demonstrated.</p> <p>Q. Every step, Dr Wright, of your evidence in relation to these White Paper LaTeX files has been clouded in deceit, hasn't it?</p> <p>A. Not from me. It's been in deceit from people who are now clearly aligned with BTC that were fired from nChain. Those people, who basically went to a lot of time and effort to make sure that anything I have got tainted, and also to threaten witnesses.</p>	<p>Dr Wright refusing to accept the obvious truth, that the images were created in Aspose. Dr Wright blaming a conspiracy of third parties involved in tainting his documents (including Mr Ager-Hanssen and people associated with BTC).</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day15/217:22} - {Day15/218:10}</p>	<p>Q. The animation that I showed you shows your forgery in progress, Dr Wright?</p> <p>A. No. And what you're now claiming is that these files were then edited somehow, but the record of this edit isn't there. That's the bit you're overlooking. Any edit of these image files wasn't done in my version of Overleaf. So, the version of Overleaf used does not show those image files being edited, it shows them being loaded. That's what I saw from your chunks and things.</p> <p>Q. Dr Wright --</p> <p>A. That means, while I had my computer being screenshotted and shown, which are in your images, by a third party computer, which wasn't on my monitor, as you said, someone has loaded these, my Lord.</p>	<p>Dr Wright blaming third parties, alleging a hack / external access to his computers.</p>
<p>{Day15/218:17} - {Day15/220:19}</p>	<p>Q. But Overleaf, unfortunately for you, recorded what you were doing, forging the files on a nearly keystroke-by-keystroke basis, right?</p> <p>A. And yet the claim you're making here about Aspose isn't there. So, your own, sort of, argument fails to note that the very changes you're saying are forgeries were done on another machine, because those files were loaded somewhere else and then onto my machine.</p> <p>Q. Dr Wright, the White Paper LaTeX files are a forgery, aren't they?</p> <p>A. Probably some of them, but not by me. What I do know is that, as you have demonstrated in your own evidence, in Sherrell, that I had third party access to my computers.</p> <p>Q. Dr Wright, they're not evidence that you're Satoshi Nakamoto, are they?</p> <p>A. They are, but unfortunately I have people who have a lot of interest in making sure that none of this gets out there.</p> <p>Q. Dr Wright, your application to adjourn the trial because of the supposed high probative value of these documents was a fraud on the court, wasn't it?</p> <p>A. No, I actually didn't want an adjournment. I actually had a fight with my lawyers over that and they made it happen.</p> <p>Q. Dr Wright, your presentation of those documents as uniquely coding for the Bitcoin White Paper was a fraud on us and on COPA, wasn't it?</p> <p>A. No, I actually believe Mr Ager-Hanssen is working with you guys.</p>	<p>Dr Wright blaming third parties, who allegedly created forgeries and loaded them onto his machine.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Dr Wright, the Bitcoin White Paper wasn't even written in LaTeX, as you would have known if you were Satoshi Nakamoto.</p> <p>A. It actually was.</p> <p>Q. And your claim -</p> <p>A. The fact that I use different tools and integrate them in unusual ways is also something that I do.</p> <p>Q. Dr Wright, your claim to be Satoshi Nakamoto is a fraudulent claim, isn't it?</p> <p>A. No, not at all. In fact, I wouldn't need to actually claim to be Satoshi, I have now proveably scaled beyond anything Silicon Valley can do. We have created a system that's doing 1.1 million transactions a second live, my Lord. That exceeds the capability of Oracle, it exceeds the capability of Microsoft, who are now talking to us, it exceeds any -- and they will argue centralised, except it's distributed. No Oracle database, as a centralised system, can do a million transactions a second, my Lord. That's actually running, and we now have governments involved in that, and none of them care that I'm Satoshi or not. What they care about is we have a distributed blockchain that is scaling to 1.1 million plus transactions a second continuously.</p>	

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
DAY 18		
CROSS-EXAMINATION OF MR ZEMING GAO BY MR HOUGH		
<p>{Day18/4:19} - {Day18/5:9}</p>	<p>Q. Now, assuming that the KeyGen algorithm produced the key pair in a properly random manner, is it right that it should be practically impossible then to compute the private key given only the public key?</p> <p>A. Yes.</p> <p>Q. Is this right also : for the purpose of verification , it's important that the message being signed is a new one chosen by the person who is verifying possession?</p> <p>A. Yes, but if you can assure that the signature, that message has never been signed before, the – you know, the old message can be signed freshly.</p> <p>Q. That's the point, isn 't it ?</p> <p>A. Yeah.</p> <p>Q. That you want to avoid the person who supposedly has the private key producing a message which has been signed in the past with that private key?</p> <p>A. That's true.</p> <p>Q. Because that would be a replay attack, wouldn't it?</p> <p>A. Yes.</p>	<p>Mr Gao agreeing with the importance of using a previously unsigned message (i.e. avoiding a replay attack).</p>
<p>{Day18/5:17} - {Day18/5:24}</p>	<p>Q. But this protection against a replay attack wouldn't be increased in that scenario if I insisted on adding some words? So for example, if I insisted on adding the words "before Mr Justice Mellor" to that text –</p> <p>A. No.</p> <p>Q. – is that right? So it wouldn't improve the –</p> <p>A. It wouldn't improve, yeah.</p>	<p>Mr Gao accepting that the security of a signing is not enhanced by adding letters to a message (e.g. Wright adding "CSW" to the message during the Andresen Signing session – adding "CSW").</p>

Appendix B: Schedule of Transcript References

<p>{Day18/7:13} {Day18/8:3}</p>	<p>-</p> <p>Q. Yes.</p> <p>Now, suppose a person provides a digitally signed message to another person by putting it onto a USB stick, putting the signed message onto a USB stick and handing it over to that other person, and suppose that that other person knows the public key, for example, because they've brought a list of public keys with them; do you understand?</p> <p>A. Yeah.</p> <p>Q. There's no real risk, is there, that the person who receives the USB stick and plugs it into their computer can, from that, compute or derive the private key?</p> <p>A. Practically not possible.</p> <p>Q. And when you say "practically not possible", it's just infeasible with current computing power, isn't it?</p> <p>A. I would think so.</p>	<p>Mr Gao agreeing that there was no risk of Gavin Andresen being able to derive the private key from a digitally signed message put on a USB which he could then verify on his own computer.</p>
<p>{Day18/8:9} {Day18/9:8}</p>	<p>-</p> <p>Q. So suppose that the person who's doing the verifying selects the message on their own and tells that message to Dr Wright, an entirely new message, okay?</p> <p>A. Mm-hm.</p> <p>Q. And suppose that, secondly, Dr Wright, assuming he has a private key associated with an early block, which we obviously dispute, signs the message on his computer with that private key and puts the signed message onto a USB stick, right?</p> <p>A. Yes.</p> <p>Q. With me so far?</p> <p>Thirdly, the verifier takes that USB stick and plugs it into their own computer, takes out the message and runs their own verification program on it on their own computer.</p> <p>A. Mm-hm.</p> <p>Q. Yes?</p> <p>And they do so by reference to a public key which the verifier has noted down and brought with them, okay?</p> <p>A. Yes.</p> <p>Q. And it's right in fact that that could be done without the verifier even having their computer connected to the internet, they could just have the verification program on it, right?</p> <p>A. As long as they have the right software.</p>	<p>Mr Gao agreeing that it was unnecessary to connect to the internet in order to verify the message.</p>
<p>{Day18/9:10} {Day18/10:3}</p>	<p>-</p> <p>Now, each stage in that process would be terribly simple, no great complexity or technical difficulty?</p> <p>A. I suppose.</p> <p>Q. It wouldn't involve anyone doing any downloads, would it?</p>	<p>Mr Gao accepting that there is a much easier way to prove access to the private key.</p>

Appendix B: Schedule of Transcript References

	<p>A. If the device didn't have the software, he would have to download the software.</p> <p>Q. But if the person doing the verifying already had a verification – form of verification software?</p> <p>A. Then no downloads required.</p> <p>Q. No downloads needed?</p> <p>A. Yeah.</p> <p>Q. It would be very quick, wouldn't it, it could be done in a matter of minutes?</p> <p>A. Yes.</p> <p>Q. And there would be no real risk in that scenario that the session was being spoofed would there?</p> <p>A. As long as the verifier is certain about his device and software.</p>	
<p>{Day18/10:6} {Day18/10:15}</p>	<p>- Q. Yes.</p> <p>And there would be no problem, in principle, with videoing the verification, because that wouldn't allow anyone to derive the private key; correct?</p> <p>A. It's correct.</p> <p>Q. And there would be no problem with having somebody minuting every stage of that process, for example an independent observer, because that wouldn't involve any risk of the private key being compromised?</p> <p>A. Agree.</p>	<p>Mr Gao accepting that there would be no concerns in terms of risking the security of the private key, by having a third party evidencing the verification.</p>
<p>{Day18/11:8} {Day18/11:18}</p>	<p>- Q. That would all be technically feasible, wouldn't it?</p> <p>A. Yes, but the assumption is that the person is willing to do that publicly.</p> <p>Q. Sure.</p> <p>And if that were done, anyone with access to the blockchain could obtain the public key related to block 9, because it's one of those early blocks, yes?</p> <p>A. Yes.</p> <p>Q. And they could verify the message for themselves, anyone in the world with the technical understanding?</p> <p>A. Yeah, that's the essence of a public proof.</p>	<p>Mr Gao accepting that there would be no technical concerns with publishing the verification proof publicly.</p>

Appendix B: Schedule of Transcript References

<p>{Day18/11:24} {Day18/12:1}</p>	<p>- Q. Sure. But the risk of actually compromising the private key, non-existent? A. I agree.</p>	<p>Mr Gao specifically confirming that there would be no risk of compromising the private key if the verification is public.</p>
<p>{Day18/12:16} {Day18/13:20}</p>	<p>- Q. So you considered, does it follow, that what you wrote in your report about the signing sessions, the procedures used and how they might have been subverted, what you wrote in your report on those matters are all matters within your expertise? A. Yes. Q. Dr Wright told the court that you weren't an expert on those matters. May we take it that you disagree with him? A. I don't think I'm a professional cryptographer. Q. No, but you had -- A. Within the context of the Bitcoin Blockchain, I'm an expert. Q. And you felt that you had enough expertise to give opinions on the matters in your report? A. Yes, I do. Q. So when Dr Wright said that you were not an appropriate expert to express opinion -- A. Well, if the subject matter goes to the detail of the cryptography itself, I don't think I'm the most qualified person. Q. Does that include matters you actually address in your report? A. No, in the report it doesn't involve specific high level cryptography itself, it's the procedure in the context of blockchain. Q. So the matters you addressed in your report you felt were within your competence despite the limitations that you've -- A. Sure, but the distinction is like a race car driver, if he's expert in driving but he doesn't necessarily know how to make the car.</p>	<p>Mr Gao defending his qualifications and addressing Dr Wright's criticisms.</p>
<p>{G/2/50} First Report of Sarah Meiklejohn</p>		
<p>{Day18/16:4} {Day18/16:9}</p>	<p>- Q. -- scroll down to make sure there isn't an (h) below; do you see that? A. Yes. Q. So you agree that that's your understanding, too, of those sessions, is it?</p>	<p>Mr Gao confirming that he accepts Professor Meiklejohn's summary of the signing sessions with Mr</p>

Appendix B: Schedule of Transcript References

	<p>A. Yes.</p>	<p>Matonis and the journalists.</p>
<p>{Day18/16:16} - {Day18/17:13}</p>	<p>Q. Now, Professor Meiklejohn has pointed out -- and we can look at paragraph 124(c) on page {G/2/51} -- that it would be simple to develop a program to which this command would point and would just output a random string that would match the pattern for an encoded signature; do you see that? That's paragraph 124(c).</p> <p>A. 24, which?</p> <p>Q. 124(c).</p> <p>A. (c), okay.</p> <p>Q. Do you want to just read that to yourself? I 've just</p> <p>Q. Now, it's right, isn't it, that you agree that that could be done, it would be simple to develop a small program with that effect?</p> <p>A. Yes, I agree.</p> <p>Q. But is this right, you stress in your annex to the joint report that the critical point in subverting the process is at the verification stage rather than the signature stage?</p> <p>A. Yeah, the reason is because even if there's forgery here, you generally in verifier -- verifying software can still detect it.</p>	<p>Mr Gao agreeing that the key point in subverting the signing sessions process is at the verification stage.</p>
<p>{Q/3.1/11} Annex A to Joint Statement of Professor Sarah Meiklejohn and Mr Zeming Gao</p>		
<p>{Day18/18:16} - {Day18/19:15}</p>	<p>”If ... the signer is cheating with the software on the signer 's side , even if the verifier 's software is not verified to be genuine, as long as the verifier himself is not colluding with the signer to deceive others, it would not be to the signer's advantage. This is because, unless the verifier 's software is designed to always produce a positive result , the result would be either always negative or unpredictable, in either case defeating the signer 's purpose of producing a reliable proof. But if the verifier 's software is designed to always produce a positive result , it would be very easy for the verifier to discover the defect by intentionally using an incorrect signature. The bottom line is that, if the signer 's purpose is to produce a reliable signature proof, there is no motivation for the signer to tamper with the software on the signer's side . The focus, therefore, is the software used by the verifier , which the signer does [not] have a motivation to tamper with.”</p> <p>Now, of course, when you refer to not having the -- the signer not having a motivation to tamper with the verification software, that assumes that the signer is not --</p>	<p>Mr Gao accepting there would be a motivation for the signer of a message to tamper with the verifying software.</p>

Appendix B: Schedule of Transcript References

	A. The signer would have. The signer would have the motivation to tamper the verifying software.	
{Day18/21:25} {Day18/22:7}	<p>Q. -- for the questions that follow.</p> <p>And then subparagraph (d), the understanding that Professor Meiklejohn derived from the materials was that Mr Andresen had brought his own laptop to the session, but that laptop, his own laptop, wasn't used for the verification. And that's your understanding as well?</p> <p>A. Yeah. Yeah.</p>	Mr Gao demonstrating broad agreement on most points put to him.
{G/2/55-59} First Report of Sarah Meiklejohn		
{Day18/26:24} {Day18/27:16}	<p>Q. Well, let's just take that in stages. If a fake site with a slightly different name were used, that fake -- the operator of that fake site could have obtained a basic level security certificate, couldn't they?</p> <p>A. Yeah, if it's -- look like website and the verifier didn't detect that ... well, that's assumption. Based on the assumption, it's not difficult to fake the website and pass the -- the security checks.</p> <p>Q. So you could set up a fake website, obtain a basic security certificate and that would allow access over an HTTPS connection; correct?</p> <p>A. Yes. Yes --</p> <p>Q. And that would show a padlock, wouldn't it?</p> <p>A. Yeah. Well, that's on the assumption that verifier wasn't able to tell the difference.</p> <p>Q. It's assuming that the verifier doesn't look at the precise spelling of the --</p> <p>A. Yeah, on that assumption, I agree.</p>	Mr Gao agreeing about the possibility of faking website security.
{Day18/30:23} {Day18/32:12}	<p>Q. And then Professor Meiklejohn said that there would have been steps to prevent that happening which were not taken. So she said if the laptop was not fully factory sealed when it was first brought in, other software could have been installed before its arrival. And you'd agree with that as a matter of principle, as a possibility?</p> <p>A. Yes.</p> <p>Q. 130(b)(ii), she said that it would have been possible to download such malware during the very long set up process</p>	Mr Gao agreeing on the possible means to corrupt the verification.

Appendix B: Schedule of Transcript References

	<p>that was described. And again, that would have been technically possible and feasible, wouldn't it?</p> <p>A. Yes.</p> <p>Q. 130(b)(iii), she said it could have been transferred through the USB drive as a method of transmission, this malware. And again, that's a possibility you accepted?</p> <p>A. Yes.</p> <p>Q. And fourthly, it could have been introduced through a network connection. And again, that's another possibility for transmission of malware which you accepted?</p> <p>A. Yeah, that's the assumption that the secure website is bypassed.</p> <p>Q. Page {G/2/58}, please.</p> <p>Professor Meiklejohn explains that malware could have been introduced via a connection mimicking the hotel WiFi, including through being introduced through a hotspot. And again, you agreed that that was technically feasible?</p> <p>A. Yeah. Possibility.</p> <p>Q. And such a compromise could have resulted in either fake Electrum software being introduced or software that would interfere with the operation of real Electrum software?</p> <p>A. Yes, unless the verifier had the separate independent source of the checksum. He would be able to detect it.</p> <p>Q. And you've said independently in your own report that tampering could have happened through the WiFi connection?</p> <p>A. It's possible.</p>	
<p>{Day18/32:17} - {Day18/33:1}</p>	<p>Q. It would also, this is right, have been possible for a form of fake Electrum software to output "true" only if the message contained a certain set of letters; is that right?</p> <p>A. There can be -- software can be specifically modified to do that.</p> <p>Q. So it would have been possible for a form of fake Electrum software to output "true" if the message included the letters "CSW", for example?</p> <p>A. Yes.</p>	<p>Mr Gao accepting the "CSW" addition could have been used in order to generate a fake 'true' output.</p>
<p>{Day18/33:13} - {Day18/33:22}</p>	<p>Q. May we then go to paragraph 131 {G/2/58} in Professor Meiklejohn's report, and Professor Meiklejohn gives an overall opinion on the signing sessions. Do you recall that this is a paragraph with which you agreed in its entirety in the joint statement?</p>	<p>Mr Gao appearing to repeat Dr Wright's position that signing doesn't prove identity</p>

Appendix B: Schedule of Transcript References

	<p>A. Yeah, that statement needs to be qualified. It's – this all depends on the confidence of the verifier.</p> <p>Q. What she wrote –</p> <p>A. My point is that even if the verifier was confident, he can't pass the knowledge reliably to others.</p>	<p>and is arguing the case for Dr Wright.</p>
<p>{Day18/34:6} {Day18/34:11}</p>	<p>- Q. Page {G/2/59}, paragraph 132, she concluded that for the signing sessions with the journalists and Mr Matonis, which were conducted entirely on Dr Wright's laptop, they could easily have been staged with a simple program, and you agreed with that?</p> <p>A. I agree.</p>	<p>Mr Gao agreeing that it would have been easy to stage (i.e. fake) the signing sessions with Mr Matonis and the journalists.</p>
<p>{Day18/38:6} {Day18/39:4}</p>	<p>- Q. You agree, don't you, that the Bitcoin Core software didn't need to be downloaded in order to sign a message with a known private key; correct?</p> <p>A. It's not the only choice.</p> <p>Q. It's not the --</p> <p>A. It's not the only choice. You could have a variety of ways to do that. So using different software.</p> <p>Q. And the Bitcoin Core software did not need to be downloaded for the verification process, because we've agreed that that could be done with software like Electrum?</p> <p>A. That's true.</p> <p>Q. So if it's not needed for signing or verification, downloading of the Bitcoin Core software was not a necessary preliminary to the signing sessions?</p> <p>A. The -- the verifier can use -- does not have to download the entire blockchain, just do the verification for the signature.</p> <p>Q. Just to answer my question, the downloading of the Bitcoin Core software was not a necessary preliminary to the signing session?</p> <p>A. Unless that's what he want, for the convenience for -- for the mutual trust. The -- technically, that's not the only choice</p>	<p>Mr Gao agreeing that it is unnecessary to download the Bitcoin Core software to sign a message.</p>
<p>{Day18/39:12} {Day19/39:19}</p>	<p>- Q. So --</p> <p>A. So Bitcoin Core is supposed to be a very widely recognised software, reason that has the -- the pragmatic advantage. It's one of the choices.</p> <p>Q. We've agreed, haven't we, that it wouldn't have prevented any of the forms of spoofing that we've looked at?</p> <p>A. I agree.</p>	<p>Mr Gao agreeing that using Bitcoin Core software doesn't actually protect against spoofing.</p>

Appendix B: Schedule of Transcript References

<p>{Day18/39:20} {Day18/40:10}</p>	<p>-</p> <p>Q. Next, downloading the blockchain. The blockchain – the full blockchain did not need to be downloaded in order to obtain the public keys for these sessions because we’ve agreed that they could be brought by anyone with enough expertise, as Mr Andresen claims to have done, yes?</p> <p>A. I agree. As far as the public keys are concerned, that’s true. But when you use Bitcoin Core software, there’s really not the option, you have to download it. The software forces you to do that.</p> <p>Q. But suppose you don’t download the Bitcoin Core software and don’t spend a lengthy period downloading the blockchain, you can conduct these signing sessions perfectly well, can’t you?</p> <p>A. You can use different methods. The reason why Dr Wright chose that particular venue, that’s his choice.</p>	<p>Mr Gao accepting that it is unnecessary to download the full blockchain to obtain the public keys for the Andresen signing sessions (see also para 3E of Annex B to the Joint Statement of Professor Meiklejohn and Mr. Gao {Q/3.2/3}).</p>
<p>{Day18/40:23} {Day18/41:4}</p>	<p>-</p> <p>Q. And downloading the Bitcoin Core software and the entire blockchain wouldn't have provided some additional security or confidence to the process, would it?</p> <p>A. No, as -- on a matter of principle, no. But you can -- you understand, using that software because it's widely accepted, widely used, might enhance the level of confidence.</p>	<p>Mr Gao accepting that downloading Bitcoin Core and the whole blockchain was unnecessary from a security and confidence perspective.</p>
<p>{I/2/62} First Expert Report of ZeMing M. Gao on Digital Currency Technology</p>		
<p>{Day18/43:23} {Day18/44:12}</p>	<p>-</p> <p>Q. Now, what you say in your report – and I can take you there if needed – you say {I/2/62}: “... it took ... extraordinary Internet detective work to connect the signature with one of the early bitcoin addresses ...” Is that right?</p> <p>A. That’s right, yeah. It’s – they had to – because on – on the chain, you can’t really find the public key, and the detectives, they were able to link it.</p> <p>Q. So you’ve made the point elsewhere in your report that if the Sartre blog was a fake proof of possession of a private key, then it was a crude fake and of low quality; do you remember saying that?</p>	<p>Mr Gao admitting that the Sartre blogpost is low quality proof of possession of a private key.</p>

Appendix B: Schedule of Transcript References

	<p>A. Yes, I do, but I was saying, if this was meant to be a genuine proof, then it's a really low quality proof.</p>	
<p>{Day18/44:20} - {Day18/46:6}</p>	<p>Q. The court is going to read the article and form its own view of what was intended, but just focusing on how easy it was to expose the signature just from the signature, that took really quite some effort and skill, didn't it?</p> <p>A. No, the fact that this was fake was quite clear, you don't need to – to do a detective work. What – what I was saying that –</p> <p>Q. You say it's clear from the signature file on its own that it's fake?</p> <p>A. Yeah, reading that, it's – it's clearly it was not the genuine proof.</p> <p>Q. Why do you say that it's clear from the signature file on its own that it wasn't a genuine proof?</p> <p>A. Because the description was not clearly saying that this is the message I signed and this is the – the public key.</p> <p>Q. Can you just focus on the signature file. If somebody in 2016 just gave you that signature file you're looking at on screen, without surrounding text, and said this is a signature using the – of a message using the private key to block 9, you wouldn't immediately be able to say that it was fake, that it was a signature of a message signed years before, would you?</p> <p>A. Yes, but the –</p> <p>Q. Sorry, are you agreeing with that, first of all?</p> <p>A. I agree, but that's – I need to qualify the statement, because here, the author – the writer didn't say, "This signature was meant to sign using the private key of the block 9 and this is the public key" –</p> <p>Q. I know you're keen to provide your view of what the author intended, but at the moment I'm just focusing upon the signature. And just working out from this signature that it's not a signature of a new message but a signature produced years before but in a different – written in a different notation, that was not obvious and took some effort?</p> <p>A. That's true.</p>	<p>Mr Gao arguing Dr Wright's case about the interpretation of the Sartre blog, and it not being designed as a proof, which is contrary to the plain reading of the blog.</p>
<p>{I/2/62} First Expert Report of ZeMing M. Gao on Digital Currency Technology</p>		
<p>{Day18/53:5} - {Day18/54:20}</p>	<p>Q. Exactly, because parce Gulliver's Travels, "big endian" and " little endian", in this context, are descriptors of systems which store the bytes of a group in different orders; correct?</p> <p>A. Yes.</p>	<p>Mr Gao addressing the withdrawn paragraph 326 of his Expert Report, in which he</p>

Appendix B: Schedule of Transcript References

	<p>Q. And so the –</p> <p>A. So the – the hexdump and the xxd, clearly one uses the little endian and the other one uses the big endian.</p> <p>Q. So the difference in order is just a result of how hexdump stores 16 bit words?</p> <p>A. Exactly, because reading the statement, order is different; when you read it separate, it – the outcome is the same.</p> <p>Q. It’s not a difference in output?</p> <p>A. It’s not.</p> <p>Q. It doesn’t reflect a change in content of the file?</p> <p>A. That’s right. That’s why the paragraph was deleted.</p> <p>Q. Now, if we look at the text below the screenshot, do we see what it refers to are hex values representing a single hash of an input value; do you see that in the first sentence?</p> <p>A. Yeah.</p> <p>Q. It doesn’t mention, does it, using three different commands for the same purpose?</p> <p>A. No, the text doesn’t say, but the image shows clearly he did it three times unnecessarily.</p> <p>Q. Yes, but the author doesn’t write, does he, “I have, for demonstration purposes, used three different commands for the same purpose”?</p> <p>A. I agree, in the text it’s not explicit.</p> <p>Q. In fact –</p> <p>A. But in – in the image, it shows he did it three times in different methods. Even for the production, that is completely unnecessary.</p> <p>Q. Sure.</p> <p>A. The only explanation is he’s trying – just trying to illustrate.</p> <p>Q. Well, or – I’m going to put this to you even though it’s not a matter of your expertise, or that he is sowing confusion.</p> <p>A. Well, that’s a different reading. Possible.</p>	<p>originally made excuses for Dr Wright’s inclusion of three commands in the Sartre Blogpost, and then accepts the possibility that Wright included three commands to confuse people.</p>
<p>{Q/3.2/1} Annex B to Joint Statement of Professor Sarah Meiklejohn and Mr Zeming Gao</p>		

Appendix B: Schedule of Transcript References

<p>{Day18/59:10} - {Day18/60:2}</p>	<p>Q. Now, would you accept that, on its face, Dr Wright's -- if Dr Wright's statement was referring to mining operations using all the computers and running up thousands of dollars in electricity costs, that would suggest dedicating a significant portion of those computers' power to the mining operations? Is that right?</p> <p>A. It depends on what he was doing. He may be doing testing or other things.</p> <p>Q. But if the court were to conclude that he was saying that he needed 70 plus machines for the purpose of running the blockchain and mining in that early period, you'd agree that was wrong, wouldn't you?</p> <p>A. If he were purely just a miner, then I would agree. But if he were the designer or the creator of the Bitcoin, he would be doing other things, because related testing for new processes, designs. So we don't know. I don't know.</p>	<p>Mr Gao accepting that Dr Wright's set up would be unnecessary for running the blockchain and mining in the early period. Mr Gao then makes further excuses for Dr Wright, by positing that he was doing other actions on the computers.</p>
<p>{Day18/60:10} - {Day18/60:23}</p>	<p>A. Yes, the hashing consumes more power than verifying the transactions. But there can be other things other than just hashing idea.</p> <p>Q. Just based on Professor Meiklejohn's figures, if Dr Wright was using even half the hashing power of his set up in mining operations, it would have been producing at least five times the power that was actually used in the Bitcoin System in 2009 and early 2010; would you agree?</p> <p>A. I would agree. If -- if half of that was dedicated to just hashing, I think it would overwhelm the system.</p> <p>Q. And you're not able --</p> <p>A. When I say "dedicated", I mean doing that 24 hours a day.</p>	<p>Mr Gao agreeing to Professor Meiklejohn's conclusion that the use of even half of the hashing power of Dr Wright's supposed set up would overwhelm the network.</p>
<p>{L19/278/3} Capture of https://web.archive.org/web/20220826165425/https://zemgao.com/why-i-believe-craig-wright-is-most-likely-satoshi/#Controversies-and-Biases</p>		
<p>{Day18/63:14} - {Day18/64:5}</p>	<p>Q. Page 3, please, middle of the page {L19/278/3}.</p> <p>A. But when I say Bayesian method in this, you never reach a final conclusion, you always adjust your conclusion based on new facts.</p> <p>Q. You see that the article contains this sentence: "First off, he did sign it ..." Referring to signing with private keys: "... on multiple occasions ... only privately." You wrote that, didn't you?</p> <p>A. Yes, I did.</p> <p>Q. And you went on to express views about the accounts given by Mr Andresen and Stefan Matthews, yes?</p>	<p>Mr Gao accepting that he wrote the article "Why I believe Craig Wright is most likely Satoshi".</p>

Appendix B: Schedule of Transcript References

	<p>A. Mm-hm.</p> <p>Q. And you're aware, aren't you, that your evidence today goes to the question of the validity of the signing sessions?</p> <p>A. Yes.</p>	
<p>{L19/277/1} Capture of https://web.archive.org/web/20221103185155/https://zemgao.com/the-wright-strategy-is-the-satoshi-strategy/</p>		
<p>{Day18/64:25} - {Day18/65:15}</p>	<p>Q. Well, we'll go through the article, but it's right, isn't it, that you argue at length in this article that Dr Wright's supposed decision not to perform a public signature with one of the keys associated with the early blocks is a legitimate decision? Not just that it's one he made, but that it was a legitimate decision, the right strategy?</p> <p>A. Yeah, because that's why he only did, selectively, just private sessions, he never committed to the public sessions.</p> <p>Q. But you didn't just describe what his view was, you said that that decision was a legitimate, proper, reasonable one, didn't you?</p> <p>A. Because I have a legal background I think that, to prove that, you have to prove your legal identity first, otherwise the signature itself means nothing.</p>	<p>Mr Gao doubling down on the idea that signing does not equal identity, again seeking to argue Dr Wright's case.</p>
<p>{L19/264/1} Capture of The key in COPA v. Wright – ZeMing M. Gao (zemgao.com)</p>		
<p>{Day18/65:20} - {Day18/66:12}</p>	<p>Q. If we go down to the middle of the page, you there try to frame COPA's expected approach to these proceedings in two bullet points, don't you?</p> <p>A. Yes.</p> <p>Q. And the second bullet point says: "They will further try to trick the court into concluding that Wright's failure to prove he is Satoshi using a specific piece of evidence means COPA's success in proving Wright is not Satoshi." You wrote that, didn't you?</p> <p>A. Yes, I did, because I have a theory of what is the right kind of proof for the impossibility. I –</p> <p>Q. You --</p> <p>A. -- I think, finding a fake -- a forgery of a signature is not impossibility proof.</p> <p>Q. You described COPA's approach as attempting "to trick the court", didn't you?</p> <p>A. That's the word I used.</p>	<p>Mr Gao accepting that he said COPA's approach was to try and "trick" the Court.</p>

Appendix B: Schedule of Transcript References

<p>{Day18/66:17} - {Day18/67:13}</p>	<p>Q. Page 5, please {L19/264/5}, under “Anticipations”: “I am not waiting for the trial result to convince me one way or another. The evidence supporting Dr Wright is so strong and clear that the trial is also a test for the court itself.”</p> <p>Did you write that?</p> <p>A. Yes, I did.</p> <p>Q. “But that does not mean I am certain of what the actual outcome will be, or that I don’t care about the result.</p> <p>“Who is more likely to win the case? I say Dr Wright. Being on the truth side does have an advantage.” And so on.</p> <p>You were telling the world in this article not only that you believed Dr Wright should win but that you cared that that should happen, didn’t you? “... that does not mean ... that I don’t care ...”-</p> <p>A. Oh, okay, yeah. Yes, I – I did write that, yeah.</p> <p>Q. And you were saying that you cared that Dr Wright should win, didn’t you?</p> <p>A. Yeah, because the result would affect the kind of Bitcoin I believe should be advanced.</p>	<p>Mr Gao admitting that he wrote the works which COPA say show his lack of independence, and that his personal beliefs impact his view on the trial.</p>
<p>{Day18/68:4} - {Day18/68:10}</p>	<p>Q. Mr Gao, this was just a few days before you were instructed. Did having written these articles give you any pause about agreeing to be an expert in this case?</p> <p>A. Personally, I believed in my independence. But in the beginning, I -- I didn't feel I was the best evidence -- the -- the expert witness. I actually recommended somebody else.</p>	<p>Mr Gao accepting he is not the best qualified expert to work on this case.</p>
<p>{L20/121/65} Gao, Z (2023) Bit & Coin (unknown publisher)</p>		
<p>{Day18/68:19} - {Day18/69:11}</p>	<p>Q. Page 65, please {L20/121/65}, a chapter headed, “The Birth of Bitcoin”. This part of the book sets out your position in favour of Dr Wright’s claim to be Satoshi, doesn’t it?</p> <p>A. Yes.</p> <p>Q. So at the bottom of this page you accept, don’t you, unquestioningly, one of his claims to have an IQ putting him in the 1/10 million percentile?</p> <p>A. Yes.</p> <p>Q. Page 67 {L20/121/67}, top of the page, you set out here Dr Wright’s qualifications, and is it fair to say you set them out in somewhat breathless terms?:</p> <p>“Having a Doctor of Theology ... Wright knew what kind of value humanity needs.</p>	<p>Mr Gao agreeing that he accepted Wright’s claims regarding his own intelligence.</p>

Appendix B: Schedule of Transcript References

	<p>"Learned in economics (eventually receiving a PhD in the discipline), Wright knew what kind of ... system is needed to realize the desired value."</p> <p>A. Yeah.</p>	
<p>{L20/252.44/20} Capture of https://zemgao.com/to-prove-a-negative-in-copa-v-wright/</p>		
<p>{Day18/72:13} {Day18/73:6}</p>	<p>- Q. Well, let's look at page 20, then {L20/252.44/20}, third paragraph. Page 20, the third paragraph of the "Summary": "In the trial of COPA v Wright, it is clear that COPA doesn't have a case." You wrote that, did you?</p> <p>A. Yes.</p> <p>Q. Page 21 {L20/252.44/21}, at the top: "Negative proof of Dr Wright's Satoshi claim does not exist, because Dr Wright is Satoshi."</p> <p>You wrote that?</p> <p>A. Yes, I did.</p> <p>Q. And then the final document, {L20/252.70/1}. 24 January 2024: "Dr Wright's settlement offer to COPA and all opposition parties." You were referring there to an open settlement offer which was – had been rejected, yes?</p> <p>A. Yes, I did.</p>	<p>Mr Gao demonstrating his firm view that Dr Wright is Satoshi.</p>
<p>{Day18/73:7} {Day18/74:4}</p>	<p>- Q. Page 4, please {L20/252.70/4}, the first main paragraph: "COPA's position is very different from others. COPA's purpose is not to fight for freedom of operation in view of the Bitcoin database and the whitepaper (the founders of COPA take that for granted). Its real purpose is to thoroughly discredit Dr Wright, kill BSV, and render nChain's IP [intellectual property] less effective. They looked at nChain's patent portfolio and decided it was necessary to do something about it. Hence the lawsuit." Are you aware that the motivations you there ascribe to COPA are motivations which COPA rejects, that it disputes those?</p> <p>A. I was making the conclusion based on what I saw.</p> <p>Q. Are you aware that COPA has presented its motivation and its purpose as being different from what you say there?</p> <p>A. Oh, yes. Yes, the -- the particulars of the claim doesn't say it was for the patents, I -- I'm aware of that.</p> <p>Q. And so you are writing here expressing a view that COPA had a sinister ulterior, unstated motive?</p> <p>A. Not necessarily sinister ulterior, but -- but it's clearly a greater goal, strategically.</p>	<p>Mr Hough KC questioning Mr Gao on his belief that COPA has an ulterior motive as if this is a logical conclusion.</p>

Appendix B: Schedule of Transcript References

<p>{Day18/74:5} - {Day18/75:12}</p>	<p>Q. Mr Gao, we've looked at a number of these articles. Would you accept that you have very publicly committed yourself as an extremely strong supporter of Dr Wright's claim to be Satoshi?</p> <p>A. I've committed myself to the facts and the Bayesian method.</p> <p>Q. No, no, you have committed yourself, haven't you, as an extremely strong supporter of Dr Wright's claim, haven't you?</p> <p>A. My support is strong, there's no question about it, but if facts come -- come out differently, I will change my mind.</p> <p>Q. But through these articles, and through your book, you have staked your personal credibility on this position, haven't you?</p> <p>A. Yes.</p> <p>Q. So being fair right now, you cannot seriously claim, can you, to be entirely objective about Dr Wright's claim to be Satoshi and about this case?</p> <p>A. Being not objective means that you don't -- you ignore the facts.</p> <p>Q. Well --</p> <p>A. I'm confident in my ability to evaluate the facts, and objectively.</p> <p>Q. But you can't seriously claim, after all you have written and after all the personal commitments you have made, to be entirely objective about Dr Wright's claim in this case, can you?</p> <p>A. What's objective? Objective is based on facts.</p> <p>Q. You cannot -- and you certainly cannot seriously claim that your evidence would be seen by other reasonable people to be objective evidence about Dr Wright's claim in this case?</p> <p>A. Well, how other people think, I can't control.</p>	<p>Mr Gao arguing that staking his personal credibility on Dr Wright being Satoshi Nakamoto does not impact his objectivity.</p>
<p>{Day18/75:13} - {Day18/76:3}</p>	<p>Q. Would you accept now that it was a real error of judgment on your part to go on posting these extraordinary articles after you had accepted instructions to be an expert in this case?</p> <p>A. These are new -- not new positions, they're -- I've written material very similar to this during the last, maybe, close to three years.</p> <p>Q. I'll give you a chance to answer the question so that you have given an answer to it, because it may be important.</p> <p>Would you accept now that it was a real error of judgment on your part to go on posting these extraordinary articles after you</p>	<p>Mr Gao is given two chances to admit that he made an error of judgment in posting the articles, but refuses to do so, and stands by his decision.</p>

Appendix B: Schedule of Transcript References

	had accepted instructions to be an expert, an independent expert in this case? A. I do not think that's the case.	
--	--	--

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
DAY 19		
CROSS-EXAMINATION OF DR CRAIG STEVEN WRIGHT BY MR HOUGH KC		
<p>{Day19/8:2} {Day19/9:3}</p> <p>-</p>	<p>Q. You're also aware, I believe, that Ontier sent an email to your current solicitors, Shoosmiths, that day, February, disputing that version and saying that you first provided them with log-in details on 9 March. Are you aware of that communication?</p> <p>A. I am.</p> <p>Q. Are you also aware that Shoosmiths passed on Ontier's response by letter to COPA and the developers on the following day, 9 February?</p> <p>A. I am.</p> <p>Q. Do you recall that Ontier's version was put to you on Day 5 of this trial {Day5/46:25}, 9 February, and you disputed it saying, and I quote?: "... I have the emails in disclosure stating that they ..."That's Ontier:"... had access [to MYOB] from 2019."</p> <p>A. I do.</p> <p>Q. Do you recall you were questioned again on the topic when you were called to give evidence on Day 15, last Friday, the 23rd?</p> <p>A. I do.</p> <p>Q. And you repeated that Ontier had received log-in details in late 2019.</p> <p>A. Yes.</p> <p>Q. And you said that you had the emails to prove that?</p> <p>A. I do.</p>	<p>Dr Wright continues to maintain that he has the emails to prove that he had received log-in details in late 2019, despite the documents provided having been found by Mr Madden to be inauthentic or manipulated.</p>
Chain of three emails dated 2 December 2019 from Dr Wright to Simon Cohen at Ontier {X/59/1}		
<p>{Day19/9:13} {Day19/10:1}</p> <p>-</p>	<p>Q. May we now go back in time to late 2019 and have on screen {X/59/1}. We see here a chain of three emails, dated 2 December 2019, and if we look at the bottom of the page, an email from you to Simon Cohen at Ontier, 2nd December</p>	<p>Dr Wright accepting that the old email (the first one in the chain), is genuine.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>2019, 12.38, with the title, "... Old ID Email" and the text just "Attached"; do you see that?</p> <p>A. I do.</p> <p>Q. You sent an email on that date at that time with that text, didn't you?</p> <p>A. I believe so, yes.</p> <p>Q. And what was attached, is this right, was a chain of emails with your Australian lawyers concerning your company Information Defense?</p> <p>A. Yes.</p>	
<p>{Day19/10:10} - {Day19/11:17}</p>	<p>Q. Then, at the top of the page, we see an email from you, craig@rcjbr.org, 2 December 2019, 15.56, addressed to Simon Cohen, subject line, "... Old ID Email", and "image002.png" attachment; do you see that?</p> <p>A. I do.</p> <p>Q. And the text says: "An old Information defense file about the IP. "Including Blacknet. "To my lawyer in Au. "I will waive privilege with Michael." Do you see that?</p> <p>A. I do.</p> <p>Q. And that, too, was a genuine email sent from you to Mr Cohen on that date, wasn't it?</p> <p>A. It is.</p> <p>Q. So, this exchange of emails took place on 2 December 2019 and what we are seeing here is a genuine exchange of emails?</p> <p>A. It's not the entirety, no.</p> <p>Q. Is this a genuine exchange of emails?</p> <p>A. It's a partial exchange of the emails. There are other parts.</p> <p>Q. What do you say are the other parts?</p> <p>A. There was a later follow-up, and on 5 March, there was a follow-up from Oliver Cain, who noted that AlixPartners had started, but not completed, the report, which was based on MYOB.</p> <p>Q. That wasn't a document that was disclosed by your lawyers and explained on Monday, was it?</p> <p>A. No, it's not.</p> <p>Q. You're aware, aren't you, that Mr Cohen is no longer at Ontier?</p> <p>A. I am.</p>	<p>Dr Wright's response in relation to a genuine exchange of emails is evasive, and the 5 March follow-up from Oliver Cain was not provided; the inference is clear that it does not exist and is another fabrication.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
Chain of emails dated 18 February 2024 {X/56/1}		
<p>{Day19/12:19} - {Day19/13:3}</p>	<p>Q. Now, it's right, isn't it, that, as Lord Grabiner explained on Monday, the email at the top of that chain was a genuine email sent from your wife to the solicitors at Shoosmiths?</p> <p>A. I believe so. I didn't send it, but I know she sent one.</p> <p>Q. And the previous email in the chain, the one at the bottom of the page, was a genuine email from you to your wife, wasn't it?</p> <p>A. Yes, I forwarded an email.</p>	<p>Dr Wright is evasive regarding whether the email to Shoosmiths is genuine, and evasive as to his own involvement in it being sent to them.</p>
Email document attached to Ms Watts email to Shoosmiths dated 18 February 2024 email sent by Dr Wright to Ontier on 2 December 2019		
<p>{Day19/13:4} {Day19/13:19} {X/56/2}</p>	<p>Q. {X/56/2}, please. Now, this is the email document attached to Ms Watts email to Shoosmiths of 18 February 2024, timed at 12.56, right?</p> <p>A. Looks like it, yes.</p> <p>Q. And you had sent that document to your wife for onward transmission to Shoosmiths by your email to her of 18 February '24 at 11.39, right?</p> <p>A. Well, I sent it to my wife. I wasn't involved in the forwarding.</p> <p>Q. But you intended that it be transmitted onward to Shoosmiths; correct?</p> <p>A. No, my wife thought it would be a good idea to send it to them.</p> <p>Q. You knew that's what she was doing?</p> <p>A. She told me that she was going to and I didn't object.</p>	<p>Dr Wright blames his wife in relation to onward transmission of the email document to Shoosmiths.</p>
<p>{Day19/13:25} {Day19/14:24} {X/56/2} {X/59/1}</p>	<p>Q. Now, what we see here is two emails we've been looking at. On the left-hand side, the email which Ms Watts forwarded to Shoosmiths, and on the right-hand side the email which you had sent to Ontier on 2 December 2019; do you see that?</p> <p>A. I do.</p> <p>Q. And you see the subject heading is the same between the two; correct?</p>	<p>Dr Wright maintains the authenticity of the two different emails on the basis of responding to the same email twice, however his answer is evasive.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>A. Yes, basically I've responded to the same original email twice. I do that quite often.</p> <p>Q. The text in the two bottom emails is the same between the two?</p> <p>A. Yes. As I said, I responded to the same email twice.</p> <p>Q. Well, we're going to come to that. Now, the chain which Ms Watts supplied to Shoosmiths {X/56/2} was not a genuine email sent with the content we see in that document on 2 December 2019, was it?</p> <p>A. No, that's incorrect. It was part of an email. At that stage, I was migrating away from rcjbr.org as my main domain to tuliptrading.net. Because of the Kleiman case, I'd been receiving hundreds of emails, including threats at craig@rcjbr.org, so I cancelled using that email for a time, the same mailbox, but I then re-added it at a later time, about a year later. So that was during the migration between those.</p>	
<p>Mr Madden's sixth report {G/11/8}</p>		
<p>{Day19/15:11} – {Day19/15:20}</p>	<p>Q. And then over the page {G/11/8}, paragraph 12, that contained an encoded timestamp giving a date of 18 February 2024 and a time 10.17; do you see that?</p> <p>A. I do.</p> <p>Q. That – the presence of that image with that encoded timestamp is only explained by the email having been created in this form on 18 February 2024, isn't it?</p> <p>A. No, actually, it shows when it was downloaded and saved. That image is stored within an EML file and the EML file is updated when you download it.</p>	<p>Dr Wright not accepting the obvious truth regarding the timestamps encoded into images attached to the emails in question.</p>
<p>{Day19/17:18} – {Day19/18:22}</p>	<p>Q. Page 11, please {G/11/11}. I've put the point to you. Page 11. The timestamp, if we look at the bottom of the page, in the Ramona version email, the Ramona version email had a transmission header which was typical from an email – for an email retrieved from sent items so it didn't provide a complete account of transmission, just the initial time of sending from the computer used to create the email on to the Gmail servers; do you understand?</p> <p>A. No, that's actually incorrect. If you look at the first thing, you see "Return-Path" then "Received: from". So this is an internal update from Google. The original email that was sent, because of the move between domains, is split. So, where it says "Received: from", that's not saying that this is the – the</p>	<p>Dr Wright attempting to explain timestamp anomalies as a result of "Google migration". Dr Wright has provided no evidence other than his say so to support this.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>original email. The original email won't have a "Received: from" at Google.</p> <p>Q. Well, I've put to you the point that this transmission header is typical for an email retrieved from sent items. But the issue I'm coming to is that the timestamp indicates a sending time of 2 December 2019 at 14.51, doesn't it? We see that highlighted in yellow.</p> <p>A. I do.</p> <p>Q. Now, that's starkly at odds with the image timestamp, isn't it?</p> <p>A. Again, this isn't the first part of the email. The email is actually split into two parts in Google because of the migration between domains.</p>	
<p>{Day19/19:11} – {Day19/20:6}</p>	<p>Q. Page 12, please {G/11/12}. Now if we look under paragraph 27, do you see that the ESTMP SA received timestamp in the transmission header for the Ramona version email, so the version of the email that was sent by Ms Watts to Shoosmiths, which gives a date of 2 December 2019, is 71 characters in length; do you see that?</p> <p>A. I do.</p> <p>Q. Now Gmail's ESTMP SA ID changed its format in late February or early March 2022, didn't it?</p> <p>A. Not sure. I know it did, but I don't know the exact date.</p> <p>Q. It changed its format from 39 to 71 characters in length; correct? Or can you dispute that?</p> <p>A. I'm not disputing that.</p> <p>Q. So a timestamp in this format is simply not consistent with the stated date of 2 December 2019, is it, Dr Wright?</p> <p>A. No, again, this is only part of the email. The actual full email is the original sent email from rcjbr.org and the internal Google message.</p>	<p>Dr Wright refusing to accept the obvious truth in relation to the timestamp in the transmission header as between the Ramona version email and the Gmail ID.</p>
<p>Email exchange between Shoosmiths and Ontier dated 23 February 2024</p>		
<p>{Day19/21:3} – {Day19/21:23} {X/57/1}</p>	<p>Q. Shoosmiths, we see, emailed Ontier to say that they'd received an attached email from December 2019 where you had disclosed access to MYOB and the MYOB link would be sent to Ontier; do you see that?</p> <p>A. Yes, I do.</p>	<p>Dr Wright providing an implausible explanation that the email sent to Ontier, purportedly dated from</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Sorry, not disclosed, discussed. And that email attached the Ramona version email document dated on its face to 2 December 2019 and referring to the MYOB log-in, right?</p> <p>A. No, it wasn't a Ramona version, it's clearly a spoofed email. If you look at the email header, you can see that there's no Google authentication, the records that I pointed out show that I had Google with DMARC, which is the full secure sort of authentication system. That goes back to 2016. Now, while you point out other things in records because Google updates and changes how they do things, Google DMARC is the full encrypted sort of requirement for sending email. Now, "SPF fail" will allow an email to send outside of a domain, but it will generally go into a spam box and be rejected --</p>	<p>December 2019, was a spoofed email.</p>
<p>{Day19/22:9} – {Day19/23:24} {X/57/2} {X/56/2}</p>	<p>Q. Okay. What I'm putting to you is that, last Friday, Shoosmiths wrote to Ontier in the terms we see here at {X/57/2}.</p> <p>A. Yes.</p> <p>Q. Do you see that? What they attached, if we can have it on screen at the same time, is {X/56/2}. That's what I'm saying that they attached and I don't think this is controversial. Now, you don't say that that was a spoofed email, do you?</p> <p>A. Unless I could see the header. From the header, the "Sent" is actually set manually. From RFC 822 in email you can manually set the date, you don't need to send it back --</p> <p>Q. Just before we go to that. Do you say that the email that referred to MYOB log-in is a spoofed email or that the email that referred to Information Defense and your lawyer in Australia was a spoofed email? Which is it?</p> <p>A. Again, unless you show me the header, the header will tell me whether it's a spoofed email or not. You cannot, from the date on what you've printed, tell whether it's spoofed or not. There is an email that was spoofed in 2024 and received by Ontier. On its face, it will show that timestamp; in the header is whether you can tell whether it's a spoofed version or not.</p> <p>Q. What we're looking at on the right-hand side of the screen, and we're all agreed on this as I understand it, I'll be corrected if I'm wrong, what we're looking at on the right side of the screen at {X/56/2} is an email document which you sent to your wife and your wife sent to Shoosmiths on 18 February and then which Shoosmiths passed on to Ontier on 23 February 2024. Now, given that this is a document that came from you, do you say that it was real or spoofed?</p> <p>A. Okay, thank you. What I was trying to get at, which version of this document it is. So if that is the one that Ramona sent</p>	<p>Dr Wright is evasive regarding whether the document being looked at was spoofed, only providing a straight answer once the Judge intervenes.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>to Shoosmiths and then was sent, then no, that came from Google.</p> <p>MR JUSTICE MELLOR: No, what?</p> <p>A. It came from Google, so it's not spoofed, my Lord.</p> <p>MR JUSTICE MELLOR: Okay, not spoofed. Right.</p>	
<p>{Day19/25:1} – {Day19/25:24} {X/57/1}</p>	<p>Q. And Ontier attached the genuine email of 2 December 2019 which referred to Information Defense and your lawyer in Australia</p> <p>A. Do you understand, that's point 2?</p> <p>A. Okay.</p> <p>Q. And point 3, Ontier reiterated their position that no link to the MYOB database was received by them in 2019, yes?</p> <p>A. That's incorrect.</p> <p>Q. That's what they've said?</p> <p>A. They said that, but I've also seen other emails from Oliver Cain noting it.</p> <p>Q. Well --</p> <p>A. That he's responded to personally.</p> <p>Q. -- you haven't relied upon any of those and none of those were put forward on Monday. And they concluded by expressing the view that the email attached to Shoosmiths' email, so the Ramona version email we're looking at on the right, was not a genuine email, and you disagree with them about that, don't you?</p> <p>A. No, what they've done is they've said they received one in 2024, which is correct. But the one in 2024 is a spoofed email. It's not gone through any of the proper checks and it hasn't got a complete header.</p>	<p>Dr Wright referring to further emails with Oliver Cain of Ontier, which have not been disclosed.</p>
<p>Email provided by Ontier to Shoosmiths which Ontier received on their systems on 18 February 2024</p>		
<p>{Day19/26:2-21} {X/58/1}</p>	<p>Now, this is the email which was provided by Ontier to Shoosmiths which Ontier had received on their systems on 18 February 2024; do you understand?</p> <p>A. I do.</p> <p>Q. And do we see that it's identical to the Ramona version email which your wife had passed to Shoosmiths, except that Ontier's systems have added "(SHARED)" by Simon Cohen's</p>	<p>Dr Wright refusing to accept the obvious truth, that the emails are materially (textually) identical.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>name, and Ontier systems have also added "[EXT]" at the start of the subject line in the header; do you see that?</p> <p>A. No, you can't say that it's identical. The -- the way that you have to do that is to look at the header and other information. So, this email is very different.</p> <p>Q. We'll come to the header in a moment, but if we put the two alongside each other, those are the differences in text; would you agree?</p> <p>A. No, there's actually also differences in some of the MIME types, etc. So what you're trying to say is that if I printout from Outlook, I can make it visually look the same but it's actually different.</p>	
<p>{Day19/26:22} – {Day19/28:5} {X/58/1} {X/56/2}</p>	<p>Q. May we have on screen then {X/58/1}, which we've got, alongside {X/56/2}. With the exception of the word "SHARED" and the word "EXT", what do you say are the differences between the face appearance of these two emails?</p> <p>A. So the face appearance is completely irrelevant. The face appearance is used by spoofer to actually spoof emails. So, the whole thing here is, this is an email that you can see has been spoofed to Ontier on that date.</p> <p>Q. Let's try the difficult challenge of answering the question.</p> <p>A. I believe I just did.</p> <p>Q. Other than those two differences, the word "SHARED" and the word "EXT", can you point to any differences in the face appearance of these two emails?</p> <p>A. Again, the question's irrelevant. What I'm answering is the fact that I can't pick up differences in the MIME types, etc, by looking at them. That is why people spoof emails. That is why Adam Back created --</p> <p>Q. I'm going to ask the question a third time. Point to any difference in the face appearance of these two emails other than the word "SHARED" and the word "EXT", please?</p> <p>A. That's not something you would do by looking at two printouts of emails. Analysis doesn't do that. To do that would be dishonest. To actually say that you have two different electronic files and try and match them that way is just dishonest. MR HOUGH: Would your Lordship please direct the witness to answer that question: whether there are any differences beyond those two words in the face appearance. MR JUSTICE MELLOR: I'm not sure it's necessary to put the question again.</p>	<p>Dr Wright remains evasive in respect of the differences between the two emails.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
Questions in relation to Mr Madden’s sixth report {G/11}		
<p>{Day19/28:18} – {Day19/29:20}</p>	<p>Q. Then over the page to {G/11/10}, we see the transmission header, and do you see, highlighted in green, timestamps for the creation of the email and those would be set according to the local clock on the computer used to create it, right?</p> <p>A. No, the date field in email is user configurable. You don't need to set back date. That goes back to RFC 822, my Lord. Because there was no authentication in the '80s, email allowed you to type in anything. So you can go to a command line, for instance, type in, like, the receipt to, sent to, etc, and even manually send information and spoofing email. The date command is just typed. You type in date, colon and then put whatever you want. In fact, I could put in date, frog and an email server would accept it.</p> <p>Q. Well, I've put to you our position that that's set according to the local computer clock.</p> <p>A. RFC 822 denies that and RFC 5822 also goes against that, so the standards of the internet deny that --</p> <p>Q. That can be set according to the local computer clock, can't it?</p> <p>A. Oh, you can set it however you want. You can type it in. As I said, you can set it by the clock, you can set it by typing it in, you can manually edit it.</p> <p>Q. So we agree on something: it can be set according to the local computer clock?</p> <p>A. It can be set any way you want. There is no -- there's no authentication in the date field.</p>	<p>Dr Wright admitting that it is possible to manipulate the clock by setting it to another time.</p>
<p>{Day19/31:25} – {Day19/33:22}</p>	<p>Q. So, Dr Wright, you're now saying somebody would have to get the content of a real email from your systems and spoof an email with that content, backdate it to 2 December 2019 and spoof that, sending it to Mr Cohen at Ontier on Sunday, 18 February?</p> <p>A. No, the date field is enterable. So, I could -- if I open up a telnet session to port 25 on an email server, my Lord, I can type in anything. If I wanted to, I could type in "date:frog" and the email server would accept it. Now, what I am saying is that, yes, someone has a copy of my email, but AlixPartners have a copy, three different providers have a copy, seven different law firms have copies, external analysis people have</p>	<p>Dr Wright is now blaming third parties by suggesting that up to 100 people could have been responsible for hacking his computer.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>copies, other companies have copies. There are at least 100 people that I could name that have copies of my email.</p> <p>Q. So somebody's managed to get hold of your real email in a native format and spoof an email sent to Mr Cohen at Ontier on Sunday, 18 February '24? That's your position?</p> <p>A. At least 100 people that I know of, if not more, have access to all of my files now. Because I've done Takeout for multiple court cases, because I have had people from corporations managing email, I'm saying my email is so sort of shared now, it's not funny. I noticed, on the weekend, people, AVP sending files, some of the COPA supporters, of messages that have never been made public that should be on disclosure platform that no one has, and yet they share them. So, as for the integrity of any of these emails right now: zero.</p> <p>Q. Dr Wright, this entire explanation is nonsense, isn't it? Not only does it not account for the encoded image timestamp, which tells its own story, but it would require somebody to get hold of your real email and spoof it by an elaborate process which you have now told the court about for the first time, right?</p> <p>A. No, it's not elaborate. There are tools online for spoofing email that allow you to actually do this by clicking on a website. I know at least 100 of those. There are ones that actually subscribe to Mimecast and allow you to send them directly from them, there are ones that do through Google. On top of that, there are Netcat and Telnet sites telling you how to do it by command line that you can replicate very easily. As I've noted, this is one of the simplest, simplest attacks you could ever do. Spoofing email is script kiddy level. Someone who's been a hacker for less than five minutes can do this.</p>	
<p>{Day19/36:9} –</p> <p>{Day19/38:21}</p> <p>{G/11/9}</p> <p>{E/34/6}</p>	<p>Q. And then do you see that paragraph 17 has Mr Madden noting that the header contains an SPF indication referring to a soft fail?</p> <p>A. I do.</p> <p>Q. So you were making these points in your 15th witness statement in order to attack an email which you've accepted today is genuine?</p> <p>A. No, I'm saying that it probably would have ended up in the spam folder. The point I'm noting is I note that the header contains an SPF indication and that's not irregular. That is an irregularity. Google should have handled that at the time and that would likely go into the spam box. So, even in this email, they would have had to go into the spam box to find it. Using Mimecast means that it would have been flagged that way.</p>	<p>Dr Wright is inconsistent, saying that it is an irregularity, and then saying that it isn't.</p> <p>Dr Wright is not responding properly to the question and failing to accept the contradictions as between his Fifteenth Witness Statement and his oral evidence in relation to that statement.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>Q. Dr Wright, all your information about SPF validation information in your 15th witness statement is put together in order to attack this email where Mr Madden refers to a soft fail and yet this email is one you've accepted today as genuine?</p> <p>A. No, it's not attacking it. What I'm saying is it's an irregularity. The likelihood is, even this email would have gone to the spam folder. So unless I actually contacted Simon and told him there's an email and he looked for it, he wouldn't have seen it. So it's quite possible that the other email was left in the spam folder and never taken out. So what I'm saying is the irregularity means that soft file would have put this into spam, the other one probably went into spam in 2019, and unlike saying this is not an irregularity, it's a complete irregularity and it would have been rejected.</p> <p>Q. Dr Wright, your 15th witness statement gives reasons why this email, the Ontier version, might have been spoofed, and now you say that that wasn't spoofed. That's --</p> <p>A. I'm saying that that's what a server will recognise. So, this demonstrates that these emails in that thread, something went wrong at Google and they got spoofed, so they got put down as being spoofed.</p> <p>Q. Dr Wright, why spend paragraph after paragraph in your 15th witness statement taking issue with or providing reasons to take issues with an email you accept is genuine and say not a word about your attack on the email which you today have said was spoofed, namely the email received on Ontier's systems --</p> <p>A. Because it points --</p> <p>Q. -- on 18 February?</p> <p>A. Because, quite frankly, it points out why a December 2019 email would not exist. If something had gone wrong and the emails were being sent with a soft fail, Mimecast would have put them into the spam folder, my Lord, and in the spam folder, unless a person actively looks for a communication, it eventually gets deleted by default after 30 days. So if I'd sent an email and then said, "Oh, I've sent one to you, Simon", and he didn't realise there were two, it's quite feasible that Ontier received both emails but basically left one in the spam folder.</p> <p>Q. The reality is you hadn't decided what version to give to the court and which email to attack when you wrote your 15th witness statement.</p> <p>A. No, I planned to come in here and explain to you that it likely ended up as spam.</p>	

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>Questions from Mr Hough KC in relation to document as handed by Mr Hough to Mr Justice Mellor earlier today {housekeeping}</p>		
<p>{Day19/39:1} – {Day19/40:22}</p>	<p>MR HOUGH: Dr Wright, if you look at the first of these records, SecurityTrails historical TXT data --</p> <p>A. Mm-hm.</p> <p>Q. -- showing the text values for the rcjbr.org domain, this shows, doesn't it, that the SPF configuration information which we see recorded there, "v=spf1" and so on, was first seen by this tool on 28 February 2024? Yes?</p> <p>A. No, this is a partial information. For rcjbr.org, the domain was set up as a DMARC domain. That means DKIM signatures as well. So, what you need to do is match the SPF which was open there, which is set by Google, with the ARC information. ARC is an advanced relay mechanism, so ARC would also need to be checked. So, what you have here is 1% of what you need to actually put this together. So when you pull down the information from Google, which you'll see my domain since 2016 has been on Google, listing all of the Google servers, which you can find from this site as well, Google require certain security mechanisms. Since 2012, Google have implemented advanced security as a requirement. When you run a domain on Google, that is managed by Google. So, what you're not picking up is the DMARC information on how Google handles that internally.</p> <p>Q. Dr Wright, you added the configuration, including the SPF validation information, in the last week, didn't you?</p> <p>A. No, I did not. Google actually runs this themselves, and if you go to the Google developer admin site, you will see that Google propagates information. Now, when you have DMARC, which is shown earlier, DMARC goes back several years on my sites, you'll see that that supersedes SPF. SPF is a very low level of security control for spamming. DMARC, DKIM and ARC, are the higher level that require signing and digital signatures to be sent.</p> <p>Q. Dr Wright, you told us in your 15th witness statement that you set up this domain with the entry "v=spf1 include:_spf.google ..." precisely the line of text we see here. That was added in the last week, wasn't it?</p> <p>A. No. The way I set it up is I migrated to Google domains. Google say that that's how they do it. Now, I don't actually do the management on the Google domains, they do that themselves. When you add, in Google Workspaces, a domain,</p>	<p>Dr Wright is evasive, providing more migration-related excuses without any evidence to support them.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	the configuration for all of these sort of mail settings are handled by Google.	
<p>{Day19/40:23} – {Day19/41:17}</p>	<p>Q. Dr Wright, next page. The empty text entry in the DNS record for 24 February 2024 is again consistent with the position that the SPF validation information had not been entered by that date, as suggested in paragraph 12 of your witness statement?</p> <p>A. No, actually, that's totally incorrect. The other way Google does all of this is they have -- what do you call it -- host name records. So, Google have a variety of different ways of propagating this. Now, on top of this, what I notice is this is different from the record I've checked. When you look at the thing you've got "rcjbr*org". When you do "rcjbr.org", the Whois records actually turn out differently, so I'm not sure why you have printed with a URL metacharacter, the type Professor Meiklejohn was actually talking about, my Lord, for deceiving people, which is actually in your page here.</p> <p>Q. Well --</p> <p>A. You'll see that it does do dots. Every other line on this page has a dot.</p>	<p>Dr Wright is not accepting the obvious truth, saying it is a star when it is a dot.</p>
<p>{Day19/42:25} – {Day19/43:7}</p>	<p>Q. It's the one you relied upon at paragraph 12 of your witness statement.</p> <p>A. No, I also put in images showing the registration with Google and I noted DMARC. So, DMARC includes SPF. But as you'll note here, the Google site information handles it. So I have a site managed by Google and Google handle all that, so that -- I don't know how they propagate the information, but it's handled by Google.</p>	<p>Dr Wright is not accepting obvious truth and relying on privilege again.</p>
<p>{Day19/43:20} – {Day19/44:6}</p>	<p>Q. Well, the attached email has been redacted in places for privilege reasons, but no doubt if it contained references to MYOB, those would have been provided to us. The reality is that that email had nothing to do with MYOB, neither it, nor its attachments mentioned it, right?</p> <p>A. The later one does. I was asked about the first time I -- I propagated. As I noted with Oliver Cain, he responded to multiple parties on 5 March noting that AlixPartners had been doing a report but hadn't completed it, and if they had been doing a report that means log-in had been already granted.</p>	<p>Dr Wright attempting to refer to an email from Oliver Cain (Ontier) in support of his position on the MYOB screenshots, without any further evidence.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day19/44:7}- {Day19/45:1}</p>	<p>Q. Dr Wright, if you are saying that there are emails which show -- genuine emails that show that Ontier had access to MYOB log-in details before 9 March 2020, you have not provided them, other than this fake email, right?</p> <p>A. One, it's not a fake email. And two, no, they were actually provided -- the solicitors had them in disclosure, but like everything else, when it's lawyers, no one likes to give out information.</p> <p>Q. So you're saying that there are more emails held by Ontier, which haven't come to light, which would show them having access to MYOB before 9 March 2020?</p> <p>A. It shows AlixPartners --</p> <p>Q. Ontier. Focusing on Ontier.</p> <p>A. I just said, it shows AlixPartners doing a report. Oliver Cain responded on 5 March saying -- 2020, saying that AlixPartners are nearing completion of their report, which was talking about the report on the accounts.</p> <p>Q. Dr Wright, we are focusing --</p> <p>A. No, no --</p>	<p>Dr Wright attempting to refer to an email from Oliver Cain (Ontier) in support of his position on the MYOB screenshots, without any further evidence.</p>
<p>{Day19/45:2} - {Day19/45:13}</p>	<p>Q. -- from the start, on when Ontier had access to MYOB log-in details. Do you say that there is an email out there, other than the one which we have said is a fake, that demonstrates that Ontier had log-in details for MYOB before 9 March 2020? It's a really simple question.</p> <p>A. Being that AlixPartners got their log-in with Ontier and Ontier did or did not accept that, I can't say whether they took it or just AlixPartners logged in. AlixPartners were engaged by Ontier, so if AlixPartners are engaged by Ontier to do something, I'm assuming that Ontier have a log-in.</p>	<p>Dr Wright blaming third parties and not accepting the obvious truth, claiming that AlixPartners got their log-in details for the MYOB account from Ontier, and referring to communications that have not been provided.</p>
<p>{Day19/48:5}- {Day19/48:18}</p>	<p>Q. Dr Wright, you forged an email during trial to back up a dishonest account, didn't you?</p> <p>A. No. And in fact, you wouldn't actually send an email. My Lord, if you wanted, what you would do is you would just create, in Outlook, a send mail. Now, you don't need to send an email, you could have your computer not connected to the internet with a backdated time. Google will not connect if you're more than an hour out, they use ORF, and on the developer page it says IMAP/IMAPS only work within one hour. If your clock is out by more than one hour, Google will not send, which is why Mr Madden had to turn his clock back, then turn it forward, recognised in his email by the 30-second gap. So what he did was --</p>	<p>Dr Wright outlining a potential process for creating a fake email.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day19/49:14} – {Day19/50:7}</p>	<p>Q: Let me give -- let me ask you one final question. I'm giving you one last chance to confess to this forgery, because it may be relevant to relief. You forged this document, didn't you?</p> <p>A. No. As I noted, my Lord, very simple check: you look at the Google Takeout and you look at the time there. Now, if you drop an email checking -- like, cheating by putting in fake times and you put that in Outlook, Outlook will have it in your PST file or OST file. You can do that on a local computer. This is the difference of why you want servers, why you want a distributed system. If you do it locally, you can cheat. On Google, Google records the time they received it. To attack Google, you would have to change their internal NTP servers -- there are, I believe, 18 of them -- you would have to attack multiple databases. We're talking a state-level attack, my Lord. It has happened before. The DigiNotar attack, in 2012, led to such a thing, but that is rare, and that was the Iranian government.</p>	<p>Dr Wright maintaining the integrity of the Google Takeout version of the document, denying that it could have been manipulated.</p>
<p>RE-EXAMINATION OF DR WRIGHT BY MR ORR KC IN RELATION TO THE DRAFT TRANSCRIPT AT {Day19/18:17}</p>		
<p>{Day19/52:4}- {Day19/52:20}</p>	<p>Q. Could you please explain what you meant when you said that.</p> <p>A. Because I was getting so much hate and abuse mail in 2019 because my email had been leaked during the Kleiman case I changed my mailbox, that was rcjbr.org as a primary thing, to Tulip Trading -- craig@tuliptrading.net, and then removed rcjbr.org for a year, which stopped some of the emails. When I did that, I had migrated between the Google platform and migrated in the old mailbox into my new one, and with the different, sort of, header ID and authentication. So the way that Google has it in Takeout is actually two parts. It has a first part of the header representing craig@rjbr.org, and then it has a second email with an internal "received by" stamp where it's sent between Google, and I've no idea what "Google logs" mean on that part.</p>	<p>Dr Wright claiming he migrated away from his RCJBR email, something he didn't refer to in his disclosure certificate or the DRD, other than listing the @RCJBR.ORG address as being a source of both retrievable and irretrievable documents.</p>
<p>QUESTIONS FROM MR JUSTICE MELLOR IN RELATION TO THE DRAFT TRANSCRIPT AT {Day19/30:18}</p>		

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
<p>{Day19/54:15} – {Day19/56:24}</p>	<p>MR JUSTICE MELLOR: Can we go back to the draft transcript at, I think, page 31 -- sorry, 30, bottom of page 30. Now, you see the question at line 18 where counsel asked: "... who do you say did this and why?"</p> <p>A. Yes, my Lord.</p> <p>MR JUSTICE MELLOR: By all means get the context, because it's about -- you're being asked about the email that you say was spoofed.</p> <p>A. Yes, my Lord.</p> <p>MR JUSTICE MELLOR: Now, those issues of who did it and why I are not separate. You explained in your answer why, but can I just be clear as to who you say did this. I mean, you referred, a little bit later, to over 100 people, but can we be any more specific than that?</p> <p>A. Unfortunately not. I suspect a number of people, my Lord, and I know that there are people who've been fired in organisations that I've been associated with and that have fled the country. Can I actually pinpoint and definitively say on this? No, because I would need more information. What I do know is that information has been on certain Reddit and other discord sites posting about these topics and also the domains, the Whois, etc. Mr Arthur van Pelt, for instance, has been taking screenshots of certain information that to my knowledge, until today, shouldn't have been public knowledge. So, there are a lot of people who want BTC to win and me to fail and the BTC Ponzi to keep going, so I can't even say that they're directly linked to COPA.</p> <p>MR JUSTICE MELLOR: But I mean, when you say you suspect a number of people, in that group, are you characterising people who are acting contrary to your interests?</p> <p>A. Oh, definitely.</p> <p>MR JUSTICE MELLOR: Just pause there. If they're acting contrary to your interests, why would they spoof an email to support evidence you gave?</p> <p>A. Oh, it doesn't support. When you send that through, the headers will always come up saying "2024". So what you're doing is fabricating an excuse basically to bring me back in court and say it's all made up. It's very easy, my Lord, to spoof an email. I would never do this, my Lord, but for instance, I could type in your address into the government server, if I was on Mimecast -- I'm not any more and I haven't been for years -- and that would then forward, but without SPF check it would end up in your spam box. Now, if you went through your spam box, you would then find it. Now, the reason why</p>	<p>Dr Wright blaming various people, including Christen Ager-Hanssen (indirectly) and Arthur Van Pelt, for being involved in the spoofed email.</p>

Appendix B: Schedule of Transcript References

<u>REFERENCE</u>	<u>QUOTE</u>	<u>COMMENT</u>
	<p>to do this would be so that you could basically cast doubt on anything. You could say that I did it only a few weeks ago, and why did I do it a few weeks ago, because one has been received by Ontier, and in fact one had been received by me. What I didn't realise at the time, because it went in my spam and I only discovered when Stroz analysed the Google Takeout, was there's a received attempt at spoofing in my Google Takeout that contains the message, but didn't come through correctly because I'm not running Outlook, my Lord.</p>	
<p>FURTHER CROSS-EXAMINATION OF DR WRIGHT BY MR HOUGH KC</p>		
<p>{Day19/57:3} – {Day19/58:7}</p>	<p>MR HOUGH: Just to be clear, Dr Wright, is it your position that the person who did this, sending the spoofed email on the morning of Sunday, 18 February 2024, happened to be doing that on exactly the same morning that your wife was sending through a real version of the same email, just by coincidence?</p> <p>A. Unfortunately, yes. It got sent beforehand. So, as I note, you wouldn't actually send to someone to actually spoof an email. As an example, my Lord, you can copy and paste something into the sent mailbox in Outlook and then change it, as they've been arguing.</p> <p>Q. But just --</p> <p>A. That doesn't ever send, though. It goes into the sent mailbox without having been sent.</p> <p>Q. But you say that the spoofing happened and was done on the same morning as your wife sent through the real version of the same email and that that was a complete coincidence?</p> <p>A. I don't know if it's a complete coincidence.</p> <p>Q. How else would the person know you were doing that?</p> <p>A. I haven't had my house bug-swept recently, and I know you're doing that, but that's not something that hasn't happened before. Diligence have come through my house twice. They're a private intelligence company, my Lord. And on both occasions I have had bugs in my house. We've had multiple break-ins, because anyone who has valuable information and things like that gets broken into these days, and the Diligence reports on each of the other ones basically showed some of the cameras had been replaced.</p>	<p>Dr Wright making an outlandish claim that his house is bugged, having not referred to this anywhere in his previous evidence.</p>