IN THE HIGH COURT OF JUSTICE
BUSINESS AND PROPERTY COURTS
OF ENGLAND AND WALES
INTELLECTUAL PROPERTY LIST (ChD)

Claim Nos. IL-2021-000019
IL-2022-000069

B E T W E E N:

CRYPTO OPEN PATENT ALLIANCE

Claimant in IL-2021-000019
(the "COPA Claim")

- and -

DR CRAIG STEVEN WRIGHT

Defendant in the COPA Claim

AND BETWEEN:

(1) DR CRAIG STEVEN WRIGHT
(2) WRIGHT INTERNATIONAL INVESTMENTS LIMITED
(3) WRIGHT INTERNATIONAL INVESTMENTS UK LIMITED

Claimants in IL-2022-000069

- and -

(1) BTC CORE
(2) WLADIMIR JASPER VAN DER LAAN
(3) JONAS SCHNELLI
(4) PIETER WUILLE
(5) MARCO PATRICK FALKE
(6) SAMUEL DOBSON
(7) MICHAEL ROHAN FORD
(8) CORY FIELDS
(9) GEORGE MICHAEL DOMBROWSKI
(10) MATTHEW GREGORY CORALLO
(11) PETER TODD
(12) GREGORY FULTON MAXWELL
(13) ERIC LOMBROZO
(14) JOHN NEWBERY
(15) PETER JOHN BUSHNELL
(16) BLOCK, INC.
(17) SPIRAL BTC, INC.
(18) SQUAREUP EUROPE LTD
(19) BLOCKSTREAM CORPORATION INC.
(20) CHAINCODE LABS, INC

(21) COINBASE GLOBAL INC.
(22) CB PAYMENTS, LTD
(23) COINBASE EUROPE LIMITED
(24) COINBASE INC.
(25) CRYPTO OPEN PATENT ALLIANCE
(26) SQUAREUP INTERNATIONAL LIMITED

Defendants in the BTC Core Claim

DR WRIGHT'S CLOSING SUBMISSIONS

[References to the trial bundles are in the form {Vol/Tab/Page} or {Vol/Tab}. References to the bundle containing Wright 11 and 12 are in the form {CSW/Tab/Page} or {CSW/Tab}. Transcript references are in the form {Day#/[page]/[line]} or {Day#/[page]}]

TABLE OF CONTENTS

I. INTRODUCTION

1. These Closing Submissions are served on behalf of Dr Wright. Save where otherwise indicated, these submissions supplement rather than replace Dr Wright's Skeleton Argument. The abbreviations used in Dr Wright's Skeleton Argument are adopted below.

II. SUMMARY OF DR WRIGHT'S EVIDENCE

2. The Identity Issue will turn primarily on the view taken by the Court of Dr Wright's evidence. A summary of Dr Wright's evidence on that issue[1] is set out below.

3. Dr Wright has the required skills, knowledge and qualifications to have created the Bitcoin system and authored the White Paper. These qualifications include: (i) his master's degree in statistics from the University of Newcastle[2] and his LLM from the University of Northumbria[3]; (ii) his numerous other degrees and qualifications including his PhD in Computer Science and Economics and postgraduate degrees spanning many other disciplines, including statistics, game theory, finance, economics and law[4]; and (iii) his cyber security certifications issued by the SANS Institute, including Global Information Assurance Certificates in forensics analysis, reverse engineering malware and the security of .NET code.[5] This combination of skills and knowledge is consistent with the creation of a system that combines and applies a wide variety of pre-existing technologies and concepts, including cryptography, digital signatures, hash functions, distributed ledgers and game theory.

4. Dr Wright has been deeply invested in the evolution of digital cash systems since the early 1990s. Examples include: his work at OzEmail, which involved the development of a payment protocol called "*Millicent*" that "*used digital signatures*" and an analogous scripting language to Bitcoin;[6] and his work at DeMorgan, which involved extensive research and development in digital cash. The latter included project 'BlackNet', which Dr Wright described as "*an encrypted internet based on crypto credits*" that "*morphed*

[1] Dr Wright's evidence in response to COPA's forgery allegations is dealt with separately in Section V below.
[2] See e.g. {L1/337}.
[3] Wright 1 [56]-[60] {E/1/12-13}.
[4] Wright 1 [6] {E/1/3}.
[5] {L1/327/1}, {L2/128/1} and {L2/282/1}.
[6] {Day 5/166/9 to 168/2}.

into Bitcoin and Metanet".[7]

5. Dr Wright worked on a number of projects from the late 1990s onwards that are relevant or related to the technology and concepts underpinning Bitcoin, including:

   5.1. At the Australian Stock Exchange (1996), Dr Wright built the "*NIPPA network*" that involved creating a distributed "*peer network*" protocol to send transactions across Australia.[8]

   5.2. At Lasseters online casino (1998), he developed "*advanced security measures and logging systems*" that were "*an early precursor to the blockchain*".[9]

   5.3. At Vodafone (around 1998 to 2002), he worked on advanced logging systems that involved a "*hash chain-based system*". [10]

   5.4. At BDO (2004-2008), he discussed proposals for a network-based immutable ledger system with Mr Matthews (who at the time was CIO of Centrebet); and worked on projects with Dr Pang concerned with "*small-world networks*".[11]

   5.5. At the University of Northumbria (2005-2008), he produced his LLM Dissertation (2005-2008), the proposal for which contains passages that closely reflect passages in the White Paper.[12] The LLM Dissertation itself was on the liability of internet intermediaries which are also known as 'trusted third parties' and are referenced in the White Paper.[13]

6. In parallel with this precursor work, Dr Wright was engaged in discussions with a number of individuals about digital cash and concepts similar to those that would appear in the White Paper (or related concepts):

   6.1. Mr Jenkins had discussions with Dr Wright about "*eGold*" in around 2000-2002; about "*grid computing*" in around mid-2007; and about "*achieving trust other than*

[7] {Day 5/171/17 to 173/11}.
[8] {Day 2/65/24 to 66/23}.
[9] Wright 1 [38]-[44] {E/1/9}ff.
[10] {Day 6/13/6 to 14/11}.
[11] Wright 1 [53]-[55] {E/1/11}.
[12] The LLM Proposal is the subject of a forgery allegation, which is addressed below and in Appendix 1.
[13] *The Impact of Internet Intermediary Liability*: {L20/178/1}.

in a central bank" towards the end of 2007 or early 2008.[14]

6.2. Mr Archbold had discussions with Dr Wright about digital currency in around 2004 or 2005, during his second stint at Lasseters.[15]

6.3. Mr Yousuf had discussions with Dr Wright about digital currency and how the financial system was flawed as far back as 2006; and, prior to 31 October 2008, they spoke about the problem-solving capabilities of "*distributed networks*".[16]

6.4. Dr Wright mentioned blockchain to Dr Pang on 1 August 2008, when Dr Pang purchased a Batman Lego set (for which he has the receipt).[17]

6.5. Mr Matthews had relevant discussions with Dr Wright about digital cash systems in the latter part of 2007 and into 2008.

7. On the drafting and sharing of the White Paper, Dr Wright's evidence is that the White Paper was drafted in LaTeX (this distinct issue is addressed in Section IV below). The evidence of Mr Matthews, Don Lynam and Max Lynam support Dr Wright's evidence on sharing drafts of the White Paper prior to its release in October 2008.

8. In relation to the launch of the Bitcoin system, Dr Wright has explained his purchase of the bitcoin.org domain; his involvement in the mining of early Bitcoin blocks, which is corroborated by contemporaneous documents and a number of third party witnesses; and his position in relation to the early Bitcoin transfers carried out by Satoshi (and other relevant interactions).

9. There is a significant body of other circumstantial evidence post-dating the White Paper that is consistent with Dr Wright's authorship, including: (i) Dr Wright helping Qudos Bank to implement an immutable event logger system with similarities to blockchain technology in around November or December 2008[18]; (ii) Dr Wright pitching an alternative payment system to Qudos Bank that was based on a "*decentralised ledger*" and involved a "*peer-to-peer payments network where transactions would be a fraction*

[14] {Day 9/54/5 to 65/24}; {Day 9/73/21 to 77/1}; Jenkins 1 [16]-[25] {E/6/5}ff.
[15] {Day 10/27-28}; {E/11/5} [15-16].
[16] Yousuf 1 [8] and [15] {E/7/3-4}.
[17] {Day 9/24-33}; the receipt dated 1 August 2008 is at {L3/57/1}.
[18] {Day 11/5-6}; cf. Bridges 1 [9]-[12] {E/9/4}.

of the cost of the existing SWIFT payment system" in around late 2008 or 2009;[19] (iii) Dr Wright pitching to Centrebet a honeypot detection system with close parallels to Bitcoin/blockchain technology at some point in 2009[20]; (iv) Dr Pang's recollection of Dr Wright asking him and a number of other BDO colleagues whether they had heard of Satoshi Nakamoto "*or something that sounds like that name*"[21] in late October or shortly thereafter; (v) Dr Wright mentioning "*blockchain*" to Mr Jenkins in 2008 (probably around December 2008); [22] and (vi) Dr Wright showing Mr Jenkins a "*Timecoin*" paper in around 2009/2010[23]; and (vii) the fact that Satoshi used idioms and colloquialisms typical of Australia in his communications, which is consistent with Dr Wright's nationality.[24]

10. Dr Wright's deeply held belief is that his identity as Satoshi should be proved through work and knowledge. In summary, "*you prove by knowledge, who you are, what you create*"[25]. In Dr Wright's view, an important aspect of this approach to proving identity lies in his extensive portfolio of patent research and development. The breadth of that portfolio is not in dispute. Dr Wright was not challenged during cross-examination in relation to his evidence that nChain has amassed a substantial portfolio of patents, encompassing nearly 4,000 patent filings, which are the fruit of Dr Wright's prior research.[26] COPA's attempt to undermine that evidence by the back door, during cross-examination of Ms Jones (without putting the equivalent points to Dr Wright), was misguided.

11. Dr Wright's demonstration during a number of private proof sessions in 2016 that he was in possession of private keys to certain of the original blocks (i.e. blocks 1 to 11) of the Bitcoin blockchain is highly probative of his claim to be Satoshi. These sessions included demonstrations with Mr Andresen and Mr Matonis, both of whom were central figures in the Bitcoin community, Andrew O'Hagan, an author who was chronicling the evolution of nChain, and journalists from the BBC (Rory Cellan-Jones) and Economist

[19] Bridges 1 [13]-[16] {E/9/4-5}. The cross-examination was at {Day 11/11/5 to 15/8}.
[20] Matthews 1 [30]-[33] {E/5/7-8}.
[21] {Day 9/35/1-2}.
[22] {Day 9/68/10-14} and {Day 9/79/5 to 81/13}.
[23] {Day 9/95-99}.
[24] See, for example, "wet blanket" {L19/11/2}; "bogged everything down" {L6/19/1}; "references galore" {L5/500/1}; and "bash the sockets" {L6/28/1}.
[25] {Day 7/144/13-14}.
[26] Wright 1 [172] {E/1/31}.

(Ludwig Siegele). In each demonstration, Dr Wright showed he had access to private keys associated with early blocks. The fact that Mr Andresen and Mr Matonis were persuaded by these demonstrations that Dr Wright was Satoshi is highly significant. Their recognition of Dr Wright as Satoshi is particularly credible. COPA's attempts to undermine the integrity of the private proof sessions are misplaced. There is no realistic basis for supposing that the sessions were deliberately subverted by Dr Wright and any case to that effect is in any event not open to COPA on its pleadings and was not fairly put to Dr Wright in cross-x.

12. In relation to the public proof sessions, Dr Wright has explained how he was pressured by Mr MacGregor into doing something he did not want to do (i.e. use a private key to prove possession of an early block in the Bitcoin blockchain before his identity had been proved by other means). As he put it, "*[t]he only way I would have signed was: first, prove my work*".[27] Consistent with that mindset, Dr Wright's evidence is that the Sartre Message was not intended to provide proof of possession. It was instead an act of defiance, which Dr Wright says was intended to convey the message, "*I'm not going to do it*". [28] He saw his use of a quote from Jean-Paul Sartre as a profound demonstration of his rejecting and choosing not to engage in a particular action.

13. Dr Wright emphasised in his evidence that there is a philosophical coherence between his own view of Bitcoin and the views expressed by Satoshi. For example, in relation to scalability (which goes to the heart of the fundamental divergence of view between Dr Wright and COPA/the Developers regarding their visions for Bitcoin), Satoshi explained to Mr Malmi[29] and Mr Hearn[30] that Bitcoin "*never really hits a scale ceiling*". Dr Wright referred to this point a number of times in his evidence[31] and explained the link between Satoshi's original code and the work that he has undertaken in the years following the creation of Bitcoin. The culmination of that work is the "*Terranode*" project, which has achieved over 1 million transactions per second.[32] Dr Wright sees this as turning Satoshi's

[27] {Day 8/19/3-16}.
[28] {Day 7/161/5 to 162/1}.
[29] {L5/54/4}. The full quotation is: "*The existing Visa credit card network processes about 15 million Internet purchases per day worldwide. Bitcoin can already scale much larger than that with existing hardware for a fraction of the cost. It never really hits a scale ceiling…*"
[30] {L18/404/1-2}.
[31] For example, {Day 8/161/21 to 162/2} and {Day 8/114/15-19}.
[32] {Day 4/32/13 to 33/3}.

vision into reality.

14. When asked about his Reliance Documents:

14.1. Dr Wright acknowledged that there were issues with the reliability of his electronic documents (though not his handwritten notes):[33]

> 10 Q. You have, over the last seven to eight days, raised
> 11 doubts over the provenance, authenticity and reliability
> 12 of most of your own chosen primary reliance documents,
> 13 haven't you, Dr Wright?
> 14 A. No, actually, that's not correct either. Ones, such as
> 15 the written documents, that I have had that have been
> 16 around for a long time have been ones that I'm not
> 17 denying.
> 18 Q. So handwritten manuscript documents?
> 19 A. That date back the time, yes. On top of that, I've also
> 20 had conversations etc with people such as Gavin.

14.2. He also explained:[34]

> 15 So, what I'm telling you is, at no point did I say
> 16 that this was a case about metadata from me. My case is
> 17 different. My case is these are the origins of
> 18 the ideas I've created, my Lord, these are the things
> 19 that led to how I have those patents.

14.3. Thus, Dr Wright's view is that the significance of his Reliance Documents lies in their content, rather than their metadata. This is consistent with his belief that identity is proved by work, knowledge and patents.

III. THE IDENTITY ISSUE

15. Dr Wright's case on the Identity Issue is set out below. COPA's forgery allegations are addressed in Section V below.

16. The key events concerning the release of the White Paper and subsequent launch of the Bitcoin system are (or should be) common ground. In summary:[35]

[33] {Day 8/108}
[34] {Day 3/18}.
[35] See also Dr Wright's Skeleton Argument at paras 62-94 {R/14/29-34}.

16.1. In August 2008, Satoshi acquired the bitcoin.org domain name, which was used to establish the Bitcoin.org Website.[36]

16.2. On 5 October 2008, Satoshi registered an account (i.e. the nakamoto2 Account) at SourceForge.[37] He used this account to create a project, entitled 'Bitcoin', on SourceForge (i.e. the SourceForge Bitcoin Project).[38]

16.3. On 31 October 2008, Satoshi released the White Paper by posting a link to it (on the Bitcoin.org Website) on The Cryptography Mailing List.[39]

16.4. On 8/9 December 2008, Satoshi uploaded the White Paper to the SourceForge Bitcoin Project.[40]

16.5. On 3/4 January 2009 (depending on time zone), Satoshi created the first block in the Bitcoin blockchain, i.e. the Genesis Block.[41]

16.6. On 8 January 2009, Satoshi uploaded the Bitcoin Software (comprising an executable file and the corresponding source code) to the SourceForge Bitcoin Project. On the same day, he announced the release of the Bitcoin Software by posting links to (i) the Bitcoin Software on the SourceForge Bitcoin Project, and (ii) the Bitcoin.org Website, containing screenshots and other explanatory information about the Bitcoin system.[42]

16.7. The first block following the Genesis Block, i.e. Block 1, was mined by Satoshi on 9 January 2009.[43] Three days later, the first transaction on the Bitcoin blockchain was recorded in Block 170, involving the transfer by Satoshi to Hal Finney of 10 Bitcoins which Satoshi had mined from Block 9.[44]

[36] Defence [7] {A/3/3} and Reply [5] {A/4/2}.
[37] Defence [6] {A/3/3}; Reply [4] {A/4/2}.
[38] Defence [9] {A/3/3}; {L4/61/1}; Malmi Day 13/12 lines 3-8.
[39] PoC [7] {A/2/3}; Defence [7] {A/3/3} and [16(2)] {A/3/5}; {L3/278/1}.
[40] PoC [7] {A/2/3}; Defence [9] {A/3/3} and [16(3)] {A/3/5}; {L3/481}.
[41] PoC [10] {A/2/4}; Defence [10] {A/3/4}.
[42] PoC [11] {A/2/4}; Defence [11] {A/3/4} and [20(1)] {A/3/7}; {L4/61/1-2}; {L18/310/2-3}.
[43] PoC [10] {A/2/4}; Defence [19(1)] {A/3/7}.
[44] PoC [10] {A/2/4}; Defence [19(2)] {A/3/7}.

16.8. On 24 March 2009, Satoshi uploaded a further version of the White Paper to the SourceForge Bitcoin Project.[45]

16.9. On 2 May 2009, Satoshi asked Mr Malmi to create an FAQ for the SourceForge Bitcoin Project.[46] Later in 2009, Mr Malmi helped Satoshi set up forums for the SourceForge Bitcoin Project.[47]

16.10. In around April 2011, Satoshi delegated responsibility for being the lead core developer of Bitcoin to Mr Andresen. On 26 April 2011, Satoshi transferred a file containing the network alert key to Mr Andresen.[48]

17. The essential dispute between the parties is whether the steps attributed to Satoshi above were carried out by Dr Wright.

18. For the reasons given below, which supplement those in Dr Wright's Skeleton Argument, Dr Wright submits that the evidence demonstrates that he authored the White Paper, created and launched the Bitcoin Software, and took the other steps identified above as having been taken by Satoshi.

A. Skills, knowledge and qualifications

Coding experience

19. Dr Wright answered COPA's attempt to undermine Dr Wright's evidence in relation to his early coding experience[49] as follows:[50]

> Q. Moving on to your early coding experiences, page 7 of this document, paragraph 25 {E/1/7}, you say that your fascination with coding began when you dabbled with C and C++ around about the age of eight or nine, yes?
> A. Mm-hm.
> 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

[45] PoC [7] {A/2/3}; Defence [16(3)] {A/3/5}; {L5/26}.
[46] {L5/53/1}; Malmi Day 13/11-12.
[47] {L5/107/1}; Malmi Day 13/13-14.
[48] {L7/220}, {D/505/34}.
[49] Wright 1 [25] {E/1/7}.
[50] {Day 5/161-163}.

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++.

Q. Dr Wright, you said in your witness statement you dabbled with C++ around the age of eight or nine. That's clear.

You're aware, aren't you, that COPA served evidence from Professor Bjarne Stroustrup, who designed C++? You're aware of that evidence, aren't you?

A. I am.

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.

Q. I see.

20. In light of the above clarification provided by Dr Wright, COPA's point about a potential inconsistency between Dr Wright's narrative regarding his early coding experience and Professor Stroustrup's evidence on when the name C++ was coined falls away.

21. COPA also attempted to downplay the significance of Dr Wright winning a C++ coding competition with the SANS Institute, which was concerned with identifying flaws in the code of certain textbooks.[51] This was put on the basis that the competition was not concerned with "*writ[ing] significant sections of code*", which Dr Wright accepted (subject to the qualification that there was a longer version of the document COPA referred to[52] that involved rewriting the flawed sections of the code more securely). This line of questioning fell short of calling Dr Wright's coding abilities into doubt.

22. Apart from the above examples, COPA did not challenge Dr Wright's coding abilities. COPA also did not challenge Dr Wright's advanced postgraduate qualifications in secure coding, including GSSP-C and GSSP-.Net certification by the Global Information Assurance Certification (GIAC), which is affiliated with the SANS Institute.[53]

23. The Developers' attempt to challenge Dr Wright's coding abilities is addressed separately below.[54]

Academic qualifications

24. COPA did not challenge the primary facts relating to Dr Wright's relevant academic qualifications. In summary:

    24.1. COPA appears not to dispute that Dr Wright undertook his master's degree in statistics from the University of Newcastle and his LLM from the University of Northumbria, which he relies on as particularly important.[55] As explained below, COPA's grounds of attack concern the substance of Dr Wright's LLM documentation.

    24.2. The fact that Dr Wright has numerous degrees and qualifications in relevant disciplines was also not challenged in cross-examination. These include his PhD in Computer Science and Economics and postgraduate degrees spanning many other

[51] {Day 5/164/5 to 165/13}.
[52] {L3/53/1, 4}
[53] {L1/327/1}, {L2/128/1} and {L2/282/1}; and Wright 11 [27] {CSW/1/5}.
[54] See [125]-[128] below.
[55] {Day 6/36/13-16} and {Day 3/55/6-19}.

disciplines, including statistics, game theory, economics and law.[56] It was not put to Dr Wright that these academic credentials are false.

24.3. Dr Wright's other relevant qualifications include several cyber security certifications issued by the SANS Institute, including Global Information Assurance Certificates in forensics analysis, reverse engineering malware and the security of .NET code (mentioned above).[57] COPA accepted that Dr Wright has these qualifications and that they are "*extensively documented*".[58]

24.4. Accordingly, there should be no issue as to whether Dr Wright's evidence in relation to his academic qualifications is accurate. The issue for the Court will be the weight that attaches to those qualifications in the context of determining the Identity Issue. For the reasons summarised in Section II above, it is one relevant factor that goes into the mix.

25. The main disputes between the parties in relation to Dr Wright's academic qualifications concern (i) COPA's plagiarism allegation in respect of Dr Wright's LLM Dissertation and (ii) COPA's forgery allegation in respect of Dr Wright's LLM Proposal. Those issues are addressed below and in Appendix 1.

July 2016 dinner with Mr Hearn

26. COPA has sought to call Dr Wright's skills and knowledge into question by way of the witness evidence of Mr Hearn and, in particular, his account of a dinner in July 2016. In short, Mr Hearn says that during the dinner he "*got the sense [Dr Wright] was routinely talking about things he didn't deeply understand*".[59]

27. Mr Hearn's evidence is unreliable:

27.1. When asked about whether the company (R3) that Mr Hearn worked for at the time of the dinner was a competitor of nChain, Mr Hearn responded that, "*I don't really know what nChain does*"; and "*I think nChain's a Bitcoin-focused company, that's about all I know*".[60] Given Mr Hearn's involvement in the world of

[56] Wright 1 [6] {E/1/3}.
[57] {L1/327/1}, {L2/128/1} and {L2/282/1}.
[58] {Day 6/36/17-20}.
[59] {C/22/6-7} [28].
[60] {Day 14/2/21-25}. See also his slightly expanded answer at {Day 14/11/13-20}.

Bitcoin/blockchain companies, this dismissive answer is unlikely to be the whole truth.

27.2. His evidence is inconsistent with the contemporaneous documents:

(a). His statement concerning what the contemporaneous documents show ("*On re-reading the emails about the dinner it looks like it was Jon who wanted me to meet Craig Wright (rather than the other way round)*"[61]) is inconsistent with the documents in question. These suggest that it was Mr Hearn who asked Mr Matonis to make an introduction to Dr Wright.[62]

(b). After it was pointed out to Mr Hearn that his evidence was inconsistent with the contemporaneous documents, he stated that in fact he had in mind some other emails that had been put in evidence.[63] However, Mr Hearn only submitted a few short exhibits and there is no alternative candidate for these "*other emails*". The reality is that Mr Hearn must have been referring in his statement to the emails included in his exhibit MCH-4, but was trying to come up with an excuse for the inconsistency between those documents and his evidence.

27.3. His oral evidence sought to give a different impression about the quality of his recollection to the more careful approach he had taken in writing:

(a). In the witness box he was keen to emphasise the quality and reliability of his recollection. For example:[64]

> 5 Q. So, understandably, you couldn't remember the detail of
> 6 what happened that far back; is that fair?
> 7 A. Well, I think I remember most of it, yeah. Actually,
> 8 when we talked about the refreshing the detail, it was
> 9 things like the name of the restaurant, or the exact
> 10 date on which it happened. So, those details I had
> 11 forgotten, indeed, but the actual discussions that
> 12 happened during the dinner, I feel I remember pretty
> 13 well.
>
> […]

[61] {C/22/5} [23].
[62] {D/507/2}.
[63] {Day 14/8/19 to 9/5}.
[64] {Day 14/4 and 6-7}

20 Q. You see, when somebody tells a story about events
21 happening eight years earlier and there's
22 a contemporaneous record which is not consistent
23 with it, it does perhaps --
24 A. Yes, I understand.
25 Q. -- suggest that the memory may not be quite accurate.

1 Is that a fair point?
2 A. Well, I think the parts I remember are the important
3 parts, which are what happened during the dinner and
4 what Craig Wright said.

(b). By contrast, in writing he was more careful in accepting the limitations with his recollection of what happened during the dinner.[65] Apart from one specific example of a technical question he asked Dr Wright (relating to "SIGHASH_SINGLE" [66]), his statement made clear that he could not remember anything else about the detail of the discussions: "*I think there were additional technical questions I asked, I can't remember the exact details…*"[67]

(c). This tension between his written and oral testimony detracts from the credibility of his evidence.

27.4. Mr Hearn accepted that Mr Matthews said at the time of the dinner that the reason Dr Wright could not answer some of Mr Hearn's questions was that they related to matters that Mr Matthews regarded as confidential / relating to intellectual property:[68]

21 Q. I mean, what he was trying to do was to get Dr Wright
22 perhaps to be less talkative about matters which he
23 regarded as being confidential and should be kept from
24 you. You didn't get any impression along those lines?
25 A. Well, that's what he said at the time, I think.

1 Q. He did say that, though?
2 A. Well, I think so, yeah.

This is therefore an aspect of Mr Matthews' evidence (see further below) that is clearly corroborated by Mr Hearn. The most likely explanation for that is that Mr

[65] See further {Day 14/9/7 to 11/1}.
[66] {C/22/6} [26].
[67] {C/22/7-8} [28].
[68] {Day 14/23-24}. An equivalent concession was made in his witness statement: Hearn 1 [25] {C/22/6}.

Matthews was keen to ensure that such confidential matters were not pursued further.

27.5. Mr Hearn, however, was reluctant to accept that the explanation he was given at the time (i.e. Mr Matthews' explanation as to why Dr Wright was not going to answer certain of Mr Hearn's questions) was true. His reason for not accepting Mr Matthews' explanation was apparently based on the fact that, "*I didn't believe you could really file patents on… things that have been published already, like Bitcoin… and certainly Satoshi never expressed any interest in patents to me previously…*".[69] Given his own commercial activities, it is implausible that Mr Hearn did not believe that patents could be filed on Bitcoin/blockchain-related technology.

27.6. He acknowledged that he did not sign a non-disclosure agreement (albeit he does not recall being asked to sign one)[70]; and he reluctantly accepted that there was at least a degree of competition between R3 and nChain.[71]

28. Mr Matthews explained what took place at the dinner.[72] Mr Hearn "*asked a lot of detailed technical stuff*" that was in Mr Matthews' view "*heavily related to a number of the patent filing activity that nChain was currently undertaking*", with the result that he told Dr Wright not to answer them.[73]

29. Dr Wright's evidence is consistent with Mr Matthew's account. Dr Wright explained in cross-x that "*[w]hat Mr Hearn was actually doing was probing areas that I was doing research into*" and "*probing into some of the patents I've filed and where they were going*".[74] In Wright 11, Dr Wright set out in further detail that (i) R3 was a competitor of nChain; (ii) Mr Hearn was then working on a system that would directly compete with Bitcoin; (iii) questions that Mr Hearn was asking related to matters that were covered by patent applications then being filed by nChain, including the Intelligent Daemon System which involved use of SigHash_Single;[75] (iv) the competition between R3 and nChain is

[69] {Day 14/23/1-9}.
[70] {Day 14/11/2-6}.
[71] {Day 14/11/21 to 12/8}.
[72] {Day 12/80/23 to 83/5}.
[73] {Day 12/81/25 to 82/4}.
[74] {Day 8/87/22 to 88/6}.
[75] {CSW/84}

demonstrated by R3's filing of a patent on 22 August 2016 which overlapped with a patent application filed by nChain on 29 July 2016.[76]

30. For the reasons given above, the Court is invited to accept Mr Matthews' (and Dr Wright's) account of the dinner, rather than Mr Hearn's.

B. Investment in evolution of digital cash systems

31. Dr Wright has explained that, since the early 1990s, he has been deeply invested in the evolution of digital cash systems, with a focus on developing systems capable of facilitating micropayments. In this context he relies in particular on his work at OzEmail [77] and project 'Blacknet', which he undertook through his company DeMorgan.[78]

32. In cross-examination Dr Wright explained the relevance of his work at OzEmail, including in particular the Millicent project, as follows:[79]

> Q. You refer in your witness statement to working at OzEmail. Do we see that that's referred to as a job you did between 1996 and 1997?
> A. I do.
> Q. And as you say there, that was managing a corporate technical team associated with large corporate clients of OzEmail?
> A. Yes. This was in the 90s, so we developed the code for the clients, we built systems, we customised code. It was all in CC++. The majority of the systems were in either DEC, or Solaris, and we did things like implementing altered versions of DNS, we implemented web servers. Web servers weren't like now, where you just run up a simple platform, we had to build them. We build code, including for New South Wales schools --
> Q. Can I pause you there, Dr Wright, because I'm not sure I'd got to a question other than asking you to accept
>
> that you had done that job.
> You've referred in your statement to the company working on a payment protocol called "Millicent"; you recall that?
> A. I do.

[76] Wright 11 [435]-[462] {CSW/1/82-87}.
[77] Wright 1 [29] {E/1/7-8}.
[78] Wright 1 [26]-[34] {E/1/7-8}.
[79] {Day 5/166-168}.

6 Q. All you say about it is that it was an efficient payment
7 system that wasn't encrypted, yes?
8 A. It used digital signatures. It's similar to Bitcoin in
9 that manner. It also used script, or scrip, which was
10 used as a way of programming the exchanges.
11 Q. You haven't provided any documents about it, have you?
12 A. I believe I have. There are some of the documents on
13 Millicent in my research.
14 Q. It wasn't, in any sense, a precursor to Bitcoin, was it?
15 A. No, that's actually incorrect. Bitcoin uses
16 a Forth-based system, so the scripting language in
17 Bitcoin is based on Forth, which most old people like me
18 remember. On top of that, similarly, so was scrip.
19 Script and Bitcoin and scrip are analogous; they work
20 exactly the same way. The distinction is that Millicent

21 couldn't find a way of distributing the server and
22 required each merchant to run their own version of
23 script as a bank. So, one of the problems, of course,
24 is, how do you convert scrip in merchant A from scrip to
25 merchant B, how do you keep them equal, either that or

1 you need a bank, once again, so therefore it didn't
2 work.

33. In response to COPA's suggestion that the Digital Equipment Computer Users' Society had nothing to do with digital cash (an attempt to undermine Dr Wright's evidence that by the late 1990s Dr Wright was "*deeply engaged with the budding digital cash industry*"[80]), Dr Wright corrected COPA as follows:[81]

24 Q. Dr Wright, I'm not suggesting that you weren't
25 interested in computers, but it had nothing to do with

1 digital cash, did it?
2 A. Actually, it did. Millicent was created by DEC, and
3 Millicent was a protocol that was being promoted by
4 Digital Equipment Corporation before Compaq took them
5 over. Now, when Compaq took them over, they closed all
6 that, because they weren't interested in things like
7 AltaVista. AltaVista didn't get the funding; that's why
8 Google exists.
9 Now, DEC wanted to create an internet that was
10 micropayment funded. Now, if they'd done that, rather
11 than an ad-based internet we see now, it would have been
12 lots of small payments in fractions of a cent. What
13 they couldn't figure out was how to have the system

[80] Wright 1 [30] {E/1/8}.
[81] {Day 5/169-170}.

14 distributed so that no one would be able to, like, have
15 to go through all multiple exchanges, and that would be
16 terrible. Imagine if you buy from merchant A, get their
17 script, have to now go to NatWest, change it again to go
18 to Lloyds, change it again to go, sort of -- what do you
19 call it -- buy your car, or pay for your fuel, change it
20 again to go somewhere else. So, not having
21 a distributed version of cash that could run everywhere
22 was their downfall. Unfortunately, Compaq had no
23 interest and it got closed.

34. When COPA attempted to challenge Dr Wright's evidence that DeMorgan was "*a platform through which I could conduct extensive research and development in digital cash and continue my work in information security*"[82], Dr Wright rejected COPA's contention and explained the significance of project 'BlackNet' as follows:[83]

17 Q. There's not a shred of evidence, is there, that DeMorgan
18 did any work on digital cash in that period, is there?
19 A. No, actually, there is quite a lot. BlackNet is
20 actually premised on crypto credits. So, the part you
21 mentioned before with b-money, the first paragraph of
22 b-money quotes Tim May and goes into the history of
23 BlackNet. BlackNet basically had crypto credits.
24 The proposal that you're mentioning that Wei Dai
25 mentioned was, I could extend crypto credits in a new

1 way. He never actually did it. I, actually, at that
2 stage, thought he would have, but he didn't continue.
3 So, what I did was trying to take an encrypted internet,
4 and the only way that is viable to make this sort of
5 distributed encrypted system is to have it economically
6 valued. Now, that meant that proof-of-work tokens would
7 be at small -- small integers of exchanges so that all
8 the transactions you mentioned before, the grabbing
9 a web page, the doing a search, the sending an email,
10 would be both economic transactions and transactions on
11 a server.
12 Q. Dr Wright, I should have put it in this way. Other than
13 the DeMorgan documents which we've put to you are fake,
14 there's not a shred of evidence that DeMorgan was
15 involved in digital currency, is there?
16 A. No, actually, you have given me AusIndustry documents,
17 both ones that -- some of those were in court cases in
18 Australia. So, in 2004, I was in a court case in
19 Australia and those documents were put forth. They were
20 put forth in the other part of the DeMorgan case in 2008

[82] Wright 1 [33] {E/1/8}.
[83] {Day 5/171-173}.

> 21 and 9. Now, they mention the AusIndustry area for
> 22 BlackNet. And there's only one BlackNet. BlackNet is
> 23 an encrypted internet based on crypto credits. That
> 24 morphed into Bitcoin and Metanet.
> 25 Q. Dr Wright, you produced a whole series of Bitcoin -- of
>
> 1 BlackNet documents, which we looked at, that say nothing
> 2 about crypto credits, didn't you?
> 3 A. You don't actually need to, but if you read BlackNet,
> 4 you see that the foundational part of it is
> 5 crypto credits. So, BlackNet is, as I said, an
> 6 end-to-end encrypted internet. My end goal, my Lord,
> 7 isn't Bitcoin, like they say, it is to create, like it
> 8 says in the White Paper and I've said to Martti Malmi,
> 9 Adam Back and all your witnesses, a timestamp server
> 10 that can have the integrity of data saved over time, and
> 11 economically, viably, way of transferring information.

C. Precursor work and discussions

35. Dr Wright worked on a number of projects from the late 1990s onwards which are relevant or related to the technology and concepts underpinning Bitcoin. This included work he carried out for the Australian Stock Exchange, Lasseters online casino, Vodafone, and BDO, as well as his LLM thesis.

Australian Stock Exchange

36. The relevance of Dr Wright's role in 1996 as Head of Information Security for the Australian Stock Exchange lies in his development of a system for the exchange of dematerialised information or tokens which played a significant part in his later development of Bitcoin.[84] In the course of questioning on a project 'BlackNet' document,[85] Dr Wright explained the significance of the "*NIPPA system*" that he built for the Australian Stock Exchange as follows:[86]

> 24 So the work, for instance, in the NIPPA network in
> 25 the Australian Stock Exchange, what we did with as we
>
> 1 integrated brokers, because they weren't a company then,
> 2 it was a mutual, and every single broker, no matter how
> 3 small, had to get the packet at the same time. So we
> 4 had to not only broadcast but do it in a way that went

[84] Wright 1 [36] {E/1/8}.
[85] {L1/79/1}.
[86] {Day 2/65-66}.

5 round the whole of Australia, and Australia's big,
6 I mean, it's like Europe, and someone in Perth and
7 Brisbane had to get it at the same time as Sydney. So
8 our NIPPA network and the protocol had to create a
9 peer network to send these transactions,
10 the transactions being the shares, the brokers,
11 the people actually making bids and orders. So --
12 Q. Can I just pause you there, because this says nothing
13 about the NIPPA network, does it?
14 A. Oh, no, this was used in the NIPPA network. So, this
15 was 2002. I was actually building this for NIPPA and
16 ASX. So, I don't need to say "NIPPA network", but that
17 was where I was deploying is. So when you look at
18 the ASX documents that I've also got you'll see that
19 the firewall and the structure was there. I mean, I
20 actually it was beautiful. I mean, we had a distributed
21 network sending on very low high latency networks across
22 the whole of Australia at a time that no one believed
23 it. […]

Lasseters

37. The evidence of Mr Archbold, who engaged Dr Wright to work for Lasseters, supports Dr Wright's evidence on how that work influenced the development of Bitcoin, including for example the "*advanced security measures and logging systems*" that were "*an early precursor to the blockchain*"[87]. Mr Archbold explained that Dr Wright's work at Lasseters in around the late 1990s / early 2000s on the storage and compression of logs was "*something that [Dr Wright] developed himself*"[88]; and that he believed Dr Wright when the latter explained that the encryption he was using was vastly superior to the "*standard hashing algorithm*".[89]

38. The focus of the cross-examination on Dr Wright's work for Lasseters was on the absence of an express reference to "*digital cash*" in a number of documents relating to his work for Lasseters (including a version of Dr Wright's CV). As Dr Wright explained, this line of attack involved too narrow a reading of the documents in question:[90]

13 Q. Now, just this question, focusing on the question:
14 there's nothing about digital cash work for Lasseter's
15 in your LinkedIn profile, the BDO CV or the McCormack

[87] Wright 1 [38]-[44]{E/1/9}ff.
[88] {Day 10/23/3-25}.
[89] {Day 10/24/6-14}. The point is borne out by Dr Wright's Secure Network Design for Lasseters, which included reference to Diffie-Hellman encryption algorithms: {L1/21/112}.
[90] {Day 6/11-12}.

16 statement, is there?
17 A. No, that's not correct. When I stated "architecture",
18 that meant the whole environment. So, at that point,
19 I hadn't actually created a digital cash system that
20 worked for them. What I had done was architect
21 a logging solution that was effectively token-based. We
22 had a hash chain-based system for the logs that ran on
23 a binary tree structure. Each of the logs were then put
24 into a series of rounds and every hour or so the --
25 the block of log information would be sent. This would

1 enable the Northern Territory government, over a slow
2 line that was often congested, to always know that
3 the logs couldn't be changed and when they had the full
4 copy of them, the integrity could be trusted.
5 Q. Dr Wright, I'm going to ask you the question again.
6 Digital cash, the words or system "digital cash", didn't
7 appear in any of those documents, did it?
8 A. Not in a one liner, no, but "architecture" includes
9 that.

39. Dr Wright's work at Lasseters also involved tripwire,[91] which is analogous to the process of timestamping and storing of the hash of a file later discussed between Satoshi and Mr Malmi in the context of Bitcoin: it is not a standard security process, contrary to COPA's suggestion.[92]

40. The close and direct connection between Dr Wright's work on online gaming security systems whilst at Lasseters (and subsequently for CentreBet) is further evidenced by inclusion of poker code in the original version of the Bitcoin source code: see e.g. Bitcoin code extracts at {L20/320/48}, referring to "*CPokerLobbyDialogBase*", and {L20/344/16} referring to a series of poker lobby code commands such as "*buttonDealHand*" and "*buttonLeaveTable*". Dr Wright explains in his witness statements that the embedded code featured functions necessary for the basic operations of a poker game and was an extension of software he had developed for incorporation into Lasseters' platform. His experience with Lasseters provided him with "*unique insights and experiences that were instrumental in the creation of Bitcoin*".[93] None of this evidence was challenged in cross-x.

[91] See, for example: {L1/21/51} and {L1/36/21}. Dr Wright also worked on later; see, for example: the DeMorgan R&D Plan {L5/15/13} and Dr Wright's book {L2/487/14}.
[92] See Bitcoin FAQ at {L5/54/14-15}, discussed further below.
[93] Wright 11 [1211] {CSW/1/207}. See also Wright 1 [43]-[44] {E/1/10} and Wright 11 [1212]-[1213] and [1435] {CSW/1/207} and {CSW/1/236}.

41. Mr Archbold's evidence confirms Dr Wright's skills in building secure systems. He explained that, after repeated failures by Deloitte to build a security system for Lasseters that passed the Northern Territory government's audits, Dr Wright was recruited to solve the problem (and swiftly did so).[94]

42. Dr Wright's professional background in the online gaming industry underlines his unique blend of skills, interests and experiences which connects him directly to Bitcoin's creation.

Vodafone

43. The evidence of Mr Jenkins supports Dr Wright's evidence[95] on the relevance of his work at Vodafone (in around 1998 to 2002) to the development of Bitcoin:

    43.1. Mr Jenkins explained the reference in his evidence to a "*genesis log entry*"[96] as follows:[97]

> 3 Q. Now, you mentioned "genesis log entry" because,
> 4 I presume, the Bitcoin Blockchain starts with
> 5 the Genesis Block. Is that why this is included in your
> 6 evidence?
> 7 A. It's included in my evidence because my recollection is,
> 8 from that long ago, as it was being described and as we
> 9 were disappearing down a rabbit hole around how you
> 10 could protect a log file from it being tampered and
> 11 tampered with, we were going through a minutiae of
> 12 scenarios, and the description that Craig gave me at the
> 13 time involved things like hashing the serials, hashing
> 14 the serial numbers associated with the log file, and
> 15 then we were talking about then, well, how do you
> 16 differentiate between an operational log file and a new
> 17 log file, you know, could a new one be started to kind
> 18 of make it look like it was an existing operational log
> 19 file. At the time when Craig was describing this to me,
> 20 he made reference to a genesis log file entry as part of
> 21 the first transaction, if you like, into the log file.

    43.2. In response to this answer, it was put to Mr Jenkins that he did not mention "*hashing*" in his witness statement.[98] It was not put to him that the conversations

[94] {Day 10/19/5-16}; {E/11/3} [7].
[95] Wright 1 [45]-[47] {E/1/10}.
[96] {E/6/4} [11].
[97] {Day 9/50}.
[98] {Day 9/50/22-24}.

he describes did not take place. Nor was Mr Jenkins' evidence on the timing of these conversations (i.e. when Dr Wright was carrying out his work for Vodafone) challenged.

43.3. Given the nature of the work undertaken by Dr Wright for Vodafone, Mr Jenkins rejected COPA's contention that Dr Wright was engaged by Vodafone for "*standard IT security work*":[99]

> 5 And it's true, isn't it, that the work that DeMorgan
> 6 was doing for Vodafone was standard IT security work?
> 7 A. Look, it depends what you mean by "standard IT security
> 8 work". It was an evolving area back in the late '90s.
> 9 So at the time, I wouldn't call it standard IT security
> 10 work, no.

44. The cross-examination of Dr Wright in relation to his work at Vodafone was limited. The only point that was put to Dr Wright is that a version of his CV[100] described the work in terms that COPA sought to characterise as "*straightforward IT security*" work.[101] This is a weak point, given the inherent limitations with any CV. In any event Dr Wright explained in response that his work for Vodafone involved essentially a "*hash chain-based system*", which is consistent with the evidence of Mr Jenkins referred to above.

45. As Dr Wright explained, the common thread to much of this precursor work (including in particular Vodafone and Lasseters) lies in the concept of immutable logging and the idea of a timestamp server:[102]

> 7 […] the firewalling and logging systems that we're
> 8 talking about, like for Vodafone, Lasseter's, etc, were
> 9 all on an early version of what became Bitcoin. They're
> 10 a hash chain system. So, the error is focusing on
> 11 cryptocurrency. Bitcoin was never primarily about
> 12 a cryptocurrency, it was really about timestamp server,
> 13 as it says in the White Paper, and the concept of
> 14 immutable logging.

[99] {Day 9/48}.
[100] {L2/102/3}.
[101] [Day 6/13/6 to 14/11}.
[102] {Day 5/176}.

BDO

46. Mr Matthews, Dr Pang and Mr Sinclair provide relevant supporting evidence on the links between Bitcoin and his work during his time at BDO.[103]

47. Mr Matthews confirms that Dr Wright discussed his interest in digital cash with him in 2007 and 2008: [104]

    47.1. He was not initially challenged on the veracity of that evidence. The only point that was initially put to Mr Matthews on that topic was that "*Centrebet didn't actually engage him to produce a digital currency project or system*", which Mr Matthews accepted.[105]

    47.2. In a subsequent question, he was challenged on this point in the following terms:[106]

> 8 Q. And the idea that Dr Wright had elaborate digital
> 9 currency plans in 2007/2008 is also a lie, isn't it?
> 10 A. No, it's not. There are -- Dr Wright made a submission
> 11 to Centrebet in early 2009 which, had I agreed to
> 12 the funding proposition, would have been, in my opinion,
> 13 the furthest application built on the back of Bitcoin.
> 14 It was by his company Information Defense and it was to
> 15 provide a timestamp server log, immutable log system to
> 16 protect our corporate network.

    47.3. Thus, Mr Matthews is able to link the conversations he was having with Dr Wright about digital currency in 2007/2008 to a proposal made to Centrebet's security sub-committee at some point in 2009 (which is addressed further below).

48. Dr Pang was cross-examined on the project he worked on with Dr Wright at BDO from around July 2008 to 10 October 2008.[107] This project used "*GEOMI visualization software*" and was concerned with "*network visualization and/or network analysis*". Dr Pang's evidence on this topic, the substance of which was not challenged in cross-

[103] See Wright 1 [48]-[55] {E/1/10-12}.
[104] See Matthews 1 [21]-[23] {E/5/5}.
[105] {Day 11/89/11-21}.
[106] {Day 11/104}.
[107] {Day 9/15/3 to 24/20}; the presentation relating to the project is at {L3/235}.

examination, remains consistent with Dr Wright's evidence on the influence of "*small-world networks*" and related concepts on the early development of Bitcoin.[108]

49. Dr Pang was not challenged on his evidence relating to Dr Wright's improvement to the "*Diffie-Hellman equation*", which he was shown when Dr Wright was still at BDO and (as Dr Pang later came to understand) is relevant to Bitcoin.[109]

50. In relation to Mr Sinclair's evidence, the following exchange during Dr Wright's cross-x is relevant:[110]

> 5 Q. Dr Wright, take this in stages. First of all, I suggest
> 6 to you, and the court can make its own mind up on
> 7 the basis of Mr Sinclair's transcript, but in
> 8 the Granath trial, Mr Sinclair made it very clear that
> 9 he had no recollection of discussing a prospective
> 10 E cash system with you, right?
> 11 A. No. As I've noted multiple times, Timecoin was
> 12 the system I was trying to run. Bitcoin is only
> 13 the economic system behind it. It's like crypto credits
> 14 in BlackNet. So, Bitcoin is not the end game, Bitcoin
> 15 is probably 0.01 of what I'm building, my Lord. Now,
> 16 what I'm building does not work unless I have an
> 17 economically viable system behind it, micro payments,
> 18 etc. So the system that I was building, timestamped,
> 19 recorded information, had distributed integrity
> 20 monitoring for files, etc. But to do that, I need
> 21 Bitcoin, scaled.

51. This is consistent with Mr Sinclair's evidence that, in the context of discussions about alternatives to traditional banking, Dr Wright was interested in improving security systems by "*better logging of the transactions*" in terms similar to what would now be described as blockchain.[111]

LLM thesis/proposal

52. Dr Wright has explained how his LLM informed his vision for Bitcoin[112].

---

[108] Wright 1 [53]-[55] {E/1/11-12}.
[109] Pang 1 [24]-[25] {E/10/9}.
[110] {Day 6/20}.
[111] {E/19/3}.
[112] Wright 1 [56]-[60] {E/1/12-13}.

53. COPA accepts that Dr Wright's (final) LLM Dissertation is authentic. This is significant because the dissertation includes reference to concepts that have parallels to the approach to financial transactions in the White Paper, including decentralisation, peer-to-peer transactions and the role of trust and intermediaries in the digital domain. For example, Dr Wright's Dissertation considers (i) issues of trust surrounding online payments, (ii) difficulties in transferring cash payments over large distances and between people who may never have met and may never meet creating the need for payment intermediaries in internet transactions, and (iii) development of peer-to-peer payment systems as an alternative to centrally minted digital cash. Dr Wright's evidence is that his work on these subjects influenced his work on Bitcoin.[113]

54. The focus of COPA's attack on the (final) LLM Dissertation is an (unpleaded) allegation of plagiarism:

54.1. The reason that the plagiarism allegation is unpleaded is that the Court has already found that the "*potential probative value*" of the allegation is "*so slight*" that COPA was refused permission to plead it.[114]

54.2. At the time of that argument about permission to amend, however, Dr Wright accepted that COPA would be entitled to cross-examine Dr Wright on the allegation that he copied passages from the identified works of Ms Pearson.

54.3. During his cross-examination on this subject, Dr Wright explained that the referencing error is a result of his use of "*EndNote*":[115]

> The initial versions of your dissertation which were produced did not credit Ms Pearson at all, did they?
> 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 made. So while her name was noted in footnotes, it was not put in the bibliography
>
> of the document.
> Q. Dr Wright, there are in this article, and we looked -- in your dissertation, we looked particularly from

[113] LLM Dissertation: {H/224.1/16, 25-26 and 51}; Wright 1 [58] {E/1/12}.
[114] {B/27/21-22} [77]-[79].
[115] {Day 6/27-28}.

4 the first page we considered, there are chunks which are
5 identical to Ms Pearson's not quoted, not in quotation
6 marks and not referenced; correct?
7 A. In that version, yes. The other version actually had it
8 -- what do you call it -- in italics and referenced.
9 Q. In italics, you say?
10 A. Yes.
11 Q. In quotation marks?
12 A. No, in italics. Italics actually works for block text.
13 Q. Dr Wright, far from your LLM dissertation representing
14 inventive thinking of a very high order, pre-figuring
15 the Bitcoin White Paper, these colour-coded passages
16 show that, in large parts, it was made up of plagiarism,
17 wasn't it?
18 A. No, that's not correct.

55. There is a separate issue as to whether Dr Wright's LLM Proposal, which includes several passages that closely reflect passages in the White Paper, is a forgery. That issue is addressed separately below.[116]

56. It is also worth noting that Mr Bridges confirmed during cross-examination that Dr Wright would have sent him his LLM proposal (or something similar).[117]

Discussions

57. The evidence in relation to Dr Wright's discussions with individuals about the concepts in the White Paper (or similar concepts) prior to its release is summarised below.

58. Dr Wright had a number of relevant discussions with Mr Jenkins about related concepts to those that would later appear in the White Paper:

58.1. Mr Jenkins was cross-examined at some length about his discussions with Dr Wright about "*eGold*" in around 2000-2002.[118] His evidence withstood the test: COPA's attempt to sow seeds of doubt about the timing of these conversations did not bear fruit. In particular:

(a). The attempt to challenge Mr Jenkins' evidence on the timing point by reference to when Paypal and eBay were launched[119] foundered when Mr

[116] See Section V and Appendix 1.
[117] {Day 11/10/4-10}; cf. Bridges 1 [23] {E/9/7}.
[118] {Day 9/54/5 to 65/24}.
[119] See Jenkins 1 [15] {E/6/5}

Jenkins clarified that he had in mind when PayPal and eBay were "*readily available in Australia*" (and he was not challenged in relation to that clarification).[120]

(b). The attempt to suggest there was a material inconsistency between Mr Jenkins' evidence in the Granath Proceedings on the timing of the "*eGold*" discussions (2001) and his evidence in these proceedings (2000-2002) – which is not a material inconsistency in any event – did not make any headway and Mr Jenkins was thanked for his clarification.[121]

(c). When Mr Jenkins was challenged more directly on the quality of his recollection, the questions were linked to an irrelevant point about his recollection of the names of the **competitors** of "*eGold*".[122]

58.2. Mr Jenkins was asked about his discussions with Dr Wright about "*grid computing*" (which involved splitting computational tasks among nodes) in around mid-2007.[123] The nub of the point that was put to Mr Jenkins was that he was "*looking back on these conversations through the prism of hindsight*".[124] This line of questioning was vague; it is unclear what other prism might be used to look back on past events; and ultimately there was no meaningful challenge to his evidence regarding these conversations.

58.3. Mr Jenkins was not challenged (at least clearly) on the fact that he had discussions with Dr Wright about "*achieving trust other than in a central bank*" towards the end of 2007 or early 2008.[125]

59. Dr Wright had discussions with Mr Archbold about digital currency in around 2004 or 2005, during Mr Archbold's second stint at Lasseters:

59.1. The relevant exchange on this topic was as follows: [126]

1 Q. Now can we please go back to your statement,

[120] {Day 9/55/3 to 56/9}.
[121] {Day 9/56/10 to 58/6}.
[122] {Day 9/64/3 to 65/24}.
[123] {Day 9/73/21 to 77/1}.
[124] {Day 9/75/22-23}.
[125] Jenkins 1 [16]-[25] {E/6/5}ff.
[126] {Day 10/27-28}; {E/11/5} [15-16].

paragraph 15, which is on page 5 {E/11/5}. In paragraphs 15 and 16, you say that you recall discussing in around 2004 or 2005 about digital currency with Dr Wright. And then in paragraph 15, you quote precisely a conversation.

Now, you recall Dr Wright asking:

"Have you heard about this digital currency?"

Now, you never recorded that conversation in writing contemporaneously, did you?

A. No, no. It was a discussion, because, you know, back in 2004/2005, all the -- the 2000s, any discussions regarding cryptocurrency, digital currencies, anything like that was just a big no-no with the Northern Territory government. Any regulatory body wouldn't touch them back then, and nor would the financial regulatory bodies. So, it was purely just a discussion, you know, and I bounced it off a couple of people that I knew, apart from Craig, who had brought it to me, and I bounced it off a couple of people and -- and got their opinions on it.

Q. Mr Archbold, you can't have been talking about cryptocurrency back then, that wasn't a term that was coined until many years later?

A. Well, then, you know, digital currency.

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?

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".

Q. And, Mr Archbold, there's no mention of any of that in your statement, is there?

A. No.

59.2. Although Mr Archbold realistically acknowledge he could not be sure of "*the precise date or words that were spoken*", that acknowledgement has little significance in circumstances where:

(a). Mr Archbold had already accepted he did not recall exactly when the conversations took place, save that it was during his second stint at Lasseters (which ended in November 2008).

(b). He therefore gave a reasonably broad range for when the conversations took place (i.e. around 2004 or 2005).

(c). As explained in his witness statement, he was able to say with a degree of confidence that the conversations happened before 2005 owing to the point at which Neil Howard left Lasseters.[127]

(d). The relevance of Mr Archbold's evidence on this point is not impacted by precisely when the conversations took place within the range given by Mr Archbold (and it was not suggested that they might have taken place in 2009 or after).

(e). The precise words that were spoken also do not matter: the relevant point is simply that Dr Wright and Mr Archbold were discussing digital currency in around 2004/2005.

60. Mr Yousuf was not challenged on the fact that he had discussions with Dr Wright about digital currency and how the financial system was flawed as far back as 2006; and that, prior to 31 October 2008, Dr Wright talked about the problem-solving capabilities of "*distributed networks*". [128] The cross-examination on this issue was directed towards establishing that the concepts under discussion had "*been around for a long time*" or were "*common features*" of cybersecurity.[129] Even if that were correct (which is not accepted), it would not detract from the point that such discussions concerned similar concepts to those that appear in the White Paper.

61. It should also be noted that Mr Yousuf was cross-examined at length (over 1.5 hours) on a number of irrelevant points relating to the ATO's investigations of one of Dr Wright's companies (C01N) that Mr Yousuf was involved with for some time.[130] As became increasingly clear, the idea was to put to Mr Yousuf that "*Dr Wright must have known he wasn't telling the truth*" when he made certain representations to the ATO.[131] Of course, such matters would need to have been put to Dr Wright, but were not. This line

[127] Archbold 1 [15] {E/11/5}.
[128] Yousuf 1 [8] and [15] {E/7/3-4}.
[129] {Day 9/111/5 to 112/22}.
[130] {Day 9/112/23 to 171/11}
[131] For example, {Day 9/161/4-8 and 167/8-12}.

of questioning did not advance matters. Nor did a similar line of questioning with Dr Pang.[132]

62. Mr Matthews' evidence that he and Dr Wright had relevant discussions about digital cash systems in the latter part of 2007 and into 2008 has been addressed above.

63. As for Dr Pang's account of the occasion when Dr Wright mentioned blockchain to him on 1 August 2008, when Dr Pang purchased a Batman Lego set (for which he has the receipt):[133]

63.1. It was put to Dr Pang, in general terms, that his recollection was "*hazy*" and "*not reliable*"[134]. It was not put to Dr Pang (directly, or at all) that the conversation did not take place when he says it took place (i.e. 1 August 2008). This is unsurprising given that Dr Pang has a firm anchor point in the form of his receipt.

63.2. In response to the contention that his recollection was hazy and unreliable, Dr Pang realistically acknowledged that his memory was imperfect but remained firm on the two points that matter, namely (i) the date it took place and (ii) the fact that the word "*blockchain*" was mentioned:[135]

> 13 Q. All I'm suggesting to you, Dr Pang, is that this hazy
> 14 recollection of a nonsensical conversation is not -- if
> 15 you're being fair to yourself, is not a reliable
> 16 recollection.
> 17 A. That is not a reliable recollection, but the date in
> 18 which I bought the Lego set and the fact that he said
> 19 the word "blockchain" was 100% clear in my mind to be
> 20 true.
> 21 Q. Well, Dr Pang, in the context of this very strange and
> 22 hazy recollection, I suggest to you that picking out one
> 23 word and trying to remember it as absolutely what he
> 24 said is not reliable.
> 25 A. The receipt and the fact that I bought the Lego set is
>
> 1 completely reliable. You have got a date –

[132] {Day 9/37/13 to 44/3}.
[133] {Day 9/24-33}; the receipt dated 1 August 2008 is at {L3/57/1}.
[134] {Day 9/32/13-16}.
[135] {Day 9/32-33}.

63.3. In light of this evidence, the Court is invited to find as a fact that he mentioned "*blockchain*" to Dr Pang on 1 August 2008. For obvious reasons, this is a significant fact in the context of the Identity Issue.

D. Drafting, sharing and releasing the White Paper

64. Dr Wright's evidence is that the White Paper was produced using both OpenOffice and LaTeX. That issue is dealt with separately in Section IV below.

65. The evidence of Mr Matthews, Don Lynam and Max Lynam support Dr Wright's evidence on sharing drafts of the White Paper prior to its release in October 2008.

66. Mr Matthews was cross-examined about his evidence that he received a draft of the White Paper in around August 2008.[136] Broadly speaking, COPA's challenges to Mr Matthews' evidence on this important topic fell into the following three categories:

66.1. First, an indirect attempt was made to challenge the evidence on the basis that "*this story about you receiving a copy of the Bitcoin White Paper has been a significant part of the pitch from these companies [i.e. nChain and Squire Mining] to the market*".[137] Mr Matthews dealt with the point robustly, pointing out that these were simply statements of fact rather than "*pitches to the market*".

66.2. Second, it was put to Mr Matthews that in a number of respects the account given by Dr Wright and Mr Matthews in relation to this incident are "*very different*".[138] However, the fact that there are differences – for example on whether the document was provided in hard copy or on a USB stick[139] – is to be expected in relation to events that took place a significant number of years ago; and such differences only add to the credibility of Mr Matthews' account (and detracts from COPA's theory that his evidence amounts to a coordinated and/or commercially motivated lie).

66.3. Third, it was put to Mr Matthews that, "*[o]n 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?*" [140] The point being made was that there were no

[136] {Day 11/89/22 to 104/7}.
[137] E.g. {Day 11/93/4-13}.
[138] The same point was put to Dr Wright {Day 6/119/12 to 123/19}.
[139] {Day 11/98/22 to 99/9}.
[140] {Day 11/98/10-16}. See also {Day 11/103/9-11}.

documents or other witnesses to corroborate their account. Mr Matthews accepted this limitation with his evidence – another illustration of his straightforward and credible answers.

66.4. None of these lines of questioning did any particular damage to Mr Matthews' evidence.

67. At the end of his evidence, the Judge asked Mr Matthews a question regarding his "*anchor points*" for the timing of Dr Wright's provision of a USB stick in August 2008:

67.1. The relevant exchange was as follows:[141]

11 MR JUSTICE MELLOR: Mr Matthews, there are a couple of
12 things you can help me with.
13 First of all, in your witness statement, you talk
14 about the USB stick --
15 A. Yes.
16 MR JUSTICE MELLOR: -- provided to you in August 2008 and
17 yet you give no detail as to how you date it
18 to August 2008. Do you have any anchor points?
19 A. Well, the anchor point, of course, is that the White
20 Paper itself was released publicly 31 October. So
21 I know that it was before that occurred.
22 MR JUSTICE MELLOR: How do you know that?
23 A. Because the White Paper didn't exist when I was looking
24 at this thing.
25 MR JUSTICE MELLOR: How do you know that?

1 A. Because I would have known if the White Paper had been
2 released.
3 MR JUSTICE MELLOR: Why?
4 A. It would have been public.
5 MR JUSTICE MELLOR: You mean, as soon as it was released, it
6 was well known?
7 A. No, no, that's not the case.
8 MR JUSTICE MELLOR: Okay.
9 A. I think I understand what you're getting at. That
10 was -- that's my best understanding of how to place it
11 in the 2008 calendar.
12 MR JUSTICE MELLOR: Okay.

67.2. It is unclear from the above exchange when exactly Mr Matthews became aware that the Bitcoin White Paper had been released, but his evidence that he would have

[141] {Day 12/97-98}.

known if it had been released is plausible. In any event, Mr Matthews is unlikely to be out by any significant amount in relation to the timing of this event in circumstances where his (unchallenged) evidence is that Dr Wright informed him around early January 2009 that the Bitcoin network had been launched; and it is clear from his evidence that his receipt of the USB stick occurred some time before that.[142]

68. Don Lynam was unable to give live evidence in these proceedings due to ill health, but his deposition evidence remains significant on this issue. Don Lynam received an "*advance and pretty rough*" copy of the White Paper in 2008 – "*probably mid 2008*". The paper was "*clearly to be a digital monetary system*". He had "*no doubt in [his] mind that it was the precursor because it had the same content as the paper that came out, or very similar content*".[143] This corroborates Dr Wright's evidence, save for an immaterial timing wrinkle: Dr Wright's recollection is that he shared a preliminary draft in 2007.[144]

69. In cross-examination, Max Lynam was asked about his evidence that Dr Wright sent him documents relating to virtual currency in the mid-2000s, but he could not recall whether he saw the exact White Paper or not:[145]

69.1. Max Lynam confirmed that the documents we saw "*were all pretty similar*":[146]

> In the course of making your witness statement, somebody showed you a copy of the Bitcoin White Paper, didn't they?
> A. Yeah.
> Q. And you said you couldn't recall Craig ever sending you that document?
> A. I said we had received numerous documents and bits of information from him. That could have been one of them.
> Q. But you couldn't --
> A. They were all pretty similar.
> Q. You couldn't single that out from many documents Craig had sent you?
> A. No, because it was all talking about the same things.

[142] Matthews 1 [28]-[30].
[143] Don Lynam Depositon, p. 26 l.6 to p.30 l.12 E/16/26-30}; see also p.61 l.13 to p.64 l.4 {E/16/61-64} and p.64 l.25 to p.65 l.16 {E/16/64-65}.
[144] Wright 1 [87] {E/1/18}.
[145] Max Lynam 1 [15-16] {E/13/5}.
[146] {Day 11/35}.

69.2. The above exchange supports the view that Max Lynam at the very least saw something similar to the White Paper prior to its release.

70. Mr Jenkins recalls seeing a version of the "*Timecoin*" White Paper, albeit his recollection is that is this happened "*around… 2009/2010*". As this event appears to post-date the release the White Paper, it falls into the category of circumstantial evidence post-dating the White Paper and is dealt with separately below.

E. Launch of Bitcoin

71. The evidence confirms that Dr Wright launched the Bitcoin system by uploading the White Paper to the SourceForge Bitcoin Project and posting links to the Bitcoin Software on SourceForge and the Bitcoin.org Website. The principal points raised during trial are addressed below.

Purchase of the bitcoin.org domain

72. Dr Wright's purchase of the bitcoin.org domain is addressed in Wright 4.[147] He confirmed the correctness of that account in cross-x: see {Day 2/25/21} to {Day 2/56/21}. In particular:

72.1. Dr Wright purchased the bitcoin.org domain in August 2008 through Anonymous Speech, which provided email and webhosting services. This was a preliminary practical step to launching his peer-to-peer electronic cash project. Through Anonymous Speech, Dr Wright set up the Satoshi@Vistomail.com email (the "**Vistomail Email**") account.

72.2. Dr Wright had used Anonymous Speech for many years. Until around 2005/2006, he paid for Anonymous Speech's services using a Westpac credit card, but that card had been discontinued. He thereafter used credit/debit cards associated with a WebMoney account which was linked to Liberty Reserve (an online currency). Through the WebMoney account, he may have used Liberty Reserve Dollars to pay for his purchase of the bitcoin.org domain.[148]

[147] Wright 4 at [13]-[24] {E/4/8-13}. See also Wright 11 at [170]-[174] {CSW/1/33-34}.
[148] Wright {Day 2/32/10} – {Day 2/33/2}; {Day 2/45/16} – {Day 2/46/11} and {Day 2/47/7-11}.

72.3. Dr Wright showed that he had access to the Anonymous Speech and Vistomail Email accounts in a series of short videos produced in June 2019 for the purposes of the Kleiman Proceedings.[149] He subsequently lost access to those accounts when they were discontinued.

72.4. The June 2019 videos were not fabricated, as explained by Dr Wright in cross-x. The website footers shown in the videos were not updated, as Mr Madden claimed; the Anonymous Speech / Vistomail site was not particularly advanced and aspects of the site did not regularly update.[150]

72.5. Dr Wright's evidence is corroborated by emails which were produced by Mr Malmi for the first time in June 2023, not having previously been made public. These emails confirm that Satoshi was familiar with Liberty Reserve and had suggested to Mr Malmi in April – July 2010 that Liberty Reserve be used in connection with Bitcoin.[151] This aspect of Bitcoin's history was not generally known before disclosure of Mr Malmi's emails.

Early Mining / Patch Tuesday

73. Dr Wright's involvement in the mining of early Bitcoin blocks is corroborated not only by contemporaneous documents but also the evidence of a number of third-party witnesses, as well as that of Dr Wright. In particular:

73.1. Dr Wright confirmed in cross-x that the systems he was running at the time of Bitcoin's launch included 69 computers in racks as well as various laptops and desktop machines.[152] These were split between his home in Lisarow and his farm at Bagnoo. Ms DeMorgan (Dr Wright's sister) said that "*[a]lmost most of [Dr Wright's] house was … full of computers and servers and cords*".[153]

73.2. Although there was a minor difference of recollection between Ms DeMorgan and Dr Wright about whether the brunt of Dr Wright's computer equipment was in a

[149] Wright 4 [20] {E/4/11}.
[150] Wright {Day 2/50/10} – {Day 2/51/20}.
[151] {L6/109/1}, {L6/117/1} and {L6/121/1}.
[152] His reference in Wright 1 to computer systems in '69 racks' was a mistake and corrected in cross-x. He had clearly referred to 69 computers, rather than 69 racks, in his evidence in the Kleiman Proceedings: {Day 8/141/16} – {Day 8/142/4} and {Day 8/172/13} – {Day 8/174/10}.
[153] DeMorgan {Day 10/10/8-9}.

converted garage or converted living or bedroom, the substance of Ms DeMorgan's evidence was not challenged and rings true. She described "*a room filled with massive computers and servers*" which was "*like this mad professor's room, there was a desk with a whole heap of computers on there, and racks on the side with servers*".[154]

73.3. The scale of Dr Wright's operations is corroborated by the ATO's Private Ruling of 23 December 29 which refers to Dr Wright having "*started mining Bitcoins*" in 2009, after investing "*a substantial amount of money in computer hardware and advanced scientific computing systems*".[155]

73.4. Although a set-up of this magnitude was not necessary to mine Bitcoin in 2009 or early 2010, Dr Wright was not running a simple mining operation. As explained in cross-x, in addition to mining early blocks, he was overseeing and testing the Bitcoin system on a real-time basis, running logging and collation systems for clients such as CentreBet, experimenting on other projects such as Timecoin and starting to develop scaling and other Bitcoin-related solutions.[156] COPA's reliance on Professor Meiklejohn's expert evidence about the hash rate and difficulty level in 2009 and early 2010 is therefore misplaced, as also is the Developers' reliance on the limited number of Bitcoin transactions during 2009. Neither of these was relevant to determining the scale of Dr Wright's operations, which extended well beyond validation of transactions and straight-forward mining computations.

73.5. Unsurprisingly, the electricity consumed by Dr Wright's set-up (including the costs of air-conditioning the machines) was substantial, amounting on Dr Wright's case to around A$11,000 per month.[157] The electricity bill shown to Dr Wright in cross-x related only to his Lisarow house and not the converted garage containing his computer set-up which was on a separate three-phase connection billed to his company, Information Defense.[158]

---

[154] DeMorgan 1 [11] {E/8/4}; DeMorgan {Day 10/9/6} – {Day 10/10/13}; and Wright {Day 8/173/3-16}.
[155] {L8/304/3}.
[156] Wright {Day 6/146/15}-{Day 6/150/1} and {Day 8/175/5}-{Day 8/179/7}. See also Wright 1 [116] {E/1/22}, referring to "*robust operations which linked to the client systems [he] was experimenting on (e.g. CentreBet)*", which "*aided in furthering [his] Bitcoin node management pursuits*".
[157] Wright {Day 8/173/18}-{Day 8/174/15}.
[158] Wright {Day 8/174/16}-{Day 8/175/4} and {Day 8/179/17}-{Day 8/180/11}. Records for the Information Defense account were, according to Dr Wright, not available from the utility provider.

73.6. Dr Wright's account is corroborated by contemporaneous documents (including forum posts and emails disclosed by Mr Malmi) showing that Satoshi was involved in devising patches and other solutions for problems which emerged following the launch of Bitcoin (such as a serious overflow bug in August 2009 and a system outage in January 2010),[159] as well as designing system enhancements such as a Linux build-up for Bitcoin.[160] These matters inevitably required testing and consumed more computer resource than would have been required to run a single mining node.

74. Dr Wright's account is further corroborated by the evidence of Don Lynam (his uncle), Max Lynam (his cousin) and Mr Jenkins:

74.1. Don Lynam (whose poor health prevented him giving evidence at trial) gave clear evidence in the Kleiman Proceedings that he had run a mining node for Dr Wright from the beginning of 2009 ("*[a]s soon as he went live with Bitcoin*") until early 2011.[161] Don Lynam's evidence was corroborated by Max Lynam, who confirmed in his witness statement in this action that he and Don Lynam were running code that Dr Wright was testing from around late 2008/early 2009 until around 2011.[162]

74.2. Max Lynam's evidence to that effect was not challenged in cross-x.[163] Rather, he was questioned about the nature of the code which he and Don Lynam were running, an attempt being made to show that it was unrelated to Bitcoin. However, while Max Lynam acknowledged that he could not remember "*the precise functions of the code*", he confirmed that it related to Dr Wright's work on "*cryptographic key authorisation*".[164] He also explained that he knew at the time that it had "*something to do with blockchain*".[165] When this was challenged on the ground that he was not "*au fait with the details of this code or the details of the work that it represented*", he pointed out that he had been provided with various

[159] {L6/375/1-5} and {L6/470/1}.
[160] {L6/12/1} and {L6/127/1}.
[161] {E/16/34-37}.
[162] Max Lynam 1 [17]-[24] {E/13/5-7}.
[163] Max Lynam {Day 11/28/1} – {Day 11/35/7}.
[164] Max Lynam {Day 11/31/15-23}; see also {Day 11/33/18} – {Day 11/34/7}.
[165] Max Lynam {Day 11/40/3-19}. The questioning on the "blockchain" point continued from {Day 11/40/20} to {Day 11/42/11}.

papers and been party to discussions with Dr Wright about those concepts before January 2009 (see above).

74.3. Whilst Max Lynam accepted in cross-x that he did not know "*directly*" that the code he and Don Lynam had been running was related to Bitcoin until the dinner he attended with Dr Wright and his wife in 2013,[166] he had already acknowledged this in his witness statement.[167] This point therefore underlines his honesty and credibility. The fact that he did not fully understand that he had been mining Bitcoin does not detract from the likelihood that this is what he was doing, particularly in circumstances where he understood that the code he was running related to Dr Wright's work on "*cryptographic key authorisation*" and had "*something to do with blockchain*".

74.4. A number of questions were put to Max Lynam to the effect that he was not "*sworn to secrecy about the running of this code*".[168] That is irrelevant. By January 2009, Bitcoin had been released, so there was no need for the mining undertaken by him and Don Lynam from January 2009 to be secret or confidential.

74.5. Mr Jenkins was also asked by Dr Wright to undertake some mining in early 2009.[169] When cross-examined, he was not challenged on whether he had in fact been asked to do so by Dr Wright at that time.[170] Indeed, the questioning expressly proceeded on the basis that he was talking about early 2009.[171]

75. COPA sought to undermine Dr Wright's evidence by suggesting that in a blogpost and other public statements,[172] he had incorrectly attributed the hiatus between the creation of the Genesis Block (3/4 January 2009) and the mining of Block 1 (9 January 2009) to the need to reconfigure the Bitcoin system following the issue of Windows software patches on Patch Tuesday. However, this attempt was misplaced. Although Patch Tuesday occurred on 13 January 2009, Dr Wright explained that he received the patches from Microsoft in the previous week as a result of being part of Microsoft's Developer

[166] Max Lynam {Day 11/38/1-4} and {Day 11/39/8-15}.
[167] Max Lynam 1 [25] {E/13/7}.
[168] Max Lynam {Day 11/34/11} – {Day 11/35/7}.
[169] Jenkins 1 [30]-[32] {E/6/8}.
[170] Jenkins{Day 9/81/14} – {Day/9/83/9}.
[171] Jenkins {Day 9/82/16-22}.
[172] Blogpost at {L14/420/2}; and public statements at {O4/25/25}, {O4/12/14} and {L15/96/14}.

Network.[173] He was therefore able to, and did, reboot and reconfigure his computer network in the week of 3 to 9 January 2009.

Inter-Actions with Other Network Participants

76. In support of their case, COPA and the Developers have sought to rely on supposed discrepancies between the accounts given by Dr Wright and various other witnesses involved in Bitcoin at or around the time of its launch. On analysis, these points do not assist COPA or the Developers; the relevant evidence supports Dr Wright's case.

77. Three individuals with whom Dr Wright interacted (as Satoshi) in the early days of Bitcoin were Dustin Trammel (also known as "*druidian*"), Zooko Wilcox-O'Hearn and Adam Back. They were all keenly interested in digital currency and were members of The Cryptography Mailing List. Mr Wilcox-O'Hearn and Dr Back were self-professed "*cypherpunks*", activists who sought to create social and political change through cryptography and privacy-enhancing technologies.[174] They interacted together in online forums and on Internet Relay Chat ("**IRC**") channels.[175]

Sharing Bitcoin code with Mr Trammel

78. COPA suggests that Dr Wright was wrong to say (in the Granath proceedings) that he "*shared*" Bitcoin code with Mr Trammel.[176] However, that is what Dr Wright did; he shared the White Paper, and subsequently the Bitcoin code, by forwarding links to them to members of The Cryptography Mailing List, including Mr Trammel.

79. Mr Trammel accepts that he (i) found out about Bitcoin in early November 2008 from the link sent to The Cryptography Mailing List by Satoshi; (ii) immediately downloaded and read the White Paper; (iii) found out about the Bitcoin code from Satoshi's announcement of the code on The Cryptography Mailing List in January 2009; (iv) downloaded the code from bitcoin.org, i.e. the site to which Satoshi's announcement directed readers of The Cryptography Mailing List; and (v) thereafter corresponded with

[173] Wright {Day 6/133/13} – {Day 6/141/5}.
[174] Wilcox-O'Hearn {Day 14/56/3} – {Day 14/57/25}; Back {Day 13/33/16} – {Day 13/34/12}.
[175] See Wilcox-O'Hearn 1 [3] {C/6/2} and {Day 14/58/1} – {Day 14/60/13}. Although Dr Back sought in cross-x to distance himself from Mr Wilcox-O'Hearn, the evidence of Mr Wilcox-O'Hearn is to be preferred, namely that they had "*many interactions*" together, including on IRC channels and various forums.
[176] Wright {Day 6/54/15} – {Day 6/57/22}.

Satoshi via email.[177] The emails between Satoshi and Mr Trammel show that they discussed, among other things, the code circulated by Satoshi.[178]

80. There is no material difference between Mr Trammel's evidence and Dr Wright's account. As Dr Wright explained in cross-x, he forwarded links to his code to the mailing list; Mr Trammel used those links to download the code and thereafter discussed the code with Dr Wright (as Satoshi). That process is fairly described as 'sharing' the code with Mr Trammel.

Bitcoin transfers to Mr Bohm / Mr Wilcox-O'Hearn

81. COPA has sought to pick holes in Dr Wright's account of his early Bitcoin transactions. These points are of little consequence. As Dr Wright explained in cross-x, Bitcoins were transferred to many people in the early days. They were then worth very little and distributing them was a useful way of promoting the network. When Mr Andresen came on board, he set up a Bitcoin 'faucet', which was a website that dispensed thousands of Bitcoins, for free.[179] Moreover, Dr Wright (as Satoshi) communicated at the time with several hundred people about Bitcoin, including on the Bitcoin forums. It is unsurprising that he may not have remembered communicating with particular individuals (such as Mr Bohm) or sending them a few Bitcoin.[180]

82. Dr Wright recalls sending Bitcoin (as Satoshi) to Mr Wilcox-O'Hearn but Mr Wilcox-O'Hearn does not recall receiving any Bitcoin from Satoshi.[181] Dr Wright submits that Mr Wilcox-O'Hearn is mistaken and that he was sent Bitcoin by Dr Wright (acting as Satoshi).

83. A number of matters support Dr Wright's recollection. As Mr Wilcox-O'Hearn accepted in cross-x:

[177] Trammel 1 [4], [5] and [9] {C/7/2}. Satoshi's announcements to The Cryptography Mailing List are at {L3/278/1}, {L4/61/1} and {L18/310/2}; and Mr Trammel's email correspondence with Satoshi is at {D2/4/1} – {D2/67/1}.
[178] See e.g. {L4/194/1}, {L4/195/1}, {L4/275/1} and {L4/318/1}.
[179] See Mr Andresen's Deposition at {E/17/21}; and emails between Mr Andresen and Satoshi at {L6/196.9/1}, {L6/460.21/1} and {L18/427/1}.
[180] Wright {Day 6/63/1-19} and {Day 7/158/1-4}.
[181] Wright {Day 7/156/19} – {Day 7/157/25}; Wilcox-O'Hearn 1 [8] {C/6/3}.

83.1. He was keenly interested in digital currency initiatives, having taken a leave of absence from his studies in the mid-1990's to join DigiCash, an early attempt to found an electronic payment system;

83.2. When DigiCash failed, he concluded that what was "*really required was a decentralised electronic payment system that did not depend upon a central trusted party*";[182]

83.3. Having learned of the White Paper from the link posted to The Cryptography Mailing List by Satoshi, he was very interested to read it;

83.4. He realised the White Paper was proposing a decentralised digital currency system that did not depend upon a centralised trusted party, i.e. precisely what he believed was needed after his experience at DigiCash: he was, in large part, "*waiting for Satoshi*";[183]

83.5. He regarded Bitcoin as "*a revelation*" and "*was definitely entranced by it*";[184] and

83.6. He wrote what is probably the first blogpost about Bitcoin on 26 January 2009, commenting in particular that unlike Nick Szabo's BitGold idea and Wei Dai's B-money idea, Satoshi had 'actually implemented' Bitcoin (by which he was referring to launch of the Bitcoin Software and other concrete steps being taken to get the system up and running).[185]

84. In these circumstances, it stands to reason that Mr Wilcox-O'Hearn would have downloaded the Bitcoin Software, tried out the system and communicated with Satoshi at an early stage. That is strongly supported by (i) the points identified in the preceding paragraph; (ii) comments made by Mr Wilcox-O'Hearn in online forums (where he said he became "*entranced and sucked in by Bitcoin pretty early*") and Mr Wilcox-O'Hearn's comments on the 'What Bitcoin Did' podcast (where he said he was 'pals with Satoshi' in 2009);[186] and (iii) Mr Wilcox-O'Hearn's acceptance in cross-x that Satoshi "*might have emailed*" him about the White Paper.[187] It is also notable that Mr Wilcox-O'Hearn

[182] Wilcox-O'Hearn {Day 14/61/22} – {Day 14/62/1}
[183] Wilcox-O'Hearn {Day 14/65/5/-12}
[184] Wilcox-O'Hearn {Day 14/73/8} – {Day 14/74/18}.
[185] {L18/312/2}; Wilcox-O'Hearn {Day 14/75/10} – {Day 14/77/23}.
[186] {X/30/21} and {X/43/12}.
[187] Wilcox-O'Hearn {Day 14/63/10-19}.

readily accepted that he had very few records of his early involvement in Bitcoin and remembering precise details without records could be difficult.[188]

85. Although Mr Wilcox-O'Hearn said that he could not have downloaded and run the Bitcoin Software in 2009 because he was not then using Windows, he agreed that he could easily have accessed Windows at that stage if he had wanted.[189] He also acknowledged that he was using Linux in 2009; if (as he said) he ran Bitcoin on Linux, he could have done so during 2009.[190]

Dr Back's dismissiveness

86. Dr Wright was challenged by COPA for describing Dr Back as having been "*dismissive*" in early communications about Bitcoin.[191] There is nothing in this point. Dr Wright could fairly have received the impression that Dr Back was being dismissive, in that:[192]

86.1. Dr Back said initially that he would take a look at the White Paper but then later reverted without having done so ("*Sorry still not read your paper …*"); and

86.2. When Dr Back reverted to Dr Wright, his email was entirely focussed on micromint, a micropayment scheme which never got off the ground. This was taken amiss by Dr Wright.

87. The question here is not whether Dr Back was in fact dismissive but whether he gave that impression to Dr Wright. For the reasons given, there is no basis for the Court rejecting Dr Wright's evidence on this point.

88. Furthermore, it is clear that Dr Back has not disclosed all of his communications with Dr Wright / Satoshi.[193] As Dr Back accepted in cross-x, he "*just provided the emails with Satoshi*"; he has therefore not disclosed (i) any of his postings or other communications on the cypherpunks or cryptography mailing lists or other online forums; (ii) his communications on IRC channels; (iii) his communications on Twitter; and (iv) emails with persons claiming to be Satoshi which he did not consider to be authentic.[194] Such

[188] Wilcox-O'Hearn {Day 14/60/8-13}, {Day 14/67/12-15} and {Day 14/81/4} – {Day 14/84/6}.
[189] Wilcox-O'Hearn {Day 14/72/18-21}.
[190] Wilcox-O'Hearn {Day 14/84/7-25}.
[191] Wright {Day 6/65/1} – {Day 6/70/3}.
[192] See emails at {L3/192/1} and {L3/193/1}; Wright {Day 6/66/24} – {Day 6/67/2}.
[193] Wright {Day 6/67/11} – {Day 6/68/23}.
[194] Back {Day 13/68/13} – {Day 13/70/11}.

selective disclosure is problematic in circumstances where Dr Back is CEO of Blockstream whose interests conflict with those of Dr Wright. In the circumstances, the Court cannot fairly draw an adverse inference against Dr Wright on the limited documentary material available.

Mr Malmi and the Bitcoin forums

89. Points of detail arise concerning Mr Malmi's involvement in setting up and maintaining the Bitcoin website forums (the "**Bitcoin Forums**"). Whilst COPA has sought to exaggerate the importance of these points, Dr Wright submits that properly analysed, the evidence supports his case (and not that of COPA or the Developers).

90. ***First,*** on the timing of Mr Malmi's first contact with Satoshi, Mr Malmi claimed in Malmi 2 that he first approached Satoshi "*on 2 May 2009*".[195] This date was taken from Mr Malmi's email to Satoshi on 2 May 2009 in which he offered to help with Bitcoin.[196] However, as the email itself indicated, there had been previous communication between Mr Malmi (using the pseudonym 'Trickstern') and Satoshi on the anti-state.com forum (the "**ASC Forum**").[197] Mr Malmi accepted in cross-x that Satoshi had in fact been part of a discussion, involving Mr Malmi, about Bitcoin on the ASC Forum.[198] This had not been mentioned in Mr Malmi's witness statement. Although Mr Malmi continued to claim that this was the limit of his prior communications with Satoshi, its notable that he has not provided any disclosure of his ASC Forum or SourceForge forum conversations.

91. ***Second,*** Mr Malmi denied in his witness statements that he shut Satoshi out of the Bitcoin Forums in June/July 2011.[199] The timeline of the establishment and subsequent migration of the Bitcoin Forums was traced during Mr Malmi's cross-x. In summary, Mr Malmi accepted that:[200]

[195] Malmi 2 [4a] {C/24/2}.
[196] {L5/53/1}.
[197] It is also clear from the face of the email that it was sent by Mr Malmi to Satoshi through the SourceForge bitcoin forum, rather than directly by email. The footer of the email states: "*This message has been sent to you, a registered SourceForge.net user, by another site user, through the SourceForge.net site. This message has been delivered to your SourceForge.net mail alias.*" {L5/55/2}.
[198] Malmi {Day 13/7/4-25}.
[199] Malmi 1 [23] {C/2/5} and Malmi 2 [4b] {C/24/2}.
[200] Malmi {Day 13/12/23} – {Day 13/19/15}.

91.1. In May-June 2009, as requested by Satoshi, he created an FAQ and set up the Bitcoin Forums on the Bitcoin project website on SourceForge (with the URL bitcoin.sourceforge.net);

91.2. The Bitcoin Forums were moved in late 2009 from bitcoin.sourceforge.net to bitcoin.org;

91.3. At that stage, Mr Malmi (then known as 'Sirius') took over control of the bitcoin.org domain ("*The bitcoin.org domain name was ... transferred from Satoshi to Sirius*");[201]

91.4. In June/July 2011, the Bitcoin Forums were moved from bitcoin.org to bitcointalk.org.

92. Importantly, Mr Malmi accepted that (contrary to his written evidence) the consequence of changing the URL and hosting arrangements of the Bitcoin Forums in June/July 2011 was to remove Satoshi's rights of access to the website, including Satoshi's rights of access to change the site content and how the site operated.[202] Mr Malmi agreed with Dr Wright's evidence that when a database is moved to a new server, the root administrator privileges from the original server do not automatically transfer. They would only do so if specifically configured, which did not happen in relation to the Bitcoin Forums.

93. Mr Malmi said that Satoshi could have regained his rights of access by asking for them. However, that begs the question of how Satoshi (i.e. Dr Wright) could have communicated such a request to Mr Malmi.

94. ***Third,*** COPA sought to make a point about Satoshi's use of the term 'cryptocurrency', particularly by reference to an announcement for the release of version 0.3 of Bitcoin discussed in email exchanges between Satoshi and Mr Malmi.[203] This is a point of limited significance.

95. The emails relied upon by COPA show that the term 'cryptocurrency' originated in a forum discussion ("*Someone came up with the word 'cryptocurrency' ...*"). Having discussed use of the term with Mr Malmi, and specifically asking whether Mr Malmi

[201] {X/32/1}; Malmi {Day13/15/23} – {Day 13/16/23}.
[202] Malmi {Day 13/19/16} – {Day 13/22/7}.
[203] {L5/106/1} and {L6/193/1}; Wright {Day 6/150/2} – {Day 6/155/17} and {Day 7/5/18} – {Day 7/8/4}.

liked the term, Satoshi then used it in the version 0.3 announcement. Dr Wright acknowledged in cross-x that he had sometimes been 'lax' about the term 'cryptocurrency' and had not consistently avoided using it. He originally thought it "*sounded cool*" but explained that he had not then researched the term and did not understand its connotations.[204]

96. When COPA later reverted to this point, Dr Wright re-iterated that he agreed to use the term 'cryptocurrency' when announcing version 0.3, but then later decided that was the wrong term. As he said: "*I haven't, at the time, gone into that deep enough, I have subsequently*".[205] This evidence is plausible and should be accepted.

Bitcoin FAQ

97. Two important points emerge from the communications between Satoshi and Mr Malmi concerning the FAQ on the Bitcoin website.

98. ***First,*** a post by Satoshi at {L5/54/15} sets out the connection between security of data and the timestamp server created to secure the Bitcoin blockchain (emphasis added):

> Before strong encryption, users had to rely on password protection to secure their files, placing trust in the system administrator to keep their information private. Privacy could always be overridden by the admin based on his judgment call weighing the principle of privacy against other concerns, or at the behest of his superiors. Then strong encryption became available to the masses, and trust was no longer required. **Data could be secured in a way that was physically impossible for others to access, no matter for what reason, no matter how good the excuse, no matter what**.
> It's time we had the same thing for money. With e-currency based on cryptographic proof, without the need to trust a third party middleman, money can be secure and transactions effortless. …
> Bitcoin's solution is to use a peer-to-peer network to check for double-spending. **In a nutshell, the network works like a distributed timestamp server, stamping the first transaction to spend a coin**. It takes advantage of the nature of information being easy to spread but hard to stifle.

99. Mr Malmi confirmed in cross-x 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.[206] This underlines the significance of Dr Wright's earlier

[204] Wright {Day 6/151/5-10}.
[205] Wright {Day 7/7/23} – {Day 7/8/4}.
[206] Malmi {Day 13/26/6-10}.

work on secure logging systems (at Vodafone) and encrypted data security systems (at Qudos Bank). That work was a directly relevant precursor to Dr Wright's establishment of Bitcoin.

100. Satoshi's communications with Mr Malmi also demonstrate Satoshi's interest in topics such as backing by fiat[207]; micropayments[208], scalability and block size[209] and the potential for Bitcoin technology to support diverse transaction types[210], all of which is consistent with the underlying ethos and rationale for Bitcoin asserted by Dr Wright.

101. ***Second,*** at {L5/54/14}, Satoshi was asked whether Bitcoin's blockchain system could be used for secure timestamping of documents (as opposed to digital currency transfers). He confirmed that it could:

> Bitcoin is a distributed secure timestamp server for transactions. A few lines of code could create a transaction with an extra hash in it of anything that needs to be timestamped. I should add a command to timestamp a file that way.

102. Mr Malmi agreed in cross-x that it was technically possible to extend the Bitcoin system to encompass transactions involving anything that needed to be timestamped; and that services already existed to facilitate this.[211]

103. This again confirms the fundamental importance of Bitcoin as a distributed timestamp server, not only for digital currency but also for any kind of transaction. COPA's attempt to belittle Dr Wright's extensive experience in creating and developing systems for securing and transmitting data is misplaced. Dr Wright's experience in that field strongly supports his claim to be Satoshi.

Hashcash

104. An issue arises concerning the White Paper's reference to using "*a proof-of-work system similar to Adam's Back's Hashcash*".[212] Dr Wright said in Wright 1 (at para 94) that:[213]

> Contrary to popular belief, Bitcoin's proof-of-work system does not utilise Adam Back's Hashcash system. Instead, it more closely aligns with the methodologies

[207] See, for example, {L5/53/1}.
[208] See, for example, {L5/54/5}.
[209] See, for example, {L5/54/10}.
[210] See, for example, {L6/190.2/1}.
[211] Malmi {Day 13/27/17} – {Day 13/28/15}.
[212] Section 3 of the White Paper at {L3/231/3}.
[213] Wright 1 [94] {E/1/19}

> described in Aura's paper. Due to Aura's lack of response, I felt it necessary to reference Adam Back in the Bitcoin White Paper due to the thematic parallels in our work and Back's notable presence in the field.

105. COPA challenges the correctness of this passage, but its criticisms are misplaced and should be rejected. Para 94 of Wright 1 is technically accurate and fairly expressed. The following points should be noted.

106. Dr Back's Hashcash system (whether as originally proposed in March 1997 (the "**Original Proposal**") or as revised in Dr Back's paper entitled "*Hashcash – A Denial of Service Counter-Measure*" (the "**2002 Paper**"))[214] was primarily designed to address denial of service attacks and spam. It was not designed to be, or intended for use as, a proof of work mechanism for a distributed peer-to-peer electronic cash system (no such system having been devised by the time of the Original Proposal or the 2002 Paper).

107. Although the 2002 Paper suggested that Hashcash could be used as a minting mechanism for Wei Dai's B-money electronic cash proposal,[215] the B-money proposal (which was never actually implemented) envisaged proof-of-work, i.e. solving a computational puzzle, as the method by which electronic money was created. That is not how Bitcoin works. As explained by Narayanan and Clark in their paper, "*Bitcoin's Academic Pedigree*",[216] declaring puzzle solutions to be cash is a "*crude*" approach. Rather, Satoshi's "*true genius*" was that:[217]

> In bitcoin, for the first time, puzzle solutions don't constitute cash by themselves. Instead, they are merely used to secure the ledger. Solving proof of work is performed by specialized entities called miners …
> 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 bitcoins issued per block is not fixed either. The block reward (which is how new bitcoins are minted) is set to halve every four years (in 2017, the reward is 12.5 bitcoins/block, down from 50 bitcoins/block). Bitcoin incorporates an additional reward scheme—namely, senders of transactions paying miners for the service of including the transaction in their blocks. It is expected that the market will determine transaction fees and miners' rewards.

[214] 1997 proposal: {CSW/168/1}; 2002 Paper: {X/22/1}.
[215] 2002 Paper, section 7: {X/22/7}.
[216] Exhibited to Professor Meiklejohn's First Report: {H/182/7-8}.
[217] {H/182/8} (emphasis added).

> Nakamoto's genius, then, wasn't any of the individual components of bitcoin, but rather the intricate way in which they fit together to breathe life into the system. The timestamping and Byzantine agreement researchers didn't hit upon the idea of incentivizing nodes to be honest, nor, until 2005, of using proof of work to do away with identities. Conversely, **the authors of hashcash, b-money, and bit gold didn't incorporate the idea of a consensus algorithm to prevent double spending**. In bitcoin, a secure ledger is necessary to prevent double spending and thus ensure that the currency has value. A valuable currency is necessary to reward miners. In turn, strength of mining power is necessary to secure the ledger.

108. Whilst Dr Back quibbled with aspects of this description, he acknowledged this was essentially a matter of emphasis. As he said in cross-x: "*we are probably just focusing on the way that people express themselves … 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*".[218]

109. The computational puzzle used in Dr Back's Original Proposal required computation of a hash which matched a target string incorporating the email sender's service name (i.e. "*a 17 bit collision on string 'flame'*").[219] By contrast, Bitcoin's proof-of-work involves "*scanning for a value that when hashed, … the hash begins with a number of zero bits*" (as stated in the White Paper, at Section 4).[220] These are clearly different methodologies.

110. In June 2000, i.e. before the 2002 Paper, Tuomas Aura ("**Aura**"), Pekka Nikander and Jussipekka Leiwo produced their own proof-of-work methodology (the "**Aura Methodology**") requiring hash solutions incorporating a specified number of zero bits at the beginning of the hash (as set out in their paper, "*DOS-resistant Authentication with Client Puzzles*" ("**Aura's Paper**") at Section 3).[221] Dr Back agreed that this was the effect of the Aura Methodology.[222]

111. In both his written and oral evidence, Dr Wright correctly described the Aura Methodology as more closely aligning with Bitcoin's proof-of-work system. As Dr Wright said:[223]

> Bitcoin doesn't use a token word. Using a token word cannot be implemented in Bitcoin and doesn't work, because there's no way of having difficulty adjustment.

[218] Back {Day 13/60/11-18}.
[219] Original Proposal: {CSW/168/1-2}
[220] {L3/231/3}.
[221] {CSW/169/5}.
[222] Back {Day 13/46/8-11} and {Day 13/11-15}.
[223] Wright {Day 6/76/18-23}. Wright 1 [94] {E/1/19} is to the same effect.

> Using a string of zeros, as Aurora did, allows you to implement a single zero at a time, making the proof-of-work more or less difficult.

112. In his 2002 Paper, Dr Back adopted a similar methodology to that of Aura, involving a target string containing a specified number of zeros ("**Back's Revised Methodology**"). This was described in the 2002 Paper as an improvement suggested by Hal Finney and Thomas Boschloo.[224] To this extent, Back's Revised Methodology could be described as "*similar*" to that used in Bitcoin, as stated in the White Paper.

113. Insofar as COPA suggests that Dr Back's Hashcash proposal, whether in its original or revised form, was the ***only*** possible source for the proof-of-work mechanism used in Bitcoin, that is plainly not the case. As Dr Back agreed in cross-x, there was by the early 2000s a "*rich source of academic materials on proof-of-work systems*".[225] This included papers from no less than 11 other researchers, aside from Dr Back, dating from 1997 to 2000 (including Aura's Paper).[226] The creator of Bitcoin was therefore not limited to drawing upon Dr Back's Hashcash proposal.

114. Further, Dr Back explained that the mechanism incorporated in the Bitcoin protocol to adjust the difficulty of the proof-of-work computation was "*a little more nuanced*" and "*more fine-grained*" than he or Aura had devised.[227] For this further reason, Dr Wright correctly described Bitcoin as using a proof-of-work system "*similar*" to Adam Back's Hashcash. As Dr Wright stressed in cross-x, when challenged about the terminology used in the White Paper:[228]

> That does not say that I'm using Adam's proof-of-work system. "Similar" to his solution. I did not say "the proof-of-work system", I said "the system". So in this, we will need, similar to Hashcash, which it does, rather than newspaper posts. All I've said is, like Hashcash, I will use proof-of-work.

115. Indeed, COPA suggested that Dr Wright was wrong to identify any difference between Hashcash and Bitcoin's proof-of-work system:[229]

> 9 Q. And in more recent years you've sought to insist that
> 10 it's different in order to give yourself some sort of
> 11 spurious expertise.

[224] {X/22/5}; Back {Day 13/51/7} - {Day 13/53/22}.
[225] Back {Day 13/44/12} – {Day 13/45/2}.
[226] Back {Day 13/42}.
[227] Back {Day 13/50/2-24}.
[228] Wright {Day 6/72/19-24}
[229] Wright {Day 6/76/9-13}

12 A. No, I have not. If you actually look at the code and
13 the implementation, you will see that it is different.

116. On this point, Dr Wright and Dr Back are (it appears) agreed. Contrary to COPA's contention, the code implementing Bitcoin's proof of work is different to both Dr Back's Original Proposal and his Revised Methodology: see Back {Day 13/50/2-24}.

117. In summary:

117.1. Bitcoin's proof-of-work system did not utilise Dr Back's Original Proposal (which uses a very different target hash methodology to that used in Bitcoin);

117.2. Bitcoin's proof of work aligns more closely with the methodology described in Aura's Paper than with Dr Back's Original Proposal;

117.3. Whilst Dr Back's 2002 Paper adopted a target hash involving a string of zeros, neither that methodology nor the Aura Methodology involved a difficulty adjustment as fine-grained as that used in Bitcoin. Hence the White Paper's reference to using a system that was "*similar*";

117.4. Notwithstanding the differences between Bitcoin's proof-of-work mechanism and Hashcash, there were "*thematic parallels*" between Dr Wright's work and that of Dr Back;

117.5. Whilst there were many others (including Aura *et al*) researching proof-of-work in the late 1990s and 2000s, Dr Back could fairly be described as having a "*notable presence in the field*" at the time of publication of the White Paper.

118. Properly understood, para 94 of Wright 1 is a fair and accurate description of a technically complex issue.

B-money

119. Dr Wright's evidence about his communications with Wei Dei (who formulated the B-money proposal in December 1998)[230] was not challenged in cross-x except for his description of Wei Dai as a "*distinguished academic*": see {Day 6/63/23} – {Day 6/64/25}. However, Wei Dai is a renowned cryptographer whose B-money proposal was

[230] {H/184/2}

a significant milestone in the digital currency field. It was not unreasonable for Dr Wright to have described him as a 'distinguished academic'.

120. In his written and oral evidence, Dr Back questioned whether Satoshi was aware of Wei Dei's B-money idea before he had mentioned the B-money proposal to Satoshi in August 2008.[231] However, Dr Back has misinterpreted Satoshi's email response to Dr Back on 21 August 2008.[232]

121. On 21 August 2008, Dr Back told Satoshi that: "*You maybe aware of the 'B-money' proposal ... by Wei Dai, which sounds to be somewhat related to your paper*". He then added, in brackets: "*The b-money idea is just described concisely on his web page, he didn't write up a paper*". Satoshi replied the same day, saying: "*Thanks, I wasn't aware of the **b-money page**, but my ideas start from exactly that point*" (emphasis added).

122. Objectively interpreted, the key words in Satoshi's response are those identified in bold above, namely that Satoshi was not aware of a ***b-money page*** (as opposed to the b-money concept). B-money had been proposed in a post by Wei Dai to the cypherpunks mailing list 10 years previously; Satoshi was in his response simply saying that he was not aware of the proposal having been posted on a webpage.

123. Having visited the B-money page, Satoshi needed to contact Wei Dai for the date of publication of the proposal because the relevant webpage (exhibited by Professor Meiklejohn to her First Report) is not dated: see {H/184/2}.

124. The notion that Satoshi was completely unaware of Wei Dai's B-money proposal is not borne out by the documents. As Dr Wright explains in Wright 11, he was well aware of the B-money proposal but was not aware of the b-money page.[233] His evidence is to be preferred to Dr Back's speculative interpretation of Satoshi's email.

Other Issues

125. In their cross-x of Dr Wright, the Developers attempted to show that Dr Wright had misunderstood the technology underlying Bitcoin (and is therefore not Satoshi). To the extent that such an argument is pursued in closing, it should be given limited (if any)

[231] Back 1 [7] {C/9/3} and Back {Day 13/62/7} – {Day 13/68/11}.
[232] {L3/192/1}.
[233] Wright 11 [370(c)] {CSW/1/70}.

weight. At the hearing on 19 September 2023, in the context of a discussion about the digital currency expert evidence (and in particular a contention in Sherrell 13 that such expert evidence may shed light on whether statements by Dr Wright demonstrated "*a misunderstanding of Bitcoin*"),[234] COPA disavowed advancing a case on the basis that Dr Wright misunderstood the technology underlying Bitcoin. Mr Hough KC confirmed that:[235]

> We have not pleaded that Dr. Wright misunderstood the technology of Bitcoin, and that that shows he is not Satoshi. That is not our pleaded case. We are not advancing such a case.

126. In these circumstances, there is no proper justification for allowing the Developers to run that case on an unpleaded basis. Dr Wright had no fair notice of any such case being run, whether by the Developers or COPA. As the Court observed at the hearing on 19 September 2023, any such contention would need to have been pleaded.

127. In any event, the Developers' reliance on Dr Wright's failure to explain what "*unsigned*" meant in the context of a section of Bitcoin code is misplaced.[236] As the Court will appreciate, Dr Wright sometimes finds it difficult to formulate a simple explanation of technical issues off the cuff. Dr Wright's difficulty in doing so on this occasion does not undermine his claim to be Satoshi.

128. Two other technical issues concerning Bitcoin code were raised in Dr Wright's cross-x:

    128.1. The Developers suggested that Satoshi, and not the Developers, had limited the ability to use script by setting a maximum size of 520 bytes on 15 August 2010.[237] Dr Wright correctly observed in cross-x that there had been an attack on the network at that point in time and a vulnerability in the system identified; the script limitation, however, was intended only to be temporary.[238]

    128.2. COPA suggested that an email from Mr Malmi to Satoshi in August 2009 showed that (contrary to Dr Wright's evidence) Satoshi had not used Visual

[234] {P1/13/5} [15].
[235] {O/7/34-35} (pp. 134-135).
[236] Wright {Day 8/143/25} - {Day 8/145/1}. Indeed, he mentioned that "*[w]riting it down would be different*" but was not given that opportunity.
[237] Wright {Day 8/150/10} – {Day 8/151/18}.
[238] The attack and identification of vulnerability in the network are recorded e.g. at {L6/370/1} and {L6/375/1}.

Studio.[239] However, as Dr Wright explained, the email relied upon by COPA referred to Satoshi having used "*VC*", i.e. Visual C++, "*only … for debugging*". Visual C++ is a compiler which forms part of Visual Studio. The email therefore corroborated Dr Wright's evidence that ***Visual Studio*** had been used in connection with creation of the Bitcoin code. Visual C++ could not have been used by Satoshi, even for debugging, unless he had the Visual Studio package.[240]

G. Further circumstantial evidence post-dating the White Paper

129. In addition to early mining and the other matters addressed above, there is further circumstantial evidence in the period around and/or following the release of the White Paper that points towards Dr Wright's authorship of the White Paper and creation of Bitcoin.

130. For example, the evidence of Mr Bridges:

130.1. Mr Bridges explained that, after Dr Wright left BDO (in November or December 2008), Dr Wright helped Qudos Bank implement an immutable event logger system with similarities to blockchain technology (albeit Mr Bridges fairly accepted that he was not in a position to say whether the system shared code in common with blockchain/Bitcoin):[241]

8 Q. Now, you say in your witness statement that he helped
9 you implement an event logger system and that one
10 feature --
11 A. Yes.
12 Q. -- and you say one feature of the system was that it
13 would make a record if somebody tried to alter
14 the logging records; is that right?
15 A. Yeah, that's right. Because our concern was, if someone
16 went in there and let's say they got admin privileges,
17 they could go and delete something and you might not
18 know they deleted it, so ...
19 Q. Now, in your witness statement, you draw a parallel with
20 blockchain technology, and the parallel you draw, as you
21 put it, is both systems keep a record of all
22 transactions and there is good traceability in both

[239] {L5/1545/1}; Wright {Day 6/58/4} – {Day 6/61/25}.
[240] Wright {Day 6/60/11} – {Day 6/61/25}. As Dr Wright noted in Wright 8, §43 {E/23/16} and in Wright 11, App. B, §16.13 {CSW/2/57}, he used MinGW in connection with Visual Studio as a C++ compiler from long before the release of Bitcoin.
[241] {Day 11/5-6}; cf. Bridges 1 [9]-[12] {E/9/4}.

systems; is that right?
A. Correct.
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 --
A. Yeah.
Q. -- technology is that both systems keep a record of transactions and there is good traceability in both systems; is that right?
A. Yeah, it would be the traceability and the immutability, right? So if you deleted something, you had a copy of the deletion, effectively.
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?
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.
Q. Yes, that's very fair of you.

130.2. Mr Bridges was also asked in cross-examination about the time in around 2008 when Dr Wright pitched an alternative payment system to Mr Bridges and his colleagues at Qudos Bank, which was based on a "*decentralised ledger*" and involved a "*peer-to-peer payments network where transactions would be a fraction of the cost of the existing SWIFT payment system*". [242] As to this:

(a). It was put to Mr Bridges that he was looking back on a conversation 15 years ago without documents to help his recollection. Mr Bridges answered that Dr Wright's LLM Dissertation triggered memories of the discussions he was having with his CEO and CFO about Dr Wright's proposal for an alternative payment system.[243] He was not challenged on that answer.

(b). Although Mr Bridges accepted that he was not in a position to explain the "*specific detailed technical IT features*" that were common between the Bitcoin system and the alternative payment system Dr Wright was proposing for Qudos bank, it was not dispute that Dr Wright's proposed system involved a secure ledger that could not be broken. Thus, on the basis of Mr Bridges'

[242] Bridges 1 [13]-[16] {E/9/4}. The cross-examination was at {Day 11/11/5 to 15/8}.
[243] {Day 11/12/9-19}.

evidence, there is at the very least a significant conceptual overlap between the Bitcoin system and Dr Wright's proposal for Qudos bank in "*around 2008*".

(c). Mr Bridges accepted in cross-examination that Dr Wright's proposal was made "*after he left BDO*"[244] (in November or December 2008). This would place the proposal after the Bitcoin White Paper was released in October 2008. This in turn means that (i) when Mr Bridges says "*around 2008*" the true position may well be that the proposal was made in 2009 and (ii) Mr Bridges' evidence in his witness statement that the proposal was made "*well before Bitcoin came out*" is probably incorrect.

(d). However, even if Mr Bridges was wrong to think that the proposal was made prior to the launch of Bitcoin, the fact that Dr Wright was pitching an alternative payment system with similarities to Bitcoin to Mr Bridges and his colleagues at Qudos Bank shortly after the release of Bitcoin is at the very least consistent with Dr Wright's creation of Bitcoin.

131. At some point in 2009 (albeit based on discussions that probably started in 2008), Dr Wright made a pitch to Centrebet's security sub-committee for a honeypot detection system with close parallels to Bitcoin/blockchain technology:[245]

131.1. In cross-examination on this topic, Mr Matthews maintained that the proposal related to an "*immutable log store and a timestamp server.*"[246] This supports the view that this proposal was linked to Dr Wright's work on Bitcoin.

131.2. The proposal in question is in the disclosure and is dated 13 April 2009. It states, consistently with Dr Wright's evidence, that the proposal is "*founded on a secure distributed timestamp sever*" (p.11). [247] COPA alleges that the document is inauthentic but not that it is forged. Dr Wright's evidence is that the anomalous features in the document identified by Mr Madden[248] result from the fact that it has been "*opened multiple times*".[249]

[244] {Day 11/11/10}.
[245] Matthews 1 [30]-[33] {E/5/7}.
[246] {Day 11/107/24-25} and {Day 11/108/15}.
[247] {L5/50} (ID_004537).
[248] PM47 {H/289/1}.
[249] {Day 6/156/12}.

132. It is notable that Dr Pang recalls Dr Wright asking him (and a number of other BDO employees) whether they had heard of Satoshi Nakamoto "*or something that sounds like that name*"[250] at around the time the White Paper was released in late October or shortly thereafter (he accepted in cross-examination that "*early November*" was possibly the right date[251]). Dr Pang was realistic about the quality of his recollection of this event: he acknowledged that his recollection was "*very hazy*" but explained that he had tried to recollect it as best he could and considers it to be true.[252] Although the precise details may be hazy, this is plainly an event that did in fact take place. Dr Pang is not making this up (and it was not put to him that he was). The event is therefore a relevant piece in the jigsaw, even if only a small piece.

133. Dr Wright mentioned "*blockchain*" to Mr Jenkins in 2008 (probably around December 2008):

133.1. Mr Jenkins confirmed during cross-examination that it was Dr Wright who first mentioned the word "*blockchain*" to him in 2008:[253]

> 10 Q. Now, in paragraph 17, that's when you say that you first
> 11 recall the word "blockchain" in 2008. That was a very
> 12 precise year, Mr Jenkins. Is it your evidence that
> 13 Dr Wright told you the word "blockchain" in 2008?
> 14 A. That's my recollection, that's correct.

133.2. This is likely to be a reference to the occasion when Dr Wright mentioned "*the term blockchain or chain of blocks over lunch*"; and, with the help of a drawing on a napkin, "*explained that these boxes/nodes would keep the same copy of the data block*"[254]. Mr Jenkins recalls that the conversation took place around the time of the general financial crash of 2008 and when Dr Wright left BDO.[255] That recollection fits with the underlying documents – in particular the emails showing when the lunch took place (2 December 2008).[256]

---

[250] {Day 9/35/1-2}.
[251] {Day 9/34/17-20}.
[252] {Day 9/37/2-12}.
[253] {Day 9/68}.
[254] {E/6/7} [28].
[255] {Day 9/79/5 to 81/13}.
[256] {L3/313/1-3}.

134. There is also evidence of Dr Wright sharing his "*Timecoin*" White Paper with Mr Jenkins following the release of the Bitcoin White Paper:

134.1. In cross-examination Mr Jenkins was asked about his evidence in the Granath Proceedings when, in response to a question about whether Dr Wright showed or sent him a White Paper related to blockchain technology, he answered: "*No, he didn't, never sent me anything…*"[257] The relevant exchange was as follows:[258]

> 23 Q. Then if we go -- if we could please go to page 12 of
> 24 the transcript {L18/62/12}, right at the top, you were
> 25 asked:
>
> 1 "Did Craig Wright ever show you or send you
> 2 a White Paper related to Blockchain technology?"
> 3 And you answered:
> 4 "**No, he didn't, never sent me anything**. There was
> 5 one meeting, I have a recollection that he did mention
> 6 to me that he had been working on documenting, you know,
> 7 what we had been discussing over a number of years, and
> 8 he pondered and thought, 'You may get something in
> 9 the post', you know?"
> 10 So your evidence in Granath, which you just accepted
> 11 is more reliable than your evidence in these
> 12 proceedings, you're quite clear there that you never
> 13 received a copy of the Bitcoin White Paper; isn't that
> 14 correct?
> 15 A. No, that's not correct. I think, actually, if you --
> 16 because this is a transcription of what I said, so there
> 17 are a smattering of errors in the transcription in any
> 18 case, and what I would more likely have said at that
> 19 stage is that, no, he didn't send me anything.
> 20 Q. So he didn't send you --
> 21 A. **And -- he didn't send me anything. Right? So that --**
> **22 it doesn't say that he didn't show me anything, just**
> **23 that he didn't send me anything, just to be specific**.
> 24 So, could you go to the recording on that and play that
> 25 to actually hear what I said, as to what's been
>
> 1 transcribed? And this is the first time I've seen
> 2 the transcription, so ...
> 3 Q. We can look at the -- we can look at the video ourselves
> 4 later on. I just want to clarify with you whether you
> 5 accept that, that he didn't send you a copy of
> 6 the Bitcoin White Paper, or do you say --
> 7 A. Correct.

[257] {L18/62/12}.
[258] {Day 9/87-89}.

8 Q. Okay. That's all I wanted to clarify…

134.2. Mr Jenkins was asked in re-examination about the distinction he was drawing here between what he was "*sent*" and what he was "*shown*":[259]

20 Q. Now, I'm not sure I've got a completely accurate note of
21 this, but can we go to page 85 of the [draft] transcript
22 of today. Is that possible? Lines 14 to 16. Here you
23 were being asked about -- something about the Norwegian
24 proceedings. Yes. So, the question was:
25 "So your evidence in ..."

1 On line 4:
2 "... your evidence in Granath, which you just
3 accepted is more reliable than your evidence in these
4 proceedings, you're quite clear that you never received
5 a copy of the Bitcoin White Paper; isn't that correct?"
6 Then you said:
7 "Answer: No, that's not correct. I think,
8 actually, if you -- because this is a transcription of
9 what I said ... there are a smattering of errors in
10 the transcription in any case, and what I would more
11 likely have said at that stage is that, no, he didn't
12 send me anything.
13 "Question: So he didn't send you --
14 "Answer: And -- he didn't send me anything. So it
15 doesn't say that he didn't show me anything, just that
16 he didn't send me anything ..." --
17 A. That's correct.
18 Q. -- "... just to be specific."
19 Did he show you anything?
20 A. I do. I do remember seeing a couple of things, besides
21 what Craig drew on the napkin. **At a -- at a subsequent**
22 meeting, I was shown a paper. It didn't make mention of
23 Bitcoin but it did make mention of -- of something
24 called Timecoin, and that was something that -- as
25 a White Paper that he -- he showed me at that time.

1 Q. You said a bit later. When was that?
2 A. It would have been in that time window I was saying. **It**
3 was before I joined Westpac and -- and after those
4 series of lunches where he drew on the -- on the napkin.
5 So, around, again, 2009/2010.
6 Q. And could you describe a little bit more fully
7 the context in which that conversation took place?
8 Where were you, for example?
9 A. It would have been in -- in one of the many cafes or

[259] {Day 9/95-99}.

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.

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?

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.

Q. And what, if any, conversation can you recall in association with it at the time it was shown to you?

A. Well, the key word for me was -- was "time". Where I cast my mind back to the initial firewall implementation that we did at Vodafone, and when we were discussing around this White Paper and some of the -- the drawings that were done on the napkin, a time server plays a critical role in the -- in the solution, and that was part of the -- not only a -- a serial increment around the entries that go into a log file but also the associated timestamp with those, and what wasn't mentioned, but was brought up today, was around the hashing of that. So when you actually looked at the -- the log file text itself, you didn't necessarily see the serialised number and/or the plain text date and timestamp on -- on each entry, but what you did see is - is a hashed version of it, and the hashed version is just an encrypted version of it, so it was less prone to -- to being tampered with.

Those -- those, and that conversation around the time server, and this concept then of using the time server as part of Timecoin, was something that wa discussed. It was -- it was a relatively esoteric part of -- of, you know, what this solution is, but nonetheless it was something that I was able to relate back to years earlier.

134.3. The Judge permitted further cross-examination on this topic because it amounted to "*quite important new evidence*" that arose directly out of Mr Jenkins' cross-examination.[260] As to this:

(a). It is accepted that, as the Judge put it, "*it's surprising it* [i.e. Mr Jenkins' evidence in relation to being shown a Timecoin paper] *hasn't been in any witness statement*".[261] However, when challenged in cross-examination about why he had not mentioned being shown the "*Timecoin*" paper previously, Mr Jenkins fairly made a point to the effect that his focus had previously been on what is known as the Bitcoin White Paper; and he clearly remembers not being shown the Bitcoin White Paper.[262] In these circumstances, the fact that Mr Jenkins had not mentioned being shown the "*Timecoin*" paper previously ought not to weigh too heavily against his evidence on this point.

(b). The further cross-examination focused on the fact that Mr Jenkins had written down the word "*Timecoin*" on a piece of paper.[263] There was some confusion about the precise sequence of events, but he clarified in the course of his questioning that he wrote down the word "*Timecoin*" during the cross-examination.[264] It was put to him that, "*that is a lie, Mr Jenkins and you did not write it down and that you wrote this before and that somebody told you to get it out*".[265] There is no justification for such a finding:

(i). Although COPA jumped to the conclusion that Mr Jenkins must be lying, there is an understandable explanation for why he had not mentioned the point earlier, namely Mr Jenkins' point that his focus had previously been on what is known as the Bitcoin White Paper.

(ii). COPA's suggestion of a dishonest 'put up job' ignores the fact that Mr Jenkins accepted that he saw the document in "*around 2009/2010*", which would place the event **after** the release of the Bitcoin White Paper in October 2008. If the conspiracy suggested by COPA had really taken

[260] {Day 9/99/6-9}.
[261] {Day 9/99/10-12}.
[262] {Day 9/101/10-19}.
[263] {Day 9/99/15 to 105/9}.
[264] {Day 9/101/5-7} and {Day/9/102-104}.
[265] {Day 9/104/12-14}; see also {Day 9/102/5-14}.

place, it would no doubt have made arrangements for a different timeline to emerge (i.e. Mr Jenkins seeing the document **prior** to October 2008). For these reasons, COPA's theory is illogical.

(iii). The allegation was not put to Dr Wright (who is presumably the person COPA would say "*told* [Mr Jenkins] *to get it out")* when he returned to the witness box after Mr Jenkins' cross-examination.

(iv). It should also be noted that Mr Jenkins was not asked at the outset of his cross-examination about whether he had any notes with him. In these circumstances the Court should be slow to find that COPA's allegation of dishonesty is made out (and, for the reasons give above, the allegation is not made out).

135. There is another significant category of circumstantial evidence post-dating the White Paper that supports Dr Wright's case on the Identity Issue, which is addressed immediately below.

H. Patent Research and Development

136. Dr Wright's deeply held belief is that identity is proved through work and knowledge:

136.1. As he explained on a number occasions during cross-x, he views his extensive portfolio of patent research and development as a key aspect of such proof:[266]

3 By early March 2016 at any rate, you were in
4 discussions with both Mr Matthews and Mr MacGregor about
5 providing proof that you were Satoshi, as required under
6 that agreement, weren't you?
7 A. Not the way you're saying**. I kept saying that we needed**
8 to prove things by knowledge, etc. An example was,
9 I had phone calls to Gavin and I spoke to him. My
10 argument for proof was I need to demonstrate, I need to
11 file patents, I need to have help getting those filed
12 and I need to demonstrate my work. Rob had a deal with
13 Silicon Valley where he was going to sell the product,
14 and the conditional part that I understand from that
15 deal is not that I proved myself in any other way than
16 anonymously, I had to basically go against all my
17 beliefs and not prove identity to use a key, but use

[266] {Day 7/135}; {Day 7/152}.

18 a key and be an anonymous cypherpunk, and that's
19 the only way that that billion dollars would come in for
20 him.

[…]

16 A. As I've actually stated multiple times, message signing
17 requires that the proof session happens. The proof
18 session wasn't just, "Here's a key and I'm going to use
19 it". There was supposed to be a proof pack, it was
20 supposed to go into all of my work, the hundreds of
21 papers I had, the thousands of patents I've now filed.

136.2. Indeed, the emphasis that Dr Wright placed on his patent portfolio in response to questions challenging the evidence in support of his claim to be Satoshi served to highlight the importance that Dr Wright attaches to this point:[267]

5 Q. Dr Wright, without genuinely supportive witnesses,
6 reliable documents or cryptographic proof, there's just
7 no basis for your claim to be Satoshi, is there?
8 A. No, absolutely wrong. I have more patents developed
9 than anyone in this industry going back even further;
10 I have a workload that when, in 2016, the company was
11 sold, shows 1,300 completed and 600 in progress papers,
12 of that now 1,000 have been granted patents, 4,000 are
13 pending. That in itself is evidence.

137. The extensive nature of Dr Wright's patent portfolio is not in dispute:

137.1. He was not challenged on his evidence that nChain has amassed a substantial portfolio of patents, encompassing nearly 4,000 patent filings, which are the fruit of Dr Wright's prior research.[268]

137.2. In the course of questioning about the Heads of Terms, Dr Wright explained that in June 2015 the documents he had amounted to research that was ready to be turned into patents (rather than patents that had been applied for or granted at that stage):[269]

20 Q. How many patents had been applied for and granted, by
21 that stage, which were the subject matter of this
22 agreement?
23 A. Patent applied for, no; that's why we needed help.

[267] {Day 8/109}.
[268] Wright 1 [172] {E/1/31}.
[269] {Day 7/97-98}.

24 I didn't know how to. What I had at this stage was
25 1,300 ready to be turned into patents documents. So,

1 when Cerian and the Australians came in, I had 1,300
2 research projects. The average of those is about five
3 to six patents per document.

(He was not challenged in relation to the above answer.)

137.3. Nor was he challenged (at least on the factual point relating to the number of patents he relies on) when he responded as follows to COPA's allegation that his claim to be the author of the White Paper is false:

4 You are not the author of the Bitcoin White Paper or
5 the Bitcoin source code or the person who invented and
6 released the Bitcoin System, are you?
7 A. I am the person who invented Bitcoin, who invented
8 the hash chain system, who invented a timestamp server,
9 as section 3 of my paper --
10 Q. The claim --
11 A. ... notes. I am the person who created over 1,000
12 granted patents on that technology --
13 Q. Your claim --
14 A. -- 4,000 pending patents.

138. A particularly significant example of Dr Wright's patent development is his work on Terranode (formerly known as iDaemon),[270] which is a scalable implementation of the Bitcoin protocol. This demonstrates, in Dr Wright's view, a deep understanding of Bitcoin's foundational technology and its potential. His investment and developmental efforts have been directed towards achieving Satoshi's vision for Bitcoin to handle a significantly higher volume of transactions. They provide, in Dr Wright's view, compelling evidence supporting his claim to be Satoshi.

139. Mr Matthews explained during cross-examination that, although nChain is "*not reliant on Craig Wright*", the company is founded on the intellectual property that it acquired from Dr Wright (via the DeMorgan Group) in 2015; and Dr Wright continues to be an inspiration to the research team at nChain:[271]

25 Q. Well, your company, nChain, has, from the start, based

[270] {CSW/84/1}.
[271] {Day 12/93/25 to 95/5} and {Day 12/96/10 to 97/5}.

its pitch to market on Dr Wright's supposed work and his claim to be Satoshi, hasn't it?

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 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.

[…]

Q. Finally, just this: your story of Dr Wright giving you the Bitcoin White Paper and telling you about his Bitcoin invention in 2008 is a falsehood to back up that claim?

A. That's not true. As I sit here, nobody can take away from me the experiences that I had during those years: the conversations, the drawings on whiteboards; I didn't imagine that. So whatever the outcome, I don't think it's going to have any material difference on nChain. Craig will continue being an inventor with a consulting agreement with our licensing company in Switzerland. He'll continue to be a provider of innovation into our research team. 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.

140. The relevance of Ms Jones' evidence is limited to providing support for Dr Wright's evidence on the extensive nature of his patent portfolio; and providing a few examples of the patents in question. As Ms Jones explains, she has been working continuously on Dr Wright's intellectual property since meeting him and Mr Matthews in 2015.[272] It is accepted, however, that the granular detail relating to the specific patent applications addressed in her evidence will be of limited (if any) assistance to the Court's resolution of the Identity Issue.[273]

141. The cross-examination of Ms Jones was used by COPA as an attempt to establish by the back door that Dr Wright may not have been the "*real inventor*" of (at least some of) the patents referred to in Ms Jones' evidence. The following exchange provides an illustrative example:[274]

> Q. Just one last question then before lunch. You have relied on number 42 in your evidence --
> A. Mm-hm.
> 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 Savanah that was involved. **Do you accept that it's possible that actually the real inventor behind number 42 was Mr Savanah and not Dr Wright?**
> A. "Possible" and actual fact are very different things, aren't they.
> Q. Do you accept it's possible?
> 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.
> MR MOSS: My Lord, we can stop there for lunch.
> **MR JUSTICE MELLOR: Well, just before we do, that piece of evidence, what use is it if none of this was raised with Dr Wright?**

[272] Jones 1 [6] {E/14/3}.
[273] {Day 10/64/5-18}.
[274] {Day 10/69-72}.

10 MR MOSS: Well, it goes -- the point was the last point that
11 I took, that she is relying on this document, but
12 the internal records appear to show -- and obviously
13 the key point here is that there are two inventors on
14 it, not just Dr Wright. It's clear from Dr Jones'
15 evidence -- I assumed that she might have had some
16 knowledge of the internal process of this, but she says
17 she doesn't, so she couldn't comment on that.
18 MR JUSTICE MELLOR: Yes, but Dr Wright wasn't challenged on
19 any of this.
20 MR MOSS: Well, Dr Wright -- this is her evidence.
21 Dr Wright doesn't rely on this patent in the same way
22 Dr Jones does.
23 MR JUSTICE MELLOR: Well, I thought he was relying on
24 thousands of patents.
25 MR MOSS: He's relying on thousands of patents, yes. His

1 story is a broad one about: his invention proves he is
2 Satoshi.

142. As the Judge's interventions indicate, this line of questioning goes nowhere in circumstances where the points that were being put to Ms Jones (i.e. to the effect that it was "*possible*" that Dr Wright was not the "*real inventor*" of the patents in question) were not put to Dr Wright.

I. The private proof sessions

143. As submitted in Dr Wright's Skeleton Argument, the private proof sessions conducted during 2016, in which Dr Wright demonstrated his possession of private keys to certain of the original blocks of the Bitcoin blockchain, are significant.[275] The fact that he separately persuaded each of Mr Matonis and Mr Andresen that he was Satoshi is highly probative of his case on the Identity Issue.

144. Dr Wright commented, in his Skeleton Argument, on the speculative nature of the expert evidence adduced by COPA from Professor Meiklejohn on the "*possibility*" of one or more of the private signing sessions having been subverted.[276] That remains the position: the expert evidence opining on the ***theoretical possibility*** of the sessions having been subverted remains speculative and, Dr Wright submits, divorced from reality.

[275] Dr Wright's Skeleton Argument [5(8)] and [157]-[166] {R/14/8} and {R/14/54-57}.
[276] Dr Wright's Skeleton Argument [164] {R/14/56}.

145. Professor Meiklejohn added speculation upon speculation in her Second Report, which was served during the course of the trial without prior notice or permission having been sought in advance from the Court.[277] In cross-x, Professor Meiklejohn appeared to resile from some of the speculation in that further report, saying that she was "*not suggesting ... at all*" that Dr Wright had engaged in particular forms of DNS hijacking which she had set out in the report.[278] When shown in cross-x that the particular kind of hijacking was discussed in her report, despite her claim to the contrary, she resorted to saying that this was "*not really what I'm suggesting*".[279]

146. This lack of clarity about precisely what COPA is contending is reflected in the unsatisfactory state of its pleadings on subversion of the signing sessions. Whilst COPA denies in its Reply that Dr Wright privately demonstrated to Mr Andresen, Mr Matonis and others during 2016 that he had access to the private keys associated with early blocks,[280] COPA does not identify anywhere in its statements of case whether it alleges that Dr Wright actually subverted any of the private proof sessions and if so, which session(s) he subverted and how he did so. This is a critical omission if and insofar as COPA intends to invite the Court to find that any particular session was actually subverted. That would amount to a finding of fraud and deception, which would need to be clearly and specifically pleaded[281] (but has not been).

147. Furthermore, COPA did not put any clear case of subversion to Dr Wright in cross-x. At most, COPA suggested to Dr Wright that it would have been "*feasible*" to create a malware program and "*straightforward for someone with [Dr Wright's] experience*" to stage the signing session with Mr Andresen.[282] It was not put to Dr Wright that he in fact created a malware program to deceive Mr Andresen (or anyone else) or that he actually 'staged' the Andresen signing session (and if so, how). Nor was Dr Wright cross-examined about subversion of the other signing sessions. Importantly, it was not suggested to him that he engaged in the elaborate DNS hijacking mooted in Professor

[277] {G/10/1-7}.
[278] Meiklejohn {Day 18/132/16-21}
[279] Meiklejohn {Day 18/132/22}-{Day 18/134/13}.
[280] COPA Re-Amended Reply [19] {A/4/5}.
[281] On the law, see the Judge's summary at {B/27/14-15} [39]-[43].
[282] Wright {Day 8/73/22}-{Day 8/74/23}.

Meiklejohn's Second Report (which was only served after Dr Wright had finished giving evidence on Day 8).[283]

148. In these circumstances, Dr Wright submits that it is not open to COPA to advance a case in closing submissions that he deliberately subverted any of the signing sessions during 2016. Accordingly, the Court should not make any findings to that effect. For completeness, Dr Wright nevertheless addresses the question of subversion, as canvassed by the digital technology experts, below.

The facts

149. The facts relating to the sessions with the journalists and Mr Matonis are addressed in Wright 1 [191]-[193][284] and [208]-[215][285], Matthews 1 [83]-[87] [286], Wright 2 [7]-[15] and [23]-[32][287] and Wright 9 [63]-[66].[288] In summary:

149.1. Dr Wright used his personal laptop, which was configured to run on two separate operating systems (i.e. Windows and Linux). This set up allowed shared access to the 'C:' partition by both operating systems. This is not in dispute.[289]

149.2. Bitcoin Core was downloaded, installed and allowed to download the whole blockchain on both machines. This is also not in dispute.[290] Dr Wright's position is that this was an optimal platform for providing such a demonstration.[291]

149.3. Dr Wright signed a message of a speech by Jean-Paul Sartre which was stored in a file named "Sarte.txt", using the private key corresponding to the public key used in the coin generation transaction in block 9.[292]

[283] Dr Wright was subsequently recalled for cross-x on the LaTeX files and Ontier emails, but no application was made to question him further on the signing sessions.
[284] {E/1/34}.
[285] {E/1/36}
[286] {E/5/17}.
[287] {E/2/4-6 and 8-10}.
[288] {E/26/18}. Subject to the qualifications expressed therein, Wright 9 accepts that Professor Meiklejohn's summary in Meiklejohn 1 [20] {G/2/50} is broadly correct.
[289] See Meiklejohn 1 [120(a)-(c)] {G/2/50}.
[290] See Meiklejohn 1 [120(e)] {G/2/50}.
[291] Wright 9 [52] {E/26/15}; see also {Day 18/93/2 to 96/23}.
[292] Block 9 is significant because it records the first Bitcoin transaction from Satoshi to Hal Finney: see e.g. Meiklejohn 1 [110] {G/2/46}.

150. Turning to the session with Mr Andresen (the "**Andresen Session**"), the facts are addressed in Wright 1 [194]-[207][293], Matthews 1 [88]-[98][294], Wright 2 [16]-[21][295] and [33]-[41][296] and Wright 9 [84]-[103][297] and the Andresen Deposition. In summary:

150.1. The meeting took place in a hotel in Covent Garden in a room downstairs.

150.2. The overall process followed was that Dr Wright signed a message on his laptop, transferred the signature to a new laptop, and verified the signature on that laptop.[298]

150.3. As indicated above, Dr Wright used his own laptop to produce the signed message. He already had Electrum installed on his own laptop.[299]

150.4. Mr Andresen had brought his own laptop with him to the session.[300] However, Dr Wright objected to Mr Andresen's laptop being used for the verification stage because he did not want any evidence to leave the room.[301]

150.5. This led to a brand-new laptop being procured by an assistant:

(a). Professor Meiklejohn refers to this as a laptop that "*seemed new*".[302] This formulation arises out of Mr Andresen's acknowledgement that he did not accompany the assistant to purchase the laptop or check that it was factory sealed;[303] and is designed to cast doubt on whether the laptop was in fact new.[304]

(b). However, Mr Andresen stated that the laptop was a "*brand-new laptop*"; explained that it was "*unpacked and booted up for the first time in front of me*";[305] and confirmed that when the computer started up, it booted up with the

[293] {E/1/34}.
[294] {E/5/18}ff.
[295] {E/2/7-8}.
[296] {E/2/10-13}.
[297] {E/26/22-25}.
[298] Wright 9 [89] {E/26/23}.
[299] Wright 2 [35] {E/2/11}.
[300] {E/17/74} (p. 73 l.13).
[301] Matthews 1 [93] {E/5/20}; {Day 8/67/7-9}
[302] Meiklejohn 1 [127(d)] {G/2/53}.
[303] {E/17/75} (p.74 ll.13-18).
[304] See {Day 18/99/18 to 103/3}.
[305] {E/17/74} (p.73 ll.18-24).

typical initial start-up that is required on a new computer.[306] A fair-minded reading of that evidence suggests that the laptop was indeed new, not merely that that it "*seemed*" new.

(c). Mr Matthews's evidence is that "*[t]he new laptop was in a sealed box*".[307] It was not put to Mr Matthews that the laptop was not in a sealed box.[308] Indeed, during Mr Matthews' cross-examination, Mr Hough KC appeared to accept that "*a new laptop had to be used*".[309]

(d). Dr Wright's evidence is that it was a "*brand-new laptop from a retail store*".[310] It was not put to Dr Wright that the laptop was not brand-new.

(e). In light of the evidence referred to above, the Court is invited to find that the laptop was brand new.

150.6. The internet connection used was the hotel WiFi. The Andresen Deposition states that the hotel WiFi was used for the download of the signing software (which is consistent with the evidence of Dr Wright[311] and Mr Matthews[312]), though Mr Andresen accepted that it is "*possible*" that the hotel WiFi was not used.[313] The noting of that possibility is not sufficient to justify a finding that the hotel WiFi was not used, particularly in circumstances where the evidence of Mr Andresen, Mr Matthews and Dr Wright is all consistent on this point.

150.7. Windows (probably Windows 10) was installed on the new computer. Professor Meiklejohn notes that "*[i]t is not clear who set up*" the new laptop.[314] Dr Wright suggests that Mr Andresen "*took the lead*"[315], whereas Mr Andresen's notes suggest that they "*setup the Laptop together… with [Mr Andresen] being present*

[306] {E/17/75} (p.74 ll.19-22).
[307] Matthews 1 [95] {E/5/20}.
[308] See {Day 12/79/4-12}. Putting to Mr Matthews that in the Kleiman Proceedings Mr Andresen said he did not check that the laptop was factory sealed does not amount to putting to Mr Matthews that the laptop was not in fact factory sealed.
[309] {Day 12/78/15-16}.
[310] Wright 2 [34] {E/2/11}. See also {Day 8/67/18-19}.
[311] Wright 2 [37] {E/2/11}; Wright 9 [91] {E/26/23}. An answer given by Dr Wright in cross-x might be said to cast some doubt on this {Day 8/68/4-5}, but not sufficient doubt to suggest that the hotel WiFi was not used.
[312] Matthews 1 [95] {E/5/20}; see also {Day 12/78/20-24}.
[313] {E/17/76-77} (p.75 l.22 to p.76 l.14).
[314] Meiklejohn 1 [127(f)] {G/2/53}.
[315] Wright 2 [36-37] {E/2/11}

at all times".[316] This is not a significant difference in circumstances where it is clear that Mr Andresen had, at the very least, oversight of this process. Hence the references in the Andresen Deposition to the new laptop being "*unpacked and booted up for the first time in front of me*" and it "*boot[ing] up with the typical initial startup that's required on a new computer*".[317]

150.8. As for the software used for the signing verification:

(a). Dr Wright accepted in cross-x that he chose Electrum.[318] This is consistent with Mr Andresen's evidence.[319]

(b). Electrum software was downloaded onto the new laptop. It is likely that Google Chrome was used.[320] The Electrum download was probably done by Mr Andresen, though in cross-x Dr Wright clarified that (i) he was "*not 100% sure*" on "*[e]xactly who downloaded each bit*" but (ii) Mr Andresen was "*looking over my shoulder*"[321] whenever Dr Wright was on the computer (which is likely given the nature of the exercise and the fact that Mr Andresen had been flown in specifically to observe and oversee the process). Mr Matthews' evidence is that Mr Andresen operated the laptop.[322]

(c). The weight of evidence supports the view that the software was downloaded from the Electrum website.[323]

(d). Mr Andresen did not recall whether he verified that the website from which the software was downloaded had the HTTPS security certificate.[324] Professor

---

[316] {L19/217/4}. The background to these notes is explained in the Andresen Deposition: {E/17/76} (p.75 ll.8-14} and {E/17/80-82} (p.79 l.10 to p.81 l.11). In summary, they are the product of messages between Mr Andresen and another Reddit user who was seeking to summarise the events in question (which Mr Andresen copied and pasted into a document for the purposes of preparing for his deposition); Mr Andresen suggested some details were incorrect but did not subsequently correct the position; nevertheless he accepted during his deposition that they are the best documentary record he had of what probably happened.
[317] E/17/74} (p.73 ll.18-24) and {E/17/75} (p.74 ll.19-22).
[318] {Day 8/69/3-6}.
[319] {E/17/76} (p.75 l.21).
[320] {Day 8/74/22}.
[321] {Day 8/68/12-17} and {Day 8/78/6-18} to similar effect. This clarification resolved the minor difference between Dr Wright and Mr Andresen on whether it was the former or latter who downloaded the software: Wright 2 [38] {E/2/11} and Andresen Deposition {E/17/74-75} (p.73 l.25 to p.74 l.1) and {E/17/76} (p.75 ll.19-21).
[322] Matthews 1 [95] {E/5/20}.
[323] Wright 2 [38] {E/2/11} and {Day 8/70/9-19}; Wright 9 [95] {E/26/24} and Andresen Deposition {E/17/77} (p.76 ll.1-2).
[324] {E/17/77} (p.76 ll. 15-19).

Meiklejohn was therefore wrong to say that this check was not carried out (as she accepted in cross-x);[325] and the premise of one of the questions put to Dr Wright (i.e. that Mr Andresen said in the Kleiman Proceedings that he did not check the security certificate[326]) was false. Professor Meiklejohn accepted that a green padlock would have been visible on the Electrum website.[327]

(e). Dr Wright's evidence is that the integrity of the software was checked by comparing its hash value with the one provided on the website.[328] Mr Andresen said that he did not verify the hash digest of the download against something he had brought with him independently.[329] As Professor Meiklejohn noted, the latter point "*does not mean that the download could not have been verified against the website hash as stated by Dr Wright*".[330]

150.9. Mr Andresen chose the message. Dr Wright added the letters "CSW" at the end.[331] The full message appears to have been "*Gavin's favorite number is 11 – CSW*".[332]

150.10. Mr Andresen was asked which of the first 11 blocks he wanted Dr Wright to use for the demonstration.[333] Dr Wright provided a signed message using (at least) the public key for block 9.[334] It is likely that block 1 was also used.[335]

150.11. Dr Wright and Mr Andresen agree that a USB stick was used to move the signed message from Dr Wright's laptop to the new laptop for the purposes of the verification.[336] Given that Mr Andresen had brought with him "*a brand-new, sealed in the package USB stick*", it is reasonable to infer that is what was used for this part of the process; and that is consistent with Dr Wright's evidence[337].

[325] Meiklejohn 1 [130(a)] {G/2/56}; {Day 18/114/20-22}.
[326] {Day 8/75/15-16}.
[327] {Day 18/116/13-16}.
[328] Wright 2 [38] {E/2/11}.
[329] {E/17/77} (p.76 ll.20-25).
[330] Meiklejohn 1 [127(j)] {G/2/54}. See also Wright 9 [96] {E/26/24}.
[331] Wright 9 [99] {E/26/24}.
[332] {E/17/83} (p.82 ll.20-24}.
[333] Wright 1 [206] {E/1/26}.
[334] Wright 2 [40] {E/2/12}; Andresen Deposition {E/17/75} (p.74 ll.8-10).
[335] Wright 9 [100] {E/26/25}. See also {L19/217/5}. Professor Meiklejohn acknowledged she missed the reference to block 1 in Mr Andresen's notes {Day 18/107/3-8}.
[336] Wright 9 [101] {E/26/25}; Andresen Deposition {E/17/83} (p.82 ll.12-14).
[337] Wright 1 [207] {E/1/36}.

However, it should be noted that Mr Andresen did not specifically recall that USB ever being removed from its bubble wrapping, albeit he said it might have been.[338]

150.12. Mr Andresen brought with him "*a list of all the early block public addresses*" and he verified "*at least the first four to six and the last four to six*" in order to check that the public addresses were correct.[339] This is consistent with Dr Wright's evidence, though Dr Wright adds that the addresses were also checked on the block explorer.[340]

150.13. For the verification, Dr Wright manually typed in the message. The first time he did so there was an error. It worked the second time when the message was typed correctly.[341]

A "rather casual interaction"?

151. In the course of her cross-x, Professor Meiklejohn expressed her understanding of the private proof session with Mr Andresen in the following terms:[342]

> 18 […] You would
> 19 reasonably expect a verifier in his position to be alert
> 20 to any indication that the process was being subverted?
> 21 A. Not really. I mean, **my understanding of the session,**
> **22 from Gavin Andresen's own words, is that he viewed this**
> **23 as a rather casual interaction designed to convince him**
> **24 and only him, and that he expected Dr Wright to follow**
> **25 up with public evidence days later. So I think he**
>
> **1 wouldn't have put the effort in to perform those checks**
> **2 given that he thought that this wasn't that big a deal.**

152. This is not a fair or objective characterisation of Mr Andresen's evidence:

152.1. In the Andresen Deposition, Mr Andresen described the purpose of the session as "*proving to me beyond a reasonable doubt that Craig Wright is Satoshi Nakamoto*".[343] Although he acknowledged that the purpose was not to "*prove to the world that Craig Wright is Satoshi Nakamoto*" and even that he did not expect

[338] {E/17/82} (p.81 ll.22-24).
[339] {D/17/87} (p.86 ll.3-8).
[340] Wright 9 [102] {E/26/25}.
[341] Wright 9 [103] {E/26/25}; Andresen Deposition {E/17/83} (p.82 ll.14-17).
[342] {Day 18/117-118}.
[343] {E/17/89-90} (p.88 l.4 to p.89 l.5).

the session to have quite as much weight as it did, the fact that Mr Andresen's understanding was that the purpose of the session was to provide proof to such a high threshold ("*beyond a reasonable doubt*") is difficult to reconcile with Professor Meiklejohn's view that Mr Andresen considered the process to be a "*rather casual interaction*" that was no big deal.

152.2. The Andresen Deposition also explains that, following the proof session, Mr Andresen was convinced "*beyond a reasonable doubt*" that Dr Wright was Satoshi.[344] The fact that Mr Andresen was convinced "*beyond a reasonable doubt*" is all the more striking in circumstances where his starting point was that he was "*extremely skeptical*".[345] Once again, Mr Andresen's language emphasises that this proof session was not a casual interaction but one designed to provide him with reliable proof.

152.3. When asked about whether he thought it was strange that he was being told "*none of this is about money*", Mr Andresen responded as follows:[346]

> "*Being Satoshi Nakamoto is about much more than money. He's almost a God-like figure in the Bitcoin community. He's the holy founder of this world-changing technology. So saying 'this is not about money' did not strike me as strange because of that.*
>
> *Because, you know, having been the chief scientist of the Bitcoin Foundation and the lead developer for the project, I had felt the kind of weight of that responsibility, and to take on the mantle of being Satoshi Nakamoto struck me as, you know, much more important than – than the money. So that's where my head space was through this conversation.*"

Mr Andresen's description of the weight of responsibility he felt in meeting "*the holy founder of his world-changing technology*" is yet another feature of his evidence that is difficult to reconcile with Professor Meiklejohn's view.

153. In addition to Mr Andresen's own words, the surrounding circumstances (of which Professor Meiklejohn was aware) are plainly inconsistent with Professor Meiklejohn's view:

---

[344] {E/17/117} (p. 116 l.5 to 117 l.3).
[345] {E/17/39} (p. 38 ll.16-17) and {E/17/40-41} (p.39 l.20 to p.40 l.2).
[346] {E/17/58} (p.57 ll.5-18).

153.1. The Andresen Deposition highlighted that Mr Andresen signed a non-disclosure agreement before attending the session.[347] It would be a rather odd "*casual encounter*" that required the signing of a non-disclosure agreement.

153.2. The Andresen Deposition explained that, prior to the session, Mr Andresen had identified four categories of evidence that any real Satoshi candidate would need to provide.[348] The fact that he was giving such careful consideration to what he would need to see in order to be convinced is another factor that undermines Professor Meiklejohn's characterisation.

153.3. Mr Matthews' witness statement, which Professor Meiklejohn had read, explained that Mr Andresen "*did not want to fly to London*" because "*[h]e was afraid of flying*".[349] It is unlikely that someone with a fear of flying would bother getting on a plane from Boston to London for the purpose of a casual encounter that was no big deal.

153.4. The Andresen Deposition makes clear that Mr Andresen was aware that the "*venture capital-type people*" working with Dr Wright wanted Mr Andresen "*to participate in a public endorsement of Craig Wright as Satoshi*".[350] A merely casual encounter would not have involved a second stage of public endorsement.

153.5. The session itself involved the procuring of what Mr Andresen described as a "*brand-new laptop*" that was "*unpacked and booted up for the first time in front of me*".[351] Even though Professor Meiklejohn has focussed on details such as Mr Andresen not accompanying the assistant to purchase the new computer and not verifying that it was factory sealed, the fact that a new computer was procured does not fit with the idea that this was merely a casual encounter. Mr Andresen also says that he brought with him "*a brand-new, sealed in the package USB stick*"[352] – yet another detail indicating the care that was being taken in relation to a session aimed to provide Mr Andresen with proof beyond a reasonable doubt.

---

[347] {E/17/37} (p. 36 l.10 to p.37 l.10).
[348] {E/17/41} (p. 40 ll.3-19).
[349] Matthews 1 [88] {E/5/18}.
[350] {E/17/43} (p.42 ll.7-25).
[351] {E/17/74-75} (p.73 l.8 to p.74 l.1).
[352] {E/17/74} (p.73 ll.12-15).

153.6. Mr Matthews' statement explained that the encounter was such a significant one for Mr Andresen that he had rehearsed in his own mind a number of times how he would respond if he ever came face to face with Satoshi. He had come to the conclusion that he simply wished to shake his hand and say thank you.[353] On any view, this was a moment of profound significance for both Mr Andresen and Dr Wright (who, according to Mr Matthews, was brought to tears by Mr Andresen's gesture of gratitude).

153.7. The fact that Professor Meiklejohn has identified a few examples of checks that could have been but were not carried out (and in respect of one of those she has inaccurately recorded Mr Andresen's evidence[354]) does not come close to justifying her mischaracterisation of the nature of the exercise.

154. In light of the evidence referred to above, no objective, independent expert could reasonably have come to the conclusion that the private proof session with Mr Andresen was "*a rather casual interaction*" that Mr Andresen thought "*wasn't that big a deal*". Professor Meiklejohn's false premise about the nature of the exercise has coloured the opinions expressed in her reports, which are addressed in more detail below.

Expert evidence on subversion of the signing sessions

155. The experts were agreed that it was in principle ***theoretically possible*** to subvert the kind of signing sessions conducted by Dr Wright during 2016. However, that does not mean that any of the sessions was actually subverted. There would have been serious practical obstacles in the way of successfully subverting the sessions. The precise nature of the obstacles would depend upon the kind of subversion which is said to have been implemented at any particular session.

156. The experts agreed that when considering the possibility of subversion of a signing session, what mattered was the integrity (or otherwise) of the verifier's software.[355] Whilst it would have been theoretically possible (and even simple) to devise software that would always output a 'true' result when verifying a signed message, the software would need to be installed on the verifier's computer to achieve its intended effect. This

[353] Matthews 1 [96] {E/5/20}.
[354] I.e. the point about checking the HTTPS certificate {Day 18/114/20-22}.
[355] Gao {Day 18/17/3}-{Day 18/20/2}.

would require either physical or remote access to that computer.[356] Certainly in the case of the Andresen Session, neither type of access would have been straightforward to procure.

157. As already explained, a brand new laptop was purchased, unpacked and booted up, with a new operating system, for the Andresen Session. The booting up and software installation was carried out in front of Mr Andresen, who can reasonably be expected to have been alert for signs of tampering or other underhand activity during that process.

158. Procuring remote access to the verifier's computer would have been more complicated in the case of the Andresen Session. Several possibilities were canvassed by Professor Meiklejohn, all of which were focussed on interfering with the Electrum wallet software that was downloaded and used for the signing session with Mr Andresen. However this might have been achieved, tampering with the download of Electrum software would have been vulnerable to Mr Andresen (a highly accomplished computer expert) identifying that (i) the wrong website URL was being accessed, (ii) the necessary website certification was not available and/or (iii) the appropriate security indicator for the website (such as a green padlock) was not showing in the browser. As Mr Gao said, whilst modifying software might be straightforward, fake software "*can be easily detected*"; "*its one thing to tamper the software, its another thing to pass the test*".[357]

159. In this context, it is pertinent to recognise the stature and expertise of Mr Andresen. He majored in Computer Science at Princeton; he had professional expertise in writing software; he became involved in Bitcoin in 2010; he assumed the role of lead core developer of Bitcoin in around April 2011; he became the Chief Scientist of the Bitcoin Foundation in around 2012; and, as Professor Meiklejohn agreed, at the time of the signing session, he was one of the most qualified experts on Bitcoin.[358] In light of his qualifications, experience and skills, Mr Andresen's presence and oversight of the process introduced an additional layer of security. The suggestion that he could inadvertently fall prey to a website download spoofing attack is highly improbable. His

[356] See Meiklejohn First Report [130] {G/2/56}-{G/2/58}: contemplating installation of malware directly on the verifier's computer or compromising the WiFi network or software download.
[357] Gao {Day 18/25/15}-{Day 18/26/8}.
[358] See Meiklejohn {Day 18/110/11} to {Day 18/111/22}.

technical prowess and experience makes it unlikely that any such attack could have succeeded.

Professor Meiklejohn's further evidence

160. In an attempt to rebut evidence given in cross-x by Dr Wright about the difficulty inherent in spoofing a download of fake Electrum wallet software, COPA adduced further expert evidence from Professor Meiklejohn on the methods that might theoretically be used to compromise the download of such software.[359] This evidence is highly speculative and lacks reality.

161. Professor Meiklejohn posited three possibilities: (i) a typosquatting attack, (ii) a homograph attack, and (iii) DNS hijacking. Each is considered in turn below.

162. **A typosquatting attack** involves the attacker setting up a fake domain with a name closely corresponding to the genuine target domain (e.g. electrurn.org rather than electrum.org). Professor Meiklejohn accepted that this type of attack was (i) crude and (ii) could be detected by careful visual inspection of the URL displayed in the computer's browser. She also agreed that Mr Andresen would have known what URL they were intended to go to in order to download the Electrum wallet software.[360] It is unrealistic to contemplate Mr Andresen being duped in this way or Dr Wright (or anyone else) thinking that such an attack could succeed.

163. There is furthermore no evidence of any fake domains having been established with names closely corresponding to electrum.org. Professor Meiklejohn said that she had looked for variations of electrum.org but was unable to explain what she had found, if anything. She did not suggest that there was any evidence of the domain names identified in paragraph 13(a) of her Second Report, including electrurn.org, electrum.com and wwwelectrum.org, having been registered.[361]

164. **A homograph attack** involves the attacker setting up a fake domain with characters from a different alphabet, thereby making it more difficult to detect visually (because the fake domain name would appear identical to that of the genuine domain). Professor

[359] Meiklejohn Second Report {G/10}; Meiklejohn {Day 18/119/23}-{Day 18/138/19}
[360] Meiklejohn Second Report [13] {G/10/4}; Meiklejohn {Day 18/120/21}-{Day 18/121/3}
[361] Meiklejohn {Day 18/121/22}-{Day 18/123/2}.

Meiklejohn noted in her Second Report that all major browsers had implemented defences against this type of attack but implied that those defences had, at least in the case of Google Chrome, been in place only since 25 May 2016, when Google released what she described as "*a defence*" in version 51.[362] The clear inference from her report was that Google Chrome had no defence against homograph attacks at the time of the Andresen Session.

165. This evidence was shown to be inaccurate and misleading in cross-x. Professor Meiklejohn accepted that (i) computer scientists had known about homograph attacks since at least 2002; (ii) the major browsers, including Google, had therefore been aware of the issue for a long time; and (iii) major browsers, and Google Chrome in particular, had defences in place against homograph attacks by no later than 2011. *The 2011 IDN Homograph Attack Mitigation Survey*, shown to Professor Meiklejohn in cross-x, recorded that Google Chrome had consistently achieved the highest ratings for mitigation against homograph attacks since 2009.[363]

166. Having been shown this material, Professor Meiklejohn sought to "*clarify*" what she had said in her report, which she acknowledged was "*confusing at best*". It was in fact misleading.[364] Professor Meiklejohn's 'clarification' was to explain that Google release 51, mentioned in her report, was the first defence that ignored special (i.e. non-default) settings that might have been configured by a user to accept a variety of alphabets. However, there is no evidence that the computer used in the Andresen Session was so configured. The only inference that can fairly be drawn on the available evidence is that cogent defences were in place on Google Chrome to protect users against homograph attacks by the time of the 2016 signing sessions.

167. Furthermore, both Mr Andresen and Dr Wright have confirmed that they set up the laptop together and that Mr Andresen was present at all times. He would likely have noticed any attempt to configure the browser with special settings (which would have been required to override Google Chrome's defences against homograph attacks). The notion that Dr Wright (or anyone else) could realistically have thought that a homograph attack would succeed in duping Mr Andresen is fanciful.

---

[362] Meiklejohn Second Report [13(a)] {G/10/4}
[363] {X/53/4-5}; Meiklejohn {Day 18/124/5}-{Day 18/126/23}
[364] Meiklejohn {Day 18/126/20}-{Day 18/127/20}.

168. There is moreover no evidence of any domains capable of being used for a homograph attack on electrum.org having ever existed. Professor Meiklejohn admitted that she had not investigated whether any such domains existed.[365]

169. **DNS hijacking** involves redirecting a computer to a malicious site. The paper exhibited by Professor Meiklejohn to her Second Report (the "**Akiwate Paper**") shows that such an attack could be carried out by an attacker configuring a computer so that it redirected to the fake site or by the attacker compromising a DNS server so that traffic to a genuine site was instead diverted to the fake site.[366]

170. Professor Meiklejohn acknowledged in her Second Report that the first type of attack, involving reconfiguration of a local computer so that it redirected to a fake site, would be vulnerable to detection by visual inspection unless the attacker had managed to secure a certificate from the genuine domain which could be passed off as applying to the fake domain. In the absence of a certificate, the browser would not display a green padlock verifying the authenticity of the connection: without a certificate, the user "*would be making an HTTP connection rather than an HTTPS connection, which would mean that you would lose the green padlock*".[367] It is, again, unrealistic to contemplate (i) an accomplished computer scientist such as Mr Andresen, who was looking to be satisfied "*beyond reasonable doubt*" that Dr Wright was Satoshi, overlooking such an obvious indication of tampering; or (ii) Dr Wright (or anyone else) thinking that they could succeed in duping Mr Andresen in that way.

171. The second type of DNS hijacking alluded to in Professor Meiklejohn's Second Report is far more sophisticated. It involves the attacker compromising an external DNS Server that was *ex hypothesi* outside the attacker's control, for example by compromising the domain registrar and flooding the DNS records with inaccurate information.[368] It is only by this route that an attacker would be able to procure a certificate to authenticate connections to a fake site. It is apparent from the Akiwate Paper and Professor Meiklejohn's evidence in cross-x that attacks of this kind are highly sophisticated; the

[365] Meiklejohn {Day 18/123/17-20}.
[366] {H/376/1-20}.
[367] Meiklejohn Second Report [13(d)] {G/10/5}; and Meiklejohn {Day 18/136/1-4}.
[368] Meiklejohn {Day 18/129/22}-{Day 18/131/15}.

Akiwate Paper refers to these attacks being carried out by "*state-affiliated actors*" and emphasises their sophistication.[369]

172. Professor Meiklejohn was evidently reluctant in cross-x to suggest that Dr Wright could have carried out a DNS hijacking attack of this kind ("*I'm not suggesting that at all, no*").[370] She wrongly claimed not even to have discussed this type of attack in her Second Report; and then re-iterated that she was "*not really … suggesting*" that this could have happened. The obvious inference is that no attack of this kind could realistically have been implemented by Dr Wright in order to subvert the Andresen Session. Any assertion to the contrary by COPA or the Developers would be unsustainable.

Conclusion

173. Dr Wright refused to accept in cross-x that it would have been "*entirely feasible*" or "*straightforward for someone with [his]experience*" to subvert the Andresen Session.[371] He was correct to do so in the light of the expert evidence, as analysed above. There is no realistic basis for inferring that the Andresen Session was in fact subverted.

174. Furthermore, no case to that effect was actually put to Dr Wright in cross-x. Suggesting that subversion would have been theoretically possible, feasible or straightforward does not amount to alleging that subversion actually took place. COPA's case on this point remains opaque, unparticularised and obscure. The same applies to the other signing sessions: no coherent case as to which, if any, of those sessions was subverted, and if so, how they were subverted, was put to Dr Wright. The incoherence of COPA's case extends to its pleadings which, as already stated, are defective for failing to identify whether COPA alleges actual subversion of the 2016 signing sessions and if so, how they are alleged to have been subverted.

175. In the circumstances, the Court is invited to reject any contention that Dr Wright deliberately subverted any signing session.

IV. LaTeX

[369] {H/376/1, 2, 11 and 14}.
[370] Meiklejohn {Day 18/132/16-17}.
[371] Wright {Day 8/73/22}-{Day 8/75/8}.

A. Introduction

176. LaTeX is a typesetting system that builds on a programming language called "TeX" and allows users to write and format text, mathematical symbols and other written-document properties.[372] LaTeX is potentially relevant to the Identity Issue in two respects:

176.1. First, there is an issue as to whether producing the BWP involved the use of LaTeX. Dr Wright says that he produced the BWP using LaTeX, among other software.[373] COPA contends that the BWP was not produced using LaTeX such that Dr Wright's account of how he says he produced the BWP must be untrue.[374]

176.2. Second, there is an issue relating to the so-called White Paper LaTeX Files[375], which are the LaTeX documents extracted from Dr Wright's Overleaf account that he says can be compiled into the BWP. COPA alleges that these Files do not compile into the BWP and are recent forgeries.

177. As further explained below, although these issues concerning LaTeX were in principle capable of being crucial to the determination of the Identity Issue, they have proved to be rather less important:

177.1. Mr Rosendahl, COPA's expert on LaTeX, explained that the BWP could in principle have been produced using LaTeX, albeit using non-standard versions of the software available at the time. He also explained that the BWP has features indicating it was produced using OpenOffice software. Dr Wright's evidence is that he used both OpenOffice and LaTeX to produce the BWP, which is consistent with Mr Rosendahl's findings. Accordingly, the evidence on how the BWP was produced is **consistent** with Dr Wright being Satoshi Nakamoto, but it does not of course establish that he **is** Satoshi Nakamoto.

177.2. The relevance of the White Paper LaTeX Files to the Identity Issue depended on Dr Wright establishing two propositions: first, that the White Paper LaTeX Files can be compiled into the BWP; and second, that it is practically impossible to reverse engineer the White Paper LaTeX Files from the publicly available BWP.

[372] Rosendahl 1, §§15-16 {G/7/5}.
[373] See, for example: {Day 3/142/12}.
[374] See, for example: {Day 3/142/9} to {Day 3/142/15}.
[375] This term was defined in Field 1, §§ 27-31 {PTR-A/5/10}, and thereafter adopted by the parties.

If **both** propositions were established, then it would not matter that the White Paper LaTeX Files do not (expressly on Dr Wright's case) date from before the release of the BWP. In the event, however, Dr Wright accepts he has not established the first proposition (not least because it has not been possible to recreate the LaTeX environment that Dr Wright says he used to produce the BWP). In these circumstances, the White Paper LaTeX Files are not probative of the Identity Issue based on the evidence available to the Court.

177.3. COPA's forgery allegations in relation to the White Paper LaTeX Files are misconceived: they are largely based on the false premise that Dr Wright maintained that these Files dated from a particular point in time (such that evidence of recent modification would be indicative of forgery). But that was never Dr Wright's case: his case was that he uniquely could produce a LaTeX file that compiled into the BWP, and that this proved he was Satoshi. Dr Wright made clear that the White Paper LaTeX Files were not a time capsule predating the release of the BWP: they were instead 'living' documents that he modified since the release of the BWP for corrections, personal experimentation and latterly for the purposes of demonstrations to Shoosmiths.

B. Was the BWP created using LaTeX

Dr Wright's case

178. On Dr Wright's case, the process of creating the BWP involved different media and software. He explains that he began crafting what was to become the BWP between March 2007 and May 2008 using hand-written pen and paper notes.[376] As for the electronic version of the document, Dr Wright states:

"*The White Paper's development involved a complex workflow utilising various software platforms, including LaTeX, OpenOffice and Microsoft Word. I also employed various LaTeX tools, including those by Apache, to uplift documents as ODT files. Moreover, all graphical images in the White Paper were produced using LaTeX code and then converted into DVI, PostScript, ODT and PDF formats.*"[377]

[376] Wright 1, §86 {E/1/17}.
[377] Wright 4, §6(c)(i) {E/4/5}.

179. In Wright 8, Dr Wright explained (in unchallenged evidence) how he converted documents between different formats:

179.1. "*I found Writer4LaTeX helpful when working with OpenOffice. It integrated well, allowing me to convert my OpenOffice documents into LaTeX format.*"[378]

179.2. "*I have used both Writer4LaTeX and Pandoc for different aspects of document conversion. I used Writer4LaTeX, as an extension for OpenOffice, to compile documents from those typed using OpenOffice to LaTeX text files and then to compile into .dvu, .ps and .pdfformats. I used this, in particular, for documents with extensive formatting or mathematical equations.*"[379]

179.3. "*I also integrated Pandoc with MiKTeX. In this, Pandoc served as a conversion tool between various document formats, and MiKTeX was used as the LaTeX distribution for typesetting documents. Specifically, I used Pandoc to convert documents from non-LaTeX formats (like Markdown or HTML) into LaTeX. I then used MiKTeX, with its comprehensive package support, to compile these LaTeX files into the desired final formats, such as PDF.*"[380]

180. Dr Wright thus describes his process of document production as involving alternating and converting between different document formats. A document might be typed using OpenOffice and then converted to LaTeX, before being compiled into PDF. As for the BWP, Dr Wright states that he used **both** OpenOffice and LaTeX. He has never suggested that he used LaTeX exclusively to produce that document.

The expert evidence

181. The expert evidence on whether the BWP was produced using LaTeX was given by COPA's expert, Mr Rosendahl, in section 2 of Rosendahl 1 {**G/7/1**}. Dr Wright chose not to call an expert on this issue. There is no doubt that Mr Rosendahl is a leading expert on the use of LaTeX. His evidence was generally fair and balanced, and it appears he,

[378] Wright 8, §61{E/23/19}.
[379] Wright 8, §63{E/23/19}.
[380] Wright 8, §64{E/23/19}.

quite properly, wrote his reports himself (indeed, the reports appear to be typeset using LaTeX and incorporate Mr Rosendahl's aesthetic preferences)[381].

182. Mr Rosendahl's evidence was, however, ultimately of limited assistance in resolving the factual question of whether producing the BWP involved the use of LaTeX. His analysis was based on an examination of the published PDFs of the BWP (the "**BWP PDF**"), and he identified a number of features of the PDF that indicated to him it was not produced using LaTeX but was instead produced using OpenOffice. As an overarching point, Rosendahl 1 does not address the possibility that the BWP was produced using **both** OpenOffice and LaTeX, and so it is inherently unlikely to assist in determining whether Dr Wright's explanation as to how he produced the BWP is true.

183. Mr Rosendahl's analysis focuses on features of the BWP PDF falling broadly into two categories.

184. The first category comprises aesthetic choices made by the author of the BWP PDF that Mr Rosendahl considers to be atypical choices by a user of LaTeX. While Mr Rosendahl's experience may well enable him to give a view as to how LaTeX users typically format documents as a population, these findings are obviously irrelevant to the question of whether the BWP was produced using LaTeX. Indeed, Mr Rosendahl fairly accepted in cross-examination that the aesthetic points he identified could have been coded-for in LaTeX, and that however the BWP was produced, the author would have had to make those aesthetic choices (whether positively, or by not modifying a default).[382]

185. The second category comprises what Mr Rosendahl describes as "*technical divergences*" between the BWP PDF and a PDF compiled from what Mr Rosendahl calls a "*standard LaTeX installation*".[383] A number of points fall to be made in relation to this category:

    185.1. The headline point is that the modifications that would have been required to a standard LaTeX installation to compile the BWP PDF directly from LaTeX were "*theoretically possible*".[384] Mr Rosendahl clarified in cross-examination that the

[381] See, for example, Rosendahl 1, §27 {G/7/8}.
[382] {Day 17/14/8} to {Day 17/14/24}.
[383] Rosendahl 1, §§65-66 {G/7/23}. See Rosendahl 1, §66 {G/7/24} for a summary of the technical divergences.
[384] Rosendahl 1, §67 {G/7/24}.

agreement recorded in his joint statement with Mr Lynch that the BWP was "*created in OpenOffice 2.4 and not LaTeX*"[385] referred (as far as he was concerned) to creation using a standard LaTeX installation: Mr Rosendahl agreed it is possible that the BWP was produced using a modified installation.[386]

185.2. Mr Rosendahl accepted that although the metadata of the BWP PDF records the "*Producer*" as "*OpenOffice.org 2.4*" and the Creator as "*Writer*" (being the word processor within OpenOffice), this is consistent both with the BWP PDF having been created in OpenOffice 2.4 and with those metadata fields having been specified by the author in LaTeX code.[387]

185.3. There are a number of other features of the PDF that are indicative of a PDF created in OpenOffice, namely: (a) the six-letter prefixes in the names of the fonts embedded in the BWP;[388] (b) the /DocChecksum element in the trailer of the PDF file;[389] and (c) the binary digits included in the header of the PDF file;[390] and (d) the text encoding in the PDF file, including the extensive specification of kerning for individual characters.[391]

185.4. As noted above, Mr Rosendahl agreed that each of these elements could have been coded-for in LaTeX, but this would have required modifying a standard LaTeX installation; he questioned why anyone would go to the trouble of using LaTeX to "*mimic the output of OpenOffice very closely while retaining the superficial appearance of a LaTeX document*", but rightly refused to speculate about that.[392] Mr Hough KC put to Dr Wright that on his case he went to "*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*"[393], no doubt seeking to imply that this was unlikely. But

[385] Joint Statement, §2 {Q/5/1}.
[386] {Day 17/19/21} to {Day 17/20/10}.
[387] {Day 17/15/25} to {Day 17/16/11}.
[388] Rosendahl 1, §47 {G/7/16}.
[389] Rosendahl 1, §§59-60 {G/7/20}.
[390] Rosendahl 1, §§61-64 {G/7/21}.
[391] Rosendahl 1, §§51-56 {G/7/18}.
[392] Rosendahl 1, §67 {G/7/24}.
[393] {Day 5/138/11} to {Day 5/140/20}.

however surprising this approach to producing the BWP might have been for a typical person, Dr Wright is not a typical draftsman.

185.5. Dr Wright explained that at the time he was working on the BWP, he was also writing papers on steganography, which involves the alteration of documents to embed messages or watermarks, and that he produced the BWP in this unusual way simply because he could:[394]

> 12 Q.So you went to a lot of effort to produce
> 13 the White Paper in this form to provide a digital
> 14 watermark, that's what you're saying?
> 15 A. Yes.
> 16 Q. And this would mark you out as the author, right?
> 17 A. No, it was more just because I could at the time.

185.6. Dr Wright's contemporaneous interest in steganography is demonstrated by the 2007 book he co-wrote with Dave Kleiman: the '*CHFI Study Guide'*,[395] in which the authors describe the use of steganography and steganographic watermarking in Chapter 8.[396]

185.7. More generally, Dr Wright's says that around the time he was producing the BWP, he was using LaTeX intentionally to specify inaccurate metadata for documents he worked on, for example by specifying a "*funky*" version of software that did not yet exist "*so that it looks like I wrote this document in the future*", as a technique he employed and taught to his students for confusing potential attackers.[397]

185.8. In re-examination, Mr Hough KC elicited from Mr Rosendahl that it would have taken "*several months' worth of work for a single person*" to have modified a standard LaTeX installation to produce one capable of creating the BWP.[398] COPA will no doubt suggest this too is implausible. Importantly, however, Dr Wright used LaTeX not only for the BWP, but also for his other writings. He explains in Wright 8 that he used LaTeX since at least 1998, in a passage that was not challenged by

[394] {Day 5/140}.
[395] {L2/180/1}. Dr Wright referred to this book in cross-examination at {Day 3/42/17}.
[396] Chapter 8 begins at {L2/180/291}.
[397] {Day 3/40/11} to {Day 3/42/19}.
[398] {Day 17/33/14} to {Day 17/33/23}.

COPA.[399] There is nothing inherently surprising in the proposition that Dr Wright might have spent, cumulatively, months tinkering with his LaTeX installation over the course of a decade to come up with a bespoke product that he used when creating the BWP.

Conclusions on whether the BWP PDF was produced using LaTeX

186. Dr Wright does not need to prove a **positive case** that the BWP was created using LaTeX to succeed on the Identity Issue. He does, however, need to resist a **negative finding** that LaTeX was **not used**, even in conjunction with OpenOffice in the manner asserted by Dr Wright.

187. The undisputed expert evidence of Mr Rosendahl is that the BWP could have been produced using LaTeX. The only issue for the Court is therefore whether **COPA** can prove that LaTeX was not used as a matter of fact. The only basis on which COPA can make that assertion is that the effort required to modify a standard LaTeX installation was so great that it is unlikely Dr Wright would have done so (COPA did not put to Dr Wright that he lacked the technical ability to do so). The Court cannot safely reach that conclusion:

    187.1. As explained above, Dr Wright used LaTeX for at least a decade before the BWP was released and had published a book on steganography by 2007. What might seem an extraordinary effort for the purposes of one document is not exceptional in the context of a decade of use by someone with an avowed interest in the use of LaTeX for stipulating irregular metadata for compiled documents.

    187.2. Dr Wright does not work with documents in the way typical people do. His method is atypical, and it is dangerous to draw conclusions based on what one might expect a typical person to do. The following exchange in cross-examination is illuminating:[400]

> Q. Dr Wright, it would be extremely eccentric to enter some LaTeX code in order to set a creation timestamp based on another year's document, but change part of it and not the rest. That is a very bizarre thing to do,

[399] Wright 8, §14 {E/23/7}.
[400] {Day 3/163}.

8 I suggest.
9 A.I suggest −− lots of people call me bizarre. I mean,
10 one thing, my Lord, inventors have never been known for
11 being normal. […]
15 […] I 'm an Aspie; your expert, after a few minutes
16 of being with me, determined that. I mean, there is
17 no −− we're strange people, we're unusual. I'm
18 currently doing multiple degrees while working and doing
19 a court case. Most people would consider that bizarre.

188. Since COPA cannot prove that the BWP was not created using LaTeX (at least in conjunction with other software), this issue is unlikely to assist in determining the Identity Issue.

C. The White Paper LaTeX Files

Dr Wright's case and the position at the PTR

189. The White Paper LaTeX Files are among the documents that Dr Wright obtained permission to rely on at the PTR. As explained in the skeleton argument for Dr Wright at the PTR, the White Paper LaTeX Files were potentially determinative of the Identity Issue on Dr Wright's case for two reasons:[401]

    189.1. First, Dr Wright contended that the Files could be compiled into the published form of the BWP; and

    189.2. Second, Dr Wright contended that it is practically infeasible for a person to "*reverse-engineer*" the LaTeX code for the BWP from its published form.

190. If Dr Wright were to establish **both** propositions, then that would be powerful evidence that he is Satoshi Nakamoto: he would have shown he possessed LaTeX code that could only have been produced by the creator of the BWP.

191. The reason Dr Wright needed to establish both propositions is that the White Paper LaTeX Files did not, on Dr Wright's case, date from before publication of the BWP. As submitted at the PTR, Dr Wright instead relied on the mere fact of his possession of what he says is a **unique** code.[402]

[401] PTR Skeleton Argument, §57 {R/2/19}.
[402] PTR Skeleton Argument, §57(4) {R/2/20}.

192. Dr Wright made clear, even before the PTR, that he **did edit** the White Paper LaTeX Files after publication of the BWP. Shoosmiths' fourth letter of 13 December 2023 explained that Dr Wright had made minor corrections to the published form of the BWP, and that references had been updated by automated software.[403] It is fair to say that Dr Wright did not explain the extent to which he modified the Files at that time, but that may be explicable for two reasons:

192.1. First, on Dr Wright's case, those modifications were made for the purposes of demonstrations to Shoosmiths that were subject to litigation privilege. It was only when the full extent of the editing between 17 to 25 November 2023 was revealed in the project history files disclosed by Dr Wright shortly before trial, that Dr Wright chose to waive privilege over the Shoosmiths demonstrations to explain the editing.

192.2. Second, since Dr Wright did not rely on the dating, metadata of forensic purity of the White Paper LaTeX Files, the mere fact of his editing those files was not inconsistent with his case.

193. Shoosmiths' 13 December 2023 letter also relayed Dr Wright's instructions that "*the compiled output of the White Paper LaTeX Files will vary depending on the parameters and process used for compilation, for example the compiling software used and font packages available to that software […] in order to produce a Compiled White Paper from the LaTeX White Paper Files it is necessary to use the compilation process in fact used by Dr Wright when he published the Bitcoin White Paper as Satoshi Nakamoto.*".

194. Dr Wright describes his LaTeX environment in Wright 8. That description was concerned with how Dr Wright used LaTeX generally (rather than with how he created the BWP specifically)[404], and his unchallenged evidence is that he used numerous packages, fonts, math settings and custom scripts with LaTeX, leading to a highly complex LaTeX environment.[405]

195. Users of LaTeX typically use software packages to produce and compile LaTeX code. These software packages are known as "*distributions*", and the two major distributions

[403] {M/2/678}.
[404] In accordance with paragraph 6 of the PTR Order {B/22/4}.
[405] Wright 8, §§12-22 {E/23/6}.

when the BWP was released were MiKTex and TeX Live.[406] Dr Wright says that he used both of those distributions. At the time, MiKTeX was available only for Windows: a point made by Mr Rosendahl in a passage of his first report to suggest that Dr Wright cannot have used MiKTeX on Linux as he had claimed.[407] This point was, however, based on a misreading of Wright 8, which makes clear that Dr Wright used MiKTeX when using Windows and TeX Live "*as an alternative to MiKTeX on Linux*".[408] Mr Rosendahl confirmed in cross-examination that it was at the time of the BWP possible to use MiKTeX on Windows, or on a Windows virtual machine running on Linux.[409] Dr Wright says he also worked with LuaLaTeX[410] (which facilitates the use of LuaTeX, an extension that allow the use of an additional programming language, "Lua", with TeX).

196. In the event, Dr Wright accepts that he was unable to prove at trial the first of the two propositions on which his reliance on the White Paper LaTeX Files depended: no-one has been able to compile the White Paper LaTeX Files into the published form of the BWP. This is not surprising on Dr Wright's case because no-one has reproduced the compiling environment that he says he used to produce the BWP[411] and, as Dr Wright explained, he does not himself now have access to the environment:[412]

> Q. […] you presented,
> at the PTR, to his Lordship, through your solicitors conveying your evidence, that your LaTeX files would produce a precise reproduction or copy of the Bitcoin White Paper, not mentioning any things that would cause differences. That's how you presented it to his Lordship in the middle of December, isn't it?
> A. No, I did not say that it would do it on Overleaf. What I said is "in the same environment", and the same environment is basically 2008/2009 system. So you take a 2008/2009 system with the same versions of MiKTex the same versions of OpenSymbol, the same versions of other fonts, and you do a recompile based on that. I don't have that environment any more.

[406] Rosendahl 1, §21 {G/7/6}.
[407] Rosendahl 1, §166 {G/7/51}.
[408] Wright 8, §75(a) {E/23/22}. See also: §76 at {E/23/23}.
[409] {Day 17/27/12} to {Day 17/27/15}.
[410] Wright 8, [70ff] {E/23/20}.
[411] See the discussion between Mr Hough KC and Dr Wright in cross-examination at {Day 5/141/11} to {Day 5/149/19}.
[412] {Day 5/128}.

197. Mr Rosendahl did not think that Dr Wright's computing environment would make a difference,[413] but he accepted he did not test the environment that Dr Wright says he used (in particular, Mr Rosendahl did not try to compile the White Paper LaTeX Files using MiKTeX or LuaLaTeX).[414]

198. Dr Wright has had more success on the reverse engineering point. The undisputed expert evidence is that while it is not difficult to reverse engineer a LaTeX source file that is superficially similar to the BWP, "*[i]t would however be extremely difficult to use LaTeX to create a PDF which was an exact match to the BWP*".[415] This is now academic and does not assist Dr Wright given that he has not established that his White Paper LaTeX Files do compile into an exact match to the BWP.

Alleged forgery of the White Paper LaTeX Files

199. COPA alleges that the White Paper LaTeX Files are recent forgeries.[416] This allegation is pleaded on a number of bases, namely that: (1) the BWP "*was not written in LaTeX*";[417] (2) the White Paper LaTeX Files do not compile into the BWP;[418] (3) the White Paper LaTeX Files incorporate LaTeX packages that did not exist in 2009;[419] (4) the code for the image in the White Paper LaTeX Files appear to have been generated using an online tool called Aspose;[420] and (5) the White Paper LaTeX Files are a recent creation, with extensive editing in the period following 17 November 2023[421].

200. It is not necessary for the Court to decide whether Dr Wright forged the White Paper LaTeX Files. Dr Wright's inability to prove at trial that the White Paper LaTeX Files can be compiled into the BWP is a sufficient basis to dismiss the relevance of the Files to the Identity Issue. In these circumstances, the Court should be cautious about reaching any concluded view about forgery. The White Paper LaTeX Files are a recent development in these proceedings, with the effect that the case on forgery was pleaded only on 23 January 2024, only 8 days before the start of trial, after Dr Wright served his reply

[413] {Day 17/35/3} to {Day 17/35/7}.
[414] See Mr Rosendahl's cross-examination at {Day 17/28/10} to {Day 17/29/2} and {Day 17/31/9} to {Day 17/32/9}.
[415] Rosendahl-Lynch Joint Statement, §4 {Q/5/2}.
[416] See COPA's 'Schedule of Dr Wright's Further Forged Documents', {A/16/4}.
[417] Schedule of Dr Wright's Further Forged Documents, §§4-5 {A/16/4}.
[418] Schedule of Dr Wright's Further Forged Documents, §§6-8 {A/16/4}.
[419] Schedule of Dr Wright's Further Forged Documents, §§12-14 {A/16/6}.
[420] Schedule of Dr Wright's Further Forged Documents, §11 {A/16/6}.
[421] Schedule of Dr Wright's Further Forged Documents, §9 {A/16/5}.

evidence and after the principal expert reports and joint statements were finalised. Although Dr Wright accepts responsibility for the compressed timetable for dealing with the Files, the reality is that he has not had a proper opportunity to deal with what are highly complex expert and factual issues, as addressed further below.

201. Dr Wright's position on each of the bases for the alleged forgery pleaded by COPA is summarised below.

202. First, it is not clear what COPA means when it says the BWP "*was not written in LaTeX*". Dr Wright's case that he used LaTeX as part of the process in creating the BWP (along with OpenOffice and Word) is addressed in paras 178 to 188 above. COPA cannot prove that LaTeX was not used in the creation of the BWP.

203. Second, as explained above, Dr Wright accepts that he cannot prove that the White Paper LaTeX Files can be compiled into the BWP on the available evidence at trial. It does not follow that COPA can prove the negative that the White Paper LaTeX Files do not compile into the BWP using the specific environment that Dr Wright says he used at the relevant time, as described in Wright 8. Mr Rosendahl did not test that environment (neither did Mr Lynch). This is not a criticism: the work done by Mr Rosendahl to produce his report in the time available is extraordinary, and it was obviously impractical to recreate the various complex and unusual permutations of Dr Wright's environment described in Wright 8, at least in the time available.[422] Although Mr Rosendahl speculated in re-examination that Dr Wright's environment would not make a difference, he does not know whether that is the case because he did not test that proposition. Mr Rosendahl's speculation is an unsatisfactory basis for making a finding of forgery.

204. Mr Rosendahl's analysis of the font for the mathematical formulae in the White Paper LaTeX Files is a good example of the difficulty in reaching conclusions on limited evidence. Mr Rosendahl says that none of the White Paper LaTeX Files with which he was provided could be the source for the BWP because none of them would correctly compile the font for the mathematical formulae "*without a custom version of the unicode-math package that would have enabled Dr Wright to change the maths fonts to Times New Roman*": see Rosendahl 1, §§153-154 {G/7/49}. However:

[422] For example, Dr Wright explained in cross-examination that it was impractical to try to teach Mr Lynch how to use MiKTeX in the time available: {Day 5/143/2} to {Day 5/143/6}.

204.1. The BWP did not use a Times New Roman as a uniform font for mathematical formulae. Contrary to the impression given in §153 of Rosendahl 1, Mr Rosendahl acknowledged in his second report that the BWP in fact "*uses the main maths font Times New Roman, but the font OpenSymbol for a few characters within those formulae*".[423]

204.2. This is consistent with the White Paper LaTeX Files, which specify OpenSymbol as the "*math font*" but also use characters in Times New Roman using the standard text font, showing that there is no need for the "math font" to be coded as Times New Roman:[424]

```
804  \[
805  {
806  \setmainfont{TimesNewRomanPSMT}
807  %\setmathfont{opensymbol}
808  {\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot
809  \left\{
810  \begin{array}{ll}
811      \left({q}/{p}\right)^{z-k} & \text{if } k \leq z \\
812      1 & \text{if } k > z
813  \end{array}
814  \right\}}}
815  \]
816
```

204.3. In any case, Dr Wright has explained that he moved his LaTeX files to Overleaf in or around 2020: Wright 14, chain of custody table at {E/33/4}.

204.4. Overleaf did not support the OpenSymbol fonts that Dr Wright says he used for creating the mathematical formulae in the BWP, and so Overleaf replaces those fonts with Times New Roman:[425]

> A. […]OpenSymbol doesn't load in Overleaf, so Overleaf replaces it with Times New Roman. So what we have in the compiled White Paper is Times New Roman instead of OpenSymbol.[…]

[423] Rosendahl 2, §29(d) {G/8/8}.
[424] This is the LaTeX code seen in the main.tex file in the last line of {L21/9.1/19} to the top of {L21/9.1/19}, reformatted for easier reading.
[425] {Day 5/144}.

204.5. Dr Wright continued to work with the White Paper LaTeX Files after the release of the BWP and, in particular, in Overleaf after moving the files into that system:[426]

> 14 Q. There were differences here, not only to be
> 15 bibliography , but spacing differences , differences in
> 16 the symbols in formulas and punctuation, other content
> 17 differences , weren't there?
> 18 A. Yes, I said I corrected a couple of things. I never
> 19 expected this, at this point, to be the document it was,
> 20 and it's been a live access document, like many of my
> 21 other things on Overleaf. This is part of why it wasn't
> 22 used early on. I said I've been accessing and using
> 23 the files that I have in my text files.

204.6. It is reasonable to infer that Dr Wright would have had to make modifications to the way fonts were encoded in the White Paper LaTeX Files in order to use and compile them in Overleaf.

204.7. In these circumstances, there is nothing inherently surprising in the fact that the files now extracted from Overleaf do not compile the fonts for the mathematical formulae in the BWP in precisely the same way as the original, especially when used in TeX Live 2008 as tested by Mr Rosendahl.[427] But again, this is a point that it has not been possible to address in detailed evidence because Mr Rosendahl's points about font encoding did not emerge until shortly before trial and after Dr Wright served his reply evidence.

205. Third, Dr Wright denies that the White Paper LaTeX Files contain LaTeX packages that were not available to him at the time the BWP was released. Whether or not this is the case is a question of fact and not opinion. Mr Rosendahl sets out in his report links to online sources that he says indicate the date that the relevant packages became publicly available, and this was put to Dr Wright at {Day 5/146}:

> 16 Q. Then, in addition to finding that your files didn't
> 17 compile under 2008 to 2009 software, he also identified,
> 18 didn't he, no less than 14 software packages referenced
> 19 in your LaTeX files which couldn't have been used in
> 20 2009?
> 21 A. No, he made comments that they weren't available. I can
> 22 demonstrate where they are. Now, they were early

[426] {Day 5/142}.
[427] Rosendahl 1, §153 {G/7/49}.

23 packages, but that doesn't mean they're not used.

206. Dr Wright does not have the evidence at trial to prove that these packages were available, but again it does not follow that COPA can prove that they were not available. COPA pleaded a serious factual assertion shortly before trial about whether certain software would have been available to Dr Wright some 15 years ago, based on the internet searches of its expert, Mr Rosendahl, as set out in an expert report served after Dr Wright's reply evidence. This is not a proper basis for making findings of forgery against Dr Wright: that case would need to have been pleaded before the service of evidence, then be subject to a detailed factual investigation, and then be addressed in evidence before trial, none of which has been possible in the time available. Dr Wright bears the responsibility for the late disclosure of the White Paper LaTeX Files, and he has to live with the consequences for his ability to adduce evidence to make good his positive case. But it is not fair in those circumstances for the Court to make findings of serious wrongdoing on COPA's positive case when Dr Wright has been unable properly to address the allegations.

207. Fourth, Dr Wright accepts that the White Paper LaTeX Files contain code that appears to have been generated using Aspose, but he denies that he generated that code. When challenged in cross-examination, Dr Wright said that he suspects this code was inserted into his Overleaf LaTeX Files by another person to discredit him.[428] Dr Wright explained his concern that Mr Ager-Hanssen had access to his Overleaf files in Wright 14: see the row for 2020-2023 in the chain of custody table at {E/33/5}. Dr Wright has not, however, had time to investigate this possibility or address it in detailed evidence.

208. Fifth, Dr Wright accepts that he edited the White Paper LaTeX Files in the manner and at the times illustrated in the animation at {L21/2/1}. His explanation for this editing history is as follows:

    208.1. Dr Wright says he first demonstrated the White Paper LaTeX Files to Shoosmiths in October 2023.[429] Following Dr Wright's evidence to this effect in cross-examination, Shoosmiths reviewed its records for October and found attendance notes stating that Dr Wright had made a demonstration of LaTeX files he said could be compiled into the BWP. This demonstration was made on 5

[428] {Day 15/213/14} to {Day 15/219/20}.
[429] {Day 15/125/17}; {Day 15/165/5} to {Day 15/166/12}.

October to a single associate, who has since left Shoosmiths, at a preliminary meeting only three days after the firm was instructed by Dr Wright.[430]

208.2. After the October demonstration, Dr Wright says he downloaded the White Paper LaTeX Files from Overleaf to his local computer "*to make sure that they didn't get changed*"[431]. Dr Wright then removed some of the code in the Overleaf versions of the relevant LaTeX files, and then re-uploaded his local copies to show Shoosmiths how changes to the code could result in differences between compiled versions:[432]

p.159

Q. 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?
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.193

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.
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

p.194

I loaded the original one that I'd downloaded, which is talking here about the existing files of similar structure.

[430] Shoosmiths' first letter of 27 February 2024 {M/3/48}.
[431] {Day 15/196/11}.
[432] {Day 15/159/9} to {Day 15/159/19} and {Day 15/193/16} to {Day 15/194/3}.

208.3. Dr Wright accepts that the editing apparent from the Overleaf project history files compiled into the animation at {L21/2/1} goes beyond the editing shown to Shoosmiths during the time of the actual demonstrations on 17 and 20 November 2024. However, Dr Wright says that he also needed to make edits outside the time of the demonstrations but still for the purposes of the demonstrations:[433]

> Q. So you gave the impression that the only changes that you had made were demonstrations that you had given to Shoosmiths, right?
> A. And for capturing things for documents for them, preparing for demonstrations, yes, it was all to do with that

209. In conclusion on the White Paper LaTeX Files, Dr Wright accepts that they do not assist his case on the Identity Issue based on the evidence available to the Court, but he denies forgery. The state of the evidence is in any event an unsatisfactory basis for a finding of forgery that is not necessary for the determination of the Identity Issue.

V. COPA'S FORGERY ALLEGATIONS

210. Dr Wright addresses below: (i) COPA's forgery allegations regarding Dr Wrights initial disclosure ("**Original Forgery Allegations**") and (ii) the additional forgery allegations made following the PTR.

A. Original Forgery Allegations

211. Although they have formed a major part of COPA's case at trial, the forgery allegations are not a freestanding part of COPA's claim and COPA is not understood to be relying on them to seek a distinct form of remedy or relief. As explained in Dr Wright's Skeleton for Trial, the forgery allegations are ultimately sub-issues to the broader Identity Issue. It follows that, if the Court considers itself able to determine the Identity Issue without having regard to Dr Wright's Reliance Documents, it will not need to trouble itself with the complex and lengthy detail of COPA's forgery allegations.

212. Should the Court nevertheless wish to determine the forgery allegations, Dr Wright's responses to the individual Original Forgery Allegations are set out in Appendix 1 to

[433] {Day 15/197/21} to {Day 15/198/1}.

these Closing Submissions.[434] However, as a more general matter, Dr Wright submits that the Court ought to be cautious before making forgery findings against him. This is for three reasons:

212.1. The **first**, and most obvious, is that the forgery allegations are of the utmost seriousness and would, if established, do great damage to Dr Wright's reputation and future endeavours. Although it was confirmed by the Supreme Court in **Re B (Children)** [2008] UKHL 35 that there is only one civil standard of proof (the balance of probabilities), the courts have maintained that, in general, it is legitimate and conventional, and a fair starting point, that fraud and dishonesty are inherently improbable, such that cogent evidence is required for their proof; see Males LJ at [117] of **Bank St Petersburg PJSC v Arkhangelsky** [2020] 4 WLR 55 and Teare J in **JSC BTA Bank v Ablyazov** [2013] EWHC 510 (Comm), at [76]).

212.2. The **second** reason, which flows from the first, is that, as became clear during Mr Madden's cross-examination, COPA's evidence in support of its allegations (which it has the burden of proving) is neither satisfactory nor cogent. This is developed in more detail below.

212.3. The **third** reason is that, due to how late in the proceedings they were raised and the unfortunate sequencing of the relevant factual and expert evidence, it has not been possible for the forgery allegations to be explored and responded to in a suitable way. The Court will recall that Mr Madden served his very lengthy first expert report on 1 September 2023 and that, on 31 October 2023, COPA pleaded 50 new forgery allegations based on Mr Madden's findings. Paragraph 5 of the Order of Mellor J dated 31 October 2023[435] provided for Dr Wright to respond to COPA's forgery allegations in his reply witness statement, but the preparation of that proved to be extraordinarily burdensome, and Dr Wright applied at the 15 December 2023 PTR for an extension of time to serve his reply evidence. In the event, the Court extended the final deadline for Dr Wright's reply witness evidence to 12 January 2024, and that evidence was served in three instalments, namely via Wright 9, Wright 10 and Wright 11. In those three statements, Dr Wright explained,

[434] Appendix 1 also summarises Dr Wright's evidence in response to allegations made in the Particulars of Claim, and which have been addressed in Appendix C to Wright 11 {CSW/3}.
[435] {B/18/3}.

for the first time and directly in response to Mr Madden's reports, that a number of the anomalies identified by Mr Madden and relied on by COPA as evidence of forgery were the innocent result of his complex computer environment and collaborative working practices. Ideally, this evidence should have formed the factual background to Mr Madden's analysis from the outset. Instead, this case has involved the reversal of the orthodox sequencing of factual and expert evidence, where the former comes first and forms the factual basis for the latter. As a result, the very lengthy detail of Dr Wright's complex computer environment has received only cursory treatment by Mr Madden, across just over 2 pages of his fourth report.[436]

213. In addition, and specifically in relation to the allegations concerning Dr Wright's original disclosure, it should be noted that:

213.1. Dr Wright has not suggested that his original Reliance Documents were never accessed or edited by anyone since the publication of the Bitcoin White Paper, such that they could be treated as a "time capsule". Indeed, the opposite was clear from Dr Wright's own Chain of Custody of Reliance Documents schedule.[437] Dr Wright re-emphasised this during his oral evidence:

{Day 3/16/5} to {Day 3/16/21}

> 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,

[436] Madden 4, paras 155-159 {G/6/51}.

[437] 13 October 2023{K/11/1}. Although the custody details provided by Dr Wright in this document were provided after service of Madden 1, COPA is not understood to have challenged them and they are consistent with Dr Wright's original 11 May 2023 Chain of Custody schedule at {M/1/778}, which also explained that the documents had been stored on third party devices.

on a voice recorder, speak to it, sometimes I write handwritten notes, and then my staff do this for me.

{Day 3/53/4}:

Q. So it follows that this document, in at least this form, must date from 2017 or later, mustn't it?
A. It could have been updated, yes.
Q. That is not something you said in your chain of custody, is it?
A. No. What I said was it was with employees and I don't know what people are doing when they have the files.
Q. You said it was believed to date from 2008?
A. The original document that I wrote and drafted was from 2008, yes.
Q. Can you at least agree that this document in this form is not authentic to 2008?
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.
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?
A. No, I would not. Again, you're --
Q. Well, what did the last answer mean?
A. You're misrepresenting what I said. I've said I drafted documents in 2008. I created systems and I'm using these documents to show what I started researching before the 350 White Papers that they led to, several thousand patents, etc. These are the documents I gave to my staff members to work on that and to do that project.

For this reason, Dr Wright submits that evidence that his documents were accessed or even edited after the publication of the Bitcoin White Paper should not, by itself, lead the Court to conclude that they have been deliberately forged by Dr Wright.

213.2. Of the 20 documents in COPA's list of 20 core alleged forgeries, 7 are not (and have never been) Reliance Documents.[438] They have simply been disclosed by Dr Wright in accordance with his procedural obligations. It follows that COPA's general plea that the purpose of the alleged forgeries "*was to create documents that would be deployed to prove that Wright is Satoshi*"[439] is misplaced in relation to

[438] As reflected in the titles given to them by COPA in that list: see {M/2/68}.
[439] POC para 35B {A/2/12}.

these documents, and (Dr Wright submits) that the Court should be even slower to make findings that any of those 7 documents have been forged by him.

214. Turning to COPA's evidence in support of its allegations, it is not in dispute that establishing that a particular document has been forged (i.e. deliberately tampered with or altered so that it could be deployed to prove that Dr Wright is Satoshi Nakamoto) requires COPA to rely on expert evidence to that effect. Indeed, it is clear from COPA's Schedule of Dr Wright's Forged Documents[440] that COPA's case on the alleged forgery of a particular document depends heavily on the Court accepting Mr Madden's analysis of its authenticity. This creates a significant difficulty for COPA's case because, as became clear during his cross-examination, there are two main problems with Mr Madden's reliability as an expert witness:

214.1. **First**, although Mr Madden has worked as a computer forensic examiner for some time, it is striking that his only relevant formal qualification or certification was an EnCase Certified Examiner qualification, which he appears to have obtained following a 12 week course.[441] It follows that he has no specific formal qualifications relevant to Citrix networks, VMWare virtual machines, or Storage Area Networks, all of which are particularly relevant for the reasons developed below.

214.2. **Second**, and more importantly, it was apparent from his own report (Madden 1), and then put beyond doubt during his cross-x, that Mr Madden's independence from COPA was undermined during the preparation of his reports. In particular:

(a). At paragraph 33 of Madden 1,[442] Mr Madden explained that COPA's solicitors had assisted him with the "*initial drafting of [his] report, and structuring and formatting the results of [his] analysis which [he] explained to them at each stage*". He added that this involved, in some cases, dictating the wording of his report to Bird & Bird during his analysis and reviewing the Report at the same time. In other cases, he explained, this unusual process involved him preparing "*drafting and notes which were then structured into report form by*

[440] {A/2/24}.
[441] {Day 16/9/7} to {Day 16/10/2}.
[442] {G/1/14}.

Bird & Bird". The same paragraph suggests that Bird & Bird even carried out some of the research underpinning Mr Madden's analysis and conclusions.

(b). When this was explored during his cross-x, Mr Madden revealed that there had been at least 6 to 8 in-person meetings between him and Bird & Bird, during which documents were analysed and Mr Madden's reports were drafted collaboratively.[443] Some of the drafting assistance appears to have been extensive, as the following exchange indicates:[444]

> A. Well, notes, basically it was bullet pointed of what the findings and meat of the issue were and it would be a matter of just explaining it. So after -- after, you know, the first few appendices, pulling them together, you kind of get a flavour for where some of it is going and, you know, an understanding of it, and I do believe that they actually grasped the topic very well.
> Q. They were essentially drafting the report for you, weren't they?
> A. No.
> Q. In large part?
> A. They were definitely helping a lot with getting through the -- what's the word for it -- assembly of it, but the actual content is mine.
> Q. No, no, Mr Madden, you said:
> "... you kind of get a flavour for where some of it is going and, you know, an understanding of it, and I do believe that they actually grasped the topic very well."

(c). Mr Madden confirmed that he had not adopted the same approach when preparing his expert evidence in other matters.[445] He also failed to provide a coherent explanation as to why such an approach was necessary in the present case, and or why he could not have dealt with any resourcing issues by engaging a suitably qualified (and independent) assistant. The suggestion that employing an assistant would have required excessive management efforts on his part or led to a lack of control over the analysis in, or drafting of, the report, were (with respect) nonsensical. To the extent that such concerns could have

[443] {Day 16/119/18} and {Day 16/120/18}.
[444] {Day 16/121/5-22}.
[445] {Day 16/122/22}.

been valid, Mr Madden could not explain why they would not apply equally to his obtaining assistance from Bird & Bird.[446]

215. At the very least, the form (and it seems the content) of Mr Madden's evidence has impermissibly been influenced by COPA's solicitors and the exigencies of this litigation. The relevant legal principles are as follows:

215.1. In **Imperial Chemical Industries Limited v Merit Merrell Technology Limited** [2018] EWHC 1577, at [237], Fraser J reiterated that: "*The principles that govern expert evidence must be carefully adhered to, both by the experts themselves, and the legal advisers who instruct them*." He went on to set out examples of the application of the well-known principles in **The Ikarian Reefer** [1993] 2 Lloyds LR 68, the first being that "*expert evidence presented to the Court should be, and should be seen to be, the independent product of the expert uninfluenced as to form or content by the exigencies of litigation (Whitehouse v Jordan [1981] 1 WLR 246 at 256, per Lord Wilberforce)*" (emphasis added), the second being that an expert should provide, to the court, independent assistance by way of "*objective, unbiased opinion*" as to matters in his area of expertise. This duty is echoed in paragraph 2.1 and 2.2 of Practice Direction 35:

> ***"2.1** Expert evidence should be the independent product of the expert uninfluenced by the pressures of litigation.*
>
> ***2.2** Experts should assist the court by providing objective, unbiased opinions on matters within their expertise, and should not assume the role of an advocate."*

215.2. As stated by the editors of **Phipson on Evidence**, at 33-29: "*In some cases the expert expresses his views to the lawyer who prepares the first draft or outline of the report for the expert to review. Whilst this can be permissible if properly done, in most cases this should be avoided as it runs the risk that the expert's views may become influenced by the lawyer's own views*."

215.3. If an expert's report is found not to be compliant with the principles of independence or impartiality, there are a wide variety of sanctions available to the court. Typically, the court will either refuse to admit the evidence of the expert, or,

[446] {Day 16/114} to {Day 16/116}.

more frequently, the matter will be taken into account when considering the weight to attach to that expert's evidence.[447]

216. Mr Madden's apparent lack of independence, or the gaps in his qualifications (or both), may have been the cause of the following three fundamental flaws in his analysis:

216.1. **First**, Mr Madden has on multiple occasions concluded with unjustified haste that a document has been dishonestly tampered with or altered, when other explanations were equally plausible from a technical perspective. This was clearly illustrated when he was cross-examined in relation to the following documents in COPA's list of 20 core forgeries: (a) ID_004013 Handwritten BDO minutes;[448] (b) ID_004019 JSTOR Article – Tominaga Nakamoto;[449] and (c) ID_000073 Statistics assessment homework.[450] The relevant details are set out in Appendix 1.

216.2. **Second**, in reaching his conclusions Mr Madden has on several occasions relied heavily on his analysis of the contents of particular documents, and in particular on what he considers to be anomalous or incongruous content. Mr Madden is not an expert (and COPA does not have permission to rely on expert evidence) in any of the multiple academic fields covered by Dr Wright's disclosed documents. Such evidence is therefore inadmissible. Alternatively, it should be given little weight. This is also addressed, where relevant, in Appendix 1.

216.3. **Third**, and most importantly, Mr Madden seems to have been unwilling to grapple properly with Dr Wright's complex IT environment, or with how that environment might have caused some of the digital anomalies on which he relied to reach his conclusions. In this respect, Mr Madden's analysis lacked rigour and was unconvincing. This gap in COPA's evidence may be the inevitable result of the unorthodox sequence and timing of the expert and factual evidence in this case (as described at para 212.3 above) but, whatever the reason for it, the fact remains that none of the documents considered by Mr Madden was analysed on the machines or within the environments from which it was collected,[451] and no

[447] *Expert Evidence: Law and Practice*, 9-013; *Phipson on Evidence*, 33-78.
[448] {L2/159}
[449] {L2/245}
[450] {L1/323}
[451] {Day 16/10/19}.

exercise was undertaken by Mr Madden to recreate the relevant IT environment (or parts of it). This matters because, as Mr Madden himself accepted, where the authenticity of documents is in question, it is prudent to analyse not just the documents themselves, but the environments in which they were authored and thereafter stored, as this can throw important light on their forensic analysis.[452] This would have assisted, in particular, in the interpretation of timestamps, which Mr Madden agreed is inherently prone to difficulties that are well recognised by digital forensic professionals, such that relying on them to prove that a particular event occurred is not a sound approach.[453]

216.4. Mr Madden accepted that metadata timestamps can be interpreted in different ways, such that, for example:

(a). A Creation Date may indicate that a document has been copied, or even "unzipped" from a zip file;[454]

(b). A Last Accessed date could report access by a computer and not a user (eg through a virus check); and

(c). A Document Modified date may not necessarily mean that any changes were made to the visual contents of a document.

217. The importance of analysing the authenticity of documents in the context of the environments in which they were created and stored must, as a matter of common sense and logic, be *a fortiori* where the relevant environment is a complex one, far removed from that of a standard home user or single machine. Mr Madden accepted that this description applied to Dr Wright's environment and that it would therefore be wrong to approach forensic analysis of Dr Wright's documents on the assumption that they were created and stored on a single computer or a single virtual machine.[455] Dr Wright's

[452] {Day 16/11/15} to {Day 16/11/23}
[453] {Day 16/12/11} to {Day 16/13/8}. See, for example, Chow et al, *The Rules of Time on the NTFS File System,* at {X/50}, in which the authors explain that "*Temporal analysis on individual digital file[s] has been adopted since the evolvement of computer forensics. However, it is not evidentially secure to rely on the timestamps of a particular file to prove a particular event occurred at the corresponding MAC times*" (p1, LH column), and (at p1, RH column) that "*since file timestamps can be altered inherently by batch operations such as automated tools scanning, previewing activities, etc, it is difficult to determine whether a particular file was accessed or opened explicitly by the user*."
[454] Which Mr Madden accepted at {Day 16/51/2}.
[455] {Day 16/24/22} to {Day 16/25/16}.

complex IT environment, as well as his (and his organisations') working practices were explained in detail in Wright 9, Appendix A,[456] and Wright 10.[457] The full detail of that evidence cannot be fully reproduced here, but some key elements for the Court to take into account (and which were explored in Mr Madden's cross-examination) include the following:

217.1. **Rocks Clusters:** Dr Wright stated that he has been running Rocks Linux (an open-source distribution designed for building high-performance computing clusters) as a base system since 2002/2003.[458] Dr Wright explained that "*A cluster is a group of linked computers that work together closely, making them appear as a single system. Rocks Linux is a specialized Linux distribution for building and managing high-performance clusters. A key feature of Rocks Linux is its ability to aggregate the resources of multiple physical servers into a unified, virtualised environment*."[459]

217.2. **Virtual Machines:** The above cluster system was used to host a series of virtualised machines, essentially separate computers running within a single physical machine, each with its own operating system and applications.[460] As part of this, Dr Wright used VMware and Xen hypervisor, the latter being "*a process that manages the creation and operation of a virtual machine*".[461]

217.3. **Citrix**: In addition to using virtual machines, Dr Wright stated that he accessed servers remotely using Citrix.[462] Citrix is software that enables users to work from remote locations using computer virtualisation.[463] Dr Wright also explains that he used Storage Area Network systems alongside Citrix,[464] and that these "*offer high performance and flexibility in handling large volumes of data, which is accessible to various users across the network*".[465]

217.4. **Access Times**: Dr Wright explained that in his SAN and Citrix virtual

[456] {E/26/32}.
[457] {E/31/1}.
[458] Wright 10 para 11{E/31/4}.
[459] Wright 10, para 12 {E/31/4}.
[460] Wright 10, para 13-14: {E/31/4}.
[461] Wright 10, para 18 {E/31/5}.; Meiklejohn 1 para 120(d) {G/2/50}; Wright 9, App A para 2.2(4) {E/26/35}.
[462] See e.g. Wright 9, App A para 2.2(4) {E/26/35}; Wright 8 para 3 {E/23/3}.
[463] Wright 9, App A para 2.2(4) {E/26/35}.
[464] Wright 10, para 84 {E/31/18}.
[465] Wright 10, para 86 {E/31/18}

environments, access times on files were often not updated as a deliberate performance optimisation strategy.[466]

217.5. **Symbolic Links**: Dr Wright stated that he made use of symbolic links,[467] which act as a window or portal to a folder somewhere else on an IT system.[468] Dr Wright said that he used symbolic linking to connect areas in his Windows systems to areas in his Linux systems, to enable him to manage and access his files across those systems.[469]

217.6. **Group Policies:** Dr Wright explained that organisations in which he worked enforced various group policies throughout their IT systems, and in particular that nChain applied a policy that enforced the use of a standard 'normal' Microsoft Word template and specified applications that were to be deployed throughout the network.[470] Such applications included both Grammarly and Math Type.[471] Dr Wright added that the relevant group policy was implemented by using the Group Policy Management Console on windows systems.[472]

217.7. **Collaborative Working**: Finally, Dr Wright explained in his witness statements, and in oral evidence, that staff in the organisations with which he has been involved worked collaboratively and shared documents, and that hundreds of those staff members had accessed and used his documents over many years.[473]

218. Dr Wright does not understand it to be in dispute that his IT environment and working practices included the above elements. Neither COPA nor the Developers cross-examined him on the topic. Further, when the above aspects of Dr Wright's environment and working practices were presented to Mr Madden, he agreed that they were technically plausible arrangements.[474] This is important because, as Mr Madden also accepted, many of the alleged indicia of forgery that he and COPA have relied on in this case could just as readily have been caused by that environment, or those working

[466] Wright 10, para 142 {E/31/28}.
[467] Wright 10 para 35 {E/31/7}, Wright 9, Appendix A para 2.44 {E/26/35} and Wright 8 para 41{E/23/15}.
[468] Wright 10 para 37 {E/31/7}.
[469] Wright 10, para 38 {E/31/8}.
[470] Wright 9, App A paras 2.17-2.20 {E/26/43}; and Wright 9, App A para 2.37-2.38 {E/26/47-48}.
[471] Wright 9, App A para 2.38 {E/26/48} and 2.57, last sentence {E/26/53}].
[472] Wright 9, App A paras 2.19-2.20 {E/26/43}.
[473] See e.g. Wright 9, para 2.55 {E/26/52}; Wright 4, para 6(c)(iii) {E/4/5}. See also {Day 2/136/4}; {Day 2/140/4}; {Day 3/19/11}; {Day 4/35/11}; and {Day 4/43/1}.
[474] {Day 16/11/23} to {Day 16/24/21}.

practices (or a combination of both). In particular, Mr Madden agreed with the following technical propositions:

218.1. It is possible to for an organisation to engineer the Normal.dotm template "*to contain…pretty much anything you want*",[475] including matters such as the use of **specific fonts** and the automatic running of certain functionalities or add-ins, such as **MathType**[476] and **Grammarly**[477] software. Mr Madden also agreed that that it is possible for a system to be configured in such a way that default styles and customisations in the Normal.dotm template are automatically applied to all Microsoft Word documents opened by a user, including pre-existing documents, and for such changes to be retained by both new and existing documents once they are saved (whether actively or automatically). [478]

218.2. What may appear to be an **anomalously long edit time** recorded in a MS Word document's metadata can have been caused by that document having been accessed by a user on a remote server during a Citrix session, and the relevant Citrix session then being disconnected without the Word document being closed.[479]

218.3. If Dr Wright's working practices involved creating and working on multiple files across multiple computers that accessed remote storage devices, that could explain different documents having **overlapping edit times**.[480]

218.4. Where a file is created by copying an existing file, including by using the Windows command XCopy, this will typically cause the **Created timestamp recorded in the metadata of the new file to post-date its Last Modified timestamp**. [481] Although this would also typically cause the Last Accessed timestamp of the destination file to be updated alongside the Created timestamp, many program, file system and operating system settings can affect whether the former timestamp will in fact be updated in that way, and indeed it is possible for a system to be configured so as to **disable updates to the Last Accessed**

[475] {Day 16/31/25}.
[476] {Day 16/31/24}.
[477] {Day 16/40/17}.
[478] {Day 16/35/7} to {Day 16/37/12}.
[479] {Day 16/25/21} to {Day 16/31/14}.
[480] {Day 16/48/3} to {Day 16/49/2}.
[481] {Day 16/45/16}.

timestamp.[482] Mr Madden suggested in oral evidence that this would not affect the destination file, but oddly he had not tested this for the purposes of these proceedings, even though COPA knew that the behaviour of the Last Accessed timestamp following a file copy was in issue.[483]

218.5. Where **multiple symbolic links are created to a single file**, it is possible for **complications to arise** as a result of changes made to the file across a network.[484]

219. In the circumstances, Dr Wright submits that the Court should not conclude that a document has been forged simply on the basis that it contains timestamps, fonts and/or versions of software that post-date the date on the face of the document.

B. Additional Forgery Allegations

220. On 5 January 2024, COPA provided notice to Dr Wright (under paragraph 11 of the PTR Order) of the 20 "documents" from the Additional Documents which it alleges to be further forgeries.[485] On 23 January 2024, COPA served its Schedule of Dr Wright's Further Forged Documents, identifying the Additional Forgery Allegations.[486] These included 17 documents, two of Dr Wright's Overleaf LaTex files, and the BDO Drive Image itself.

221. Dr Wright's response to the allegations concerning the LaTex files has been set out in Section IV above.

222. So far as concerns the BDO Drive Image, and the 17 other documents in the Samsung Drive alleged to be forgeries:

222.1. Dr Wright's submissions under the previous heading, regarding (a) whether the Court needs to determine the forgery allegations at all; (b) the reliability of Mr Madden's evidence; and (c) the nature and effect of Dr Wright's IT environment and working practices, are repeated in relation to these Additional Forgery Allegations.

[482] {Day 16/45/16} to {Day 16/46/10}.
[483] {Day 16/46/14} to {Day 16/47/13}.
[484] Wright 10 para 42 {E/31/8-9} and {Day 16/21/16}.
[485] {M/2/813}.
[486] {A/16}.

222.2. In addition, Dr Wright has drawn to the Court's attention that his computer systems were hacked by Mr Ager-Hanssen prior to Mr Ager-Hanssen's dismissal from nChain.[487] Dr Wright's evidence is as follows:

(a). On 19 October 2023 (before any independent analysis of the Samsung Drive had taken place), Dr Wright stated in **Wright 3, para 18** that Mr Ager-Hanssen had contacted Dr Wright's wife on 25 September 2023 and sent her screenshots of Dr Wright's browsing history, which were later published on social media. Dr Wright believed that Mr Ager-Hanssen had obtained these from his Wright International Investments UK Ltd laptop, by using a policy install attached to software from nChain Ltd to push unauthorised changes to Dr Wright's system. Dr Wright stated that this was reported to both nChain and the police at the time. Dr Wright understands that Mr Ager-Hanssen was dismissed by nChain shortly after this incident.

(b). On 1 December 2023, Dr Wright set out his account of his discovery of the Samsung Drive. At paragraph 22, he explained that after finding the drive at his home on 15 September 2023, he plugged it into his laptop to ensure that it was working.[488]

(c). On 11 December 2023, Dr Wright explained in **Wright 7** that tweets and photographs subsequently posted by Mr Ager-Hanssen on 5 October 2023 revealed that the latter had obtained access to the BDO Drive, because those photographs revealed the contents of the BDO drive being displayed on a laptop that was not his.[489]

(d). In **Wright 14**, Dr Wright stated his belief that Mr Ager-Hanssen had access to his company laptops and files from around May 2023.[490]

(e). When the Additional Forgery Allegations were put to him in cross-examination, Dr Wright repeatedly denied them and maintained that they must have been caused by whomever had obtained unauthorised access to his

[487] Wright 3 [18] {E/3/6}; Wright 7, paras 11-14 {E/22/5-7}; and Wright 11, para 280 {CSW/1/52};
[488] {E/20/7}.
[489] Wright 7, paras 12-14 {E/22/6-7}
[490] {E/33/5}.

systems in 2023.[491] He confirmed orally, when asked, that he had left the Samsung Drive connected to his laptop for some time after checking that it worked, and that he did not recall having logged out of it before stepping away from it.[492] Notably, COPA has not challenged Dr Wright's account of his systems having been hacked.

(f). Moreover, Mr Madden accepted in cross-examination that, if a hacker had gained unauthorised access to Dr Wright's computer through, for example, the use of a Trojan, that hacker could have gained full control of that computer, maintained access to it through a remote network connection, and used such access to steal information or spy on Dr Wright. Further, the hacker would have gained and maintained access to other computers on the same network, as well as to any drive that was connected to it. This in turn would have given that person access to the Samsung Drive when it was connected to Dr Wright's computer, and in turn to the BDO Drive.[493]

222.3. For completeness, the Court should note that Dr Wright takes issue with COPA's reliance on the evidence of Mr Hinnant[494] and Professor Stroustrup[495] as support for the forgery allegation concerning ID_004712 and ID_004713.[496] In Particular:

(a). COPA's case is that these C++ source codes (which Dr Wright has disclosed as models for Bitcoin) have been backdated because they refer to the use of C++ elements (namely the <chrono>, <thread> and <random> standard libraries) that were not in existence at their purported date of October 2007.[497]

(b). However, as Dr Wright has explained both in Wright 11[498] and in his oral evidence,[499] the relevant C++ code in these documents was not making use of the standardised "chrono" library but of a modified version of a separate (and

[491] {Day 5/23} to {Day 5/121}
[492] {Day 5/36}.
[493] {Day 16/84/17} to {Day 16/88/5}.
[494] {C/18/1} and {C/24/2/1}.
[495] {C/2{C/3/1}.
[496] {A/16/24}
[497] {A/16/24} at para 3.
[498] At paras 463 to 471 {CSW/1/87}.
[499] {Day 5/113/24} to {Day 5/119/16}.

then existing) library named Project Chrono, which was a simulation package that he used to test the interaction of nodes. Dr Wright has also described how he modified that library so that his code could call it using the command "#include <chrono>", and that he had developed C and C++ libraries and produced them commercially when at Integyrs. In oral evidence, he described in relation to the inclusion of "<random>" that he had been using random number generation algorithms since the 1980s.[500]

(c). As a result, so far as Mr Hinnant's or Professor Stroustrup's evidence addresses the factual question of when certain standardised libraries became available, Dr Wright does not dispute the content of that evidence, only its relevance to ID_004712 and ID_004713. Indeed, the inapposite nature of that evidence was confirmed when Mr Hinnant was cross-examined,[501] and he accepted that (i) the C++ Standards Committee does not have a monopoly on creating libraries; (ii) third party programmers working outside that committee can create their own libraries; (iii) Project Chrono is an example of such a library; (iv) from a technical perspective, there was nothing to prevent Dr Wright doing what he describes in Wright 11; (iv) random number generators were used extensively by programmers, using the Boost library, before the standardised random library was created; (v) there was nothing to stop Dr Wright from modifying the Boost library[502] and setting his own environment so that the random number generator could be used in the way seen in ID_004712 and ID_004713; and that (vi) his witness statement answering Bird & Bird's question as to whether it was possible for his standardised chrono library to have been used in 2007.

(d). Mr Hinnant's (inadmissible) opinion that what Dr Wright has described is "*like saying I started with a Mustang fighter plane to create a Ford Mustang car*"[503] reflects a misunderstanding of Dr Wright's account. Dr Wright's evidence was not that he had modified Project Chrono to create code equivalent to Mr

[500] {Day 5/119/21} to {Day 5/120/8}.
[501] {Day 14/13/29} to {Day 14/42/22}.
[502] Which Dr Wright states he used at the time: {Day 4/52} and {Day 6/51/10}.
[503] {Day 14/34/15}

Hinnant's standardised chrono library. It was that he had modified Project Chrono so that his simulation code would include elements of time.[504]

C. Ontier Email Forgery Allegations

223. Documents ID_004076[505], ID_004077[506], ID_004078[507] and ID_004079[508] are screenshots of the MYOB accounting software (the "**Screenshots**"). COPA pleaded in its Schedule of fifty forgery allegations served on 31 October 2023 that the Screenshots (other than ID_004076) are forgeries.[509] ID_004077 also features among COPA's Schedule dated 14 December 2023 of the twenty of its existing forgery allegations that it would rely on at trial.[510]

224. Mr Madden identified that accounting entries reflected in the Screenshots, dating on their face from 2009 to 2011, were added to the MYOB system on 6 and 7 March 2020.[511] On Day 3 of trial, Dr Wright was cross-examined on the basis that the Screenshots were made on 9 March 2020 and therefore post-dated (and reflected) the entries made on 6 and 7 March 2020.[512] Dr Wright's response was, in summary, that the entries identified by Mr Madden as being made on 6 and 7 March 2020 were made for the purposes of creating a document in the Kleiman proceedings and reflected authentic entries dating from 2009 to 2011, and that the Screenshots were made by Ontier before 6 and 7 March 2020 and showed the authentic original accounting entries.[513] On Day 4 of trial, Dr Wright stated that he did not know precisely when the Screenshots were created, but that the login details for MYOB *"was given to both Ontier and Alix Partners in late 2019*".[514]

225. On 8 February 2024, Ontier wrote to Shoosmiths by email stating that Ontier was first provided with login details for MYOB on 9 March 2020 and then created the Screenshots on 9 and 10 March 2020.[515] Shoosmiths disclosed the contents of Ontier's email by its

[504] See, for example {Day 5/118}.
[505] {L16/252/1}.
[506] {L5/150/1}.
[507] {L5/471/1}
[508] {L5/146/1}.
[509] {A/2/118}.
[510] {M/2/684}.
[511] PM7, §64 {H/47/34}.
[512] {Day 3/125/23} to {Day 3/128/9}.
[513] *Ibid.*
[514] {Day 4/6/11}.
[515] {X/55/1}.

letter dated 9 February 2024.[516] Dr Wright was recalled for cross-examination on day 15 of trial, during which the following exchange took place between Dr Wright and Mr Hough KC:[517]

23 Q. You told the court that Ontier received MYOB log-in
24 details in late 2019, didn't you?
25 A. I did, and I have the emails for it.

226. Dr Wright was referring to an email that had been provided to Shoosmiths by Dr Wright's wife, Ramona Watts, on 18 February 2024.[518] That email (the "**Ramona Version**") appears on its face to contain a three-message chain between Dr Wright and Mr Cohen of Ontier on 2 December 2019.[519] The top message in the chain is an email from Dr Wright in which he refers to both Alix Partners and Ontier being provided with login details for MYOB.

227. During Dr Wright's cross-x on Day 15, Shoosmiths asked Ontier to confirm whether they were able to locate the Ramona Version email on their systems and to reconfirm when they were provided with login details for MYOB. Ontier replied on the same day, stating, in summary, that:[520] (1) an email in the form of the Ramona Version was received by Ontier for the first time on Sunday 18 February 2024 (the "**Ontier Received Version**");[521] and (2) Ontier had received an email on 2 December 2019 timed 15.56 , which was sent in response to the same email that the Ramona Version responded to, but which referred to Information Defence and Blacknet and did not mention MYOB login details (the "**Ontier ID Version**")[522]. Dr Wright's counsel disclosed the Ramona Version, the Ontier Received Version and the Ontier ID Version, together with the related correspondence with Ontier in Court on Day 16 of trial.[523] COPA served Madden 6 on 28 February 2024, which addressed these emails. On the same day, COPA served a Schedule pleading that the Ramona Version was a forgery.[524] Both Dr Wright and Mr Madden were recalled for cross-x on Day 19 of trial.

[516] {M/2/1000}.
[517] {Day 15/14}.
[518] {X/56/1}.
[519] {X/56/2}.
[520] {X/57/1}.
[521] {X/58/1}.
[522] {X/59/1}.
[523] {Day 16/128/14} to {Day 16/136/21}.
[524] {A/17/1}.

228. Dr Wright's position on these Ontier emails is set out below:

229. **First**, Dr Wright maintains that the Ramona Version is an authentic email, sent by him on 2 December 2019 as a second reply to Mr Cohen's email of 1:45pm (the first reply being the Ontier ID Version). As Dr Wright put it: "*I've responded to the same original email twice. I do that quite often.*".[525]

230. **Second**, Dr Wright accepts that the headers in the Ramona Version are incomplete. He explains that this is because the email was split into two parts as a result of migrating his email mailbox:[526]

> A. … 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.

231. Mr Madden did not think that the migration of Dr Wright's mailbox would have caused the anomalies he identified in the headers of the Ramona Version, but he also accepted in cross-x that he did not test for this possibility.[527] Indeed, Mr Madden did not have time to analyse the alternative more complete version of the Ramona Version[528], because that was disclosed by Dr Wright only after Madden 6 was served.[529]

232. **Third**, Dr Wright says that he did not send the Ontier Received Version on 18 February 2024, and he believes that this version of the email was sent to Ontier by a malicious third-party seeking to discredit him.[530] As to this:

---

[525] {Day 19/14/8}.
[526] {Day 19/52}.
[527] {Day 19/91/3} to {Day 19/91/18}.
[528] The second version is at {X/71/1}.
[529] {Day 19/90/18}.
[530] See, for example: {Day 19/30/23} to {Day 19/31/24}.

232.1. There is no dispute that it is relatively easy to "spoof" an email, i.e., for an attacker to send an email impersonating a different sender, subject to security protocols that have been developed to mitigate this vulnerability.[531]

232.2. SPF, DKIM and DMARC are security protocols developed to mitigate spoofing. These protocols allow a receiving email server to check whether the sender of an email is authorised by reference to an approved list of IP addresses from the purported sender's domain records (SPF) or against the purported sender's public cryptographic keys (DKIM), and then implement policies (such as diverting to spam) for emails that fail those checks.[532]

232.3. The headers of the Ontier Received Version do not show any SPF or DKIM checks having been performed or DMARC policies having been implemented.[533] This is significant for two reasons.

232.4. First, it is consistent with the email having been spoofed (in that failing to carry out the checks designed to mitigate spoofing makes spoofing more plausible). Mr Madden sought to suggest in cross-examination that other Google security systems would have "*come into play*" to prevent the email being spoofed, but he did not identify any such system, and there is no record of any Google authentication check in the header of the Ontier Received Version.[534] Indeed, Google's own Security White Paper mentions only SPF, DKIM and DMARC as methods for mitigating spoofing attacks.[535]

232.5. Second, Dr Wright has set up SPF and DKIM policies for his domains tuliptrading.net and rcjbr.com.[536] As a result, an email genuinely sent from those domains should record SPF and DKIM checks being passed. Mr Madden accepted this in cross-x, but noted this depended on the receiving mail server performing the relevant check.[537]

---

[531] See Mr Madden {Day 19/69/13} to {Day 19/71/21}.
[532] See Mr Madden {Day 19/71/22} to {Day 19/73/1}.
[533] See Mr Madden {Day 19/83/20} to {Day 19/84/2}. The email header is shown on page 10 of Madden 6 {G/11/10}.
[534] {Day 19/85/2} to {Day 19/85/19}.
[535] {X/66/19}.
[536] Wright 15, §§8-10 {E/34/5}} and Figure 3 {E/34/7}.
[537] {Day 19/85/20} to {Day 19/86/6}.

233. COPA sought to attack the credibility of Dr Wright's account in three ways:

233.1. First, it was put to Dr Wright that it was implausible that an attacker would have access to the Ramona Version in order to be able to spoof the Ontier Received Version, but Dr Wright pointed out that at least a 100 people had access to his emails. On that basis, it is not unlikely that an attacker could have obtained a copy of the Ramona Version.[538]

233.2. Second, it was put to Dr Wright that the timing of the alleged spoofing of the Ontier Received Version on the same day as Ms Watts sent the Ramona Version to Shoosmiths was implausible. However, Dr Wright explained that it is possible his house was bugged, and that a private security firm had previously identified bugs in his house.[539]

233.3. Third, it was suggested that Dr Wright had added SPF and DKIM policies for tuliptrading.net and rcjbr.com only after 18 February 2024. This allegation was made on the basis of print-outs of public DNS records handed-up in Court, which were explained by Mr Madden in chief. Dr Wright identified visual anomalies with the printout, which caused him to question their accuracy.[540] Mr Madden accepted that public DNS records are not always reliable for dating when a particular change was made:[541]

7 Q. Now, you were shown DNS records in your
8 evidence−in−chief, weren't you?
9 A. Yes.
10 Q. Now, you will accept, won't you, that those records are
11 only as accurate as the data collected by the particular
12 service?
13 A. Yes, I think I've said that several times over
14 Q. Can I ask you to be shown page 2 of that record. What
15 this record shows is, first of all , looking at
16 the bottom line, that as at 26 May 2017, there was no
17 SPF check set up?
18 A. Yes.
19 Q. That's correct?
20 A. Yes.
21 Q. It is also shown that as at 28 February 2024, there was

[538] {Day 19/31/25} to {Day 19/33/4}.
[539] {Day 19/57/3} to {Day 19/58/7}.
[540] {Day 19/41/18} to {Day 19/41/25}.
[541] {Day 19/86} to {Day 19/87}.

22 an SPF check set up?
23 A. Yes.
24 Q. It does not enable you to identify when, between those
25 two dates, the SPF check was added
1 A That comes down to how you interpret this, the "first
2 seen" and "last seen". What we cannot say is when in
3 that period they have done their snapshots or how
4 regularly.
5 Q. Exactly, and that is the point you made when you and
6 I were discussing the Abacus emails?
7 A. Yes.

234. In conclusion in relation to the Ontier emails disclosed during the course of trial, the position is that COPA's allegation of forgery depends on two propositions. First, that the Ontier Received Version was sent by Dr Wright rather than a malicious third party on 18 February 2024; and second, that the Ramona Version is not authentic to 2 December 2019. COPA cannot prove either proposition. There is no technical reason that the Ontier Received Version could not have been spoofed, and as Dr Wright explained there are plenty of people who might have had motive and opportunity. Conversely, it makes no sense for Dr Wright to have sent a version of the email to Ontier on 18 February 2024 – the fact of an email on that date would be easily verifiable and would inevitably lead to the assertion that the 2019 versions were inauthentic. As for the Ramona Version, the principal reason it is alleged to be a forgery is that it is inconsistent with the dates of the Ontier Received Version, but if the latter is a spoofed email, then that reason falls away. Dr Wright says the header anomalies identified by Mr Madden can be explained by his email migration, and although Mr Madden doubted that explanation, he did not actually test it. Even if the Court harbours doubts about Dr Wright's account, it should not make a finding on forgery against him based on evidence that was produced at great speed, and so could not fully address the detail of Dr Wright's account.

V. RELIEF

235. If the Identity Issue is resolved in Dr Wright's favour, no issue of relief arises at this trial. COPA's claim would have failed, with the result that it is not entitled to any relief. The BTC Core Claim would continue based on the determination, as a preliminary issue, that Dr Wright is Satoshi Nakamoto.

236. The issue of relief arises only if COPA succeeds in proving that Dr Wright is not the author of the Bitcoin White Paper. This section of these submissions therefore proceeds on the basis that the Court has, contrary to Dr Wright's case, concluded that he is not Satoshi Nakamoto. In that case, it will be necessary for the Court to consider whether to grant the relief sought by COPA, namely:[542]

236.1. **Declarations** that (a) Dr Wright is not the author of the Bitcoin White Paper; (b) that Dr Wright is not the owner of the copyright in the Bitcoin White Paper; and (c) use by COPA of the Bitcoin White Paper will not infringe any copyright owned by Dr Wright.

236.2. An **injunction** restraining Dr Wright from: (a) claiming he is the author of and/or owner of copyright in the Bitcoin White Paper; and (b) taking steps which involve him asserting the same.

236.3. An order **dissemination and publication** of the Court's judgment or order.

237. There is no basis for any such relief irrespective of the outcome of the Identity Issue, and COPA's claim is therefore fundamentally misconceived. Dr Wright's position was set out in the skeleton argument served on his behalf for trial and is further developed below.

A. Declarations

238. The power to make declarations is a discretionary one[543] and can include (as between the parties to a claim) a declaration as to their rights or as to the existence of facts (**Financial Services Authority v Rourke** [2002] CP Rep 14, per Neuberger J).

239. The declarations that COPA seeks are all negative in nature.[544] The principles relevant to the grant of negative declaratory relief were helpfully summarised by Cockerill J in **BNP Paribas SA v Trattamento Rifiuti Metropolitani SpA** [2020] EWHC 2436 (Comm), [78] (omitting citations):

i) The touchstone is utility;

[542] COPA's Re-Re-Re-Amended Particulars of Claim, prayer for relief at {A/2/22}.
[543] The jurisdiction is statutory: section 19 of the Senior Courts Act 1981.
[544] PoC, §68 {A/2/21}.

ii) The deployment of negative declarations should be scrutinised and their use rejected where it would serve no useful purpose;

iii) The prime purpose is to do justice in the particular case;

iv) The Court must consider whether the grant of declaratory relief is the most effective way of resolving the issues raised. In answering that question, the Court should consider what other options are available to resolve the issue;

v) This emphasis on doing justice in the particular case is reflected in the limitations which are generally applied. Thus:

a) The court will not entertain purely hypothetical questions. It will not pronounce upon legal situations which may arise, but generally upon those which have arisen.

b) There must in general, be a real and present dispute between the parties before the court as to the existence or extent of a legal right between them.

c) If the issue in dispute is not based on concrete facts the issue can still be treated as hypothetical. This can be characterised as "the missing element which makes a case hypothetical."

vi) Factors such as absence of positive evidence of utility and absence of concrete facts to ground the declarations may not be determinative; Zamir and Woolf note that the latter "can take different forms and can be lacking to differing degrees". However, where there is such a lack in whole or in part the court will wish to be particularly alert to the dangers of producing something which is not only not utile, but may create confusion.

240. The principles stated by Cockerill J at [78(v)] bear particular emphasis in this case: the Court will grant declarations only to resolve real disputes relevant to the existence or extent of a legal right **between** the parties. This was explained by O'Farrell J in **Office Depot International (UK) Ltd v UBS Asset Management (UK) Ltd** [2018] EWHC 1494 (TCC), [47], citing Lord Diplock in **Gouriet v Union of Post Office Workers** [1978] AC 435:

> *Declaratory relief will be granted only where there is a real dispute between the parties: Gouriet v Union of Post Office Workers [1978] AC 435 per Lord Diplock at p.501:*
>
> > *"…The only kinds of rights with which courts of justice are concerned are legal rights; and a court of civil jurisdiction is concerned with legal rights only when the aid of the court is invoked by one party claiming a right against another party, to protect or enforce the right or to provide a remedy against that other party for infringement of it, or is invoked by either party to settle a dispute between them as to the existence or nature of the right claimed. So for the court to have jurisdiction to declare any legal right it must be one which is claimed by one of the parties as enforceable against an adverse party to the litigation,*

either as a subsisting right or as one which may come into existence in the future conditionally on the happening of an event …

… the jurisdiction of the court is not to declare the law generally or to give advisory opinions; it is confined to declaring contested legal rights, subsisting or future, of the parties represented in the litigation before it and not those of anyone else."

241. The Court will scrutinise carefully the utility of granting a negative declaration, and it does not follow from a party's success on the substance of a dispute that it will be entitled to some or all of the declarations it has sought. In **Deutsche Bank AG London v Comune di Busto Arsizio**, Cockerill J applied the principles set out in [78] of her judgment in **BNP Paribas** to scrutinise each of the 14 declarations sought by the Bank consequent to its success in establishing that certain interest rate swaps between the Bank and 'Busto' were valid and enforceable. The court refused to make a number of the declarations, including where they lacked utility: see [16]-[61].

242. Adopting this approach, it is necessary to scrutinise each of the three declarations sought by COPA.

243. The first declaration, which is to the effect that Dr Wright is not the author of the Bitcoin White Paper has no utility and is inappropriate as a form of declaratory relief. It seeks to declare the answer to a purely academic question which does not on any view engage any legal right or legal interest of COPA, not least because COPA does not claim to have authored the Bitcoin White Paper. The Courts rightly do not entertain academic disputes that do not engage legal rights or interests: see **Office Depot International** cited above.

244. The second declaration sought by COPA is different in that it concerns whether Dr Wright has copyright in the Bitcoin White Paper, and thus on its face concerns Dr Wright's legal rights and interests (or rather, the absence thereof). However, the declaration would have no practical utility going beyond the consequences of a judgment determining the Identity Issue against Dr Wright: that issue would be *res judicata* between the parties, and a declaration adds nothing to that. It is on that basis wholly unnecessary.

245. The third declaration sought by COPA is entirely redundant: if the Court were to grant the second declaration sought by COPA, then the third declaration is tautologous because COPA could not infringe a right that Dr Wright does not have; if the Court refuses to

make the second declaration, then the third declaration should be refused for the same reason.

B. Injunction

246. By its claim COPA seeks a novel form of draconian injunctive relief that would have sinister consequences.

247. An injunction restraining Dr Wright from claiming he is the author of the Bitcoin White Paper and from "*taking steps which involve him asserting the same*" (the "**Identity Injunction**") would mean, among other things, that Dr Wright would face imprisonment for asserting that the Court's judgment was mistaken, criticising the Court's conclusions or, at least on its face, applying for permission to appeal. Such restrictions are alien in a democratic society adhering to principles of open justice. Dr Wright would be precluded from telling anyone, including friends and family, about who he says he is, which, whether the Court agrees or disagrees, is obviously an important part of his personal identity. Unsurprisingly, no similar injunction has ever been granted in this jurisdiction, and it is precluded both by statute and binding authority.

248. An injunction preventing Dr Wright from claiming that he owns copyright in the Bitcoin White Paper (the "**Copyright Injunction**") is on its face less sinister, but it is similarly contrary to established principle. COPA has no sufficient right or interest to claim such an injunction and the injunction would serve no legitimate purpose.

Legal principles: jurisdiction

249. The leading case on the scope and exercise of the Court's injunctive jurisdiction is the Supreme Court's decision in **Wolverhampton City Council v London Gypsies and Travellers** [2024] 2 WLR 45. The case concerned applications by various local authorities under s.37 of the Senior Courts Act 1981 ("**SCA 1981**") prohibiting "*persons unknown*" from setting up unauthorised encampments within their administrative areas. In finding that the English Courts could properly exercise the jurisdiction to order injunctions "*against the world*" (*contra mundum*) and against persons who were not yet party to any proceedings, Lords Reed, Briggs, and Kitchin (with whom Lords Hodge and Lloyd-Jones agreed) set out the following broad propositions:

249.1. The injunction remains an equitable remedy notwithstanding that it now has a statutory basis in s.37(1) of the SCA 1981 (at [17]).

249.2. While the jurisdiction to grant an injunction under s.37(1) is broad ("*in all cases in which it appears to the court to be just and convenient to do so*"), "*the power to grant an injunction must be exercised in accordance with principle and any restrictions established by judicial precedent and rules of court*" (at [19]).

249.3. The "*equitable principles*" relevant to the exercise of the court's discretion include that an injunction will be granted where common law remedies are **inadequate to vindicate the claimant's legal rights**:

> *[149] The basic general principle by reference to which equity provides a discretionary remedy is that it intervenes to put right defects or inadequacies in the common law. That is frequently because equity perceives that the strict pursuit of a common law right would be contrary to conscience. … But that conscience-based aspect of the principle has no persuasive application in the present context.*
>
> *[150] Of greater relevance is the deep-rooted trigger for the intervention of equity, where it perceives that available common law remedies are inadequate to protect or enforce the claimant's rights. The equitable remedy of specific performance of a contractual obligation is in substance a form of injunction, and its availability critically depends upon damages being an inadequate remedy for the breach …*

250. Lord Leggatt had previously explained the relevance of the claimant's interest to the jurisdiction to grant injunctive relief in the Privy Council's decision in **Convoy Collateral Ltd v Broad Idea International Ltd** [2023] AC 389, at [52]:

> *"The proposition asserted by Lord Diplock in The Siskina and Bremer Vulkan on the authority of North London Railway was that an injunction may only be granted to protect a legal or equitable right. There can be no objection to this proposition in so far as it signifies the need to identify an interest of the claimant which merits protection and a legal or equitable principle which justifies exercising the power to grant an injunction to protect that interest by ordering the defendant to do or refrain from doing something. In Beddow v Beddow (1878) 9 Ch D 89, 93, Jessel MR expressed this well when he said that, in determining whether it would be right or just to grant an injunction in any case, "what is right or just must be decided, not by the caprice of the judge, but according to sufficient legal reasons or on settled legal principles". As described above, however, within a very short time after The Siskina was decided, it had already become clear that the proposition cannot be maintained if it is taken to mean that an injunction may only be granted to protect a right which can be identified independently of the reasons which justify the grant of an injunction."*

251. Thus, the grant of an injunction requires that (i) a legal interest of the claimant which *merits protection* and (ii) a legal or equitable principle which *justifies exercising the power to grant an injunction to protect it,* to be identified. The claimant's interest, however, need not amount to a freestanding right which can be identified (and enforced) independently.

252. This approach reflects the position in the prior authorities:

252.1. In **Day v Brownrigg** (1878) 10 Ch D 294, the Court of Appeal held that a claimant who lived at "Ashford Lodge" could not obtain an injunction to restrain his neighbour from changing the name of his house from "Ashford Villa" to "Ashford Lodge" because there was no infringement of any legal or equitable right.[545] James LJ observed at 305 that:

> *"It appears to me there is no damage alleged, there is no legal right alleged, the violation of which was the cause of damage. That being so, it is not for this Court to say that because somebody is doing something which it thinks not quite right, a thing which ought not to be done by one person to another, it should interfere. This Court can only interfere where there is an invasion of a legal or equitable right. No such legal or equitable right exists …"*

252.2. In **Cowley (Earl) v Cowley (Countess)** [1901] AC 450, the House of Lords declined to grant an injunction sought by Earl Cowley against his ex-wife to prevent her from continuing to use the title of 'Countess' on the basis that he had no right (or legally recognised interest) in doing so.[546]

252.3. Both **Day** and **Cowley** are cited with approval in **Gee on 'Commercial Injunctions'** (7th Ed.), at §1-011, footnote 47. **Day** was recently cited in **Prescott Place Freeholder Ltd v Batin (No 2)** [2023] 1 WLR 2926 by Richards J at [67].

253. These basic principles are entirely consistent with the IP cases cited by COPA in its skeleton argument for the "*principles [that] apply to the discretion to grant injunctive relief in the context of infringement of IP rights.*".[547] The key point is that in those cases an injunction is justified to protect the applicant's IP rights. As COPA put it: "*The normal*

[545] **Day** continues to be cited with approval in the English Courts, on this specific point: see for instance **Prescott Place Freeholder Ltd v Batin (No 2)** [2023] 1 WLR 2926 *per* Richards J at [67].
[546] At 456.
[547] §§288*ff* {R/11/113}

*position in IP cases is that, **where there has been an infringement**, an injunction usually follows*".[548]

254. COPA asserts that "*a comparable approach must also apply when a party establishes non-infringement*".[549] This is a bold assertion, but of course there is no reason to apply principles concerned with **restraining the infringement of established IP rights** to the very opposite situation where there has been **no infringement** of any such right. To the contrary: such an approach would be directly contrary to the basic equitable principles underlying the jurisdiction to grant an injunction cited above.

255. COPA cites only one authority in support of its approach: **Samsung Electronics (UK) Ltd v Apple Inc** (No.2) [2013] ECDR 2. That case does not, however, assist COPA. In **Samsung**, Apple alleged that Samsung's Galaxy tablets infringed its patents. HHJ Birss QC (as he then was) found at first instance that there had been no infringement and made an order requiring Apple to publicise the fact of the non-infringement on its website and in certain newspapers. Apple appealed both the finding of non-infringement and the publicity order, the latter on the basis of the massive publicity which HHJ Birss QC's judgment had already received. The Court of Appeal dismissed both appeals.

256. The relevant order at issue in **Samsung** was an order for Apple to "*to publicise the fact that it had lost in manners specified in the consequential order*".[550] Such a publicity order is of a completely different nature to the restrictive injunctions of perpetual effect sought by COPA in this case. The Court of Appeal considered a publicity order to be simply an "*adjunct to the declaration [of non-infringement]*".[551] Indeed, COPA itself pleads a separate claim for a publicity order, reflecting the fundamentally different nature of that relief to the restrictive injunctions it seeks.

257. **Samsung** gives no support for the proposition that the Court can grant a restrictive injunction preventing a non-infringer from claiming IP rights, let alone from claiming that they authored a document more generally. Nothing in the order at issue in **Samsung**

[548] Skeleton Argument, §290 {R/11/113}.
[549] Skeleton Argument, §293 {R/11/114}.
[550] **Samsung**, [1].
[551] **Samsung**, [75].

prevented Apple criticising the Court's decision or continuing to assert that Samsung's Galaxy tablets infringed its IP.

258. COPA also fails to mention that this very point was addressed at first instance in **Samsung Electronics (UK) Limited v Apple Inc** [2012] EWHC 2049 (Pat), which was one of decisions upheld on appeal in **Samsung** (albeit on a different point). In that decision, HHJ Birss QC refused an injunction sought by Samsung that would have restrained Apple from representing "*to any person*" that Samsung's Galaxy tablets infringed a patent owned by Apple. HHJ Birss QC's reasoning at [28]–[29] is instructive:

> *"28 Mr. Hacon described an injunction of this kind as sinister. I agree that there is a very serious question whether the court should go around granting injunctions purporting to restrain people from saying that they disagree with a judgment. As I think was attributed to Jeremy Bentham, "publicity is the soul of justice" and it is very important that the courts can be held up to public scrutiny and what happens in them can be discussed in public.*
>
> *29 In my judgment overall, that is one very powerful factor and is quite sufficient for me to say that there should be no injunction in this case."*

259. **Samsung** is somewhat more relevant to COPA's claim for a publicity order and is addressed further in that context below.

Legal principles: freedom of expression

260. It is common ground that the injunctions sought by COPA would be an interference with Dr Wright's right to the freedom of expression under Article 10 of the ECHR.[552]

261. Section 6(1) of the Human Rights Act 1998 ("**HRA**") makes it unlawful for the Court to act in a way which is incompatible with a Convention Right. Section 12 of the HRA "*applies if a court is considering whether to grant any relief which, if granted, might affect the exercise of the Convention right to freedom of expression (s. 12(1))*". In such cases, s. 12(4) requires that "*The court must have particular regard to the importance of the Convention right to freedom of expression*".

[552] COPA's Skeleton Argument, §289 {R/11/113}.

262. The Court can therefore grant an injunction only if it is satisfied that the injunction is compatible with Dr Wright's right to freedom of expression, having had particular regard to the importance of that right.

263. The right to freedom of expression may be infringed only as prescribed by Article 10(2), namely by such restrictions:

> *"as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."*

264. Thus, any infringements of the right must be (a) prescribed by law; (b) pursuant to a legitimate aim; and, critically, (c) necessary in a democratic society. Only the latter two requirements are relevant to this case (it is accepted that an injunction made by the Court pursuant to s. 37(1) SCA 1981 would be prescribed by law).

265. The right to freedom of expression is one of the "*core rights*" protected by the ECHR, and so the exceptions in article 10(2) must be "*construed strictly and the need for any restrictions must be established convincingly*": **Sürek and Özdemir v Turkey** (1999) 7 BHRC 339, [57 (i)], cited in **R (Lord Carlile) v Secretary of State for the Home Department** [2014] UKSC 60, [2015] AC 945, [13] (Lord Sumption JSC) and [165] (Lord Kerr JSC).

266. In deciding whether an interference with Article 10 is justified, the court must ask itself whether the proposed interference is proportionate to the legitimate aim pursued: As Lord Sumption JSC explained in **Lord Carlile** at [19]:

> *"the question depends on an exacting analysis of the factual case advanced in defence of the measure, in order to determine (i) whether its objective is sufficiently important to justify the limitation of a fundamental right; (ii) whether it is rationally connected to the objective; (iii) whether a less intrusive measure could have been used; and (iv) whether, having regard to these matters and to the severity of the consequences, a fair balance has been struck between the rights of the individual and the interests of the community."*

Analysis

267. COPA's justification for its claimed injunctions is set out in paragraph 299 of its skeleton argument {R/11/115}. It says that the injunctions are justified because "*Dr Wright's campaign of litigation and threatened litigation asserting supposed IP rights of Satoshi (which the real Satoshi never saw fit to assert) needs to be brought to an end*." COPA's professed concern is therefore to restrain Dr Wright from further litigation and threats of litigation regarding "*supposed IP rights*".

268. There are two threshold points that COPA must overcome. The first is whether COPA has standing to claim the injunctions it seeks. Dr Wright's position is that it does not. COPA cannot point to any legal or equitable interest that **it has** that would be vindicated by either of two the injunctions sought. This is *a fortiori* in relation to the injunction restraining Dr Wright from claiming, or taking steps in relation to claiming, that he authored the Bitcoin White Paper (COPA does not claim that it authored the White Paper).

269. As explained above, COPA gains no assistance from the IP cases it cites: these simply apply the general rule that an injunction must protect some legal or equitable right of the applicant. COPA is instead in the position of the unsuccessful applicants in **Day** and **Cowley** – it doesn't like what Dr Wright is calling himself, but that does not mean it can restrain him at pain of imprisonment from doing so.

270. The second threshold point is that the form of injunction sought is not one that the Court can (or at least should) grant:

    270.1. This is most obvious in relation to the Identity Injunction, which imposes extraordinary restrictions on Dr Wright's ability to assert his own identity and comment on the correctness of any judgment of the Court in a way that cannot be justified. The Identity Injunction impermissibly seeks to restrain Dr Wright from doing an inherently lawful act: **Bradford Corp v Pickles** [1895] A.C. 587.[553] The mere making of a statement by Dr Wright that he is the author of the White Paper would not involve infringing any of COPA's rights, even if the statement were untrue. Moreover, there has been no attempt by COPA to plead (or even explain)

[553] See in particular Lord Halsbury L.C. at pp. 591-595.

how such a statement would, in and of itself, give rise to any cause of action, let alone one actionable by COPA. In circumstances where it is not even suggested that the injunction would involve restraining a legal wrong (as opposed to an act that is in itself lawful), there is no proper basis for an injunction in this form.

270.2. Even the Copyright Injunction goes far beyond any restriction previously imposed by the Courts in this jurisdiction: it is analogous to the injunction refused by HHJ Birss QC in **Apple v Samsung**, which was rightly described as sinister.

271. Even if COPA could establish an entitlement to the injunctions it seeks in principle, those injunctions must be refused as an unjustifiable interference with Dr Wright's right to freedom of expression. It is necessary to consider each of the four questions stated by Lord Sumption in **Lord Carlisle**:

271.1. **Whether COPA's objective is sufficiently important to justify the limitation of a fundamental right.**

(a). COPA's avowed objective is to bring to an end Dr Wright's campaign of threatened and actual litigation. This is not a legitimate aim of a civil injunction, and these matters are separately provided for in legislation and the common law, where appropriate.

(b). The appropriate route to prevent a party from conducting a campaign of unwarranted litigation is an Extended Civil Restraint Order ("**ECRO**") pursuant to Practice Direction 3C. COPA has not sought such an order, no doubt because it is obvious that the requirements are not met. It is not appropriate for COPA to try to achieve the same objective through the backdoor by means of an ordinary civil injunction.

(c). The law provides remedies to a person aggrieved by unjustified threats of IP infringement. The Intellectual Property (Unjustified Threats) Act 2017 codified protections against groundless threats of infringement proceedings by the holder of a patent, trade mark, unregistered design right or registered design, following a lengthy consultation process by the Law Commission that carefully considered the appropriate scope of those protections.[554] The

[554] See: https://lawcom.gov.uk/project/patents-trade-marks-and-designs-unjustified-threats/

common law also provides causes of action for malicious falsehood, defamation and causing loss by unlawful means that protect a person from statements that the law has deemed should give rise to protection. In serious cases, threats can give rise to criminal liability. COPA cannot assert a claim under any of these causes of action, and there can be no justification for COPA to circumvent the carefully balanced statutory regime or long-established common-law causes of action by means of a claim for a novel civil injunction.

271.2. ***Whether the injunction is rationally connected to the objective***

(a). The Copyright Injunction is rationally connected to COPA's stated objective; the Identity Injunction is not.

(b). Preventing Dr Wright communicating to anyone that he is Satoshi Nakamoto goes far beyond preventing Dr Wright from commencing or threatening proceedings in relation to supposed IP rights relating to Bitcoin.

271.3. ***Whether a less intrusive measure could have been used***

(a). As explained above, the Identity Injunction is not necessary to prevent Dr Wright from commencing or threatening proceedings. The Copyright Injunction on its own would achieve that purpose.

(b). In any case, as explained below, even the Copyright Injunction serves no useful purpose, and so it is unnecessary.

(c). In so far as the injunctions would have any utility beyond the fact of a judgment on the Identity Issue adverse to Dr Wright, those purposes could also be addressed through the declarations sought by COPA (although, as noted above even those are unnecessary).

271.4. ***Whether a fair balance has been struck between the rights of the individual and the interests of the community.***

(a). As explained above, the claimed injunctions, and particularly the Identity Injunction, involve a grave interference with Dr Wright's right to freedom of

expression in relation to a core part of his beliefs and identity and the Court's judgment.

(b). As Lord Sumption observed in **Lord Carlisle** at [40]:

> *"There are degrees of interference with even so important a right as freedom of expression. The degree of interference involved necessarily has a significant impact on one's assessment of its proportionality. Relevant factors include the degree of control asserted by the state over the dissemination of the relevant information or opinion, the methods by which it exercises that control and whether the freedom of the press is curtailed. At one extreme there is a case like Sürek which involved the total suppression of a particular point of view, enforced with criminal sanctions including imprisonment. At the other are cases where the measure impugned restricted only the method by which the opinion or information was conveyed. Absent unusually compelling considerations of public order, it is difficult to think of any circumstances in which the first extreme would be consistent with article 10. But short of that, the position is more nuanced and less susceptible to absolute positions.*

(c). The Identity Injunction would entail the "*total suppression*" of Dr Wright's belief that he is Satoshi Nakamoto, and this would be "*enforced with criminal sanctions [through the risk of contempt]*". Although this does not entail the curtailment of press freedom, like the example of **Sürek** Lord Sumption refers to, discourse over the identity of Satoshi Nakamoto and Dr Wright's views as to the purpose of Bitcoin are matters of significant public interest. Importantly in this context, the Supreme Court has made clear in **PJS v News Group Newspapers Ltd** [2016] AC 1081 at [24] that "*article 10 is not only engaged but capable in principle of protecting* ***any form of expression***" and in **City of London v Samede** [2012] HRLR 14, Lord Neuberger MR confirmed at [41] that it is not for Judges to accord "*greater protection to views … with which they agree*".

(d). COPA's interest (if any) in the injunctions pales in comparison to this degree of interference with Dr Wright's core right to freedom of expression. Indeed, as explained above, it is not clear that COPA has any interest at all.

(e). In any event, even if COPA does have a legitimate interest in preventing Dr Wright from commencing or threatening future litigation, the injunctions would still be of at best limited utility for this purpose.

(f). If the Court determines that Dr Wright is not Satoshi Nakamoto and so does not own any copyright in the White Paper, then any threats that Dr Wright makes on the basis that he does own such copyright would carry little or no weight.

(g). It is also notable that COPA seeks to restrain only Dr Wright from asserting that he is Satoshi Nakamoto. He would be the only person in the world subject to that prohibition. There would be nothing stopping Dr Wright's supporters from continuing to argue that Dr Wright is Satoshi Nakamoto, nor would there be anything stopping any other person claiming (even falsely) that they are Satoshi Nakamoto. Indeed, the Court will be aware of numerous such claims being made to the Court by email during the course of the trial, none of which COPA has sought to injunct.

272. In conclusion, COPA has no sufficient interest to claim the unprecedented injunctions it seeks and those injunctions are in any case manifestly inappropriate and would involve an unjustified interference with Dr Wright's freedom of expression for no clear benefit to COPA, beyond vindicating its obvious animosity towards Dr Wright. For his part, Dr Wright made clear in cross-examination that he had no interest in pursuing further litigation, preferring instead to move on to his patents: "*So what I would say is, as long as they [COPA] stop and they leave me alone, I will leave them alone*".[555]

C. Dissemination of judgment

273. COPA "*seeks dissemination of judgment as an appropriate remedy to help ameliorate the chilling effect caused by [Dr] Wright's actions…*".[556] It is unclear precisely what form of "*dissemination*" COPA has in mind.

274. The only precedent for the order that COPA seeks is **Samsung**, but that was a very different case. In **Samsung** there was clear evidence of substantial and direct commercial harm **to Samsung** from Apple's assertion of patent infringement: at [78(i)], the Court accepted Samsung's evidence that "*its market share of tablets in the United Kingdom had plummeted from 10 per cent to 1 per cent and ha[d] only recovered to 3 per cent*". Further, the Court indicated that it would not have made the order "*Given the massive*

[555] {Day 8/112/10} to {Day 8/114/1}.
[556] PoC [72] {A2/22}.

publicity of H.H.J. Birss's judgment [as to non-infringement]", but for the fact that Apple had thereafter sought to enforce an inconsistent judgment in Germany, which had also generated publicity.[557] It was in this context that the Court of Appeal held that a publicity order could be justified to dispel the commercial uncertainty created by Apple. But the Court of Appeal made clear that such an order was not the norm:

> *69 … In saying this I am far from saying that publicity orders of this sort should be the norm. On the contrary I rather think the court should be satisfied that such an order is desirable before an order is made—otherwise disputes about publicity orders are apt to take on a life of their own as ancillary satellite disputes. They should normally only be made, in the case of a successful intellectual property owner where they serve one of the two purposes set out in art.27 of the Enforcement Directive and in the case of a successful non-infringer where there is a real need to dispel commercial uncertainty in the marketplace (either with the non-infringer's customers or the public in general).*

275. There is no need for such an order in this case. If COPA succeeds, COPA is unlikely to stay quiet or need any assistance from the Court in publicising its success. COPA's members include substantial US technology businesses that are well able to generate such publicity as they might require in the event of a favourable judgment. Moreover, the case has generated considerable media interest, and any judgment is likely to be widely reported. COPA will have no difficulty disseminating any judgment.

VI. CONCLUSION

276. For the reasons given above and in Dr Wright's Skeleton Argument, Dr Wright respectfully invites the court to resolve the Identity Issue in Dr Wright's favour.

LORD GRABINER K.C.
CRAIG ORR K.C.
MEHDI BAIOU
TIM GOLDFARB
One Essex Court, Temple, London EC4Y 9AR
agrabiner@oeclaw.co.uk, corr@oeclaw.co.uk, mbaiou@oeclaw.co.uk

RICHARD GREENBERG

[557] [79]-[82].

Twenty Essex, 20 Essex Street, London WC2R 3AL
rgreenberg@twentyessex.com

8 March 2024