

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

Before: Mr Justice Mellor

CRYPTO OPEN PATENT ALLIANCE v WRIGHT (IL-2021-000019)
(“the COPA Claim”)

WRIGHT AND ORS. v BTC CORE and ors. (IL-2022-000069)
(“the BTC Core Claim”)

SKELETON ARGUMENT OF THE CLAIMANT IN THE COPA CLAIM
FOR TRIAL COMMENCING 5 FEBRUARY 2024

*Note: References to the Opus2 electronic bundles take the form: {**Bundle / Tab / Page**}*
References to statements / expert reports give the name and number of the statement / report.
A suggested pre-reading list is appended.

JONATHAN HOUGH KC
JONATHAN MOSS
TRISTAN SHERLIKER

29 January 2024

Instructed by Bird & Bird LLP

Introduction	4
Housekeeping	5
Summary of COPA’s Position.....	6
The Factual Background.....	7
Digital Cash before Bitcoin	7
Satoshi’s Release of Bitcoin.....	7
Satoshi’s initial communications and release of the Bitcoin White Paper	7
Release of the Bitcoin Source Code and creation of the early blocks.....	9
Satoshi’s later communications and his departure	9
Dr Wright and his Life up to 2011	10
The ATO Investigations and Decisions.....	12
The Tulip Trust.....	16
The Bailout of Dr Wright and the Outing / “Doxing” in Late 2015.....	17
The EITC Agreement of February 2016	19
The “Signing Sessions” of March and April 2016	21
The Sartre Blog Post of 2 May 2016 and its Aftermath.....	23
Dr Wright’s Work with nChain and Calvin Ayre	25
Dr Wright’s Threats to Assert IP Rights	26
Dr Wright’s Other Litigation.....	26
Events since September 2023	29
What is COPA?	30
Relevant Procedural History.....	30
Procedural chronology for the COPA Claim.....	30
Dr Wright’s Disclosure.....	33
Overview of the Reliance Documents.....	37
Overview of Cryptocurrency Technology	39
Introduction	39
Digital Signatures	40
Transacting in Bitcoin	40
Transaction Ordering.....	41
Blockchain Forks.....	42
Storage and Use of Bitcoin.....	42
Security of Digital Signatures	43
Public keys Associated with Satoshi	44
The Evidence at Trial	44
COPA’s Fact Evidence.....	45
COPA’s Hearsay Evidence.....	49

Dr Wright’s Fact Evidence	50
Dr Wright’s Hearsay Evidence.....	52
Forensic Document Examination / LaTeX Code Experts	53
Cryptocurrency Experts.....	54
ASD Experts.....	55
Submissions on the Law Relevant to Resolution of the Identity Issue	56
Burden and Standard of Proof.....	56
Pleading and Proof of Fraud.....	57
Evidence – Recollections of Witnesses and Documentary Evidence.....	58
Points on Expert Evidence.....	58
Drawing of Inferences (including from absence of witnesses)	59
Evidence on Character and Credibility.....	59
Hearsay Evidence – Admissibility and Weight.....	60
Admissibility of Public Reports and of Judgments in Other Proceedings	60
Dr Wright’s Claim to be Satoshi	60
Project BlackNet.....	61
Lasseter’s and Vodafone	62
Dr Wright’s Employment at BDO.....	62
Dr Wright’s LLM Dissertation	63
Dr Wright’s MStat Degree	64
Dr Wright’s Claims about Writing the Bitcoin code.....	65
Drafting of the White Paper	66
Creation of the Genesis Block, Release of the Source Code and the First Transaction.....	69
Dr Wright Leaving the Satoshi Persona	70
Overview of COPA’s Case.....	71
(1) Dr Wright’s Use of False and Forged Documents.....	71
Examples from the Schedules of Forgeries	74
(1) MYOB records [ID_004077, ID_004078 and ID_004079] - Appendix PM7 {H/47/1}	74
(2) Project BlackNet document [ID_001379] – Appendix PM8 {H/60/1}	75
(3) NAB Records [ID_003455] (with attachments) – Appendix PM17 {H/78/1}	76
(4) Spoofed Email [ID_001546] – Appendix PM21 {H/104/1}.....	76
(5) Bitcoin.exe [ID_000739] – Appendix PM12 {H/68/1}	77
(6) Timecoin ODT [ID_000254] – Appendix PM2 {H/17/1}	77
(7) LLM Dissertation Proposal [ID_000217] – Appendix PM25 {H/118/1}	78
(8) BDO Quill minutes [ID_004013] – Appendix PM5 {H/31/1}	79
(9) Backdated Draft of the White Paper [ID_000536] – Appendix PM3 {H/20/1}	79

(10) King2.rtf [ID_004695] – PM46 {H/278/4}.....	80
Dr Wright’s Excuses and Changes of Story	81
Change of Story Sase Study: the NAB Screenshots.....	85
Chain of Custody Schedule	87
The New Documents	88
The BDO Drive Documents	88
The Overleaf LaTeX files.....	90
(2) Dr Wright’s Failures to Provide Proof of his Claim.....	90
Failure to Produce Supportive Witnesses.....	91
Failure to Provide Reliable Documentary Evidence	93
Failures of Cryptographic Proof – the Sartre Blog Post and its Aftermath.....	96
Failures of Cryptographic Proof – Destruction of the Hard Drive and no Proof Since 2016	98
Failures of Cryptographic Proof – Overview of the Signing Sessions.....	99
Failures of Cryptographic Proof – the Signing Sessions with Mr Matonis and the Journalists	101
Failures of Cryptographic Proof – the Signing Session with Mr Andresen	102
(3) The Implausible and Inconsistent Nature of Dr Wright’s Accounts.....	103
BlackNet and Spyder Projects	104
Supposed Collaboration with Prof Wrightson and Dr Furche.....	105
Early Events in the History of Bitcoin	105
Further Submissions on Dr Wright’s Credibility	108
Relief Claimed.....	110
Legal Principles for Declaratory Relief.....	111
Justification for Declaratory Relief	111
Legal Principles for Injunctive Relief	112
Justification for Injunctive Relief.....	114
Conclusion.....	115

Introduction

1. On 31 October 2008, a person or group of people writing under the pseudonym Satoshi Nakamoto released the Bitcoin White Paper, the foundational text of the Bitcoin system and other cryptocurrencies.¹ In early 2009, Satoshi released the Bitcoin source code and created the first blocks of the Bitcoin blockchain. Satoshi continued working on the development of the system until early 2011, then ceased communication and handed over its administration to others. Since that time, there has been intense speculation about the true identity of Satoshi Nakamoto.
2. Since 2016, Dr Craig Wright has publicly made a claim to be Satoshi and to have authored the Bitcoin White Paper. Backed by the wealthy gambling entrepreneur Calvin Ayre, he has asserted rights in the White Paper, the name “Bitcoin” and the Bitcoin blockchain. He has threatened and pursued multiple pieces of litigation against cryptocurrency developers. He and his lawyers have touted his claims as being worth “*hundreds of billions of pounds*” (including in the Claim Form in the BTC Core Claim²).
3. COPA’s case is, simply, that Dr Wright’s claim to be Satoshi is a lie, founded on an elaborate false narrative and backed by forgery of documents on an industrial scale. As his false documents and inconsistencies have been exposed, he has resorted to further forgery and ever more implausible excuses. A striking recent example is his claim that the Bitcoin White Paper was written in LaTeX code and that he has LaTeX files which uniquely compile into the paper. The parties’ experts are now agreed that the White Paper was not written in LaTeX and also that Dr Wright’s files do not produce a replica, while metadata show the files to be recent forgeries.
4. COPA is a non-profit mutual benefit corporation, formed to promote cryptocurrency technologies. It has seen first-hand the chilling effect of Dr Wright’s aggressive threats and conduct of litigation. It therefore brought the COPA Claim to seek a declaration that Dr Wright is not the pseudonymous author of the White Paper. Since the COPA Claim began, Dr Wright has issued multiple sets of proceedings which raise the same issue, including the BTC Core Claim (in which Dr Wright claims damages from numerous

¹ The White Paper as released on 31 October 2008 is document ID_000226 {L3/231/1}. The version as published on 24 March 2009 is document ID_000865 {L5/26/1}. These versions are authenticated by COPA’s expert, Mr Madden, in Appendix PM3, at §39-40 {H/20/14}).

² See statement of value at {A1/1/2}. See also equivalent statements in the Claim Forms in the Kraken Claim {A2/1/2} and Coinbase Claim {A3/1/2}.

Bitcoin developers and COPA itself for infringement of database rights in the Bitcoin blockchain and copyright in both the White Paper and File Format).

5. By an order dated 21 July 2023, the Court directed that this trial should be to resolve “the Identity Issue”, framed as “*whether Dr Wright is the pseudonymous ‘Satoshi Nakamoto’, i.e. the person who created Bitcoin in 2009*”.³ This trial serves as the main trial of the COPA Claim and as a preliminary issue trial in the BTC Core Claim. The result will also be binding for the parties to two other sets of proceedings (the Coinbase and Kraken Claims).

Housekeeping

6. There are two matters to be dealt with at the beginning of trial. First is the status of Wright 11. The statement runs to over 330 pages (244 pages plus appendices). It is seriously in breach of PD57AC and most does not constitute reply evidence (as the Court order required). Much of it is irrelevant, inadmissible opinion and/or argument dressed up as evidence (including very long sections with Dr Wright’s views on COPA’s cryptocurrency expert report and on the Bitcoin system today).⁴ It contains plainly inadmissible expert evidence, including (remarkably) an attempt to adduce a further expert report through a footnote with a weblink. It includes unsupported allegations against COPA, its members and the Developers. Dr Wright is applying to have his solicitors absolved from certifying compliance under the Practice Direction. He has refused to fix the myriad deficiencies in his statement, instructing his solicitors that he wishes to rely on all of Wright 11.⁵ Shoosmiths have, however, confirmed in writing that COPA does not need to put to Dr Wright every aspect of Wright 11 with which they do not agree.⁶
7. The second matter of housekeeping is the removal of confidentiality terms for Dr Wright’s LaTeX documents. COPA has sought agreement to this in correspondence, so that (for example) the content of the files may be addressed without clearing the court, but Dr Wright has refused. COPA has therefore issued an application to be addressed at the start of trial.

³ {B/12/4}: at §1.

⁴ For further detail, see letters from Bird & Bird dated 15 January {M/2/858} and 19 January 2024 {M/2/898}.

⁵ See correspondence from Shoosmiths at {M/2/902}, §2.

⁶ Ibid, §4.

Summary of COPA's Position

8. COPA's position is that Dr Wright has spun a false narrative over a period of years, backed up with numerous forged documents. Dr Wright has consistently failed to supply genuine proof of his claim to be Satoshi: instead, he has repeatedly proffered documents which bear clear signs of having been doctored.
9. It is COPA's case that Dr Wright produced these forgeries himself or alternatively (if others were somehow involved) he at least knew that he was presenting false evidence. Furthermore, Dr Wright's forgeries and lies are not merely historic. This is not a case of some past forgeries being exposed, but a scheme of forgery and lies continually adapting and re-inventing itself (most recently with the BDO Drive in September 2023 and the Overleaf LaTeX files in November / December 2023). Once one aspect of Dr Wright's story is discredited, he supplements it with yet further forgeries, moves his story in a different direction and casts blame on others (often casting lawyers and experts as his scapegoats, to take advantage of legal professional privilege).
10. In this skeleton, COPA presents its case in three parts:
 - 10.1. Use of false and forged documents: Dr Wright has produced a large number of false and forged documents, manipulated in such a way as to give support to many aspects of his story. The forged documents are of numerous kinds, and they demonstrate a wide range of techniques of forgery. In accordance with orders of the Court, COPA has (a) pleaded 50 forgeries from Dr Wright's original disclosure, while agreeing to focus upon 20 of those; and (b) pleaded a further 20 forgeries from the "new" documents which Dr Wright supposedly found between September and November 2023.
 - 10.2. Failures of proof: Despite having the strongest incentives to do so, Dr Wright has failed to supply evidence which might actually support his claim to be Satoshi, such as by producing verifiable emails or draft documents from 2007-2009 or by offering reliable cryptographic proof of his control of Bitcoin addresses linked to blocks associated with Satoshi. Indeed, not only has Dr Wright not taken such steps, he has on key occasions undertaken to do so and then failed to come good on his promise. Two examples are (a) his signal failure to undertake a public key

signing or transaction in May 2016 and (b) his empty boast that he could prove purchase of Satoshi's email account and web domain.

- 10.3. Inconsistent and implausible account: Dr Wright's account is full of inconsistent and implausible features. The inconsistencies are both internal (in the sense that Dr Wright's own story has changed) and external (where Dr Wright's story conflicts with reliable evidence or established fact). Furthermore, certain aspects of Dr Wright's story are simply so incredible they cannot be believed.

The Factual Background

11. The Court is aware of the background to these proceedings. The following is a summary which provides context to the issues for trial. A word of caution: because COPA's position is that Dr Wright is lying about all aspects of his claim to be Satoshi, any reference to his version of events should not be read as COPA accepting it.

Digital Cash before Bitcoin

12. Concepts of digital cash date back to the early 1980s, when an American cryptographer called David Chaum proposed a form of token currency which could be transferred safely between individuals, supported by encryption tools. In the 1990s, several further electronic currency systems were proposed, including E-Gold (Dr Jackson and Mr Downey); Bit Gold (Nick Szabo); B-Money (Wei Dai); and Hashcash (Adam Back). Hashcash used a proof-of-work algorithm, as many modern cryptocurrencies do. The expression "*block chaining*" in the context of cryptographic cyphers dates back to the 1970s,⁷ while public discussion of Hashcash in the late 1990s used the expression "*block chain*" in the context of data structures.⁸

Satoshi's Release of Bitcoin

Satoshi's initial communications and release of the Bitcoin White Paper

13. Bitcoin is based on concepts first set out in the Bitcoin White Paper ("**the White Paper**"), the full title of which was: "Bitcoin: A Peer-to-Peer Electronic Cash System". It was

⁷ See US Patent 4074066, 1976: "*Message verification and transmission error detection by block chaining*" (Ehram et al.).

⁸ See for example: <http://mailing-list-archive.cryptoanarchy.wiki/archive/1997/12/e080a2180e912b9b129e8be3e4d114421b0c9bc11217ac2e40b3b8f112305572>

written by Satoshi Nakamoto, which is agreed to be a pseudonym. In late August 2008, Satoshi contacted Dr Back by email, referring him to a draft of the White Paper hosted on the “upload.ae” site and asking to check a reference to his paper on Hashcash.⁹ Dr Back replied, informing Satoshi about Wei Dai’s B-Money Paper.¹⁰ Satoshi then wrote to Wei Dai to check the reference for that paper.¹¹ These early emails contain abstracts of the draft paper. It should be noted that the Satoshi / Wei Dai emails were published before these proceedings, while the Satoshi / Adam Back emails were not.

14. On 31 October 2008, Satoshi released the White Paper by sending an email to the “metzdowd cryptography mailing list” (“**the Metzdown List**”) (a group of individuals interested in cryptography) and directing them to a link on the “bitcoin.org” site, where the document was hosted.¹² From around 9 November 2008, the White Paper was also hosted on a document repository, SourceForge. The final version of the White Paper was posted on SourceForge.net on 24 March 2009,¹³ and published under the MIT License.¹⁴
15. The White Paper describes a system for electronic payments, whereby transactions may be made between participants without a central trusted intermediary. It uses cryptographic signatures and addresses the risk of double-spending by transactions being recorded in blocks, validated by proof-of-work. It is further described in the section of this skeleton headed “Overview of Cryptocurrency Technology”.
16. A number of email addresses have been associated with Satoshi. These have included: satoshi@vistomail.com; satoshin@gmx.com; and satoshi@anonymousspeech.com. The last of those three was used in the emails to Adam Back and Wei Dai of late August 2008, while the first was used to post the White Paper in October 2008.
17. Over the period from 31 October 2008 to January 2009, Satoshi wrote a series of emails to the Metzdown List. In one, dated 8 November 2008, Satoshi explained that the code had been written before the White Paper.¹⁵ In another, dated 14 November 2008, Satoshi

⁹ See email of 20 August 2008, exhibited by Mr Back at {D/80/1}.

¹⁰ See email exchange of 21 August 2008, exhibited by Mr Back at {D/76/1}.

¹¹ See email of 22 August 2008 {L3/195/1}.

¹² The email to the Metzdown List may be found at {L3/278/1}. As noted above, the Bitcoin White Paper as released on 31 October 2008 is ID_000226 and may be found at {L3/231/1}.

¹³ As noted above, the White Paper as released on 24 March 2009 is ID_000865 and may be found at {L5/26/1}.

¹⁴ The Defence takes issue with that proposition, but the effect of the MIT License was ordered to be heard as part of a second trial following the resolution of the Identity Issue: see CCMC Order at {B/7/6}, §34-35.

¹⁵ {L3/290/2}.

claimed to be “*better with code than with words*”. In a third, dated 17 November 2008, Satoshi wrote of having worked through various “*little details over the last year and a half while coding [Bitcoin]*”, adding that the source code for the system was coming soon but was available on request in the meantime.¹⁶

Release of the Bitcoin Source Code and creation of the early blocks

18. On 3 January 2009 (GMT), Satoshi created the first block of the Bitcoin blockchain, on the basis of the framework set forth in the White Paper. This is referred to as Block 0 or the “Genesis Block”. On 9 January 2009 (GMT), the second block in the blockchain (known as Block 1) was mined. Meanwhile, on 8 January 2009, Satoshi published a link to the first release of the Bitcoin executable file and the related source code on SourceForge (the “**Bitcoin Code**”), announcing the release to the Metzdowd List.¹⁷ Before releasing the source code, Satoshi shared source code with developers, including Ray Dillinger and Hal Finney. Shortly afterwards, the first transaction in the Bitcoin blockchain was recorded in Block 170, involving the transfer of 10 Bitcoins from Satoshi to Mr Finney (which had been created as a result of the mining of Block 9).

Satoshi’s later communications and his departure

19. Over the period from early 2009 to late 2010, Satoshi released a series of further versions of the Bitcoin Code (up to Bitcoin 0.3.19 on 13 December 2010). Satoshi communicated messages about the system by means of Bitcoin forums, and also exchanged private emails with a number of individuals. Some of these emails were published, while others were not. Meanwhile, from mid-2009, a community of developers emerged who contributed to the iterations of the code.
20. At the end of 2010, Satoshi informed a developer, Gavin Andresen, of an intention to step back from day-to-day Bitcoin management. Satoshi left Mr Andresen with administrative privileges for the source code repository. In December 2010, Mr Andresen established a new code repository on GitHub. While Dr Wright insists that he as Satoshi was very unhappy about this, Mr Andresen posted contemporaneously that he was acting with Satoshi’s blessing and emails recently disclosed between Satoshi and Mr Andresen

¹⁶ {L3/306/1}.

¹⁷ {L4/63/1}.

bear this out.¹⁸ Meanwhile, on 13 December 2010, Satoshi updated nearly all the Bitcoin files on SourceForge, amending the copyright notices (in version 0.3.19) so that they referred to “Bitcoin Developers” in place of “Satoshi Nakamoto”. In April 2011, Satoshi sent a final series of emails and at the same time handed over the network alert key and broadcast code to a number of developers. The last email uncontroversially attributed to Satoshi was written to Gavin Andresen on 26 April 2011.¹⁹

21. Since Satoshi’s departure, a series of individuals have been speculatively identified as Satoshi, including Mr Finney (who died in 2014), Mr Szabo and a man called Dorian Nakamoto. Each of those three denied the rumours. Dr Wright is also not the only individual to have claimed to be Satoshi and numerous others have, for example, registered the White Paper as their copyright at the USPTO.²⁰

Dr Wright and his Life up to 2011

22. Dr Wright is an IT security professional with a range of academic interests, who claims more than 16 Master’s degrees and two doctoral degrees, including a PhD in Computer Science and Economics from Charles Sturt University.²¹ He was born and raised in Australia, and spent most of his life there until late 2015.
23. In the early to mid-1990s, he worked at OzEmail (an ISP in Australia) as a corporate account manager.²² In 1997-1998, he held a post as IT security consultant for the Australian Stock Exchange, where he developed IT security systems.²³
24. From 1997 to 2003 he worked primarily through DeMorgan Information Security Systems Ltd (“**DeMorgan**”), an IT security consultancy business that he founded.²⁴ In 1998, DeMorgan was engaged by Lasseter’s Online Casino.²⁵ During that time, he worked on “*designing the [IT] security architecture*” for Lasseter’s. It was during his time at Lasseter’s when he first came into contact with Mark Archbold.²⁶ From 1998 to

¹⁸ See post of 19 December 2010 {L19/255/1}. See emails of 18 December 2010 [MACPROD_0000491] {L6/500.2/1} and [MACPROD_0000581] {L6/500.3/1} and 18 January 2011 [MACPROD_0000661] {L7/18.12/1}. These documents are in the process of being uploaded onto OPUS as this skeleton is filed.

¹⁹ {L7/220/1}.

²⁰ See for example {L20/185/1} and {L20/188/1}.

²¹ Wright 1, §6 {E/1/3}. See also his 2007 CV at {L2/102/4} and his 2015 LinkedIn profile at {L11/130/16}.

²² Wright 1, §29 {E/1/7}. See also his 2007 CV at {L2/102/4}.

²³ Wright 1, §36 {E/1/8}. See also his 2007 CV at {L2/102/3} and his 2015 LinkedIn profile at {L11/130/7}.

²⁴ Wright 1, §32 {E/1/8}. See also his 2007 CV at {L2/102/3} and his 2015 LinkedIn profile at {L11/130/6}.

²⁵ Wright 1, §38 {E/1/9}. See also his 2007 CV at {L2/102/2-3}.

²⁶ Wright 1, §39 {E/1/9}.

2002, DeMorgan worked with Vodafone on IT security project work which involved implementing a firewall system.²⁷ Whilst working with Vodafone, he met Rob Jenkins.²⁸

25. In 2003, Dr Wright and his then wife (Lynn) sold their shares in DeMorgan. They later gave undertakings to the Court not to compete with the new shareholder. Dr Wright was subsequently held in contempt for breach of those undertakings. At first instance and on appeal, the Courts rejected a key claim by Dr Wright that an email found on his computer had been fabricated.²⁹
26. In late 2004, Dr Wright started work as an Associate Director of Information systems with the accountancy firm, BDO Kendalls (“**BDO**”). His work is said to have involved IT audits, digital forensics and fraud prevention.³⁰ From 2005, Dr Wright as part of a BDO team provided services to CentreBet, an Australian sports betting site. During the course of that work, he first met Stefan Matthews, who was then CIO of CentreBet.³¹
27. While working at BDO, Dr Wright from 2006 to 2008 undertook an LLM at the University of Northumbria, with his dissertation focusing on the legal status and liabilities of internet intermediaries.³² As noted below, Dr Wright claims that his proposal for his LLM dissertation (although not the dissertation itself) included elements of the White Paper. It is COPA’s position that the dissertation proposal which Dr Wright has disclosed is a forgery, and that the dissertation itself has nothing to do with Bitcoin and is in any event heavily plagiarised from work by Hilary Pearson.³³ From 2007 to 2008, Dr Wright was also heavily occupied with studying for a series of IT security qualifications and with writing books and papers on IT security, regulation and audit.
28. Dr Wright was made redundant from BDO in November or December 2008, with his formal employment ending in January 2009.³⁴ In 2009, he started the companies Information Defense Pty Ltd and Integryrs Pty Ltd. Over the following years, he founded a series of other companies.³⁵ It was also from 2009 that Dr Wright found himself the

²⁷ See Dr Wright’s 2007 CV at {L2/103/1}.

²⁸ Wright 1, §45, 46 {E/1/10}.

²⁹ See NSW Court of Appeal judgment at {L1/334/1}.

³⁰ Wright 1, §48 {E/1/10}. See also his 2007 CV at {L2/102/1} and his 2015 LinkedIn profile at {L11/130/6}.

³¹ Wright1, §49 {E/1/11}.

³² Wright 1, §56 {E/1/12}. The thesis can be found at {L2/195/1}.

³³ The plagiarism is set out in an article exhibited to Ms Pearson’s statement: {D/490/1}.

³⁴ Wright 1, §61 {E/1/13}.

³⁵ He gives some details in Wright 4, §61-67 {E/4/25}.

subject of investigations by the Australian Tax Office (“ATO”), as set out below. Around late 2010, Dr Wright’s first marriage to Lynn Wright was failing, and they separated officially in January 2011.³⁶

The ATO Investigations and Decisions

29. Dr Wright’s dealings with the ATO formed a significant part of his life from 2010 to 2016, and they were important to his finances. Indeed, in August 2014, the ATO estimated that 94% of the income he had received in the previous two years had come from tax refunds to his companies.³⁷ This forms the backdrop for Dr Wright in 2015 needing money and receiving a bailout which involved him staking a claim to be Satoshi.
30. These dealings may be divided into two phases. First, from early 2010 he was subject to enquires in relation to his personal tax return for the 2008/9 tax year, which were resolved by agreement in early 2013. Secondly, he had contentious dealings with the ATO over the period from 2013 to 2016 which primarily concerned (a) claims for repayment of goods and sales tax (“GST”) in business activity statements (“BASs”) for several companies; and (b) claims for R&D credits by various of his companies. It is in the second set of dealings that Dr Wright first appears to have made claims of mining and dealing in Bitcoin. It was also in these claims that he said he had worked on business ventures with Dave Kleiman, a US computer forensics expert (who died on 26 April 2013).
31. As regards Dr Wright’s first set of dealings with the ATO, he calculated his capital gain for the 2008/9 year by claiming a CGT event resulting from sale of IP to related parties (Information Defense Pty Ltd and Integryrs Pty Ltd) for sums totalling AU\$ 2,235,000.³⁸ The IP sale contract on which he relied in relation the sale to Information Defense Pty Ltd referred to IT security projects entitled Spyder, Redback, TripleS and Black Net, and cited a DeMorgan R &D plan.³⁹ It is significant because Dr Wright later produced forged documents to suggest that his Spyder and Black Net projects involved elements of Bitcoin, whereas this and other contemporaneous documents show that they did not.

³⁶ Wright 1, §129-130 {E/1/25}.

³⁷ See ATO Submission at {L9/274/9}, §36.

³⁸ See generally the Administrative Appeals Tribunal Documents file at {L7/431/1}.

³⁹ {L4/462/1}.

32. The ATO decided that Dr Wright's dealings with his companies carried no actual liability and were attempts at wash transactions. It also rejected claims for deduction of various work-related expenses. It imposed administrative penalties for recklessness in completing the tax return and for false and misleading statements.⁴⁰ Dr Wright submitted notices of objection, which were rejected by the ATO, including on the basis of failure to substantiate the IP sales.⁴¹ He applied for review to the Administrative Appeal Tribunal. The result was that the ATO agreed to lift the administrative penalty and to allow various expense deductions,⁴² but it does not appear that the CGT issue was specifically addressed.
33. Dr Wright's second set of dealings with the ATO (from 2013) involved a number of companies, some established in 2013, and they included claims relating to dealings in Bitcoin. The outcome of these dealings was a set of decisions in which his claims for GST refunds and R&D tax offsets were refused, and a number of his companies were wound up.
34. In 2013, Dr Wright applied to the ATO for private rulings, including one application by which he claimed to have begun mining Bitcoin in 2009 and to have invested in computer equipment for that purpose. The application appears to have been for decisions on the tax treatment of transfers of Bitcoin.⁴³ In early 2014, he made a further application for a ruling as to the viability of a tourist tax refund of GST in relation to sale to him of rights in a Bitcoin address by Hotwire PE (one of his companies) for US\$19.5 million. The ATO decided against him.⁴⁴
35. For the tax quarter ending September 2013, Dr Wright's companies submitted claims for GST refunds: AU\$2.8 million in respect of Cloudcroft Pty Ltd; AU\$3.7 million in respect of Coin-Exch Pty Ltd; AU\$4.1 million in respect of Denariuz Pty Ltd; and AU\$3.4 million in respect of Hotwire Pre-Emptive Intelligence Pty Ltd. These related to supposed acquisition of rights to software held by the Wright Family Trust (trading as DeMorgan). Dr Wright subsequently claimed that all consideration for the acquisition

⁴⁰ See Interim Report at {L7/431/119}.

⁴¹ See Reasons for Decision at {L7/431/9}.

⁴² See letter from the ATO dated 15 January 2013 {L8/117/1}.

⁴³ See decision letter dated 23 December 2013 {L8/305/1}.

⁴⁴ See letter of 28 February 2014 {L8/422/1}.

of the software had been given by transfer of equitable interests in a Seychelles trust (the Tulip Trust), whose trust property comprised 650,000 BTC.

36. He and his advisers described a complex scheme involving Dr Wright acquiring software and IP rights from W&K Information Defense Research LLC (“**W&KID**”) (a company founded by himself and Mr Kleiman) and another company; the software and rights being subject to repeated assignments in return for rights in Bitcoin; and the assignments being ultimately financed by a Bitcoin loan dated 23 October 2012 from the Tulip Trust to Dr Wright (with the loan agreement executed by Dr Wright’s associate, Uyen Nguyen, for a company acting for the trust). The ATO took the view that this scheme involved various sham transactions.⁴⁵
37. Dr Wright’s corporate tax issues from 2013 included claims in relation to the 2012/13 year for C01N Pty Ltd. The claims of over AU\$ 7 million were ultimately rejected in a detailed decision of 11 March 2016.⁴⁶ The principal claims were (a) for sums supposedly paid to W&KID for operating a supercomputer; and (b) AU\$ 2 million for materials and assistance supposedly received from Prof David Rees, a UK-based mathematician and veteran of Bletchley Park.
 - 37.1. As to the former claim, Dr Wright sought to establish proof of payment by describing a byzantine set of equity and loan transactions with related entities and the Tulip Trust. In that connection, he provided two copies (dated 24 June 2011 and 17 October 2014) of an email from David Kleiman attaching a document under which Mr Kleiman supposedly agreed to hold 1.1 million Bitcoin on trust for Dr Wright. The ATO found a series of anomalous features in this account and Dr Wright’s documents.
 - 37.2. As to the latter claim, Dr Wright maintained that payment had been made to Prof Rees by way of Bitcoin rights. However, evidence from Prof Rees’s daughters established a series of falsehoods in the claim. For instance, they told the ATO that, at the time when Dr Wright claimed Prof Rees had made a Bitcoin transaction (after 28 June 2013), Prof Rees was in a nursing home and had stopped using a computer at all. None of the daughters was aware of Dr Wright and they

⁴⁵ See ATO Decision at {L16/456/1}; Preliminary GAAR Submission dated 29 August 2014 {L9/274/1}.

⁴⁶ {L11/354/1}.

all disputed the notion that he had sold research documents. It is noteworthy that, since 2013, Dr Wright has maintained a claim that Prof Rees gave him notes which assisted in his work on Bitcoin more generally.⁴⁷

38. Dr Wright's corporate tax disputes also included a number in relation to tax returns of his companies for the 2013-14 year. These were rejected in a series of decisions of March and April 2016, concerning respectively C01N Pty Ltd,⁴⁸ Denariuz Pty Ltd,⁴⁹ Zuhl Pty Ltd⁵⁰ and Integrys Pty Ltd.⁵¹ The disallowed claims totalled nearly AU\$30 million. In broad terms, they included (a) R&D activities involving supposed payments for provision of computing services from a facility located in Panama; (b) expenses supposedly incurred for acquisitions from Prof Rees; and (c) losses due to reduction in value of Bitcoin assets. In his dealings with the ATO, Dr Wright claimed to have mined 1.1 million Bitcoin in 2009 and to have transferred it to Mr Kleiman. Once again, he told a story of the Tulip Trust entering into a deed of loan (executed by Uyen Nguyen). He also said that the Bitcoin could be accessed under a Shamir Secret Sharing Scheme, whereby private keys were split into segments (held by Dr Wright, Mr Kleiman and Ms Nguyen) and needed to be reconstituted.⁵² It appears to have been in these tax claims that Dr Wright first claimed to have been involved in Bitcoin from a very early stage.
39. In his dealings with the ATO, Dr Wright was found to have backdated documents. For example, he supplied a Deed of Assignment and Charge and "invoice" documents bearing the ABN of Wright Family Trust (trading as DeMorgan) from a time before the date when it had been allocated an ABN.⁵³ Dr Wright sought to explain this on the basis that "*the trustee entered into the transactions on the understanding that an ABN had been obtained prior to that date*",⁵⁴ though he later accepted backdating the invoices.⁵⁵
40. On Dr Wright's own account, the ATO investigations led to him running up very large legal bills with the Australian firm, Clayton Utz, which he has put at over £1 million. In July 2015, Clayton Utz ceased acting for Dr Wright on the basis that he had submitted

⁴⁷ See Dr Wright's book, "Satoshi's Vision" at {L15/96/18}.

⁴⁸ See decision dated 21 March 2016 at {L11/354/1}.

⁴⁹ See decision dated 21 March 2016 at {L9/381/1}.

⁵⁰ See decision dated 12 April 2016 at {L12/176/1}.

⁵¹ See decision dated 21 March 2016 at {L11/404/1}.

⁵² For example, see in the C01N Pty Ltd decision at §179ff {L9/382/31}.

⁵³ See for instance ATO Decision at {L11/362/10}, at §52ff.

⁵⁴ See Dr Wright's response to the ATO draft objection decision at {L14/333/2}.

⁵⁵ {L9/140/29} at line 8: "*I ended up doing the backdating because I thought it was correct*".

apparently false copies of emails with the ATO.⁵⁶ The differences between the emails submitted by Dr Wright and the copies held by the ATO were “*intended to support the position Craig wanted to advance.*”

The Tulip Trust

41. The supposed Tulip Trust, which formed part of Dr Wright’s story in the tax claims (and whose existence was doubted by the ATO⁵⁷), features in Dr Wright’s narrative in these proceedings as well. His evidence is that he placed in this trust a number of assets, including his (unspecified) intellectual property and all Bitcoin mined by his companies since 2009, in order to keep them out of the reach of the ATO.⁵⁸ He also claims that, under this structure, private keys linked to the blocks associated with Satoshi could only be accessed by assembling key slices (separated using a Shamir Scheme), held by various individuals responsible to the Trust and so gaining access to an encrypted drive.⁵⁹
42. The materials provided to the ATO to demonstrate the existence of the Trust were the two versions of the supposed email (with trust document attached) from Mr Kleiman dated 24 June 2011⁶⁰ and 17 October 2014⁶¹ respectively. A different Deed of Trust, dated 23 October 2012 and supposedly between Wright International Investments Ltd and Tulip Trading Ltd was relied upon by Dr Wright in the *Kleiman* litigation.⁶²
43. In the course of the ATO investigations, Dr Wright was asked to prove his control of several tranches of Bitcoin addresses, using the message signing feature of Bitcoin software. He failed to do so, and came up with a series of excuses, involving transfers and loss of keys.⁶³ COPA will say that there are parallels between these and Dr Wright’s excuses for not providing comparable proof of his control of Bitcoin addresses linked to Satoshi. A further point to note is that Dr Wright told the ATO that Bitcoin in three addresses supposedly lent to him had not been spent and had been returned to Tulip Trust,

⁵⁶ See email from Clayton Utz to Ramona Watts, forwarded to Dr Wright on 4 July 2015 {L10/66/1}.

⁵⁷ See ATO Decision at {L16/456/19}, §109.

⁵⁸ Wright 1, §138-139 {E/1/26}. It is notable that, despite Dr Wright saying that he put all his IP on trust and out of reach of the ATO, that cannot be his position now. If it were, then Dr Wright would have none of his IP rights in relation to Bitcoin as he asserts in these joined proceedings and he would have no standing to sue.

⁵⁹ Wright 1, §140-143 {E/1/26} and §186-187 {E/1/33}.

⁶⁰ In disclosure at {L7/382/1}.

⁶¹ In disclosure at {L9/218/1}.

⁶² The copy used as an exhibit in the *Kleiman* litigation is at {L8/17/1}.

⁶³ See Decision concerning C01N Pty Ltd of 21 March 2016 {L9/382/45}, at §247-261.

including Bitcoin in an address known as 16cou.⁶⁴ On 16 May 2019, the owner of that address signed a message on social media stating that the address did not belong to Satoshi or to Dr Wright and “*Craig is a liar and a fraud*”.⁶⁵

The Bailout of Dr Wright and the Outing / “Doxing” in Late 2015

44. In 2014, while he was in the midst of the ATO investigation, Dr Wright says that he contacted Stefan Matthews to explore possible investment in his (Dr Wright’s) work.⁶⁶ By email dated 3 February 2014,⁶⁷ Mr Matthews introduced him to a businessman called Rob MacGregor, who ran a company called nTrust. According to Dr Wright, this led to discussions about Mr MacGregor investing in Dr Wright’s business ventures.⁶⁸ Dr Wright says that nothing came of the introduction at that stage.⁶⁹
45. In or around April 2015, Dr Wright was again in contact with Mr MacGregor and Mr Matthews. Calvin Ayre was now also involved. By this stage, Dr Wright’s businesses were in serious difficulties and he was heavily in debt to Clayton Utz.⁷⁰ By late April 2015, the men were discussing investment in Dr Wright’s businesses.⁷¹ By June 2015, those discussions had progressed to detailed negotiations about an agreement for Mr Ayre and Mr MacGregor to provide financing for Dr Wright’s businesses.⁷² Dr Wright appears to have put up as collateral a sum of Bitcoin in the 1Feex wallet, ownership of which is in issue in the *Tulip Trading* case.⁷³
46. Dr Wright claims that, on 29 June 2015, he entered into an outline agreement, recorded in a Term Sheet between DeMorgan Ltd and Mr Matthews’ company, “The Sterling Group”. It appears that a first version of the document was prepared,⁷⁴ which was immediately superseded by a second version.⁷⁵ The stated purpose was for DeMorgan

⁶⁴ See Decision concerning C01N Pty Ltd of 21 March 2016 {L9/382/49}, at §266.2 and fn. 241. The full address is: 16cou7ht6wjtzufydbnht9hmvxytg6xdvt.

⁶⁵ {L17/382/46}.

⁶⁶ Wright 1, §149 {E/1/28}.

⁶⁷ {L8/340/1}.

⁶⁸ Wright 1, §151 {E/1/28}.

⁶⁹ Wright 1, §150-152 {E/1/28}.

⁷⁰ Dr Wright’s wife, Ramona Watts, told Ira Kleiman in an email of 23 June 2015 that they owed \$1 million to Clayton Utz and would need to pay those lawyers another AU\$1 million to prevent the ATO shutting down Dr Wright’s businesses {L9/495/2}.

⁷¹ See meeting note for 27 April 2015 {L9/395/1}.

⁷² See for example email exchanges of 10 June 2015 {L9/445/1} and 18 June 2015 {L9/461}.

⁷³ See email of 18 June 2015 at {L9/460/1}.

⁷⁴ {L10/33/1}. The fact that this was superseded by the second version is stated in an Implementation Deed dated 7 January 2016 {L11/285/3}.

⁷⁵ {L10/34/1}.

Ltd to receive funding for its research projects and tax obligations in light of the ATO issues.⁷⁶ The Term Sheet had the following provisions (in summary):

- 46.1. A NewCo would purchase for AU\$1.5 million all IP and technology held by DeMorgan Ltd and all company subsidiaries to “*get the IP out of danger and put some capital back into the company.*”
 - 46.2. DR Technologies Ltd would enter into a technology development and consulting agreement with DeMorgan Ltd for up to two years on a monthly retainer of AU\$200,000.
 - 46.3. The NewCo would issue a convertible loan of AU\$2.5 million to DeMorgan Ltd, with an option for AU\$1 million more, with the purpose to fund solicitor fees and disbursements associated with the ATO matters as well as pending patent filings.
 - 46.4. The NewCo would enter into a direct and exclusive services agreement with Dr Wright as “Chief Scientist” for AU\$3.5 million over five years. The initial version of the Term Sheet stated that these services would “*grant NewCo the exclusive rights to Craig’s life story for subsequent publication or release.*”
47. As noted above, it was shortly after the execution of this Term Sheet that Clayton Utz terminated their retainer with Dr Wright. Thereafter, the ATO decisions went against Dr Wright. Meanwhile, over the period September to November 2015, Dr Wright was in discussions with Mr MacGregor, Mr Matthews and Mr Ayre about his future business ventures and the plan to make public his claim to be Satoshi.⁷⁷
48. By late November / early December 2015, reporters at WIRED and Gizmodo were making enquiries about the possibility that Dr Wright might be Satoshi.⁷⁸ On 8 December 2015, the two magazines published articles on the subject, identifying him as Satoshi and referring to some pieces of evidence.⁷⁹ Dr Wright was contacted by reporters in advance of the publications, though he does not recall engaging with their enquiries other than briefly to end the conversation. It has been reported that, hours after the

⁷⁶ Wright 1, §153 {E/1/28}.

⁷⁷ See for instance emails of 11 September 2015 {L10/339/1}, 21-26 October 2015 {L10/424/1} and 24/25 November 2015 {L11/54/1}.

⁷⁸ Wright 1, §161 {E/1/30}.

⁷⁹ See {L11/206/1} and {L11/212/1}. The evidence is set out in a Gizmodo article of the following day: {L11/213/1}.

articles were published, the Australian Federal Police raided Dr Wright’s home and business premises in connection with the ongoing ATO investigations.⁸⁰ Shortly after the articles were published, Dr Wright moved from Australia to the UK, although he maintains that this move was planned a few months earlier.

49. It is not known who “outed” Dr Wright to the media, but emails sent that day (including from Ira Kleiman⁸¹ and Robert MacGregor⁸²) suggest that some thought it could have been Dr Wright himself.
50. Shortly after the publication of the articles, the publication Motherboard and the Bitcoin developer Greg Maxwell (a defendant in the BTC Core Claim), issued posts identifying problems with the evidence cited by WIRED and Gizmodo (e.g. in relation to PGP keys cited as associated with Satoshi).⁸³ Doubts about Dr Wright being Satoshi surfaced immediately, with a number of outlets publishing stories the next day on 9 December 2015 calling the evidence into question.⁸⁴ On 11 December 2015, WIRED retracted the claim that Dr Wright was Satoshi, publishing an article entitled “*New Clues Suggest Craig Wright, Suspected Bitcoin Creator, May be a Hoaxer*”.⁸⁵ Gizmodo published an equivalent article the same day.⁸⁶
51. In December 2015 or January 2016, Dr Wright met the writer Andrew O’Hagan, who had been identified by Mr MacGregor as an author who might write an extended piece about Dr Wright’s life and his claim to be Satoshi. Mr O’Hagan was to write a significant long article about the following months entitled “*The Satoshi Affair*” (published on 30 June 2016).⁸⁷

The EITC Agreement of February 2016

52. On 7 January 2016, Mr Matthews arranged for an Implementation Deed⁸⁸ to be produced, setting out the manner in which the June 2015 Term Sheet terms would be carried into

⁸⁰ See for instance the opening passage of *The Satoshi Affair*, by Andrew O’Hagan (LRB) {L13/491/2}.

⁸¹ {L11/198/1}.

⁸² {L11/196/1}. Mr MacGregor suggested that Dr Wright may have been responsible for the “Tessier-Ashpool” emails referenced in the WIRED article (see the article at {L11/212/11}).

⁸³ See Vice article dated 21 December 2015 at {L11/215/1}.

⁸⁴ See for example {L11/214/1}: “*Have journalists found the inventor of Bitcoin or simply been duped?*”.

⁸⁵ {L11/218/1}.

⁸⁶ {L11/220/1}.

⁸⁷ {L13/491/2}.

⁸⁸ {L11/285/1}.

effect. It recorded that Ncrypt Holdings Ltd (which later became EITC Holdings Ltd) (“EITC”) was the NewCo identified in the Term Sheet. At section 7, it set out terms for Dr Wright’s rights and services agreement, including stating that he would enter into a further agreement for services of recounting his life story.

53. On 17 February 2016, Dr Wright duly entered into a contract entitled “*Life Story Rights and Services Agreement*” (“**the EITC Agreement**”).⁸⁹ Under its terms:

53.1. The Recitals recorded that EITC, relying on Dr Wright’s representations, warranties and undertakings in the agreement, wished to acquire sole and exclusive rights to his life story and various rights which would allow EITC commercially to exploit that story: see Recital (B).

53.2. By clause 2(a), EITC agreed to pay Dr Wright AUS\$ 1 million in consideration for the Rights granted, defined as all rights, title and interest in “*the Story*”, “*the Subject’s Materials*” and “*the Works*”. By clause 2(b), Dr Wright acknowledged having received an advance of AU\$ 250,000 of that sum in 2015. By clause 2(c), it was agreed that further payments of the sum would be made at milestone events (including preparation and publication of a biography). That clause envisaged that a public announcement might be made by EITC of the identity of the creator of Bitcoin.

53.3. By clause 3, Dr Wright granted EITC a series of licences and consents to exploit the Story. By clause 4, he agreed to recount “*the Story*” and provide full information and details about it to EITC; to make himself available for media interviews; to provide “*the Subject’s Materials*” within 30 days of entering the agreement; and to assist in marketing efforts. The “*Story*” was defined as the entire life story of Dr Wright including matters set out in Annex A, which described him as “*the inventor of the Blockchain technology and Bitcoin*”.

53.4. The “*Subject’s Materials*” were defined as “*all information, documents, photographic and audio-visual works, email correspondence, electronic files and records, computer software applications and code, and any other documentary or other records relevant to the Story*”, including “*at least 400 photographs*”.

⁸⁹ {L11/342/1}.

54. In his Re-Re-Amended Defence, Dr Wright says that he did not provide any “*Subject’s Materials*,” but did have discussions before the agreement was executed in the course of which he “*identified certain documents relating to his authorship of the White Paper*”.⁹⁰ In Wright 4 (responding to an RFI question asking him to specify the documents), Dr Wright said that he did not identify any particular documents to EITC, but that the passage in his Defence was describing Mr MacGregor and his lawyers receiving general access to Dr Wright’s research papers for due diligence in 2015.⁹¹
55. By March 2016, Mr MacGregor had persuaded Dr Wright to participate in interviews saying that he was Satoshi and in private demonstration sessions to support that claim.⁹² In preparation for the interviews, Dr Wright underwent media training sessions with Milk Publicity and the Outside Organisation (including sessions on 18 and 22 March 2016).⁹³ Over the following two months, Dr Wright gave interviews to the media, specifically the BBC, the Economist and GQ. As detailed below, he claimed to the media to have given technical proofs that he had private keys giving access to early blocks in the Bitcoin blockchain which were associated with Satoshi.
56. To complete the story regarding EITC, on 22 August 2016, Dr Wright and the company entered into a Deed of Amendment to the EITC Agreement,⁹⁴ deferring his obligations to take the various steps (of preparing and publishing his book) required for the milestone payments. Clause 2.2 to this Deed of Amendment noted that “*CSW’s obligations under those milestones have not yet been discharged*”. On 4 May 2020, EITC (now renamed nChain Holdings Ltd) agreed with the Defendant to terminate the EITC Agreement in consideration of him paying back the sum of AU\$ 1 million as a termination fee: see Termination Agreement at Recital (B).⁹⁵

The “Signing Sessions” of March and April 2016

57. Around early March 2016, Dr Wright performed two private demonstrations for Andrew O’Hagan during which he said that he had used the private key from one of the original blocks on the Bitcoin blockchain which were associated with Satoshi. This is said to

⁹⁰ {A/3/11}, at §31C.

⁹¹ Wright 4, §56-59 {E/4/23}.

⁹² Wright 1, §183 {E/1/33}.

⁹³ See records of these sessions at {L11/399/1} and {L11/406/1}.

⁹⁴ {L14/10/1}.

⁹⁵ {L16/382/1}.

have been a dry run for demonstrations to be carried out for two of the early developers of Bitcoin, Jon Matonis and Gavin Andresen (both subject to NDAs).⁹⁶ Dr Wright says that the first demonstration took place in an apartment near Soho where he was staying and the second took place at his then home in Wimbledon.⁹⁷

58. Jon Matonis met Dr Wright in mid-March 2016 in a hotel in Covent Garden, as arranged by Mr MacGregor and Mr Matthews.⁹⁸ Dr Wright then met Mr Andresen in London on or about 7 April 2016, having briefly corresponded by email.⁹⁹ Again, they met in a hotel, and Mr MacGregor and Mr Matthews were present. For this session, Dr Wright claims a new IBM ThinkPad laptop was purchased from a retail store by an assistant for the demonstration.¹⁰⁰ Dr Wright claims to have signed messages using the keys associated with blocks 1 and 9.¹⁰¹ As noted below in relation to the signing sessions, there are some differences between Dr Wright’s recollection and that of Mr Andresen in his *Kleiman* deposition (the latter given with reference to some notes¹⁰²). Based on the agreed expert evidence, these are important to whether the session was genuine.
59. Towards the end of April 2016, Dr Wright met Rory Cellan-Jones of the BBC. At this meeting, Dr Wright claims to have demonstrated possession of keys from among the first blocks, including block 9.¹⁰³ Dr Wright also met with Ludwig Siegele from the Economist and, similarly, claims to have demonstrated using private keys, including for blocks 1 and 9, to sign messages.¹⁰⁴ Dr Wright was then interviewed by Stuart McGurk GQ, with the reporter being accompanied by a cryptologist, Dr Nicolas Courtois.¹⁰⁵ Dr Wright says he cannot “*recall the demonstrations exactly*” that were made to the journalists.¹⁰⁶ However, he does say that he did at least demonstrate possession of the private key associated with block 9 in all his signing sessions.¹⁰⁷

⁹⁶ Wright 1, §188 {E/1/33}. Further details about the signing sessions are found later in the submissions which deal with the expert evidence on what they actually showed.

⁹⁷ Wright 1, §189 {E/1/34}.

⁹⁸ Wright 1, §192 {E/1/34}.

⁹⁹ Wright 1, §196-197 {E/1/34}.

¹⁰⁰ Wright 1, §204 {E/1/35}.

¹⁰¹ Wright 1, §206 {E/1/36}.

¹⁰² Mr Andresen’s deposition transcripts are at {E/17/1}; {E/18/1}. The notes are at {L19/217/1}.

¹⁰³ Wright 1, §211 {E/1/36}.

¹⁰⁴ Wright 1, §212 {E/1/36}.

¹⁰⁵ Wright 1, §214 {E/1/37}.

¹⁰⁶ Wright 2, §23 {E/2/8}.

¹⁰⁷ Wright 2, §24, 32 and 40 {E/2/9}.

The Sartre Blog Post of 2 May 2016 and its Aftermath

60. The various articles arising out of those interviews were initially embargoed, then released on 2 May 2016. On the same day, a post on Dr Wright’s blog was released entitled “*Jean-Paul Sartre, signing and significance*”.¹⁰⁸ The post began by acknowledging the significance of him signing messages as Satoshi. It then described a process of verifying cryptographic keys by signing a quotation from Sartre. The issuing of this blog post was a key part of the plan for the “big reveal” of Dr Wright as Satoshi.¹⁰⁹ The articles by the Economist and GQ referred to the blog post and indicated that its purpose was to demonstrate possession of the private key linked to block 9 (a block associated with Satoshi because of the Hal Finney Bitcoin transfer).¹¹⁰
61. Within hours of the Sartre blog post being issued, articles were published making the point that the post had not presented any proof at all, since the signature provided had been of 2009-era Bitcoin transaction that was publicly available on the blockchain.¹¹¹ The Economist immediately published a piece saying that his proof had come under fire and that it had requested a corrected version.¹¹² Dr Wright now accepts that the blog post did not prove his possession of any private key, but says that (contrary to what others plainly expected) it was not an attempt to prove he was Satoshi.¹¹³ Dr Wright also now says that his version of the Sartre post was edited by Mr MacGregor and that the version posted differed from what he had intended.¹¹⁴ The Court will be able to form its own view, as Dr Wright’s draft post (attached to an email of 29 April 2016) is available.¹¹⁵
62. When the blog post was issued, Dr Wright was on a brief trip to Paris, and he travelled back to London that day. Meanwhile, his own team went into a panic. In a series of communications, Mr MacGregor, Mr Matthews and Mr Ayre pressed him to provide a proper, verifiable proof that he controlled keys to addresses linked to Satoshi.¹¹⁶ The

¹⁰⁸ The blog as posted is at {L18/257/1}. Dr Wright later altered the introductory section.

¹⁰⁹ See for example the email of Victoria Brooks (Milk Publicity) dated 29 April 2016 {L13/40/1}.

¹¹⁰ See: {L13/205/11}; {L18/330/4}.

¹¹¹ See for example a post by Dan Kaminsky at {L13/171/1}. As is explained in the post, it required analytical work involving special software to search the public blockchain and establish the falsity of the “proof”.

¹¹² {L13/206/1}.

¹¹³ Wright 1, §219 {E/1/37}.

¹¹⁴ Wright 1, §220-221 {E/1/37}.

¹¹⁵ See email at {L13/88/1} and draft blog post at {L14/327/1}.

¹¹⁶ See for instance emails at {L13/109/1-4} and {L13/116/1}.

email traffic shows that Mr Matonis and Mr Andresen reacted with a sense of betrayal.¹¹⁷ According to Dr Wright, he had a meeting that afternoon at his house in Wimbledon, with Mr MacGregor and Mr Matthews, with Mr MacGregor pressing him to make a public transfer of Bitcoin associated with Satoshi.¹¹⁸ Dr Wright's position is that he told Mr MacGregor he was not prepared to make such a transfer and that any public signing process would be, in his eyes, "*selling out*".¹¹⁹ However, Mr Cellan-Jones of the BBC was told that this transfer would be performed, and small sums in Bitcoin were then transferred by himself, Mr Andresen and Mr Matonis to an address associated with Satoshi, with a view to Dr Wright having them transferred back.¹²⁰ Moreover, contemporaneous emails show that Dr Wright was aware of this plan and at least initially appeared to support it.¹²¹

63. On 3 May 2016, Dr Wright attended a brunch in central London with Mr MacGregor and Mr Matthews. That afternoon, a blog entitled "*Extraordinary Proof*" was published under Dr Wright's name on his blog.¹²² This blog stated that, over the following days, Dr Wright would "*be posting a series of pieces that will lay the foundations for [his] extraordinary claim, which will include posting independently-verified documents and evidence addressing some of the false allegations that have been levelled, and transferring bitcoin from an early block*". Dr Wright now says that this blog post was drafted by Mr MacGregor and that he did not himself review it before it was published. However, it was enthusiastically approved by an email from his wife, who was with him at the time.¹²³
64. During the afternoon and evening of 3 May and the morning of 4 May 2016, email exchanges continued about various forms of proof which Dr Wright might provide. On 4 May 2016, there were further discussions at Dr Wright's home in which, according to Dr Wright, Mr MacGregor repeatedly sought to pressure him into moving Bitcoin from block 9.¹²⁴ Mr Matthews describes Dr Wright speaking over the phone to Mr Andresen

¹¹⁷ See also Mr Andresen's evidence in the *Kleiman* litigation: "*He certainly deceived me about what kind of blog post he was going to publish, and that gobbledygook proof that he published was certainly deception, if not an outright lie.*" {E/17/154}.

¹¹⁸ Wright 1, §223 {E/1/38}.

¹¹⁹ Wright 1, §223-224 {E/1/38}.

¹²⁰ Cellan-Jones, §16 {C/5/4}. See also Mr Andresen's email exchange with Mr Matthews at {L13/234/1}.

¹²¹ See email to Mr Andresen dated 3 May 2016 {L13/261/1}.

¹²² See Wright 1, §228 {E/1/39}. The blog post as published is at {L13/263/1}.

¹²³ See email at {L13/249}. The draft post which she approved is at {L13/209/1}.

¹²⁴ Wright 1, §231 {E/1/39}.

and to suggest that there was a technical reason why the Bitcoin transfer transactions could not take place. However, Mr Andresen is said to have replied that the suggested problem should not arise.¹²⁵ At that point, Dr Wright apparently went up to the bathroom and cut his neck with a knife. He was taken to hospital and treated with the record showing that he suffered “*bilateral abrasions*” with “*no blood loss*” and that he was released later that day.¹²⁶

65. At this point, the plan for a staged revelation of Dr Wright as Satoshi came to an end. On 6 May 2016, a short piece was posted on Dr Wright’s blog saying that he did “not have the courage” to “*publish proof of access to the earliest keys*”.¹²⁷ As explained above, the EITC Agreement which laid the groundwork for that plan was later amended and then terminated. Mr MacGregor ceased to have any association with Dr Wright and his companies.

Dr Wright’s Work with nChain and Calvin Ayre

66. From October 2015, as a result of the deal done in June 2015, Dr Wright was employed as the Chief Scientist of nChain UK Ltd (a new company), which acts as the R&D arm of the nChain Group of companies.¹²⁸ Dr Wright recently left that post, around late September 2023. He apparently continues to act as a consultant for the company. This change of role followed the revelations of Christen Ager-Hanssen which are discussed below.
67. In his campaign of litigation, Dr Wright has received substantial financial support from Calvin Ayre, who has an interest in the nChain Group.¹²⁹ Mr Ayre has also promoted Dr Wright’s claim to be Satoshi, including through the content of his Coingeek website and through social media.¹³⁰

¹²⁵ Matthews 1, §108 {E/5/23}.

¹²⁶ {L13/360/1} and {L13/361/1}.

¹²⁷ {L13/409/1}.

¹²⁸ Wright 1, §7 {E/1/4}. nChain UK Ltd was formerly named nCrypt Ltd (up to November 2016) and nChain Ltd (up to February 2022).

¹²⁹ According to an article dated 11 August 2023, the nChain Group is now substantially controlled by Mr Ayre, who made an investment of up to ChF 500 million in the Group {L19/210/4}.

¹³⁰ See for instance his tweets at {L17/128/1}; {L17/300/1}; {L17/459/1}.

Dr Wright's Threats to Assert IP Rights

68. Over recent years, Dr Wright has issued numerous threats to enforce his alleged IP rights and to bring financial ruin on the developers responsible for Bitcoin and Bitcoin Cash. In a blog post on 13 February 2020, he insisted that he owned “*full rights to the Bitcoin registry*”.¹³¹ On 21 January 2021, Dr Wright through Ontier wrote letters before action to those responsible for various Bitcoin-related sites (including Bitcoin.org) demanding that they cease hosting the White Paper.¹³²
69. Dr Wright has since followed through on those threats by issuing the other claims which were considered with these proceedings in the hearing of 15 June 2023. Whilst the resolution of those IP rights issues is not for this trial, those proceedings include him asserting (in summary): (a) that he has database rights in the bitcoin blockchain; (b) that he has passing off rights associated with the name Bitcoin; and (c) that he has copyright in the Bitcoin File Format as well as in the White Paper.
70. Meanwhile, Dr Wright and Mr Ayre have been tweeting threats to bankrupt and cause criminal prosecutions to be brought against developers. Examples of those threats and their effects in deterring development are set out in the statement of Steve Lee (a COPA board member and a product manager at Block).¹³³

Dr Wright's Other Litigation

71. Dr Wright is a serial litigant in the Courts of this country and other jurisdictions. In the cases discussed below, as well as in the *Ryan* case (above), he has been held to be dishonest and clear evidence of forgery has been found. COPA does not rely upon previous Court conclusions to prove his dishonesty or forgeries in this case, but the judgments are relevant to show that Dr Wright ought to have been careful in presenting documents and their chain of custody in this case. Furthermore, the evidence given in the cases touching on his claim to be Satoshi (especially those of *Kleiman* and *Granath*) is directly relevant to this case.
72. The *Kleiman* Proceedings (USA): Following Dr Wright's attempts to tout his claim to be Satoshi and his naming of the deceased David Kleiman as a collaborator in creating the Bitcoin system and mining Bitcoin, the estate of Mr Kleiman (along with WK&ID, now

¹³¹ “*Forking and Passing Off...*” {L16/225/1}.

¹³² See for instance Ontier letter to Square Crypto and others {L17/86/1}.

¹³³ Lee 1 at {C/12/1}.

controlled by the estate) brought an action against Dr Wright in the Southern District of Florida. The plaintiff claimed that Dr Wright had defrauded the estate of large sums in Bitcoin and of IP rights.¹³⁴ This claim was based on Dr Wright’s own assertions about his having created Bitcoin and conducted mining with Mr Kleiman. After a trial in November / December 2021, the jury found Dr Wright liable to W&KID for conversion of intellectual property and awarded compensatory damages of US\$100 million.¹³⁵

73. In an interlocutory judgment of 27 August 2019¹³⁶ ordering Dr Wright to disclose early Bitcoin holdings, Judge Reinhart concluded that Dr Wright had “*engaged in a willful and bad faith pattern of obstructive behavior, including submitting incomplete and deceptive pleadings, filing a false declaration, knowingly producing a fraudulent trust document and giving perjurious testimony at the evidentiary hearing*”.¹³⁷ More particularly, the Judge found that there was “*substantial credible evidence that documents produced by Dr Wright to support his position in this litigation are fraudulent*”, and a strong (and unrebutted) inference that he had created the fraudulent documents.¹³⁸ The judgment provides evidence of the account Dr Wright gave of putting Bitcoin assets in an encrypted file protected by a Shamir encryption protocol, which is relevant to his account in this case of how he first regained and then lost access to the private keys which were used in the “signing sessions”.
74. The McCormack Proceedings (UK): Dr Wright brought a defamation claim against Mr McCormack, who had publicly disputed his claim to be Satoshi. In that case, Mr McCormack initially raised a defence of truth but then dropped that defence because of the cost of maintaining it, instead relying on the argument that on any view the allegedly defamatory publications (certain tweets) had caused no serious harm reputation. The case went to trial before Chamberlain J in August 2022.¹³⁹ In cross-examination, Mr McCormack’s counsel raised points showing that Dr Wright and Mr Ayre had coordinated threats to ruin those who took issue with Dr Wright’s claim to be Satoshi.¹⁴⁰

¹³⁴ The Complaint in *Kleiman* is at {L14/114/1}. A good understanding of the issues can be gleaned from the oral closing argument, at {L17/333/56}.

¹³⁵ See completed Verdict Form at {L17/352/1}.

¹³⁶ {L15/207/1}. Note that, at p2, the Court confirmed that it was not required to decide, and did not decide, whether Dr Wright was Satoshi.

¹³⁷ {L15/207/27}.

¹³⁸ {L15/207/20}.

¹³⁹ See the principal judgment dated 1 August 2022 ([2022] EWHC 2068 (QB) {L17/457/1}) and the judgment on consequential orders dated 21 December 2022 ([2022] EWHC 3343 (QB) {L18/85/1}).

¹⁴⁰ See transcript, internal pages 121ff {O2/12/32}. These matters are relevant to relief in this case.

75. Dr Wright was found by Chamberlain J to have advanced a deliberately false case, then sought to explain it away with further falsehoods.¹⁴¹ He was awarded only nominal damages (a decision upheld on appeal). Again, COPA does not rely upon the Judge’s finding, but will rely upon the account of what happened in the proceedings, as it is relevant to Dr Wright’s credibility. In the judgment on consequential orders, Chamberlain J made an indemnity costs order and also referred him for contempt proceedings in relation to an apparent breach of the judgment embargo.
76. In the contempt proceedings that followed, Dr Wright claimed that a report submitted to the Court by his solicitors (Ontier) on which Chamberlain J had relied had been put in without his instructions or agreement. The Divisional Court surveyed the facts, explaining that “*all the circumstances point towards the conclusion that the Ontier report was prepared and provided to the Court on the instructions of Dr Wright*”.¹⁴² This event is relevant to the credibility of Dr Wright when he seeks to place blame on his lawyers, as he repeatedly does in these proceedings. Again, COPA does not rely on the finding, but the facts and events recorded in the judgment.
77. The Granath Proceedings (Norway): These concerned whether Dr Wright had been defamed by a blogger, Magnus Granath (aka Hodlonaut), who had disputed his claim to be Satoshi. The case went to trial in the Oslo District Court in late 2022. A number of witnesses in the present proceedings (including Dr Wright) gave evidence on his claim to be Satoshi. In a judgment on 20 October 2022,¹⁴³ the Court held that *Granath* had “*sufficient factual grounds basis to claim that Wright had lied and cheated in his attempt to prove that he is Satoshi Nakamoto*”.¹⁴⁴ It recorded that documents produced by Dr Wright which he had claimed were early versions of the White Paper and Source Code had been found by both parties’ experts to “*contain at best unexplained changes which are likely to have been made after the date the documents are claimed to be from*”.¹⁴⁵
78. The Tulip Trading Proceedings (UK): A further case in this jurisdiction which is not joined with these, but is also heard by the same docketed judge (and is another claim for billions of pounds against some of the developer defendants in the BTC Core Claim) is the *Tulip*

¹⁴¹ See judgment at §147 {L17/457/32}. See also the judgment on consequential orders at §4 {L18/85/2}.

¹⁴² See judgment at [2023] EWHC 1030 (KB) at §27.

¹⁴³ {L18/66/1}.

¹⁴⁴ {L18/66/19}. Also as cited by Chamberlain J in the consequential orders judgment in *McCormack*, at §5.

¹⁴⁵ {L18/66/20}.

Trading case. Dr Wright’s statements in those proceedings are also before this Court, given a certain amount of factual overlap – indeed, it was disclosure in this case that led to Dr Wright having change his reliance on the doctored MYOB accounting records in the *Tulip Trading* case, as he now just says that they are not contemporaneous.

Events since September 2023

79. Christen Ager-Hanssen was until late September 2023 the CEO of nChain Ltd. On 29 September 2023, he began a series of postings on X (tweets) in which he claimed to have “found compelling evidence that Dr Craig Wright has manipulated documents with the aim to deceive the Court he is Satoshi”.¹⁴⁶ Mr Ager-Hanssen added that he was “convinced that Dr Craig Wright is NOT Satoshi”.¹⁴⁷ He said that he had submitted a whistleblowing report making these points, and also to have raised concerns about illegitimate control of the nChain group by Mr Ayre.
80. After service by COPA of the first Madden Report (which had found many of Dr Wright’s documents to be inauthentic), nChain had arranged for Dr Wright to undergo a mock trial exercise on 22 September 2023 in which he was cross-examined by a criminal barrister, Zafar Ali KC, on a number of his primary reliance documents. A mock judgment, apparently given by a judge who had been drafted in to help, was delivered on 24 September 2023, finding Dr Wright’s Satoshi claim to be false. The day after the mock trial, Mr Ayre sent Dr Wright an email (which Mr Ager-Hanssen posted on X) making clear that Mr Ayre now believed that Dr Wright had forged documents and should confess to having done so.¹⁴⁸ The mock trial exercise was revealed by Mr Ager-Hanssen, and it has since been admitted by Dr Wright, Mr Matthews and Mr Ali.¹⁴⁹
81. Among Mr Ager-Hanssen’s revelations was one that Dr Wright had come up with a new hard drive supposedly containing reliable documents. Mr Ager-Hanssen alleged that the browsing history showed that Dr Wright had researched topics of manipulating files and

¹⁴⁶ {P2/111/44}.

¹⁴⁷ The document he identifies as the report is called “*The Fairway Brief*” and is at {L5/469/1}.

¹⁴⁸ See email of 23 September 2023 at {L19/212/6}. Mr Ayre later acknowledged that the email was his. Mr Ayre proposed a narrative covered by his website Coingeek as follows: “*We will say that we believe you did forge some documents to replace ones you destroyed earlier to try to pretend you were not Satoshi. We will say this is because your Asperger’s makes you not think and act like an adult...*” {L19/212/7}.

¹⁴⁹ See Wright 3 {E/3/1} and Matthews 2 {E/27/1}. For Mr Ali’s account, see Clyde & Co letter at {M1/1/707}.

backdating metadata, and also that he had made searches to discover whether Satoshi had compiled any part of his original Bitcoin paper in LaTeX format.¹⁵⁰

82. Very shortly before Mr Ager-Hanssen’s revelations began to be released, Dr Wright’s then solicitors wrote (on 25 September 2023) to say that he had further disclosure to give. Since then, Dr Wright has made the claim to have discovered in mid-September 2023 two hard drives which were not previously imaged and which supposedly contain more reliable versions of documents supporting his claim.

What is COPA?

83. COPA is the Claimant in the COPA Proceedings and a Defendant in the BTC Core Claim. It is a US-based non-profit mutual benefit corporation established in September 2020. It was formed to encourage the adoption and advancement of cryptocurrency technologies and to remove barriers to growth and innovation in the cryptocurrency space.¹⁵¹ COPA brings this action for itself and as a representative claimant under CPR 19.6. The parties represented by COPA (collectively, the “**Represented Parties**”) have the same interests in this dispute. The Represented Parties have consented to be represented by COPA in this matter and agreed to be bound by any judgment or order, as required by CPR 19.6(4).

Relevant Procedural History

Procedural chronology for the COPA Claim

84. Certain aspects of the procedural history of this case are relevant to this trial and discussed below. In summary, the key procedural steps in this case have been:
 - 84.1. In April 2021, COPA issued the COPA Claim (for itself and the represented claimants. Pleadings in the COPA Claim closed in July 2021 (subject to subsequent amendments that have been made).
 - 84.2. In the months after issue of proceedings, there were applications by Dr Wright to strike out parts of COPA's case and for an evidence exclusion order which sought

¹⁵⁰ See {L20/195/1}.

¹⁵¹ See Lee 1 at {C/12/3}. COPA’s webpage and membership agreement, setting out its aims, are at {L19/91/2}.

to disbar COPA from relying on any documents disclosed in the *Kleiman* litigation. Both were rejected by HH Judge Matthews in December 2021.¹⁵²

- 84.3. A CCMC took place before Master Clark in September 2022 at which the directions timetable was set.¹⁵³
- 84.4. On 7 March 2023, the parties gave extended disclosure and, in accordance with the CCMC order, Dr Wright identified the documents on which he primarily relied for his claim to be Satoshi (the “**Reliance Documents**”). There were initially 100 documents in the list served on 4 April 2023¹⁵⁴ and Dr Wright later added a further seven documents on 2 June 2023.¹⁵⁵ Since then, Dr Wright has provided many further tranches of disclosure (now 21 tranches in total).
- 84.5. On 15 June 2023, a joint CMC took place in four actions involving Dr Wright, including the COPA Claim and the BTC Core Claim. The Court ordered that two of the cases should be stayed and the third (the “**BTC Core Claim**”) should be stayed against some defendants.¹⁵⁶ This trial was to act as the main trial in the COPA Claim and the trial of the Identity Issue in the BTC Core Claim.
- 84.6. On 28 July 2023, the parties exchanged most of their principal witness statements and hearsay notices (with short extensions agreed for a few more).
- 84.7. On 1 September 2023, COPA served its expert report on forensic document examination from Patrick Madden (the “**Madden Report**”).¹⁵⁷ As noted above, Mr Madden concluded that many of Dr Wright's reliance documents, as well as many other documents in his disclosure set, have been altered, often with the apparent purpose of supporting his claims.
- 84.8. At a hearing in mid-September 2023, the Court addressed a number of applications.¹⁵⁸ The most substantial was an application by COPA for Dr Wright to answer the Consolidated RFI (served in late June 2023). Dr Wright was

¹⁵² See judgment at {B/23/1}.

¹⁵³ See CCMC order at {B/7/1}.

¹⁵⁴ See: {M/1/712}.

¹⁵⁵ See: {M/1/842}.

¹⁵⁶ See judgment at {B/26/1} and order at {B/10/1}.

¹⁵⁷ The main report is at {G/1/1} and its appendices are in the H Section of the Opus2 platform. References to “the Madden Report” are to this main, first report.

¹⁵⁸ See judgment at {B/25/1} and order at {B/14/1}.

ordered to answer many of the requests, and he did so in two statements: Wright 2 (concerning the signing sessions); and Wright 4 (concerning remaining matters), served on 23 October 2023.

84.9. At a hearing on 12 October 2023, the Court considered an application by COPA amend its statement of case to plead that Dr Wright had forged documents and/or knowingly relied on forged documents, based upon the findings in the Madden Report.¹⁵⁹ The Court permitted the amendments, subject to COPA’s case in this regard being limited to 50 forged documents (beyond those originally pleaded) and to COPA being required to provide a Schedule with particulars of the indicia of alteration and the links to Dr Wright. COPA duly served its Schedule, pleading reliance on 50 forged documents.¹⁶⁰

84.10. On 23 October 2023, the parties exchanged expert reports on the subject of cryptocurrency technology and the “signing sessions”. On the same date, Dr Wright served his forensic documents report of Dr Placks. On 17 November 2023, COPA served a reply report of Mr Madden (Madden 2).¹⁶¹ The experts in each discipline held discussions in late November 2023 and produced joint statements. As set out below, Mr Madden and Dr Placks reached broad agreement.

84.11. A PTR took place on 15 December 2023, at which the Court decided to defer the trial by a few weeks, while rejecting a much longer adjournment.¹⁶² It allowed Dr Wright to rely on some “new” documents he claimed to have discovered since receiving the Madden Report. There was also provision for further expert evidence. In its judgment, the Court accepted an offer by COPA to focus on 20 of the original forgeries pleaded and gave permission to add a further 20 from the new documents.

84.12. Since the PTR, the parties have exchanged reply evidence. They have served further reports from experts in forensic documents examination and LaTeX

¹⁵⁹ See judgment at {B/27/1} and order at {B/18/1}.

¹⁶⁰ The full Schedule begins at {A/2/24}.

¹⁶¹ {G/3/1}.

¹⁶² See judgment at {B/28/1} and order at {B/22/1}. Madden 3 {G/5/1} was served ahead of the PTR.

software.¹⁶³ The experts have produced joint statements, reaching near complete agreement. COPA has pleaded the additional 20 forgeries in a Schedule.

Dr Wright's Disclosure

85. Dr Wright was ordered to give disclosure against a long list of issues.¹⁶⁴ These were granular issues save for the first two, which were catch-all categories: (1) Whether the Defendant is the author of the Bitcoin White Paper; and (2) Whether the Defendant is the person who used the pseudonym "Satoshi Nakamoto." So, any suggestion by Dr Wright in his evidence that other documents might make good his claim or address apparent weaknesses in his case must be considered against the backdrop of him knowing that he should have conducted a thorough search of documents against these broad issues.
86. Disclosure was originally ordered for 31 January 2023, but the deadline was extended to 7 March 2023. Disclosure was also ordered against a wide range of keywords.¹⁶⁵ After the CCMC, Bird & Bird wrote to Ontier (Dr Wright's then solicitors) reminding them of the search parameters and that disclosure was not limited to keyword searches but required active involvement by Dr Wright.¹⁶⁶
87. As noted above, Dr Wright was ordered at the CCMC to produce a list of his Reliance Documents. Dr Wright had previously identified 71 such primary reliance documents in the *Granath* litigation and had submitted a similar list in response to an order in the *McCormack* case.¹⁶⁷ The CCMC Order also required him to provide chain of custody information for his Reliance Documents. While he purported to comply on 11 May 2023, he only served a list identifying himself as the custodian for most documents.¹⁶⁸ After further correspondence, on 8 July 2023 he provided a further schedule of metadata without any detail of intermediate custodians or of handling / transmission of documents.¹⁶⁹ He maintained until early September 2023 that this was proper compliance, before finally agreeing to provide information on intermediate custodians.

¹⁶³ Madden 4 {G/6/1} and Rosendahl 1 {G/7/1} for COPA; Lynch 1 {I/5/1} and Placks 2 {I/6/1} for Dr Wright.

¹⁶⁴ See DRD at {K/1/1}.

¹⁶⁵ See Section 2 Annex 2 to the DRD {K/2/15}.

¹⁶⁶ See letter of 5 January 2023 {M/1/572}.

¹⁶⁷ See order of 30 July 2020 at §2 {L17/18/1}.

¹⁶⁸ See letter at {M/1/778}.

¹⁶⁹ See letter at {M/1/943}.

88. Even on his own case, Dr Wright’s disclosure exercise has been wholly inadequate.¹⁷⁰ This can be seen from (a) the fact that the original extended disclosure was followed by 15 further tranches up to the time of the PTR; and (b) Dr Wright’s attempt at the PTR to defer the trial due to his discovery of new documents which were said to be “better” than the ones previously relied upon.
89. Dr Wright’s position on disclosure and the documents he had provided changed markedly following the service of the main Madden Report on 1 September 2023. First, he claimed that he had discovered a large store of new documents on a USB stick. Secondly, he served a Chain of Custody schedule casting doubt on the reliability of his original reliance documents. Thirdly, he claimed to have a store of LaTeX files on an online editor, Overleaf, including LaTeX drafts of the White Paper.
90. Dr Wright has accepted at least one of Mr Madden’s findings, namely that one important document (ID_003455¹⁷¹) was inauthentic. This was an email with a screenshot of Dr Wright’s NAB bank records apparently showing him having purchased Satoshi’s Vistomail email account in 2008. On 27 September 2023, he disclosed bank statements which contradicted the document and did not include any transaction supporting his claim to be Satoshi.¹⁷²
91. Dr Wright’s account of finding new documents is as follows. On 15 September 2023, he discovered two encrypted USB drives: (a) a Samsung USB drive containing an image of a hard drive said to date from when he worked at BDO (referred to as the “**BDO Drive**”) and (b) a MyDigital USB drive. He claimed that the BDO Drive was captured in October 2007 and remained untouched (protected by encryption) until he found it. The existence of this material was alluded to briefly in a letter from Travers Smith (his solicitors at the time) to the Court on 25 September 2023¹⁷³ and later explained in a letter from Shoosmiths of 11 October 2023.¹⁷⁴ The Court will recall these drives and their discovery being the subject of debate at the PTR. Dr Wright’s story is now undermined by agreed

¹⁷⁰ Deficiencies were pointed out in a long letter from Bird & Bird dated 18 May 2023 {M/1/805}. That letter went unanswered until 12 July 2023 {M/1/951}, and the response was limited, avoiding many questions. A full history of disclosure up to late November 2023 is in a long letter from Bird & Bird of 27 November {M/2/525}.

¹⁷¹ The email is at {L15/100/1} and the screenshots at {L15/101/1} and {L15/102/1}.

¹⁷² See letter at {M/2/205}.

¹⁷³ {P2/116/3}.

¹⁷⁴ {M/2/245}.

evidence of the parties' experts that the BDO Drive was subject to extensive manipulation and backdating in mid-September 2023.

92. Shortly after Dr Wright's "discovery" of the BDO Drive came his schedule of further Chain of Custody Information for his original Reliance Documents. Having previously refused to provide more than very limited information based on external metadata (until an application was made), Dr Wright on 13 October 2023 served a schedule purporting to describe the transmission of each document.¹⁷⁵ Entries are confusing and internally inconsistent, but the overall effect of this document was to suggest that most of his Reliance Documents had been used or accessed by others after being produced, such that they could have been altered. It repeatedly indicated that more reliably authentic versions of Reliance Documents might be available on the "new drives". In his statement of 23 October 2023 answering the RFI requests (Wright 4), Dr Wright also provided a schedule addressing versions of the White Paper in disclosure in which he told a similar story of those documents being unreliable.¹⁷⁶
93. The "discovery" of the Overleaf LaTeX documents supposedly came in late November 2023 and was announced in Shoosmiths' letter of 27 November 2023.¹⁷⁷ In that letter and in later correspondence, it was claimed that these documents were important because they included some which would compile into a replica of the White Paper and they could not have been produced by reverse-engineering. Dr Wright's story of using LaTeX in drafting the White Paper was new to his fourth statement, and a detail he had never mentioned previously. Dr Wright claimed that these Overleaf documents had not been disclosed earlier because Ontier had taken the view that they fell outside the scope of disclosure date ranges. At the PTR, COPA argued that it was implausible that Ontier should have taken that view and sought disclosure of their advice on grounds that privilege had been waived. The Court agreed and ordered disclosure, at which point Ontier stated firmly that they had never given any such advice.¹⁷⁸
94. Following the PTR, Dr Wright was permitted to rely on three categories of "Additional Documents": (i) 97 documents from the BDO Drive; (ii) LaTeX documents stored in Dr Wright's Overleaf account which were said to compile into the White Paper; and (iii) a

¹⁷⁵ See Schedule at {K/11/1}.

¹⁷⁶ See Exhibit CSW5 at {F/148/2}.

¹⁷⁷ {M/2/540}.

¹⁷⁸ See Shoosmiths' letter of 18 December 2023 {M/2/687}.

few documents concerning documentary credits assignments of Dr Wright which had (unaccountably) been omitted from disclosure. It is important to keep in mind that these documents were cherry-picked by Dr Wright after searches against his own selected keywords: they were not the result of proper disclosure searches in accordance with the DRD. He was also ordered to provide an updated list of Reliance Documents. In response, he nominated all his original Reliance Documents and all the Additional Documents.¹⁷⁹

95. Mr Madden examined documents from the BDO Drive and produced a third report (Madden 3) before the PTR addressing individual documents and finding numerous signs of forgery. As a result of the PTR Order, he was given access to the raw image taken of the Samsung drive and the BDO Drive it contained. This enabled him and his counterpart to do substantial further work, revealing that between 12 and 17 September 2023 the BDO Drive was created from a predecessor image and heavily edited (presumably by Dr Wright, who claims to have been the only person with access to it over that time). At least 71 of the 97 new Reliance Documents on the drive (including all which appear to support Dr Wright's claim to be Satoshi) were added and/or edited during that period. These are matters fully agreed between Mr Madden and Dr Wright's expert, Mr Lynch.¹⁸⁰ Another feature of the new Reliance Documents is that they contain either no or very few direct equivalents of the original Reliance Documents, despite the indications in the Chain of Custody Schedule.
96. The LaTeX files on Dr Wright's Overleaf account have also been the subject of expert examination. They too are forgeries, since the parties' experts agree¹⁸¹ that (a) the White Paper was not written in LaTeX, but in OpenOffice; (b) Dr Wright's LaTeX files do not compile into a good replica of the White Paper; (c) it would not be difficult to reverse-engineer the published White Paper to Dr Wright's LaTeX version; and (d) the only reason Dr Wright's LaTeX files produce anything like the White Paper is that they make use of software packages that did not exist in 2008/9.
97. In short, Dr Wright has fought multiple pieces of litigation in which he has had to identify the documents supporting his claim to be Satoshi. Against that background, he put

¹⁷⁹ See Shoosmiths letter of 21 December 2023 {M/2/717}.

¹⁸⁰ See Madden / Lynch joint report {Q/6/1}.

¹⁸¹ See Rosendahl / Lynch joint report {Q/5/1}.

forward his 107 Reliance Documents in this case. He has not withdrawn reliance on any of these. Following receipt of the Madden Report which identified signs of alteration in many of them, Dr Wright (1) suddenly “discovered” the “new drives” and (2) sought to call into question his own Reliance Documents in favour of “better” documents supposedly discovered on the new drives. Even the least congenitally suspicious person would be deeply sceptical of this account.

98. Quite apart from the difficulties with Dr Wright’s account of the fortuitous discoveries, there are two further problems with his new case. First, as demonstrated in Madden 2 (and Appendices PM43 and PM44),¹⁸² the cover story given in the Chain of Custody Information is hopeless in numerous respects. In particular, Dr Wright sought to explain away various documents by saying that these documents had been handled by others since 2008. However, Dr Wright posted these documents to Slack on dates corresponding to forensically established dates of creation (in 2019/20). Further, many of the original Reliance Documents were within a zip file attached to an email from Dr Wright to Lynn Wright dated 18 January 2020, and Mr Madden was able to establish a chronology whereby such documents were interacted with and backdated in the days preceding the sending of that email.
99. Secondly, as summarised above, although COPA has not been able to engage in the kind of comprehensive examination of documents in the “new drives” which was undertaken for Dr Wright’s previous disclosure, there is clear evidence that the BDO Drive and the new Reliance Documents are recent forgeries.

Overview of the Reliance Documents

100. The 107 Reliance Documents can be broadly summarised as follows:

100.1. Documents addressed by Mr Madden – 45 of the documents have been specifically addressed by Mr Madden and found to bear signs of inauthenticity or outright forgery. All 28 of the original Reliance Documents which appear on COPA’s Schedule of 50 forgeries have been agreed by the experts to be unreliable (and in most cases to have had metadata manipulated).¹⁸³

¹⁸² See Madden 2, from §120 {G/3/42}. See also Appendices PM43 {H/219/1} and PM44 {H/238/1}.

¹⁸³ See joint expert statement from {Q/2/6}.

- 100.2. Other prior work of Dr Wright – 39 of the documents are papers / articles / notes written by Dr Wright mostly prior to the release of the White Paper. This set includes emails and attachments, so the number of the substantive articles is less than 39. None of these documents shows anything other than a general interest in various tech-related fields.
- 100.3. Documents relating to the signing sessions and “reveal” of 2016 – 17 of the documents are from 2015/16 and show Dr Wright communicating with Mr Matthews and others prior to the public making of his claim. None of these can be said to support the claim.
- 100.4. Academic qualifications – Two of the documents show Dr Wright’s academic qualifications (for Northumbria and Charles Stuart Universities). Again, neither of these helps prove that Dr Wright is Satoshi.¹⁸⁴
- 100.5. Bitcoin Notes – 15 of the documents are handwritten or hand annotated notes relating to Bitcoin. These cannot be reliably dated by Dr Wright and some are clearly forged (e.g. the notes on the Datastation notepad).
101. As noted above, the Additional Documents added as Reliance Documents since the PTR include the following categories:
- 101.1. The 97 documents from the BDO Drive: These are categorised in Section 2 of Madden 3¹⁸⁵ and further addressed both there and Appendix PM46 to Madden 4.¹⁸⁶ They are almost all in file formats which did not feature in Dr Wright’s original Reliance Document and are light in metadata (suggesting deliberate reliance on documents which can be less easily assessed by forensic means). Nevertheless, many bear signs of inauthenticity, and analysis of the BDO Drive shows that they were added in the recent forgery of the drive image.

¹⁸⁴ No evidence has ever been provided for any of the other degrees Dr Wright claims – at last count, over 30.

¹⁸⁵ {G/5/8}.

¹⁸⁶ {H/278/1}.

101.2. Certain LaTeX documents stored in (one of) Dr Wright's Overleaf accounts:¹⁸⁷

As noted above, the expert evidence debunks Dr Wright's claim that these were precursor versions of the White Paper.

101.3. The Documentary Credits Assignment Documents: These are a few documents evidencing Dr Wright's work on topics which Dr Wright's expert accepts are inauthentic, but which COPA says are anyway irrelevant to his alleged development of Bitcoin.

Overview of Cryptocurrency Technology

Introduction

102. Bitcoin was the first cryptocurrency, originating in 2009.¹⁸⁸ COPA's expert, Prof Meiklejohn, has provided a report which gives a basic account of the technology underpinning Bitcoin: see p9-40 of the report.¹⁸⁹ That basic account is largely agreed by Dr Wright's expert, Zeming Gao. The Joint Report sets out the areas in which Mr Gao disagrees with Prof Meiklejohn, but he accepts the rest of her report.¹⁹⁰

103. Bitcoin is a peer-to-peer system, meaning users can transfer payments between themselves without an intermediary or central authority.¹⁹¹ Transactions between users are incorporated into blocks by a process called mining. These blocks are in turn distributed among and verified by peers on the network, who store them by adding them to a ledger. Each block added to the ledger includes information in the form of a hash, which is affected by the blocks added before it. This ledger is therefore created by linking the blocks together to form the blockchain. The contents of one block thus cannot be changed without changing the contents of all subsequent blocks.¹⁹²

¹⁸⁷ At the PTR the evidence was that there was *an* Overleaf account, and Dr Wright was ordered to disclose the relevant contents of this along with metadata. It now transpires that Dr Wright claims that he had numerous Overleaf accounts and that the documents now relied upon arrived in his current account at the end of a complex and poorly explained process of transmission through one or more other accounts. {M/2/820-823}.

¹⁸⁸ Meiklejohn, at §21(a) {G/2/9}.

¹⁸⁹ {G/2/9}.

¹⁹⁰ Joint statement of Prof Meiklejohn and Zem Gao at §2 {Q/3/2}.

¹⁹¹ Meiklejohn §24 {G/2/9}.

¹⁹² Meiklejohn §25 {G/2/10}.

Digital Signatures

104. A digital signature is an example of an asymmetric or public-key cryptographic primitive. It operates using two related keys, a public and a private one. The public one can be given to anyone, and the pair is known as a keypair.¹⁹³ A digital signature acts to verify the signing of a given message and involves three algorithms: KeyGen, Sign and Verify.¹⁹⁴ There are several standardised digital signature schemes, with the one being used in Bitcoin known as ECDSA (Elliptic Curve Digital Signature Algorithm).¹⁹⁵ The curve used in Bitcoin is secp256k1, and ECDSA signatures are usually encoded and expressed as 64 alphanumeric characters.

Transacting in Bitcoin

105. Bitcoin users can identify themselves using, for example, their public key or (more commonly) addresses, which are alphanumeric identifiers that are different from, but often related to the public key.¹⁹⁶ Prior to 2012, the only type of address used in Bitcoin transactions was a pay-to-public-key-hash (P2PKH), whereas sending to a public key was referred to as pay-to-public key (P2PK).¹⁹⁷

106. When addresses are derived from public keys, each address has its associated private key that can be used to sign messages. Accordingly, given an address, a public key, a signature and a message, anyone can verify whether or not (a) the address was derived from the public key and (b) the signature and signed message are valid for that public key.¹⁹⁸ It is these properties that allow Bitcoin users to transfer ownership of bitcoins they possess such that they can be independently verified, but without disclosing the real world identity of the individual with the private key.

107. A transaction contains, in its simplest form, an input corresponding to the sender and one output corresponding to the recipient.¹⁹⁹ The transaction output consists of the recipient's address and the value of bitcoin sent to that address. A Bitcoin transaction also contains a digital signature from the sender, where the message being signed

¹⁹³ Meiklejohn §31 {G/2/11}.

¹⁹⁴ Meiklejohn §32 and Fig. 1 {G/2/12}.

¹⁹⁵ Meiklejohn §34 {G/2/13}.

¹⁹⁶ Meiklejohn §36 {G/2/13}.

¹⁹⁷ Meiklejohn §38 {G/2/14}.

¹⁹⁸ Meiklejohn §39 {G/2/14}.

¹⁹⁹ Meiklejohn §43 {G/2/15}.

contains the rest of the information detailing the transaction.²⁰⁰ This allows peers on the network to verify the transaction, as they can look at the address, public key and signature to check that the public key aligns with the address and the signature verifies it.²⁰¹

108. As transactions are public, it is possible to check to see if the address was used before, to confirm that the address did in fact receive the number of bitcoin it is now spending.²⁰² To prevent double spending, Bitcoin tracks which transaction outputs are unspent and allows only those unspent outputs to spend the coins they receive.²⁰³

Transaction Ordering

109. As different peers on the network will see transactions at different times, transaction ordering is essential to ensure that there is no instance of bitcoins being recorded as being sent to two different users.²⁰⁴ This is the role of the Bitcoin blockchain, which acts as a ledger of all valid transactions propagated through the network.
110. The first block in the Bitcoin blockchain was Block 0 (the Genesis Block) which was hardcoded into the Bitcoin software. It was produced on 3 January 2009 at 18:15:05 UTC and contains a single coin generation transaction.²⁰⁵ The script used to input this transaction contains an encoded message which when decoded reads “*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks*”. The purpose of using this Times headline message was apparently to show that the Genesis Block could not have been created before that date.²⁰⁶
111. The initial block reward was 50 Bitcoin, but that halves with every 210,000 blocks. It is presently 6.25 bitcoin. The total number of bitcoin capable of being generated as rewards is capped at 21 million bitcoins in total.²⁰⁷ Bitcoin is configured to have a new block produced every 10 minutes on average. This means that the target hash needs to change according to the collective computing power of the peers competing in the mining process.²⁰⁸ The difficulty level itself changes according to the expected time to produce

²⁰⁰ Ibid.

²⁰¹ Meiklejohn §44 {G/2/15}.

²⁰² Ibid.

²⁰³ Ibid.

²⁰⁴ Meiklejohn §58 {G/2/20}.

²⁰⁵ Meiklejohn §59 {G/2/21}.

²⁰⁶ Ibid.

²⁰⁷ Meiklejohn §69 {G/2/28}.

²⁰⁸ Meiklejohn §71 {G/2/29}.

blocks divided by the actual time, meaning that difficulty increase or decrease depending on the collective computation power.²⁰⁹

Blockchain Forks

112. If Bitcoin participants want to change parameters of the system, this can be done by consensus of those on the network. Any rule change which is backwards-compatible is known as a soft fork.²¹⁰ A backwards-incompatible change is known as a hard fork, which creates two different blockchains diverging at a single block.²¹¹ The most popular cryptocurrency based on the White Paper and Genesis Block is Bitcoin. Further hard forks have created the cryptocurrencies Bitcoin Cash, and Bitcoin Satoshi Vision. Wright asserts that his Bitcoin Satoshi Vision blockchain is the real "Bitcoin". To avoid an uninteresting and irrelevant terminology debate we refer to these cryptocurrency systems by their ticker symbols: BTC, BCH, and BSV.

Storage and Use of Bitcoin

113. Typically, users store bitcoins in an electronic wallet, a piece of software that stores private keys and keeps track of any associated transactions. This can be run on a computer or mobile device.²¹² Wallets often provide users with a recovery phrase, so that if the device containing the wallet is corrupted or lost, it can still be downloaded again and reused.²¹³ Solutions to the risks entailed in storing bitcoin on one's own device include storing on an exchange and cold storage (on an offline computer or written down).²¹⁴

114. It is also possible to use multi-signature addresses, whereby any participant who produces a valid signature completes and validates the transaction. A related concept is that of Secret Sharing, with the most common version of being known as Shamir Secret Sharing.²¹⁵ This concept involves the user splitting a private key using a cryptographic primitive and giving "slices" to different users. Then, depending on how the sharing has

²⁰⁹ Ibid.

²¹⁰ Meiklejohn §76 {G/2/33}.

²¹¹ Meiklejohn §78 {G/2/34}.

²¹² Meiklejohn §87 {G/2/37}.

²¹³ Meiklejohn §89 {G/2/38}.

²¹⁴ Meiklejohn §90, 91 {G/2/39}.

²¹⁵ Meiklejohn §94 {G/2/40}.

been performed, a certain number of individuals in a group (sometimes all, but in other cases only a lesser number of the set) can reconstruct the private key.²¹⁶

Security of Digital Signatures

115. The extent of security provided by a digital signature depends on the nature of the exercise undertaken to prove access to or control of a private key. Signing a message with a private key produces an output such that the Verify algorithm can be run to ensure that this message was signed by the person with the private key.²¹⁷ The message must be a new one, since otherwise the recipient could simply copy a signed message and later hold it out as proof of ownership of the underlying private key (a process known as a “replay attack”). It is for this reason that a user must be asked to sign a new message.²¹⁸ This explanation is significant for the topic of the Sartre message.
116. As with any validation process, there are certain steps in the digital signature process which require trust and verification, so that a party can be as sure as possible that what is being demonstrated is what it purports to be. If a user controls the software performing the signature verification or the software contains a bug, then the signature can appear to be verified when it is not truly verified.²¹⁹ Trust in the software that is being used is therefore important. In a section of her report agreed by Mr Gao, Prof Meiklejohn sets out several requirements which must be fulfilled to establish possession of a private key:
- 116.1. Unique message – The message to be signed must not have been signed before for that public key.²²⁰
- 116.2. Method of and result of verification – The verification algorithm must be run using the public key, the new message and the signature given by the user.²²¹
- 116.3. Semi-manual verification – Verification is rarely if ever performed on paper due to the size of the numbers involved. If instead it is done using software on a computing device, then the verifier must trust that the computing device is accurately performing each step.²²²

²¹⁶ Meiklejohn §95 {G/2/41}.

²¹⁷ Meiklejohn §97 {G/2/41}.

²¹⁸ Meiklejohn §99-100 {G/2/42}.

²¹⁹ Meiklejohn §102 {G/2/42}.

²²⁰ Meiklejohn §103(a) {G/2/43}.

²²¹ Meiklejohn §103(b) {G/2/43}.

²²² Meiklejohn §103(c) {G/2/43}.

- 116.4. Software integrity – Usually, the verifier runs the verification algorithm using an existing piece of software. Here, the person must trust that the correct algorithm is being run, that it is using the correct inputs and that the software is secure and has not been altered. This would include that it has been downloaded properly and not over an unsecure connection.²²³
- 116.5. Software and hardware integrity of the computing device – It is also necessary that the verifier trusts the hardware, operating system and software on any computing device (i.e. not limited to the verification software itself).²²⁴

Public keys Associated with Satoshi

117. There is only one key that could have belonged only to the creator of the system (Satoshi), which is that associated with the Genesis Block. However, the coinbase reward associated with the block cannot be spent, as the Bitcoin software does not allow that. So, while there is a public / private key pair for the Genesis Block, it is not certain that anyone has ever known the private key.²²⁵ Whilst early blocks are associated with Satoshi, they could theoretically have been mined by other early individuals right after launch. The Bitcoin community, however, does associate block 9 with Satoshi, because this block was the one involved in the first transaction from Satoshi to Hal Finney.²²⁶

The Evidence at Trial

118. The trial schedule was provisionally set in the PTR order²²⁷ to be: (a) one week of pre-reading from 29 January 2024; (b) one day of oral openings on 5 February 2024; (c) 19 days of evidence from 6 February 2024 to 1 March 2024; and (d) oral closings from 12 to 15 March 2024. The judgment following the PTR indicated²²⁸ that the 19 days of evidence should be divided as to (i) 6 days for Dr Wright; (ii) 3.5 days for Dr Wright's other fact witnesses; (iii) 4 days for COPA's fact witnesses; (iv) 3 days for Mr Madden; (v) 1 day for Dr Placks; (vi) 1 day for a witness from Stroz Friedberg; and (vii) 0.5 day for Prof Meiklejohn and Mr Gao.

²²³ Meiklejohn §103(d) {G/2/43}. Mr Gao agrees that the status of the software can also be a source of doubt – Gao §293.

²²⁴ Meiklejohn §103(e) {G/2/44}.

²²⁵ Meiklejohn §108-109 {G/2/9}. This section is agreed by Mr Gao {Q/3/3}.

²²⁶ Meiklejohn §110 {G/2/46}.

²²⁷ Order of 20 December 2023, §2 {B/22/3}.

²²⁸ Judgment dated 20 December 2023, §166 {B/28/40}.

COPA's Fact Evidence

119. COPA relies upon witness statements from 18 factual witnesses. At the date of writing, COPA understands that all except Mr Bohm, Mr Hudson, Mr Andrae and Mr Ford are required for cross-examination. Mr Bohm sadly died earlier in January 2024.

119.1. Joost Andrae {C/1/1} – Mr Andrae is a software engineer who contributed to the OpenOffice.org project. He gives evidence on Open Office 2.4.0 being released on 26 March 2008, which supports a conclusion that one of the Reliance Documents is not authentic to its suggested date.²²⁹

119.2. Martti Malmi {C/2/1} / {C/24/1} – Mr Malmi is a computer scientist who corresponded with Satoshi from shortly after the release of Bitcoin in January 2009 until early 2011, during which time he helped set up website content and worked on the Bitcoin Code, as well as the Linux port of the Bitcoin software. Mr Malmi rejects various claims that Dr Wright has made about him and denies that he wrote a Satoshi post describing Bitcoin as a “cryptocurrency” (an allegation made by Dr Wright to explain away that post in circumstances where he disputes that label). He also exhibits emails he exchanged with Satoshi that previously were not public (correspondence never mentioned by Dr Wright). Mr Malmi also provided a short reply statement correcting statements made by Dr Wright about him.

119.3. Hilary Pearson {C/3/1} – Ms Pearson is a former partner (retiring in 2015) at Bird & Bird who was a pioneer in writing about IT law. She authored two papers, “Liability of Internet Service Providers” from 1996 and “Intellectual Property and the Internet: A Comparison of UK and US Law” from 1998. She exhibits a comparison made between her work and Dr Wright’s LLM dissertation which shows the extent of Dr Wright’s plagiarism and copyright infringement of her work.²³⁰ As was common ground in the hearing of 12 October 2023, this evidence is admissible and can be considered in relation to Dr Wright’s credibility.

²²⁹ See Madden 1 Appendix PM23 {H/107/1}.

²³⁰ {D/490/2}.

- 119.4. Daniel Bernstein {C/4/1} – Mr Bernstein is a cryptographer and professor at the University of Illinois. He is a member of the team that jointly developed the digital signature scheme known as “EdDSA” and he recounts that term being coined in February to April 2011 and first used publicly in July 2011. Dr Wright had put forward a Reliance Document (ID_004009)²³¹ which appeared to be a set of manuscript notes dating from prior to the release of Bitcoin and which contained reference to EdDSA. After receiving Mr Bernstein’s evidence, Dr Wright has claimed that some of the notes (including the reference to EdDSA) were written in or after 2011 (an account which has its own difficulties that will be explored at trial).
- 119.5. Rory Cellan-Jones {C/5/1} – Mr Cellan-Jones is a technology journalist who was involved in the 2016 signing sessions, which he addresses in his evidence. He was told that Dr Wright could prove he was Satoshi and in reliance on that he transferred bitcoin on 4 May 2016 to the Bitcoin address that Satoshi used for the first transaction, on the understanding that Dr Wright would send it back. To date Mr Cellan-Jones has not received this Bitcoin back.
- 119.6. Zooko Wilcox-O’Hearn {C/6/1} – Mr Wilcox-O’Hearn is a computer scientist in the field of cryptography and cryptocurrency. He wrote early blogposts about Bitcoin and states that he never received any Bitcoin from Satoshi, as Dr Wright has claimed he did.
- 119.7. Dustin Trammell {C/7/1} – Mr Trammell is an Information Security Research Scientist who corresponded with Satoshi in January 2009. He gives evidence of his correspondence with Satoshi and exhibits it. He denies a claim Dr Wright made in his evidence in the *Granath* proceedings that Dr Wright as Satoshi shared Bitcoin code with him.
- 119.8. John Hudson {C/8/1} – Mr Hudson is the lead designer of the font Nirmala UI and confirms it was not publicly available until March 2012 at the earliest. This is relevant to a number of Mr Madden’s findings that documents of Dr Wright are not authentic to their suggested dates and have been backdated.

²³¹ {L1/115/1}.

- 119.9. Adam Back {C/9/1} {C/21/1} – Dr Back is a cryptographer and inventor of “Hashcash”, which was cited in the White Paper. He gives evidence of some email communications with Satoshi which had not previously been made public. They undermine Dr Wright’s accounts of his work on the White Paper before its release (as largely reiterated in Wright 1). For instance, Dr Wright says that Wei Dai’s work profoundly influenced his development of Bitcoin for years, whereas Dr Back’s emails show that he told Satoshi about Wei Dai’s work on 21 August 2008 and that Satoshi had not previously known of it. This is also telling because Dr Wright’s supposed precursor drafts of the White Paper (said to predate August 2008) have the reference to Wei Dai’s B-money paper. Dr Back also provided a short second statement rebutting some of the claims Dr Wright makes about Dr Back’s attitude and interactions with Satoshi.
- 119.10. Nicholas Bohm {C/10/1} – Mr Bohm was a retired solicitor who corresponded with Satoshi shortly after the release of Bitcoin in January 2009. Mr Bohm has provided evidence of his email communications with Satoshi that were not before made public (and to which Dr Wright had never referred). He has also provided a version of the White Paper that he downloaded in January 2009, which Mr Madden has authenticated²³² and which is used as a control copy.
- 119.11. Ben Ford {C/11/1} – Mr Ford is the director of a company trading as DataStation who gives evidence about a DataStation notepad which is one of Dr Wright’s Reliance Documents (ID_004018).²³³ This presents as being a set of pre-release development notes on the Bitcoin concept. Mr Ford explains that the notepad was not printed until 22 May 2012. Dr Wright has reacted to this evidence in his Chain of Custody schedule by saying that the notes were written in 2011 / 2012. Again, this cover story has its own difficulties that will be explored at trial.
- 119.12. Steve Lee {C/12/1} – Mr Lee is a board member of COPA. He is a Bitcoin developer and works for a team called Spiral, which is funded by Block, Inc (a Represented Party). He gives evidence on the chilling effect of Dr Wright’s claims to be Satoshi, giving examples of how Dr Wright wishes to people to lose

²³² See Appendix PM3, from §41 {H/20/14}.

²³³ {L7/471/1}.

their families and be subject to criminal law sanctions (including reference to the death penalty).

- 119.13. Howard Hinnant {C/18/1} – Mr Hinnant is a software developer who was Chairman of a C++ Standards Committee in 2005-2010. He gives evidence that certain C++ features were not available in October 2007 as found in certain of Dr Wright's documents (from the BDO Drive) dated to that period.
- 119.14. John MacFarlane {C/19/1} – Professor MacFarlane is a professor of Philosophy who has designed his own software tools, one of which is pandoc (a universal document converter). He states that templates were only added to it in 2010, with the default LaTeX template being added in 2017. It cannot therefore have been used in 2006 when it features in documents of Dr Wright (from the BDO Drive) dated to that period.
- 119.15. Mico Loretan {C/20/1} – Mr Loretan is a software developer who created the software package selnolig. He first released that package in May 2013. This contradicts the face dating of various documents (from the BDO Drive) which contain reference to selnolig.
- 119.16. Michael Hearn {C/22/1} – Mr Hearn is a software developer who worked on Bitcoin at the beginning and corresponded with Satoshi over email. He had dinner with Dr Wright and Mr Matthews in July 2016, when Mr Hearn asked Dr Wright questions about Bitcoin that he believed Satoshi would be able to answer. His impression was the Dr Wright could not answer his questions and that Mr Matthews shut down the conversation when Dr Wright got into difficulties.
- 119.17. Bjarne Stroustrup {C/23/1} – Professor Stroustrup is a professor of Computer Science and the designer of the C++ programming language. He gives evidence that certainly libraries were unlikely to be in use in 2007-2008, even though these appear in some of Dr Wright's documents said to have been from that period.
- 119.18. Richard Gerlach {C/20.1/1} – Prof Gerlach is now a professor of Business Analytics, but was in 2005 a lecturer in statistics at the University of Newcastle, where Dr Wright studied for an MStat course. He gives evidence that various

features of a statistics assignment document in Dr Wright's disclosure are anomalous.

120. The bundles for trial also contain interlocutory statements (in Section P on the Opus2 system). COPA asked that they be included in order to ensure that there is a full record of the accounts given to the Court at every stage of the litigation, given Dr Wright's propensity to change his story and cast blame on his lawyers.

COPA's Hearsay Evidence

121. COPA has adduced the following documents under a CEA Notice:

121.1. A letter from Lucas de Groot dated 14 June 2023 explaining that the Calibri Light font was not available until 2012 {C/15/1}. This is relevant to a number of Mr Madden's findings that documents of Dr Wright are not authentic to their suggested dates and have been backdated.

121.2. A letter from Michael Stathakis and Lee Li dated 10 July 2023 addressing a form of "Quill" notepad {C/16/1}. One of Dr Wright's Reliance Documents (and a document which he has personally verified) is a set of purported BDO meeting minutes from 2008 on this form of notepad.²³⁴ Mr Stathakis and Ms Li explain in some detail that this form of Quill notepad was not available until 2012.

121.3. A witness statement from Andreas Furche {C/13/1} – Mr Furche has provided a witness statement but is not willing to give oral evidence, so his evidence is now relied upon under a CEA Notice. He is a professor and researcher in fintech. He confirms that neither he nor Professor Wrightson worked at Newcastle University after 2000 (which contradicts Dr Wright's account that he engaged with both of them 2005-2009). His account falsifies a series of statements Dr Wright has made about his work on the development of Bitcoin in various particulars.

121.4. Emails in April and May 2022 from Professor Graham Wrightson confirming Mr Furche's account and that he did not know Dr Wright {C/17/1}.

121.5. Extracts from the Lynn Wright deposition transcripts from the *Kleiman* proceedings {C/27/1}.

²³⁴ ID_004013 {L2/159/1}.

121.6. An extract from the First Witness Statement of John Chesher dated 1 May 2023 which was submitted by Dr Wright in the Coinbase proceedings {C/26/1}. He has provided bookkeeping and accounting services to Dr Wright and gave evidence on the assets of Wright International Investments Limited.

121.7. Emails from Wei Dai from October 2023 confirming, amongst other things, that Mr Dai never provided code to Satoshi, contrary to what Dr Wright claims {C/28/1}.

Dr Wright's Fact Evidence

122. Dr Wright has made 11 statements: (i) Wright 1 {E/1/1} providing his principal evidence in chief; (ii) Wright 2 {E/2/1} addressing RFI requests about the signing sessions; (iii) Wright 3 {E/3/1} giving his version of the mock cross-examination (in response to a Court order); (iv) Wright 4 {E/4/1} addressing the remaining RFI requests; (v) Wright 5 {E/20/1} explaining why the two new hard drives were not previously included in his disclosure; (vi) Wright 6 {E/21/1} confirming the facts and statements in Ms Field's first statement (for the adjournment); (vii) Wright 7 {E/22/1} addressing the tweets for Mr Ager-Hanssen about the new documents being fake; (viii) Wright 8 {E/23/1} relating to his computer environment, which he apparently blames for signs of inauthenticity in his documents; (ix) Wright 9 {E/26/1} responding to Prof Meiklejohn's report (with an appendix attempting to explain some signs of inauthenticity); (x) Wright 10 {E/31/1} providing yet more unsupported assertions about his computing environments; (xi) the disputed Wright 11 {CSW/1/1}, which was supposed to give his final reply evidence; and (xii) Wright 12 {CSW/7/1} which further addresses the BDO Drive.

123. Most of his other witnesses give no more than limited evidence that Dr Wright was a capable IT professional who had an interest in digital currency. That evidence has no bearing on Dr Wright being Satoshi, considering those two factors are shared by many thousands of others (as evidenced by the number of people on the Metzdown list that Satoshi used). The only one of Dr Wright's witnesses who positively supports his account of doing work on the Bitcoin system before the White Paper was released is Stefan Matthews, the CEO of nChain and one of the small team backing his claim. As Mr Matthews accepts, he has strong personal and financial motivations for supporting Dr Wright. COPA will challenge Mr Matthews' honesty.

124. Dr Wright's witnesses are as follows:

- 124.1. Danielle DeMorgan {E/8/1} – Ms DeMorgan is Dr Wright's youngest sister. She gives evidence that Dr Wright was interested in Japanese culture and sometimes used nicknames for himself.
- 124.2. David Bridges {E/9/1} – Mr Bridges is a personal friend of Dr Wright who worked at Qudos Bank and worked with Dr Wright from 2006. He describes what he perceived as Dr Wright's skill in computer security and also talks about his interest in Japanese culture.
- 124.3. Stefan Matthews {E/5/1} {E/27/1} – Mr Matthews is the Co-Founder and Executive Chairman of the Board for the nChain Group of companies. He first met Dr Wright in 2005, and he claims that Dr Wright used him as a sounding board for discussions about digital cash systems in 2007/08 and that he provided him with a draft of the White Paper in 2008 (now since lost). He was instrumental in the bailout and the "big reveal". Mr Matthews has also provided a reply statement addressing the mock cross-examination and messages he exchanged with Mr Ager-Hanssen.
- 124.4. Ignatius Pang {E/10/1} – Mr Pang has known Dr Wright since 2007 and he recounts doing some analysis with Dr Wright on social network predatory behaviour. He claims that, in the summer of 2008, Dr Wright used the word "blockchain" in a very odd conversation about a Lego Batman set (The Tumbler Joker's Ice Cream Surprise). He also says that Dr Wright asked people in the office if they knew someone with a Japanese name which he now thinks was probably Satoshi Nakamoto. He says that this happened some time after he had had whooping cough, which was in October 2008.
- 124.5. Mark Archbold {E/11/1} – Mr Archbold has known Dr Wright since 1999 when they both worked for the online casino, Lasseter's Online. He gives evidence that Dr Wright was a capable IT security professional, had a lot of computers at his home and at one point expressed an interest in digital currency.
- 124.6. Max Lynam {E/13/1} – Mr Lynam is Dr Wright's cousin. He gives evidence that he and his father ran some computer code for Dr Wright at their farm in Australia

at some time in or after 2009, and that Dr Wright later (in 2013) told them that it had been mining Bitcoin.

- 124.7. Cerian Jones {E/14/1} – Ms Jones is a patent attorney who has filed patents on behalf of nChain and Dr Wright since February 2016. She gives evidence about some of his patent applications and claims to have been convinced that he is Satoshi by a combination of “*his academic knowledge, his professional background and [his] previous employment experiences*”.
- 124.8. Shoaib Yousef {E/7/1} – Mr Yousef is a cyber security expert who has known Dr Wright since 2006. He says that in the late 2000s they discussed some general digital security topics and digital currency (as a broad concept).
- 124.9. Robert Jenkins {E/6/1} – Mr Jenkins met Dr Wright in around 1998/1999 when Dr Wright worked on security measures for Vodafone in Australia. He says that he discussed concepts of electronic ledgers involving linked blocks of data which in hindsight he relates to the Bitcoin blockchain.

Dr Wright’s Hearsay Evidence

125. Dr Wright relies on four documents served under a CEA notice:

- 125.1. A video-taped deposition with Don Lynam, his uncle, dated 2 April 2020 taken in the *Kleiman* proceedings (with the corresponding transcript included) {E/16/1}. Mr Lynam is elderly and unwell, and it is common ground that he is not fit to give evidence. He did claim to have received the White Paper from Dr Wright before its release, but there are a series of issues with his account and COPA has given due notice of taking issue with its credibility.
- 125.2. The transcript of the deposition of Gavin Andresen dated 26 February 2020 in the *Kleiman* proceedings {E/17/1} and its continuation the next day {E/18/1}. This transcript contains Mr Andresen’s account of his “signing session” with Dr Wright. COPA sought to call Mr Andresen for cross-examination to explore his evidence further, but he is out of the jurisdiction and has not agreed. His written evidence already undermines Dr Wright’s account of this event. In the transcript, Mr Andresen volunteered repeatedly that he may have been “*bamboozled*” in the

session.²³⁵ In an email on 4 May 2016,²³⁶ Mr Andresen acknowledged that Dr Wright may have been lying all along, and suggested a way that the signing session could have been staged. In a blog post in February 2023, he wrote that it had been “*a mistake to trust Craig as much as I did.*”²³⁷

125.3. A video of Neville Sinclair, a former partner of BDO, giving his oral evidence in the *Granath* litigation date 14 October 2022 (with the corresponding transcript) {E/19/1}. COPA sought to call Mr Sinclair for cross-examination to explore his evidence, but he is out of the jurisdiction and has not agreed. His account as recorded in the transcript gives no support to Dr Wright’s claim to be Satoshi.

Forensic Document Examination / LaTeX Code Experts

126. COPA has adduced four reports of Mr Madden,²³⁸ and Dr Wright has adduced two reports from Dr Placks²³⁹ and one from Spencer Lynch.²⁴⁰ Mr Madden has analysed a large number of Dr Wright’s documents and has found that many of his original Reliance Documents and others contain clear signs of alteration and tampering (including backdating) which have had the effect of making them appear to support Dr Wright’s claim to be Satoshi. Dr Placks initially limited his work to analysis of Reliance Documents which Mr Madden has addressed. In his second report, Dr Placks addressed remaining documents in COPA’s original Schedule of Forgeries.

127. Following without prejudice discussions, Mr Madden and Dr Placks have produced two joint reports in which they have almost entirely agreed on Mr Madden’s technical findings that the documents are manipulated or inauthentic: {Q/2/1} and {Q/4/1}. There are some respects in which Dr Placks does not feel able to go as far as Mr Madden, since he considers that his task is to focus on the particular document rather than reviewing each in the context of the set of disclosed materials. However, there is no real dispute as a matter of the findings made, nor in most cases about what they mean. In the first joint statement, Dr Placks agrees findings of manipulation for 23 Reliance Documents, while finding nine more to be unreliable in some way. In the second, findings of manipulation

²³⁵ See deposition transcript at {E/17/88}; {E/17/115}.

²³⁶ {L13/351/1}.

²³⁷ {L18/242/1}.

²³⁸ Madden 1 at {G/1/1}; Madden 2 at {G/3/1}; Madden 3 at {G/5/1}; and Madden 4 at {G/6/1}.

²³⁹ Placks 1 at {I/1/1}; Placks 2 at {I/6/1}.

²⁴⁰ Lynch at {I/5/5}.

are made for a further 16 documents, while Dr Placks agrees that the remaining five are unreliable.

128. Madden 4 {G/6/1} deals with the new documents and the BDO Drive, with Mr Lynch giving equivalent evidence for Dr Wright. In their joint statement {Q/6/1}, they agree that BDO Drive image is not authentic; that it was actively edited in the period 17 to 19 September 2023 by a user (i.e. not by an automated process); and that its content has been significantly manipulated, including clock / timestamp alteration. They both agree that 71 of the 97 New Documents are manipulated. These include all the documents which would have given any material support to Dr Wright's claim to be Satoshi.
129. As for the LaTeX experts (Mr Rosendahl and Mr Lynch), they agree that:²⁴¹
 - 129.1. The White Paper was not written in LaTeX but in OpenOffice 2.4 (a finding consistent with the metadata of the public White Paper versions).
 - 129.2. The main.tex file identified by Dr Wright as producing a replica of the White Paper does not do so, instead exhibiting substantial discrepancies from it.
 - 129.3. Reverse engineering the White Paper into LaTeX source code to make something superficially similar is not too difficult.
 - 129.4. Dr Wright's LaTeX file only produces a PDF copy at all resembling the White Paper because it uses software not available in 2008/9.

Cryptocurrency Experts

130. The cryptocurrency experts address two topics: (a) basic facts of the technology underpinning Bitcoin and other cryptocurrencies; and (b) the signing sessions. COPA's evidence is from Prof Meiklejohn {G/2/1}, and Dr Wright's from Zeming Gao {I/2/1}.
131. Most of the report of Mr Gao addresses the first topic, and in that section he strays far from his proper remit. Rather than simply addressing the basic facts of the technology, he pursues an argument that BSV, the cryptocurrency created by a hard fork in the Bitcoin blockchain, is superior to Bitcoin Core and Bitcoin Cash and better reflects the philosophy underlying the White Paper. Following the PTR order,²⁴² Dr Wright is not

²⁴¹ Joint Report at {Q/5/1}.

²⁴² {B/22/6}, at §19. See judgment at {B/28/39}, §§158-159.

permitted to rely on these parts of Mr Gao’s report which deal with his assertion that BSV is the superior implementation of Bitcoin and/or the alleged fidelity of BSV to the suggested intentions of Satoshi.²⁴³

132. It will be necessary to address Mr Gao’s independence in cross-examination, principally because he has committed himself to supporting Dr Wright and his claim to be Satoshi in a series of extraordinary articles and posts that have continued up until recently (including January 2024) and which are in the trial bundles.²⁴⁴
133. Following without prejudice discussions, the two experts have produced a joint report in which Zeming Gao agrees with most aspects of Prof Meiklejohn’s evidence: {Q/3/1}. On the topic of the signing sessions, they both agree that they sessions could have been faked and on how that could have been done. The two experts have produced short reply reports explaining the rationale for their disagreements,²⁴⁵ which are actually of quite limited importance to the issues in the case.

ASD Experts

134. Dr Wright served a report of Prof Fazel {I/3/1}, diagnosing him with high-functioning ASD and addressing its potential effects on his demeanour when giving evidence, as well as suggesting adjustments for his evidence. In response, COPA served a report from Prof Craig {G/4/1} which accepts the diagnosis and also describes effects on presentation which the Court should take into account. Prof Craig also dealt with adjustments.
135. In the joint statement of the experts {Q/1/1}, Prof Fazel withdrew his support for the extreme adjustments sought by Dr Wright (which would have included all questions being given to him in advance of his cross-examination). His change of position was because he had not originally been provided with videos and transcripts showing how Dr Wright had coped with cross-examination. As a result, the parties agreed on the

²⁴³ The parts of his report which COPA says fall into this category are §§65-89, 102-154, 180-197 and 217-225. COPA gave notice of this position in its PTR Skeleton {R/1/24}.

²⁴⁴ By way of example only, see his article dated 3 November 2022 (“*The Wright strategy is the Satoshi strategy*”) {L19/277/1} and his article dated 4 October 2023 (“*The key in COPA v Wright*”) {L19/264/1}. In his book, *Bit & Coin* (2023), the dedication reads: “*To Satoshi, who brought a gift to mankind, and suffered because of it. It is outrageously unfair to you, but it is fate for Satoshi to bear the burden of full proof-of-cost and proof-of-work. It is the divine principle of the cross. It is why truth has value...*” {L20/121/6}. The book then contains a lengthy argument for Dr Wright’s claim to be Satoshi (from {L20/121/65}), adding that Dr Wright’s education and background bore “*the marks of a deliberate Divine preparation for this creation*” {L20/121/67}.

²⁴⁵ See Annexes to joint statement at {Q/3.1/1} and {Q/3.2/1}.

adjustments for trial, which are (a) that Dr Wright’s evidence should be clearly timetabled (which has happened); (b) that he should be given pen and paper, and access to the Opus live transcript; and (c) that more regular breaks may be needed if Dr Wright becomes visibly emotionally dysregulated.

Submissions on the Law Relevant to Resolution of the Identity Issue

Burden and Standard of Proof

136. In a civil action, the burden of proof rests on the party who “*asserts a proposition of fact which is not self-evident*”: see *Robins v National Trust Company Ltd* [1927] AC 515 at 520. Where “*a given allegation, whether positive or negative, forms an essential part of a party’s case, the proof of such allegations rests upon them*”: see *Emmanuel v Avison* [2020] EWHC 1696 (Ch) at §54. Thus, in the COPA claim, COPA bears the burden of proving that Dr Wright is not Satoshi Nakamoto; whereas, in the BTC Core Claim (and in the other cases where the parties are to be bound by the result of this trial), Dr Wright bears the burden of proving that he is Satoshi.
137. In general, a Court ought to attempt to make positive findings of fact on disputed issues if it is able to do so. The Court will only resolve an issue by resort to the burden of proof in the “*exceptional situation*” where “*notwithstanding that it has striven to do so, it cannot reasonably make a finding in relation to a disputed issue*”: *Stephens v Cannon* [2005] CP Rep 31 (CA) at §§37-46] *Verlander v Devon Waste Management* [2007] EWCA Civ 835 at §24. “*Choosing between conflicting factual and expert evidence is a primary judicial function*” and “*the judge’s task is generally to decide the case by choosing one over the other*”: *Lysandrou v Lysandrou* [2018] EWCA Civ 613 at §29.
138. The standard of proof applying to all factual issues in civil proceedings is the balance of probabilities. It applies equally to allegations which amount to criminal conduct: see *Phipson on Evidence (20th ed.)* at §6-57. It is not a flexible or sliding standard. In applying the standard, a Court may where appropriate take account of the inherent probability of particularly serious allegations: see *Re H (Minors)* [1996] AC 563 at 586. However, there is no necessary connection between the seriousness of an allegation and its inherent probability, as Lord Hoffmann explained in *Re B (Children)* [2009] 1 AC 11 at §15:

“There is only one rule of law, namely that the occurrence of the fact in issue must be proved to have been more probable than not. Common sense, not law, requires that in deciding this question, regard should be had, to whatever extent appropriate, to inherent probabilities. If a child alleges sexual abuse by a parent, it is common sense to start with the assumption that most parents do not abuse their children. But this assumption may be swiftly dispelled by other compelling evidence of the relationship between parent and child or parent and other children. It would be absurd to suggest that the tribunal must in all cases assume that serious conduct is unlikely to have occurred. In many cases, the other evidence will show that it was all too likely.”

See too Baroness Hale at §70:

“Neither the seriousness of the allegation nor the seriousness of the consequences should make any difference to the standard of proof to be applied in determining the facts. The inherent probabilities are simply something to be taken into account, where relevant, in deciding where the truth lies.”

139. Where a story involves a sequence of events, each of which is independently improbable, there is substantial authority that the Court should have regard to the cumulative effect, which may support an alternative conclusion: see *Suez Fortune Investments Ltd v Talbot Underwriting Ltd (“Brillante Virtuoso”)* [2019] 2 Lloyd’s Rep 485 at §§67-68.

Pleading and Proof of Fraud

140. The principles governing pleading and proof of fraud are well-established and are summarised by Arnold LJ in *Sofer v Swissindependent Trustees SA* [2020] EWCA Civ 699 at §§23 and 24:

- “(i) Fraud or dishonesty must be specifically alleged and sufficiently particularised, and will not be sufficiently particularised if the facts alleged are consistent with innocence: Three Rivers District Council v Governor and Company of the Bank of England (No.3) [2003] 2 AC 1.*
- “(ii) Dishonesty can be inferred from primary facts, provided that those primary facts are themselves pleaded. There must be some fact which tilts the balance and justifies an inference of dishonesty, and this fact must be pleaded: Three Rivers at [186] (Lord Millett).*
- “(iii) The claimant does not have to plead primary facts which are only consistent with dishonesty. The correct test is whether or not, on the basis of the primary facts pleaded, an inference of dishonesty is more likely than one of innocence or negligence: JSC Bank of Moscow v Kekhman [2015] EWHC 3073 (Comm) at [20]-[23] (Flaux J, as he then was).*
- “(iv) Particulars of dishonesty must be read as a whole and in context: Walker v Stones [2001] QB 902 at 944B (Sir Christopher Slade).*

[24] To these principles there should be added the following general points about particulars:

- (i) *The purpose of giving particulars is to allow the defendant to know the case he has to meet: Three Rivers at [185]-[186]; McPhilemy v Times Newspapers [1999] 3 All ER 775 at 793B (Lord Woolf MR).*
- (ii) *When giving particulars, no more than a concise statement of the facts relied upon is required: McPhilemy at 793B.*
- (iii) *Unless there is some obvious purpose in fighting over the terms of a pleading, contests over their terms are to be discouraged: McPhilemy at 793D.”*

141. Overall, “*pleading is not a game and it is about fairness and fairly understanding the case that has to be met, and points about whether a case has been adequately pleaded are to be looked at in that context*”: see *National Bank Trust v Yurov* [2020] EWHC 100 (Comm) at §249 and the cases there cited.

Evidence – Recollections of Witnesses and Documentary Evidence

142. The Courts have long recognised in cases of fraud the importance of testing the veracity of accounts “*by reference to the objective facts proved independently of [witnesses’] testimony, in particular by reference to the documents in the case, and also to pay particular regard to their motives and to the overall probabilities*”: *Armagas Ltd v Mundogas SA (The Ocean Frost)* 1985 1 Lloyd’s Rep 1 at 57 (Lord Goff). It has thus, and rightly become a commonplace in commercial litigation that contemporaneous documents “*are generally regarded as far more reliable than the oral evidence of witnesses, still less their demeanour while giving evidence*”: *Simetra Global Assets Ltd v Ikon Finance Ltd* [2019] 4 WLR 112 at §§48-49. See too the well-known observations of Leggatt J in *Gestmin SGPS SA v Credit Suisse (UK) Ltd* [2020] 1 CLC 428 on the difficulty of placing excess reliance on witness recollections (given the reconstructive tendencies of human memory) and the need to “*base factual findings on inferences drawn from documentary evidence and known or provable facts*” (at §22).

Points on Expert Evidence

143. Witness statements of fact should not be used as a vehicle to deliver what ought to be expert evidence (with the proper safeguards attached to such evidence applying), and the Court may disallow opinion evidence put in fact witness statements on this basis: *New Media Distribution Co SEZC v Kagalovsky* [2018] EWHC 2742 (Ch) at §10; *Glaxo Wellcome UK Ltd v Sandoz Ltd* [2019] RPC 26 at §§5-15. However, a witness of fact

may give opinion evidence directly related to the factual evidence he/she gives: see the survey of authority in *Polypipe Ltd v Davidson* [2023] EWHC 1681 (Comm) at §§17-31.

144. On many points in this case, the experts on each side are in agreement with each other but Dr Wright takes issue with the common views. The legal position is clear that “*where experts are agreed on a matter within their technical expertise, a judge will only rarely reject that evidence; and should not do so without applying considerable caution and giving adequate reasons*”: *Whiting v First / Keolis Transpennine Ltd* [2018] EWCA Civ 4 at §34.

Drawing of Inferences (including from absence of witnesses)

145. The Court may draw adverse inferences from a party’s failure to deploy forms of evidence or proof which he/she could reasonably have been expected to adduce. Thus, in appropriate cases “*a court may be entitled to draw adverse inferences from the absence or silence of a witness who might be expected to have material evidence to give on an issue in the action*”, unless a credible reason is given for the witness’s absence: *Wisniewski v Central Manchester HA* [1998] PIQR P324 at 340. As Lord Leggatt explained in *Efobi v Royal Mail Group Ltd* [2021] 1 WLR 3863 at §41, this is “*a matter of ordinary rationality*” and a feature of the process of a Court drawing inferences:

“*So far as possible, tribunals should feel free to draw, or to decline to draw, inferences from the facts of the case before them using their common sense without the need to consult law books when doing so. Whether any positive significance should be attached to the fact that a person has not given evidence depends entirely on the context and particular circumstances. Relevant considerations will naturally include such matters as whether the witness was available to give evidence, what relevant evidence it is reasonable to expect that the witness would have been able to give, what other relevant evidence there was bearing on the point(s) on which the witness could potentially have given relevant evidence, and the significance of those points in the context of the case as a whole.*”

Evidence on Character and Credibility

146. Evidence may be admissible “*when it affects the weight of other evidence tendered, e.g. evidence that affects the credit of a witness*”: *Phipson* at §7-04. In addition, evidence of character may be admissible as directly relevant to factual issues in the case, and in this context “*character*” encompasses a person’s reputation and their “*disposition to conduct themselves in some way or other*”: *Phipson* at §§17-01 to 17-02. A witness may be required to give evidence in cross-examination on matters going solely to credit.

Hearsay Evidence – Admissibility and Weight

147. The general admissibility of hearsay evidence in civil proceedings is provided for by s.1 of the Civil Evidence Act 1995. That Act also lays the ground for hearsay notices (see s.2) and cross-examination on hearsay statements (see s.3). The weight to be given to hearsay evidence is addressed by s.4, which gives a non-exhaustive list of considerations:

- “(a) *whether it would have been reasonable and practicable for the party by whom the evidence was adduced to have produced the maker of the original statement as a witness;*
- (b) *whether the original statement was made contemporaneously with the occurrence or existence of the matters stated;*
- (c) *whether the evidence involves multiple hearsay;*
- (d) *whether any person involved had any motive to conceal or misrepresent matters;*
- (e) *whether the original statement was an edited account, or was made in collaboration with another or for a particular purpose;*
- (f) *whether the circumstances in which the evidence is adduced as hearsay are such as to suggest an attempt to prevent proper evaluation of its weight.”*

Admissibility of Public Reports and of Judgments in Other Proceedings

148. As noted above, Dr Wright has been involved in various pieces of relevant litigation, in which judgments have been delivered. Such judgments are conclusive evidence of their existence, date and legal effects, and they are also admissible evidence of what happened in the proceedings they describe: see *Phipson* at §§43-01 to 43-02. Thus, Judge Reinhart’s judgment of August 2021 in the *Kleiman* litigation is admissible in describing the account Dr Wright gave of putting assets out of his reach and the “bonded courier” story he gave. However, judgments in other proceedings are not admissible for the purpose of proving that the other judges’ assessments and findings are correct: the rule in *Hollington v Hewthorn* [1943] KB 857.

Dr Wright’s Claim to be Satoshi

149. Dr Wright’s story for the purpose of these proceedings is set out in his witness statements. It is often contradictory – both internally between his own statements and between what he has said elsewhere. That will be the subject of cross-examination. The following is the story he advances at present in these proceedings.

150. Dr Wright claims that he dedicated a “*substantial amount of time*” to researching the foundational problems of Bitcoin and blockchains and that he documented these in the White Paper.²⁴⁶ His evidence sets out how he says he got to that point. His story starts with him programming games aged 11 (so, in 1981) by writing code in C and C+.²⁴⁷ Dr Wright says that he was “*deeply invested*” in the evolution of digital cash systems since the late 1990’s and that Bitcoin is the work which has “*defined [his] professional journey*”.²⁴⁸

Project BlackNet

151. Dr Wright claims that he began his journey with working at OzEmail on the implementation of a payment protocol known as Millicent.²⁴⁹ This led, in 1998, to him embarking on a project known as “Project BlackNet”, the purpose of which he says was to create a fully secure encrypted internet explicitly for business-to-business transactions.²⁵⁰ Dr Wright says the concept of “*crypto credits*” in BlackNet was conceived by a combination of ideas Dr Wright says he took from Millicent, and he adds that this “*laid the foundational groundwork*” for Bitcoin.²⁵¹ He says little else in Wright 1 about Project BlackNet, but it features heavily in his Reliance Documents and is as prominent in the Madden Report.

152. In fact, Project BlackNet had nothing to do with cryptocurrency. Instead, it was a (real or purported) project based on his IT security work and involved creating an end-to-end encrypted network. This can be seen in the document dated Thursday 3 October 2002 called “ITOL Project “BlackNet”,²⁵² with the stated objective being “*to integrate a number of off the shelf products in a clever and unique way to develop a product that will provide Fire-walling, IPSEC VPN’s, Intrusion Detection and SSL Acceleration Management.*”²⁵³ Some other versions of Project BlackNet documents, on which Dr Wright relies, contain sections which appear to foreshadow elements of Bitcoin, but (a) those documents have been backdated; (b) the sections are incongruous (as well as being

²⁴⁶ Wright 1, §11 {E/1/4}.

²⁴⁷ Wright 1, §25 {E/1/7}.

²⁴⁸ Wright 1, §26 {E/1/4}.

²⁴⁹ Wright 1, §29 {E/1/7}.

²⁵⁰ Wright 1, §31 {E/1/8}.

²⁵¹ Wright 1, §32 {E/1/8}.

²⁵² {L1/80/1} – Mr Madden accepts this document is genuine to 2002, see Appendix PM8 at {H/60/6}. There is another document “Integyrs Project Spyder” from 2009, which is to similar effect {L7/211/1}.

²⁵³ {L1/80/5}.

absent from genuine versions); and (c) the new sections envisage a further phase involving a peer-to-peer transaction system, but that phase is absent from the budget (which describes the previous phase as the “final” one).

Lasseter’s and Vodafone

153. During his time working with Lasseter’s Online Casino, Dr Wright claims that his work there on robust security and logging, along with distribution of logs, led to the creation of an early precursor of the blockchain.²⁵⁴ It was his time at Lasseter’s that he says “*planted the seeds that would later germinate into the idea of Bitcoin*”.²⁵⁵ Similarly, Dr Wright charts his further career development working at Vodafone as being significant to how he would create Bitcoin. He says that, while there, he worked on the creation of secure logging and payment channels, with all system events and transactions being carefully tracked.²⁵⁶

154. However, all the contemporaneous evidence of Dr Wright’s work with Lasseter’s and Vodafone (including in his own CV and profile cited above) describes it as straightforward IT security work. Based on the documents and the evidence of Dr Wright’s own witnesses (Mr Archbold and Mr Jenkins), his work involved putting together online security features, such as firewalls. Nothing in his work for either company was out of the ordinary for IT security work which is carried out for many companies every day. Dr Wright strains to characterise working on logging systems (totally normal for IT security) as being somehow a precursor to Bitcoin and suggests a continuing professional thread, ineluctably leading towards the creation of Bitcoin. The reality is that these were simply IT security projects over a few years in the IT security sector, and nothing to do with the creation of a revolutionary cryptocurrency.

Dr Wright’s Employment at BDO

155. Dr Wright’s period at BDO from 2004 to 2008 is the time when his story really begins to describe him planning out the Bitcoin system. He claims that his education by Allan Granger (a BDO partner) in triple-entry accounting played a pivotal role in Bitcoin.²⁵⁷ Dr Wright says that, in 2007, he introduced Mr Granger to what would become Bitcoin,

²⁵⁴ Wright 1, §39 {E/1/9}.

²⁵⁵ Wright 1, §42{E/1/10}.

²⁵⁶ Wright 1, §45-47 {E/1/9}.

²⁵⁷ Wright 1, §50 {E/1/11}.

though without that name.²⁵⁸ He also claims he discussed Bitcoin with Neville Sinclair. He has said on other occasions that he tried to interest BDO in investing in his nascent cryptocurrency project.

156. In his evidence in the *Granath* case, Mr Sinclair said that he had no recollection of discussing a prospective electronic cash system with Dr Wright while they worked together.²⁵⁹ Dr Wright has never had any supportive evidence from Mr Granger or the other two supposed attendees at BDO meetings. Dr Wright has repeatedly relied upon a set of BDO minutes of one meeting to back up this story, but they are forged. These minutes, handwritten on a Quill notepad, are dated August 2007 but that form of notepad was not released until 2012.²⁶⁰

Dr Wright's LLM Dissertation

157. Dr Wright also claims that work on his LLM dissertation at the University of Northumbria (submitted in 2008) fed into the development of Bitcoin. The dissertation, which is published, concerns legal liabilities of internet payment intermediaries.²⁶¹ He says that he analysed online payments and the cost issues plaguing online intermediaries, which “*informed [his] vision for Bitcoin*”.²⁶²
158. Dr Wright's LLM dissertation, in reality, is simply a legal dissertation on the circumstances in which internet intermediaries are liable in the modern environment. The 89-page published document does not use language or concepts prefiguring the White Paper or the Bitcoin system. Dr Wright's original Reliance Documents, and some documents on the BDO Drive, purport to be draft proposals for the dissertation which include some of the language from the White Paper, incongruously inserted into a section about the postal rule for acceptance in contract. However, these documents have been established by Mr Madden to be forgeries.²⁶³ In August 2019, Dr Wright posted a copy

²⁵⁸ Wright 1, §52.

²⁵⁹ Transcript at {E/19/3}.

²⁶⁰ See Appendix PM5 to Madden 1 {H/31/1}.

²⁶¹ The dissertation is at {L18/373/1}.

²⁶² Wright 1, §58 {E/1/12}.

²⁶³ The three original Reliance Documents are ID_000199 {L2/130/1}, ID_000217 {L2/131/1} and ID_003702 {L15/442/1}. These are addressed by Mr Madden in Appendix PM25 {H/118/1}. The New Drive documents are ID_004696 {L2/53/1} and ID_004697 {L2/54/1}. They can be shown to be forgeries, including because they are .rtf files whose metadata indicate that they were prepared in a version of Windows dating from 2020: see Madden 3 at §§86-91 {G/5/35}.

of the falsified proposal document on both the SSRN website²⁶⁴ and his Slack channel,²⁶⁵ as well as emailing a copy with the subject line “FYI. The start of bitcoin”.²⁶⁶

159. Furthermore, Dr Wright’s reliance on his LLM dissertation work as embodying inventive thinking of the highest order is undermined by the fact that it is in fact heavily plagiarised. Dr Wright modestly describes it a “*masterwork*” in his acknowledgements,²⁶⁷ but perhaps the most obvious acknowledgements are missing. Large sections are plagiarised from the work of Ms Hilary Pearson, representing wholesale copyright infringement.²⁶⁸
160. So, as with Project BlackNet, Dr Wright has taken work he did which bore no relation to the concepts of Bitcoin, has sought to draw spurious connections between the two and has created false documents to give credence to this story of a long intellectual journey towards Bitcoin.

Dr Wright’s MStat Degree

161. Dr Wright also cites work he did in a Master’s in Statistics course at Newcastle University (NSW) as contributing to his design of Bitcoin. He dates that course to the period 2005-2009. He claims that his intention was “*to focus [his] dissertation on statistical and graph theoretical aspects of Bitcoin*”, but that he had to choose another topic instead.²⁶⁹ In a blog post about this course,²⁷⁰ he has told an elaborate story of choosing Newcastle University because it gave him access to two individuals versed in the mathematics of monetary systems, Graham Wrightson and Andreas Furche. His disclosure includes a supposed statistics assignment²⁷¹ completed by him for a tutor, Richard Gerlach, in October 2005 which contains text matching that in the White Paper.
162. In fact, the statistics assignment is a forgery, apparently based on a genuine document in disclosure.²⁷² The genuine document²⁷³ addresses statistics questions and does not have any connection to Bitcoin. Prof Gerlach has given a statement in which he points to

²⁶⁴ See Exhibit PM25.2 {H/120/1} and Appendix PM25 at §46 {H/118/21}.

²⁶⁵ See Appendix PM43 from §45 {H/219/18}.

²⁶⁶ Email of 18 September 2019 {L15/441}.

²⁶⁷ {L18/373/16}.

²⁶⁸ See {D/490/2}.

²⁶⁹ Wright 1, §95-96 {E/1/19}.

²⁷⁰ “Fully Peer-to-Peer” (June 2019) {L15/88/2}.

²⁷¹ ID_000073 {L1/323/1}.

²⁷² As demonstrated by Mr Madden in Appendix PM38 {H/145/1}.

²⁷³ ID_000077 {L1/337/1}.

anomalous features in the forged document (thus giving independent support for Mr Madden’s forensic findings). As detailed below, Prof Wrightson and Prof Furche deny nearly every aspect of Dr Wright’s account about them and his dealings with them.

Dr Wright’s Claims about Writing the Bitcoin code

163. Dr Wright says he began working on the source code in 2007 using C++.²⁷⁴ He says he initially engaged in web testing and then progressed to coding a minimum viable product prototype.²⁷⁵ He then went on to work on the parameters that would govern the functioning of the Bitcoin network, which included the creation of the Genesis block.²⁷⁶ He says he created a repository on SourceForge to provide a centralized location for Bitcoin source code.²⁷⁷
164. He maintains that he kept up his full-time position at BDO whilst developing Bitcoin in parallel, saying that he dedicated around three hours each day to Bitcoin during the week, with eight to ten hours at the weekend.²⁷⁸ He claims that, by early 2008, he had what he regarded as a preliminary version of the code. He says that he coded alone but sought input from others in this early stage, and that when engaging with others he used both his real name and the Satoshi pseudonym.²⁷⁹ He says that in early 2008 he discussed the code with Mark Turner using his real name, and that Mr Turner gave candid feedback on the UI calling it ugly.²⁸⁰ Mr Turner has never given evidence for Dr Wright.
165. Included at Annex 1 to this Skeleton are a “scatter plot” and a bar graph showing the times of day when the Satoshi emails, forum posts and code check-ins (from August 2008 until April 2011) were sent or posted. On the scatter plot, the y axis is the time on the 24-hour clock for the time zone Sydney, Australia, where Dr Wright was living over this period, and the x axis is the date. On the bar graph, the x axis is the hour of day in Sydney and the y axis the number of Satoshi emails/posts timed in that hour. These both show Satoshi’s communications focused in the period from midnight through to 5pm / 6pm in Sydney time, with the greatest concentrations in the period from 2am to 11am (highest at 4-5am).

²⁷⁴ Wright 1, §70 {E/1/14}.

²⁷⁵ Wright 1, §72 {E/1/15}.

²⁷⁶ Wright 1, §73 {E/1/16}.

²⁷⁷ Wright 1, §75 {E/1/16}.

²⁷⁸ Wright 1, §76 {E/1/16}.

²⁷⁹ Wright 1, §78 {E/1/16}.

²⁸⁰ Wright 1, §79 {E/1/16}.

166. Dr Wright has identified only two documents which supposedly represent drafts of code dating from the period up to early 2008: ID_004014 and ID_004015.²⁸¹ The latter appears to be an edited version of the Bitcoin source code dating from November 2008, which is publicly available.²⁸² The former is not a piece of source code at all, but set-up notes apparently based on the original “readme” notes released publicly by Satoshi in January 2009.²⁸³
167. Dr Wright says that the first email account he set up was the Satoshi GMX account in around December 2007,²⁸⁴ before later acquiring the Vistomail account. He also claims to have acquired the domain name bitcoin.org in August 2008 and that Martti Malmi approached him to run the site in February 2009. As explained below, there are serious problems with Dr Wright’s account of having acquired the Satoshi email account and web domain. Also, Mr Malmi first contacted Satoshi in May 2009, not February 2009.²⁸⁵

Drafting of the White Paper

168. In Wright 1, Dr Wright claims to have started writing the White Paper by hand, between March 2007 and May 2008.²⁸⁶ He then claims to have started the drafting process using voice recognition software known as Dragon.²⁸⁷ He does not in Wright 1 mention the use of LaTeX, despite its importance to the account he later gives. He says that the initial draft of the White Paper was more extensive than necessary and in 2007 he shared preliminary drafts with family and trusted contacts.²⁸⁸
169. In Wright 4, after being forced to respond to the RFI request, Dr Wright listed the individuals with whom he says he shared drafts in his own name.²⁸⁹ There are 21 people on that list, of whom five are witnesses in this case and two are the subject of hearsay notices.²⁹⁰ Only two of the 21 have ever corroborated Dr Wright’s account in this respect

²⁸¹ See {L2/242/1} and {L2/243/1}. These are identified as the only available source code documents from this early period, both in Wright 4, §48 {E/4/20} and in Shoosmiths’ responses to requests for documents identified in Wright 1 {M/2/348}.

²⁸² See {L20/206/1}.

²⁸³ {L4/15/1}.

²⁸⁴ Wright 1, §81 {E/1/16}.

²⁸⁵ See Malmi 1, §4a {C/24/2} and email of 2 May 2009 {D/487/1}.

²⁸⁶ Wright 1, §86 {E/1/17}.

²⁸⁷ Ibid.

²⁸⁸ Wright 1, §87 {E/1/18}.

²⁸⁹ Wright 4, §49 {E/4/20}.

²⁹⁰ The five who are witnesses are Ms DeMorgan, Mr Matthews, Max Lynam, Mr Yousuf and Robert Jenkins. The two who are subject of hearsay notices are Mr Sinclair and Don Lynam.

– his backer Mr Matthews and his uncle Don Lynam. None of the 21 has ever produced a copy of the draft that Dr Wright allegedly shared, and Dr Wright himself has never produced an email or other document evidencing such sharing.

170. From March 2008 to May 2008 Dr Wright says that the draft started to look like the version that is now publicly known.²⁹¹ Dr Wright also gave an account in the *Kleiman* proceedings of writing the White Paper which he has avowed for these proceedings.²⁹² Although Dr Wright has provided many drafts of the White Paper in his disclosure, he says in Wright 4 that he is unable to identify the order of production of the drafts, since he never used a versioning system.²⁹³ A series of White Paper drafts in disclosure, including reliance documents, have been found by Mr Madden to be forgeries (notably versions which give Dr Wright’s details as author).²⁹⁴
171. Dr Wright claims that between March and May 2008 he shared a draft with Mr Kleiman, who was at the time “*his closest friend*”, over email, Skype and online forums.²⁹⁵ According to Dr Wright, Mr Kleiman provided edits to the draft.²⁹⁶ A significant email by which Dr Wright supposedly sought Mr Kleiman’s help in editing the draft (“**the Kleiman email**”) has been established by Mr Madden to be a forgery.²⁹⁷ This email was among the trove of documents leaked to Wired and Gizmodo in late 2015²⁹⁸ and it is among the forgeries originally pleaded in COPA’s Particulars of Claim.²⁹⁹
172. Dr Wright says that, in around July 2008, he tried to communicate with Tuomas Aura, a computer science professor, but his efforts to contact him remained unanswered.³⁰⁰ Then in August 2008 he says he reached out to Wei Dei and Adam Back under the Satoshi pseudonym. He sent them a link to upload.ae where he had uploaded the draft.³⁰¹ Both

²⁹¹ Wright 1, §88 {E/1/17}.

²⁹² The account is in his trial evidence on 22 November 2021 (am), from internal p93 {O2/10/93}. Dr Wright through Ontier confirmed that he would maintain it: letter of 7 March 2022 {M/1/240}.

²⁹³ Wright 4, §6(c) {E/4/5}.

²⁹⁴ See generally Appendix PM3 to Madden 1 {H/20/1}. Drafts pleaded by COPA as forgeries are ID_000254, ID_000536, ID_000537, ID_000538, ID_003732, ID_004010 and ID_004011. Of those, ID_000254, ID_000536 and ID_004011 are among the 20 forgeries on which COPA will be focusing at trial.

²⁹⁵ Wright 1, §89 {E/1/18}.

²⁹⁶ Ibid.

²⁹⁷ See Appendix PM18 to Madden 1 {H/83/1}. There are various versions of this email. The one originally identified as a forgery in COPA’s Particulars of Claim is at ID_001318 {L8/446/1}. A further version in COPA’s Schedule of Forgeries is ID_000465 {L2/318/1}.

²⁹⁸ See Gizmodo article of 9 December 2015 {L11/213/4}.

²⁹⁹ See Re-Re-Re-Amended Particulars of Claim from §28 {A/2/10}.

³⁰⁰ Wright 1, §90 {E/1/18}.

³⁰¹ Wright 1, §91 {E/1/18}.

of these individuals have their work cited in the White Paper and are known to have been in correspondence with Satoshi which referred to the upload.ae link. However, as noted above, Dr Wright has suggested that he (as Satoshi) knew of Wei Dai's work well before August 2008, when the previously unpublished emails of Mr Back show that the real Satoshi did not. Furthermore, Dr Wright has given false and inconsistent accounts of Dr Back's reaction to Satoshi's early communications and about whether Satoshi used Dr Back's Hashcash as the model for the proof-of-work system in Bitcoin (as detailed below). In addition, Dr Wright has given false accounts about the upload.ae site (as also detailed below).

173. Dr Wright then says that, while working on the White Paper, he presented his concepts to Microsoft under his own name but there was no interest in it.³⁰² He claims to have attended a series of business meetings at the Microsoft campus in Seattle in autumn 2008, but the specific names from those meetings “*have become hazy with time*”.³⁰³ However, the few communications he has provided with Microsoft³⁰⁴ suggest that he was simply looking for a job at the time he was taking redundancy from BDO. They do not indicate that he was making a proposal to sell Bitcoin to Microsoft, as he claimed in his evidence in the *Granath* case. He then claims to have implemented the core of the Bitcoin system in Hoyts, a cinema chain in Australia, and for QCSU, a bank.³⁰⁵ However, in his dealings with the ATO, he said that he had dealt with Hoyts as a client “*in his security role*”³⁰⁶ and that he managed the company's firewalls.³⁰⁷ Meanwhile, his work for Qudos Bank (formerly known as QCSU) was done through BDO, where he did straightforward IT security and audit work.
174. These events are said to have led to the release of the White Paper on 31 October 2008 on the metzdowd.com cryptography mailing list. This included a link to the White Paper which was uploaded to the Bitcoin.org site, with Dr Wright claiming that he had registered that site two months earlier.³⁰⁸ The evidence he has deployed to demonstrate purchase of that site has been demonstrated to be forged.

³⁰² Wright 1, §96 {E/1/19}.

³⁰³ Wright 1, §98 {E/1/19}.

³⁰⁴ See {L3/247/1} and {L3/249/1}.

³⁰⁵ Wright 1, §96 and 98 {E/1/19}.

³⁰⁶ {L8/408/5}.

³⁰⁷ {L7/431/133}.

³⁰⁸ Wright 1, §100 {E/1/20}.

175. Dr Wright asserts that the essential elements of the code were already in place by the time of the upload.³⁰⁹ Dr Wright then mentions that he engaged with Hal Finney and Mike Hearn as Satoshi³¹⁰ These are also known contacts of Satoshi derived from with emails in the public domain.³¹¹

Creation of the Genesis Block, Release of the Source Code and the First Transaction

176. Dr Wright says that he manually crafted the Genesis Block rather than mining it³¹² and that to ensure that it was timestamped he used the headline of an article published in the written UK edition of The Times that day.³¹³ He says that he chose this headline, which referred to the bank bailouts after the 2008 crash, because he strongly disagreed with the policy.³¹⁴ Dr Wright was not in the UK at this time, but claims to have had access to The Times through a university portal.³¹⁵ Dr Wright says he uploaded the v0.1 Alpha of Bitcoin on 9 January 2009 onto SourceForge and at the same time he sent a link to this to the Bitcoin Project’s relevant section on the mailing list.³¹⁶

177. Again, Dr Wright strains to provide meaning and rationale to all aspects of how Satoshi chose to do certain things but cites only publicly known matters. His account of the Genesis Block now involves assertions that there is neither a public nor a private key linked to it; assertions rejected by agreed expert evidence.³¹⁷

178. Dr Wright asserts that in the “*early days*” the only individuals involved in mining were himself, and his family (including Don and Max Lynam).³¹⁸ Alongside his family’s mining activity, Dr Wright claims to have been using his own mining set up in 69 racks at his Australian residence, with numerous other laptops and desktops he was running.³¹⁹ He claims that the considerable electricity associated with mining amounted to thousands

³⁰⁹ Ibid.

³¹⁰ Wright 1, §105 {E/1/21}.

³¹¹ As explained by Mr Hearn: {C/22/4}, at §14.

³¹² Wright 1, §108 {E/1/21}.

³¹³ Wright 1, §110 {E/1/21}.

³¹⁴ Wright 1, §110-111 {E/1/21}.

³¹⁵ Wright 1, §110 {E/1/21}.

³¹⁶ Wright 1, §112 {E/1/22}.

³¹⁷ For his account, see Wright 1, §107 {E/1/21} and Wright 4, §102 {E/4/34}. For the expert evidence which establishes that there is a public key for the Genesis Block and that there would be a corresponding private key, see Meiklejohn at {G/2/46}, §108-109 (paragraphs agreed by Mr Gao in the joint statement). The public key for the Genesis Block is shown at {G/2/22}. Note also that Dr Wright’s present account differs from what he told GQ in April 2016, when he claimed that he would not sign “*every fucking key I own in the world*” before adding: “*I’ve got the first fucking nine keys, I’ve got the fucking genesis bloody block...*” {O4/23/4}.

³¹⁸ Wright 1, §115 {E/1/22}.

³¹⁹ Wright 1, §116 {E/1/22}.

of dollars, but that he was willing to go to this expense to set the Bitcoin Blockchain in motion.³²⁰ It is to be noted that mining at that time would not have entailed such a cost. Dr Wright also goes on to say that his motivations in those days (2009-10) were primarily driven by a desire to implement the technology and not the pursuit of financial gain.³²¹ That of course conflicts with the position he now takes, having issued claims which seek in effect total control of Bitcoin under a range of different IP rights.

Dr Wright Leaving the Satoshi Persona

179. Dr Wright says that circumstances of late 2010 / early 2011 (including his marital problems and the ATO investigation) led him to decide to move away from the Satoshi persona, phasing out communications under the pseudonym in April 2011.³²² Dr Wright recounts sending Gavin Andresen a file containing a copy of the network alert key (with Dr Wright keeping a copy himself) in October 2010 and that he was willing to handover to Mr Andresen due to Dr Wright's belief that he was dedicated to the project.³²³ He says that he also granted Mr Andresen access to the Bitcoin code on SourceForge, though only on a lower-level administrator basis.³²⁴
180. Dr Wright then paints a picture of disappointment. He says that Mr Malmi took down the bitcoin.org server and initiated a new server (bitcointalk.org) over which Dr Wright (as Satoshi) had no administrator rights, while Mr Andresen and Wladimir van der Laan transferred the Bitcoin code from SourceForge to GitHub.³²⁵ There is no evidence that Mr van der Laan was involved at all, other than Dr Wright's account. He claims that these changes were against his wishes. However, the forum move did not alter the forum database, and (as noted above) it is clear from contemporaneous emails that Satoshi was perfectly content with the move to GitHub.
181. Dr Wright claims that, by August 2011, he was facing the full force of the ATO investigations and, due to his concerns about them seizing his assets (including IP rights), he decided to put them out of his direct control. He says that he did this by putting in trust all these assets, including bitcoin he claims to have mined since 2009.³²⁶ He claims that

³²⁰ Wright 1, §117 {E/1/22}.

³²¹ Wright 1, §121 {E/1/23}.

³²² Wright 1, §127-130 {E/1/24}.

³²³ Wright 1, §131-132 {E/1/25}.

³²⁴ Wright 1, §133 {E/1/25}.

³²⁵ Wright 1, §134 {E/1/26}.

³²⁶ Wright 1, §138-140 {E/1/26}.

he stored “terabytes” of research data on a hard drive and put it beyond his control by encryption with a Shamir Sharing Scheme involving 15 key slices held by various individuals, with eight slices needed to give access.

182. Dr Wright claims that a requisite number of key slices were reassembled in early 2016, giving access to a part of the drive containing private keys to the early Bitcoin blocks (or perhaps an algorithm from which those keys could be produced).³²⁷ His accounts of how these slices were reassembled are complex, and need to be traced through his evidence in the *Kleiman* and *Granath* proceedings, as well as his communications with Mr MacGregor and others in early 2016. These accounts are tied up with bogus Tulip Trust documents, and they will be explored in cross-examination. For the moment, it should be noted that there is no reliable evidence of communications about the supposed establishment of the Shamir Sharing Scheme or the supposed assembly of the key slices. It is also a curious feature of Dr Wright’s story that he claims to have put his early research data beyond his use, but this did not include any of the documents he has produced in recent years of supposed precursor work to the White Paper.

Overview of COPA’s Case

183. As set out in the introduction to this skeleton argument, COPA’s case that Dr Wright is not Satoshi can be presented in three parts: (a) that his claim to be Satoshi has been supported with a large volume of false and forged documents, with clear signs that he was involved in the work of forgery (e.g. both experts agreeing that the BDO Drive documents were manipulated in September 2023); (b) that, despite his repeated boasts of proofs he would give, he has consistently failed to prove his claim to be Satoshi in a range of ways which would be open to the real Satoshi; and (c) that numerous aspects of his story are implausible, internally inconsistent or at odds with verifiable facts or cogent witness evidence.

(1) Dr Wright’s Use of False and Forged Documents

184. The four reports of Mr Madden and their appendices show the astonishing level of forgery featuring in Dr Wright’s documents. Time and again, Dr Wright has had the opportunity to adduce documentary evidence to back up his claim. When he has done so, the documents have been false or forged. Unlike many cases of fraud, this case is not

³²⁷ Wright 1, §187 {E/1/33}.

one with a handful of forged documents. The Madden Report (as well as other fact evidence which further demonstrates the falsity of his materials) has hundreds of instances of documents being altered.

185. The pleaded forgeries are found in three parts: (a) the four originally featuring in the Particulars of Claim; (b) those added by amendment and pleaded in the Schedule of Forgeries {A/2/24} (with 20 focused upon: {M/2/684}); and (c) a further 20 added as a result of the PTR judgment and order, now pleaded in the Schedule of Further Forgeries {A/16/1}. There are numerous more documents on which COPA could rely as forged. As explained above, many of Dr Wright's original Reliance Documents are forged, while the remainder are inauthentic and/or do not support his claim anyway. For each of the forgeries in COPA's Schedules, there are multiple pleaded features which tie Dr Wright to the forgery and give rise to a strong inference that he was responsible, or at least knew of its falsity. On the whole of the evidence, it is very likely that Dr Wright was personally involved in making most or all of the forgeries.
186. Dr Wright's forgeries demonstrably form part of an effort to support a dishonest back-story. His forgeries are not limited to doctored versions of the White Paper, but to a wide range of documents supporting what he claims is the evolution of his ideas in the years before the launch of Bitcoin. For example, he has put forward a series of forged papers about game theory, network theory, economics and mathematics with added elements relating to Bitcoin. He has provided forged versions of his BlackNet paper, his LLM dissertation proposal and his MStat assignment to support false claims that his work on those matters involved or led to his developing Bitcoin. Those forgeries are particularly telling because the added material is so incongruous in its setting.
187. The documents found by Mr Madden to have been altered include:
 - 187.1. Many documents on which Dr Wright has relied in other litigation as supporting his claim to be Satoshi (including for example supposed Bitcoin White Paper drafts, Project Blacknet documents and the Quill Minutes, which were also relied upon in *Granath*).
 - 187.2. Many documents that Dr Wright has sent to others, apparently to support his claim to be Satoshi (including for example his LLM dissertation proposal documents and the NAB Records (discussed above)).

- 187.3. Some documents featuring Dr Wright's own handwriting (including for example the JSTOR document (ID_004019) and the coffee-stained draft of the White Paper (ID_004010)).
 - 187.4. Very many documents authored by Dr Wright, obtained from his own devices and/or publicly shared by him (including for example the documents shared by Dr Wright over Slack which are addressed in Appendix PM43³²⁸).
 - 187.5. Other documents personal to Dr Wright, such as the accounting records bearing his log-in information, emails connected with his private accounts and the screenshots of his banking records.
188. Mr Madden also found numerous indicators of tampering. By way of example only:
- 188.1. Internal metadata timestamps contradicted by the face dating, apparent dating or external provided metadata timestamps.
 - 188.2. Metadata containing references to fonts and schemas which did not exist at the supposed time of creation of the document.
 - 188.3. Timestamps showing interaction of the software Grammarly with documents at dates contradicting face dating or provided metadata (in some cases appearing in documents supposedly authored before Grammarly was released).
 - 188.4. The presence of touchup textedit tags showing later editing of the document.
 - 188.5. Residual data showing text which had evidently been edited out to make the document appear to come from an earlier date (e.g. descriptions of later events, URLs from websites which would be anachronistic, etc.).
 - 188.6. Edit times and overlaps in editing times that were either impossible or very difficult to square with anything like normal user behaviour.
 - 188.7. Emails apparently sent from domain names which did not exist at the supposed time of sending.

³²⁸ {H/219/1}.

189. This skeleton will now briefly address 10 examples of the forgeries of Dr Wright, of which nine are from the Schedule of Forgeries and one from the Schedule of Further Forgeries. Dr Wright will be cross-examined on the pleaded forgeries and all 44 will be addressed in a composite Schedule to closing submissions.

Examples from the Schedules of Forgeries

(1) MYOB records [ID_004077, ID_004078 and ID_004079] - Appendix PM7 {H/47/1}

190. These appear as accounting records from the MYOB system: {L5/150/1}, {L5/471/1} and {L5/146/1}. The Court will recall them, as they have featured prominently in the *Tulip Trading* case. Dr Wright disclosed copies in this case and nominated them as Reliance Documents. Although he never provided the source of those records, Mr Madden discovered the source (in a zip file, within another zip file, attached to an email in the disclosure). Mr Madden’s analysis of security logs relating to these records indicates that a person repeatedly sought to log in using Dr Wright's email address, before logging in as “admin” and then creating records in March 2020, backdating them to dates from 2009 to 2011.³²⁹ In their first joint expert statement, Dr Placks agrees with this conclusion.³³⁰ Dr Wright has since admitted that these documents are inauthentic, but has not indicated when he became aware of that fact and why he deployed them in the first place. He has suggested that the documents were produced by his former solicitors, Ontier, and in the *Tulip Trading* case he has suggested that Ontier is somehow responsible for unreliable records being proffered (although it is not clear that he is accusing Ontier of falsifying the records).³³¹

191. Dr Wright tried to provide replacement MYOB records by directing his expert, Dr Placks, to MYOB databases containing records which supposedly supported aspects of his claim (including a supposed entry for purchase of the bitcoin.org domain hosting).³³² However, Mr Madden has shown in his Second Report (notably Appendix PM42) that the “new” database records were forged in May / June 2023 – in the course of this litigation – by

³²⁹ See {H/47/33} at §§58-65 and the logs at {H/53/1} and {H/55/1}.

³³⁰ {Q/2/9}.

³³¹ Dr Wright’s fifth statement in the *Tulip Trading* case, at §39 {S1/1.13/13}.

³³² See Placks 1 at {I/1/32}, §§9.15 to 9.42.

person(s) using the email addresses of Dr Wright and his current wife (Ramona Ang).³³³
This finding is agreed by Dr Placks in the first joint statement.³³⁴

(2) *Project BlackNet document [ID_001379] – Appendix PM8 {H/60/1}*

192. Dr Wright has put forward a number of documents to support his account that he worked on a project with the names BlackNet and Spyder well before the publication of the White Paper and that project bore distinctive features of Bitcoin. The documents in disclosure, including this one, which appear to support that case bear clear signs of falsity.
193. The following features have been found in the BlackNet documents in disclosure:
- 193.1. The document entitled “*ITOL Project BlackNet*” (ID_001379 {L1/79/1}), which is one of Dr Wright’s Reliance Documents, is dated 2002 on its face and contains wording which appears in the White Paper. However, the document bears metadata indicating that it was created in 2014. Further, the sections which reflect content of the White Paper are incongruous with the rest of the document, which describes an IT security project without any transactional features.
- 193.2. Another document, ID_000013 {L1/80/1}, is similar to ID_001379 and appears to be authentic to 2002. However, the wording appearing in the White Paper does not feature in this document, supporting COPA’s case that that wording was introduced after the document had been produced.
- 193.3. A third document, ID_001016 {L7/211/1}, contains an email address “*craig@intergyrs.com*”, and Dr Wright’s signature alongside a date “*15/Mar/2009*”. However, the domain Intergyrs.com was not registered until about 6 weeks after that, so that the document must be backdated.
194. The BlackNet documents share a common theme with a number of the other documents Dr Wright has forged, in that there is a genuine underlying document into which he has sought to retrospectively introduce Bitcoin concepts. This has evidently been done to try and give the impression that all of Dr Wright’s activities led up to the creation of Bitcoin.

³³³ See Appendix PM42 at {H/209/7}, especially §§31ff.

³³⁴ {Q/2/9}.

(3) NAB Records [ID_003455] (with attachments) – Appendix PM17 {H/78/1}

195. The NAB records ({L15/101/1} and {L/15/102/1}) comprise screenshots in an email from Dr Wright to his colleague Jimmy Nguyen that appear on their face to come from Dr Wright’s personal internet banking records. They appear to show purchase of hosting services from Anonymousspeech, which might support Dr Wright’s claim that he purchased both the Satoshi Vistomail email account and the bitcoin.org domain from that organization. He has repeatedly asserted that he could “*categorically*” prove his ownership of Satoshi accounts by way of his bank accounts / credit cards statements.³³⁵
196. The Madden Report demonstrated that these records are inauthentic, because the screenshots were taken at a time (in 2018) when the records (from 2008) could not have been accessed. Dr Placks agrees with this conclusion.³³⁶ Following the service of the Madden Report, Dr Wright admitted that these bank records are not authentic,³³⁷ and he has disclosed entirely different copies of bank records over the period which do not show the same transactions. As explained below, Dr Wright has come up with an excuse for the original records being fakes, but it is wholly unconvincing.

(4) Spoofed Email [ID_001546] – Appendix PM21 {H/104/1}

197. Appendix PM21 addresses emails which appear to have been sent by Satoshi Nakamoto and appear on their face to support Dr Wright’s case on the Identity Issue. However, Mr Madden has determined that “spoofing” techniques were used to set the “sender” details to indicate a false origin; an email address unconnected to the actual sender.³³⁸ Mr Madden’s conclusions link the spoofed emails to Dr Wright’s own mailbox. COPA has included one of these in its list of forgeries (ID_001546 {L8/338/1}); a 2014 email apparently being from Satoshi to Uyen Nguyen (Dr Wright’s erstwhile associate). For that email, the spoofing is indicated by simple use of the cursor over the email addresses, but there are also multiple indicia in the transmission header. COPA also points also to another (ID_002586) as evidence of the same techniques.³³⁹

³³⁵ See his article, “*Evidence and Law*” dated 12 April 2019 {L14/451/3} and a transcript of a Daily Exchange April 2019 interview with him by Fred Schebesta at {O4/25/34}.

³³⁶ {Q/2/9}.

³³⁷ See letter from Travers Smith dated 27 September 2023 {M/2/205}.

³³⁸ See Appendix PM21 at §6-35 {H/104/2}.

³³⁹ See Appendix PM21 at §§36-55 {H/104/10}.

(5) Bitcoin.exe [ID_000739] – Appendix PM12 {H/68/1}

198. This is a different type of forgery from most of the others, in that it is an example of Dr Wright seeking to lay a false trail thorough doctored program code. Dr Wright has disclosed a bitcoin.exe file, ID_000739 {L3/474/1} (along with four others), which contains signs of hex editing of the .exe files (which are of course publicly available) to suggest that Dr Wright was an author of the code. The files also contain metadata irregularities.
199. Using a standard hex editor, Mr Madden was able to determine that the name Satoshi Nakamoto was replaced by Dr Craig Wright in the copyright notice. Mr Madden states that these changes are more consistent with edits being made in hexadecimal by way of binary editing, rather than being different compiled versions of the same code. Further, when checking the checksum for ID_000739, Mr Madden found that the checksum set out in the header was invalid, i.e. the checksum matched the genuine bitcoin file but the amends made by Dr Wright changed the actual checksum when that was checked.

(6) Timecoin ODT [ID_000254] – Appendix PM2 {H/17/1}

200. This is a Reliance Document which purports to be a precursor to the White Paper: {L2/441/1}. In reality it is a modified version of the published White Paper (PDF), and there are numerous indicia of forgery:
 - 200.1. Notes appear in the text in a font (Arial) different from that in the main text and different from the font attributed to the empty lines above and below the notes, consistent with the font having been derived from a flowchart that appears in the published White Paper in the relevant places.
 - 200.2. An odd “OBJ” symbol appears below text where, in the equivalent part of the White Paper, a flowchart appears. The symbol is an object replacement character in Unicode which is typically inserted automatically when a document is converted from a source containing embedded objects that cannot be displayed in text form. This shows the document to be a conversion, not an original (and earlier) draft of the White Paper.

- 200.3. Mr Madden found indentations in the empty lines above and below supposed drafting notes which match precisely the indentations of flowchart images in the published White Paper. The “OBJ” symbol had the same indentation. Although the indentations vary through the document, they always precisely match indentations in the published White Paper which give space for the flowcharts. It would be infeasible for the writer of a draft to predict so precisely the indentations required for flowcharts yet to be prepared.
- 200.4. The document omits hyphens (e.g. in “*proof-of-work*”) which would be expected, but (tellingly) they are only missing where in the published White Paper the word happens to cross into the next line. This suggests conversion of a document from PDF to Word.
- 200.5. In various places, the document omits formulae which feature in the published White Paper but which would corrupt on conversion from PDF to Word.
- 200.6. There are irregularities in line breaks and structuring of tables which similarly appear to be artefacts of conversion from a PDF original.
- 200.7. Whilst the Timecoin document is an OpenOffice document it does not carry any of the normal metadata associated with a typical OpenOffice document.

(7) *LLM Dissertation Proposal [ID_000217] – Appendix PM25 {H/118/1}*

201. As set out above, a key part of Dr Wright’s story on how he developed Bitcoin relies upon the work in his LLM, which he has supported with versions of a dissertation proposal. As noted above, one of them is attached to an email from him which describes it as “*The start of bitcoin*”, and he has posted copies on SSRN and Slack (with the email and postings dating to August / September 2019). Mr Madden’s analysis of this set of documents shows that they are various different backdated versions, apparently created by a series of editing steps. He has established a likely chronology of this editing process,³⁴⁰ which corresponds in time to the period of the email and the postings.
202. The version at ID_000217 (the pleaded forgery) {L2/131/1} has metadata with a creation date of 18 June 2007 and a last saved date of 28 October 2007. However, its internal

³⁴⁰ See Appendix PM25, at §24 {H/118/12}.

metadata contain a Grammarly timestamp dated to 18 August 2019. The raw data included references to the Calibri Light and Nirmala UI fonts, both released after 2007, as well as a Microsoft schema published in 2012. The process of forgery is further supported by the fact that other versions of the LLM dissertation proposal bear clear signs of manipulation, including (a) ID_003935 (showing text deleted in the editing chain) and (b) ID_000849 (showing an anachronistic footer).

(8) *BDO Quill minutes [ID_004013] – Appendix PM5 {H/31/1}*

203. The BDO Quill minutes {L2/159} are a slightly different type of forged document, in that they are handwritten. They are said to date from August 2007, and Dr Wright has relied upon them (notably in his evidence in *Granath*³⁴¹) to support his account of proposing a Bitcoin project to Mr Granger and others at BDO. Dr Wright's Chain of Custody Schedule³⁴² states that this document is Dr Wright's and was stored in his office from its creation until it was scanned for the purpose of litigation. The evidence we have from Mr Stathakis and Ms Li, who were responsible for manufacturing this form of Quill notepad, is that the first version of this pad was produced in March 2012.³⁴³ They provided a sample proof of the version (MS1), which Mr Madden and Mr Placks have authenticated.³⁴⁴

(9) *Backdated Draft of the White Paper [ID_000536] – Appendix PM3 {H/20/1}*

204. In Appendix PM3, Mr Madden addresses various documents purporting to be versions of the White Paper. In undertaking this exercise, Mr Madden established a control version from public sources, before addressing the various drafts. One of these disclosed drafts, ID_000536 {L2/474/1} is among COPA's pleaded forgeries. It appears as a PDF version of the White Paper, albeit with Dr Wright's details at the top of it and he dates it to 21 May 2008. However, there are numerous indicia of forgery.³⁴⁵

204.1. The metadata timestamp for creation (on 24 January 2008) precisely matches that for the control copy of the White Paper³⁴⁶ (to the day, minute and second),

³⁴¹ See transcript for 14 February 2022, internal p33ff {O2/11/10}.

³⁴² {K/11/1}.

³⁴³ {C/16/2}.

³⁴⁴ See joint expert statement at {Q/2/9}.

³⁴⁵ See Appendix PM3, from §89 {H/20/27}.

³⁴⁶ The control copy is ID_000865.

though one year earlier. This is either a clear sign of backdating or the most extraordinary coincidence.

- 204.2. Content in this document matched the White Paper control copy version as published in 2009, including in respects where it differed from the White Paper as issued in October 2008.³⁴⁷ This makes it implausible that the document is a preliminary draft dating to May 2008.
- 204.3. Touchup textedit tag show words being added to the document by the editing process, with these edits corresponding to the differences between the document and the control version of the White Paper.³⁴⁸
- 204.4. A further touchup textedit tag was found which referenced Dr Wright's contact details at nChain, a company which did not exist in 2008/9.
- 204.5. Metadata showed reference to Dr Wright's details at nChain (which of course he did not join for many years).
- 204.6. Font files were embedded that included 2017 copyright notices.
- 204.7. There were internal metadata streams which recorded contradictory timestamps, consistent with clock manipulation or hex editing of the timestamps.

(10) King2.rtf [ID_004695] – PM46 {H/278/4}

- 205. This is a document which presents as an article on network security, involving discussion of quorum systems, work on which Dr Wright says fed into Bitcoin. It is a Rich Text File created with the editor version associated with the May 2020 update of Windows 10.³⁴⁹ It did not exist in this form before 17 September 2023, and was modified at some point between that date and 19 September 2023 with the computer set back to 2007.³⁵⁰ A precursor version was included in a deleted image (InfoDef09.raw) and that deleted version was recovered. It showed (a) indications that “Craig S Wright” was the author and the operator of the software in use; (b) a timestamp dating its creation to 12

³⁴⁷ See the illustrative comparison document at Exhibit PM3.6 {H/26/3}.

³⁴⁸ See the illustrative comparison document at Exhibit PM3.7 {H/27/1}.

³⁴⁹ Madden 3, §86-91 {G/5/34}.

³⁵⁰ See Appendix PM46, §12 {H/278/4}.

September 2023 and a Grammarly tag with the same date; and (b) a reference to Zotero software version 6.02.27, which was not released until 5 September 2023.

Dr Wright's Excuses and Changes of Story

206. Dr Wright has a track record of excuses, both in this litigation and in his other cases, for why he has been so unfortunate in repeatedly having found himself in possession of, and deploying, documents which turn out to be forged. The common theme is that the excuses are only produced after he has been found out. Dr Wright has blamed numerous others for the inauthenticity of his documents, ranging from potential alteration by staff members (alluded to repeatedly in the Chain of Custody Schedule) to the work of his lawyers (e.g. Ontier's transmission of the MYOB records) and the unidentified Reddit source of the forged NAB screenshots. In addition, in his recent statements (notably Wright 9 to Wright 12), he has at great length sought to present his complex operating systems as explaining signs of apparent document alteration.
207. However, Dr Wright has consistently failed to identify anomalies in documents before others have pointed them out. Given Dr Wright's avowed expertise in forensic document examination and IT more generally, it would be surprising if he repeatedly produced key reliance documents for a series of important legal cases without noticing serious anomalies in them. His conduct and excuses must be assessed against that professed expertise:

"So I used to work in digital forensics and I have written a textbook on the subject. I taught it with the New South Wales police college, and what I have to say is the KPMG methodology is not replicable. It is not scientific." (*Granath* evidence³⁵¹)

"As somebody who designed multiple forensic certifications, published several books and founded methodologies used within the industry, I believe that the number of people in the forensic environment who have experience with this type of IT environment and the issues it can give rise to is smaller again." (Wright 10³⁵²)

Dr Wright's case must be that, despite this supposedly unparalleled expertise, he either (a) failed to notice any of the myriad problems with his documents pointed out in the Madden Report, or (b) noticed some, but chose not to mention them.

³⁵¹ Transcript for 14 September 2022, internal p71 {O2/11/19}.

³⁵² Wright 10, §6 {E/31/2}.

208. Similarly, as explained above, in providing Chain of Custody information, Dr Wright originally simply presented himself as author and custodian, treating requests for intermediate custodian information as disproportionate. With the service of the Madden Report, he changed tack and produced the long and confusing Chain of Custody Schedule which suggests that numerous unnamed staff members might have altered documents.³⁵³
209. More generally, the service of the Madden Report is the watershed date in the procedural history of this case. It was Mr Madden's exhaustive and detailed unpicking of Dr Wright's Reliance Documents which has caused so many of Dr Wright's changes in story. As explained above, this led to (a) the provision of the Chain of Custody Schedule and the Schedule of White Paper versions (CSW5), which suggested that many of the original Reliance Documents could have been changed by others; (b) his "discovery" of the new documents on the BDO Drive and on his Overleaf account; and (c) the complex explanation of his operating systems in Wright 9 (Appendix A) and Wright 10, which suggested that features of those systems could account for apparent signs of document alteration and tampering.
210. The excuses provided in the Chain of Custody Schedule are addressed in more detail below. In short, the Schedule is internally inconsistent and unreliable, as demonstrated by Madden 2 and Appendices PM43 and PM44. It also takes a position which is at odds with previous chain of custody information (which simply presented Dr Wright as author and custodian).
211. The BDO Drive raw image has been shown to be the product of an editing process carried out in mid-September 2023, apparently to produce documents to replace those debunked in the Madden Report. Many individual documents on the BDO Drive show independent signs of forgery. The Overleaf LaTeX files are also false documents, produced in a chain of edits intended to create one which could be passed off as a draft of the White Paper. Quite apart from all these signs of forgery, Dr Wright's accounts of discovering these key stores of documents late in the day are implausible.
212. As for Dr Wright's excuses relating to his operating systems (in Wright 9, Wright 10 and Wright 12), his claims in summary are that other individuals in his companies will have

³⁵³ It appears from the Chain of Custody that Dr Wright's case is that this happened as the result of ordinary working practices or innocent mistakes. He has not (yet) advanced a case that colleagues, employees or others have deliberately sought to sabotage his case by planting documents with signs of manipulation on his systems.

accessed his documents on networked computers, with the result that the documents will have automatically updated to include what would otherwise be anachronistic metadata features (e.g. Grammarly timestamps). These excuses are comprehensively rejected by his own experts, Mr Lynch³⁵⁴ and Dr Placks,³⁵⁵ as well as by Mr Madden.³⁵⁶

213. Despite the length of the statements and the elaborate account of Dr Wright's past IT systems, they merely speculate on effects which might occur, without any supporting technical evidence. In general terms, the experts for both parties dispute that these effects would occur as suggested. If and insofar as Dr Wright claims that features of his IT systems in fact account for particular signs of alteration, his counsel would need to put the points to Mr Madden (although it is difficult to see this being done with any foundation, given the joint expert evidence). It is on any view inconceivable that features of his systems can account for the many and diverse signs of forgery such as those in the 10 documents discussed above. Furthermore, they could not in any event explain non-technical forgeries, such as the notes on the Quill notepad which Dr Wright claims were drafted in 2008 on a notepad that did not exist until 2012.

214. Furthermore, as noted above, another issue with Dr Wright blaming his system architecture now is that he never mentioned this topic before service of the Madden Report. This is surprising in view of his vaunted expertise. One would have expected him to say, when serving his Reliance Documents, that certain features of his IT systems might give rise to metadata anomalies of particular kinds. He said no such thing. Indeed, when COPA asked in their Consolidated RFI for information on the operating system used for each of the Reliance Documents, part of Dr Wright's response was that this was "*in any event, irrelevant*".³⁵⁷

215. Another startling feature of this case is the period of time over which Dr Wright's forgeries have been produced.

215.1. As noted above, the ATO investigations involved him producing two versions of the same supposed email from Mr Kleiman attaching a Tulip Trust deed from 2011 and 2014. Mr Madden has found a number of Tulip Trust and Tulip

³⁵⁴ See Lynch 1 at §123-128 {I/5/37}; joint statement Madden / Lynch at §9 {Q/6/3}.

³⁵⁵ See joint statement Madden / Placks at §8 {Q/4/6}.

³⁵⁶ See Madden 4 at §§155-162 {G/6/51}.

³⁵⁷ See RFI Response 66 at {A/13/23}.

Trading Ltd documents to bear signs of having been forged in 2014/15.³⁵⁸ There is full documentary evidence showing that Dr Wright purchased Tulip Trading Ltd as an “aged shelf company” in late 2014 from Abacus Seychelles.³⁵⁹ Meanwhile, a series of documents were produced, each bearing signs of alteration, to suggest that the company had been in his hands since 2011.

- 215.2. It is also in 2014 that Dr Wright appears to have produced his first forged documents supporting his claim to be Satoshi. For instance, the Kleiman Email was apparently forwarded by Dr Wright to Ira Kleiman (David Kleiman’s brother) in March 2014.
- 215.3. Through the documents considered in the Madden Report and to be addressed at trial, there are signs of forgery going on over the following years, notably in 2019-20 (when evidence was being collected for the *Kleiman* litigation). For instance, it was in August 2019 that Dr Wright produced various documents and posted them on Slack, as discussed in Appendix PM43.³⁶⁰
- 215.4. This case itself is hardly immune from such forgeries in service of Dr Wright’s changing stories. The evidence shows that Dr Wright has continued producing forged documents right up to the present day, with the experts’ analysis showing that he produced the BDO Drive image by adding manipulated files around 17 September 2023 and with metadata indicating work on the Overleaf LaTeX files in November / December 2023.

If even some of COPA’s allegations of forgery are made good, this represents a serious abuse of the Court systems of several jurisdictions; England and Wales, Norway and the USA at least. This is not some private matter in which a person has produced a false will

³⁵⁸ See Appendix PM14 {H/73/1}. COPA’s Schedule of Forgeries includes: (a) the email from Mr Kleiman attaching the Tulip Trust deed (ID_001386); (b) an Abacus Seychelles invoice which appeared to show ongoing accounting services for Tulip Trading Ltd in 2014 but was actually a doctored version of the invoice for purchase of that company in late 2014 (ID_001421); (c) a Declaration of Trust of 21 July 2011 for Tulip Trust (ID_001925); and (d) a company incorporation form for Tulip Trading Ltd which was doctored to change the date from 2014 to 2011 and make other changes consistent with the date change (ID_001930). These are not among the 20 forgeries of original documents on which COPA will focus at trial.

³⁵⁹ For evidence of the purchase of Tulip Trading Ltd in October 2014, see for example: the email chains at {L9/188/1} and {L9/287/1}; the incorporation form at {L9/183/1}; the purchase invoice at {L9/189/1}; and the Commonwealth Bank payment transfer receipt at {L9/191/1}.

³⁶⁰ See: {H/219/2}.

or invoice to gain a financial advantage. It is the deliberate production of false documents to support false claims and use the Courts as a vehicle for fraud.

Change of Story Sase Study: the NAB Screenshots

216. It is not possible in this skeleton argument to address every aspect of Dr Wright’s changes of narrative. However, the story of the NAB screenshots offers a case study of how incredible those changes can be.
217. As noted above, when Satoshi was operating, the email address satoshi@vistomail.com and the web domain bitcoin.org were associated with him. The address and website were apparently purchased from the organisation Anonymous Speech. In Wright 4, Dr Wright claims to have used the vistomail account as Satoshi in 2008.³⁶¹ On 12 April 2019, in an article entitled “*Evidence and law*” he wrote that “*Bitcoin was birthed using a credit card payment*”.³⁶² He then went to on claim specifically that the “*source of the funds that went to pay for the bitcoin.org domain registration on AnonymousSpeech.com derived from my credit card*”,³⁶³ finishing the article by saying he would provide that evidence and would do so by using the “*courts and law*.”³⁶⁴ In this article, Dr Wright was telling the world that he would prove his creation of Bitcoin, not through signing with a private key³⁶⁵ but through tangible proof such as bank statements. His position was made even clearer in an interview two weeks later (27 April 2019), when he stated:

“Proof is something simple, like a credit card statement saying that you actually bought the Bitcoin.com – sorry, Bitcoin.org domain... and paid for the Satoshi email account.”³⁶⁶

“I’m an evil little prick, I’ve got bank statements and credit card statements and all of this stuff and, you know, the bank has to keep those for 25 years... So I can’t fundamentally change them... The bank issues a statement... the court checks, that’s it.”³⁶⁷

³⁶¹ Wright 4, §13 {E/4/8}.

³⁶² {L14/451/2}.

³⁶³ {L14/451/5}.

³⁶⁴ Ibid.

³⁶⁵ Notably the “Evidence and law” article is one of the key steps in him backtracking away from the position that he would prove his claim by a signature linked to an early block. He says that signing merely shows possession of private keys, not ownership (or creation of Bitcoin). Of course, this supposed stand on principle follows his failure to provide a proper signature in public.

³⁶⁶ {O4/25/34}.

³⁶⁷ {O4/25/36}.

218. Dr Wright followed up on that promise by producing screenshots of his NAB banking records (discussed above). He sent these to Jimmy Nguyen (then CEO of nChain Group) in an email dated 10 June 2019.³⁶⁸ These two screenshots appear to be NAB banking records showing two transactions: AU\$ 687 to Anonymous Speech; and an AU\$ 8 transaction fee (both dated 30 August 2008).³⁶⁹ The covering email said: “*Anonymous Speech is vistomail. [Number] is my old credit card. All the credit card shows is ‘Anonymous’. You need to have the Vistomail document as well.*”
219. As noted above, Dr Wright has now admitted these are inauthentic (although he did so only after they had been debunked in the Madden Report). Dr Wright does, however, give an excuse. In his third witness statement in the BTC Core claim, he says that these screenshots were sent to him by Amanda McGovern (his lawyer in the *Kleiman* litigation from the firm Rivero Mestre) on 9 or 10 June 2019. As to how Ms McGovern obtained these, Dr Wright says they were sent to her by a pseudonymous Reddit user whose “*identity remains undisclosed*”.³⁷⁰ Ms McGovern has passed away, so that the account cannot be checked with her.
220. Dr Wright then says that, at that time, he did not think that the records were genuine and that he emailed them to Mr Nguyen to check. However, the email did not suggest that they were inauthentic, and its short text indicates that he regarded them as genuine. It is also implausible that Dr Wright would send the documents to Mr Nguyen to check (and there is no suggestion in the evidence of what checks were to be made or even could have been made, given that the records purported to be Dr Wright’s financial records). Furthermore, Dr Wright goes on in his statement to say that he used other payment methods for the domain name,³⁷¹ and he adds in Wright 4³⁷² that he cannot remember what methods he used. It must follow from this evidence that he was lying in his article and interview of April 2019 when he said that he could remember and prove what payment method he had used. It must also follow that he disclosed documents in this action which he knew to be fakes planted on him (presumably a memorable event), but did not inform COPA or the Court when giving disclosure.

³⁶⁸ {L15/100/1}.

³⁶⁹ {L15/101/1}.

³⁷⁰ Wright 3 in BTC Core, §3 {E1/4/2}.

³⁷¹ Wright 3 in BTC Core, §7 {E1/4/3}.

³⁷² Wright 4, §16 {E/4/10}.

221. Dr Wright's story cannot be believed. The reality is that he announced that he would prove his Satoshi claim with bank records, forged the records and sent them to Mr Nguyen (all in mid-2019). When the forgery was exposed in the Madden Report, he concocted his incredible tale of the anonymous Reddit user planting fake documents.

Chain of Custody Schedule

222. As pointed out above, the Chain of Custody Schedule of 13 October 2023³⁷³ embodied, or at least laid the ground for, a series of further excuses. As well as being confusing and internally contradictory in many places, it is demonstrably wrong on various points of fact. It is addressed in some detail in Appendix PM43 to Madden 2.³⁷⁴ For example:

222.1. Bond Percolation in Timecoin (ID_000525):³⁷⁵ Dr Wright claims that this MS Word (.doc) document was drafted by him and typed up either by Lynn Wright or former assistants using his handwritten notes or dictation software. He claims it was originally written using OpenOffice and LaTeX. He says that it was put on a Verbatim CD-R drive at some time between 2005 and 2015, from which it was collected on 23 January 2020. Mr Madden concludes that the artefacts he found in the document indicate that it had been created from a .docx file, with no evidence of an origin in LaTeX. He also finds that Dr Wright posted an equivalent .docx file on Slack on the same day (16 January 2020) as the day indicated by the Grammarly timestamps in the document, suggesting that ID_000525 was created then, by conversion from the document posted on Slack.

222.2. LLM Proposal (ID_000217):³⁷⁶ Dr Wright claims that this document was drafted by him, Lynn Wright or his former associates using OpenOffice, and he dates it to May 2008. Mr Madden finds that Dr Wright posted an equivalent .doc file on Slack on the same day (18 August 2019) as the day indicated by the Grammarly timestamps in the document, suggesting that ID_000217 was created then, by conversion from the document posted on Slack.

³⁷³ {K/11/1}.

³⁷⁴ {H/219/1}.

³⁷⁵ See PM43, §§17-35 {H/219/7}.

³⁷⁶ See PM43, §§36-53 {H/219/16}.

222.3. Project BlackNet (ID_001379):³⁷⁷ The Chain of Custody information states that Dr Wright originated the document (along with Lynn Wright and Dave Dornback) and that it was copied from a server owned by DeMorgan to one owned by Ridge Estates in 2002. Both Mr Madden and Dr Placks agree that this document does not date from 2002 (as it says on its face) but from February 2014, when it was emailed by Dr Wright to Ms Nguyen.

The New Documents

223. An important feature in this case are the new documents which were supposedly discovered from September 2023; principally, the 97 selected documents from the BDO Drive and selected LaTeX files from Dr Wright's Overleaf account. These represent a final effort by Dr Wright to "fix" his evidence. Although most of these new documents are in file formats which are light on metadata, they show as much evidence of forgery as the earlier Reliance Documents.

The BDO Drive Documents

224. Dr Wright's position is that the 97 documents contained on the BDO Drive were captured on or around 31 October 2007 and that he never edited or amended any documents in this image after that date.³⁷⁸ He claims that the BDO Drive (which was an image located on a Samsung Drive) was hidden, encrypted and password protected.³⁷⁹ The Samsung Drive (including the BDO Drive) was then imaged by KLD on 20 September 2023. On Dr Wright's account, the BDO Drive ought to be a "time capsule" of documents from 2007 which have no sign of alteration since then. Accordingly, it only takes one document to be anachronistic within that BOD Drive for the entire contents to be rendered suspect.

225. Mr Madden has found widespread forgery in the BDO Drive. In summary, Madden 4³⁸⁰ makes the following findings:

225.1. Wholesale manipulation of the BDO Drive: The internal content of BDOPC.raw as a whole is not authentic to 2007 and has definitely been

³⁷⁷ See PM43, §§62-68 {H/219/27}.

³⁷⁸ Wright 5, §§7-9 {E/20/4}.

³⁷⁹ Wright 5, §20 {E/20/7}.

³⁸⁰ {G/6/1}.

manipulated. Having been given access to the raw images since the PTR, Mr Madden has established from the internal timestamps and other forensic signs that its content was edited between 17 and 20 September 2023. There are a variety of timestamps relating to the Samsung Drive and the various images recording actions taken in 2007, 2009, and 2017. These are contradicted by other timestamps relating to September 2023, and by the presence of software dating from after 2020 and 2022 (for example). This indicates the use of clock manipulation techniques, and that the 2007, 2009 and 2017 timestamps are not reliable.

- 225.2. Recovery of deleted files from the Samsung drive: The Samsung drive contains deleted files. Among these, there are at least three deleted drive image files, two of which are fully recoverable and which Mr Madden recovered. Those recovered deleted drive images are previous revisions of BDOPC.raw which must have been deleted on or after 17 September 2023.
- 225.3. At least 71 of the 93 BDO Documents are not original to the BDO PC and were entirely added: Most of the 97 New Documents did not exist on the BDO PC in 2007.
- 225.4. Of the 71 mentioned above, around a third of these documents were further manipulated after they were added to an image: Furthermore, the signs of editing were to assist Dr Wright's case. For example, the editing included modifying "Bitcoin" to "Timecoin" and altering references to 2009 and 2016 dates.
- 225.5. Clock manipulation and metadata editing appears to have been used in relation to the drive: There are impossible metadata records (for example files being deleted "before" they were created), indicating the use of clock manipulation techniques to interact with the BDO Image and the Samsung Drive on which it resided. There are also indications that timestamps of files in the drive may have been edited directly.

The majority of these findings were independently arrived at by Dr Wright's expert, Mr Lynch. As noted above, the experts agree on the manipulation of the BDO Drive in mid-September 2023 and the adding of the 71 new Reliance Documents.

226. In addition, as set out in COPA's skeleton argument for the PTR, Madden 3³⁸¹ made individual findings of forgery in relation to various of the 97 documents from the BDO drive, including (a) eight which were .rtf files created with a version of Windows dating from 2020; (b) two LaTeX documents with references to software packages that did not exist in 2007; (c) metadata timestamps for a PNG image and two related LaTeX files indicating the use of tools to edit metadata directly; (d) a document created using a version of MS Word not released at the time of its supposed creation; and (e) code files with anachronistic references to <chrono> libraries. Further findings of manipulation of individual documents are set out in Appendix PM46³⁸² to Madden 4.

The Overleaf LaTeX files

227. As noted above, the LaTeX experts are agreed that the White Paper was not written in LaTeX, that Dr Wright's LaTeX files do not compile into the White Paper and that they could not have been produced in 2008/9. It follows that these files are forgeries, a conclusion supported by the circumstances of their disclosure and by the metadata.

228. The finding of the experts that the White Paper was written in OpenOffice, not LaTeX, is particularly significant. The real Satoshi would know how the document was written, and would have no reason to lie about that, whereas Dr Wright has committed to a position that the document was written in LaTeX and that has been proved to be wrong.

229. These files and the expert findings are also important because Dr Wright relied upon the files so heavily in advance of and at the PTR. He claimed that they were unique in compiling to a replica of the White Paper and demanded special terms of confidentiality. His real reason for that demand must have been to limit scrutiny of the files. On the basis of both parties' expert evidence, Dr Wright made his applications at the PTR (including for the adjournment and for permission to rely on the LaTeX files) on dishonest grounds.

(2) Dr Wright's Failures to Provide Proof of his Claim

230. Dr Wright has singularly failed to provide proof of his claim to be Satoshi, in circumstances where (a) he has boasted of his ability to provide proof and has failed to come good; (b) one would expect the real Satoshi to be able to provide proof; and (c) Dr

³⁸¹ {G/5/1}.

³⁸² {H/278/1}.

Wright’s excuses are belated and defy belief. His failed attempts to supply proof fall into the categories of (i) supportive witnesses; (ii) documentary evidence; and (iii) cryptographic exercises.

Failure to Produce Supportive Witnesses

231. In terms of potential witnesses, Dr Wright claims to have told hundreds of people that he was Satoshi in Australia alone. In *Kleiman*, in November 2021, it was put to him that he and David Kleiman had kept secret their supposed partnership to create and monetise Bitcoin. He denied this, saying:³⁸³

“No. I actually registered a company called Information Defense in Australia. I listed the shareholders. I recorded it with the government and I sought a banking charter. So at least three, four hundred people knew that I was Satoshi in Australia. So no.” (emphasis added)³⁸⁴

232. Dr Wright has repeatedly said that he would prove his case to being Satoshi and that he could not wait to do so in Court. In *McCormack*, in May 2022, it was put to him that he was using a defamation case against an individual to prove his claim to be Satoshi. He denied that:³⁸⁵

“When I said I would prove, I meant I will prove. I meant with proper evidence, people, documents, et cetera. When I was saying that I was not referring to this case either. I am referring to the passing off cases that are starting, I am referring to the database claims that are starting and I am referring to those.”

In *Granath* on 14 September 2022, discussing proof of his claim, he said he would “*put together 90 or 100 people to put the past together*” and that he had changed lawyers because his previous representatives were not prepared to assemble the witnesses he had.³⁸⁶ At the time of that boast, he was well into the current proceedings (it was the time of the CCMC in the COPA Claim).

233. Wright has failed to bring these witnesses to Court to give evidence. With the exception of one or two witnesses – who are either economically motivated to support Dr Wright’s story or close relatives – none of the witnesses he is calling gives any direct evidence that they knew him to be Satoshi or saw the White Paper or Bitcoin source code before their

³⁸³ Transcript of trial for 9 November 2021 {O2/6/45}.

³⁸⁴ Dr Wright’s claim that hundreds of people knew somewhat flies in the face of his claim for privacy and desire not to be identified as Satoshi.

³⁸⁵ {O2/12/37} at internal p140.

³⁸⁶ {O2/11/37} at internal p142.

release. As noted above, almost all of his witnesses do no more than say that *they think* he is Satoshi or that he *could be* Satoshi, based on his range of interests and their view of his computing abilities.

234. More specifically, there are a series of individuals who, on Dr Wright's case, would be able to support his claims and who are not being called:

234.1. Witnesses from BDO: Dr Wright says that he introduced Allan Granger of BDO in 2007 to what would become Bitcoin, noting that they exchanged ideas and that Mr Granger's insights "*proved instrumental*" in refining Bitcoin.³⁸⁷ He claims that at least a few partners from BDO participated in the meeting(s) in which he outlined his Bitcoin system. None has ever given evidence or made any public comment to support Dr Wright's position. The only one who has given evidence (Mr Sinclair) has no recollection of seeing the White Paper or discussing the Bitcoin system with Dr Wright before its release.

234.2. Colleagues from Dr Wright's companies: Based on his Chain of Custody information, colleagues at De Morgan and other companies in which he worked had access to and/or worked on the papers he produced before the White Paper was released (including apparently drafts of the White Paper itself). At least some of these would surely have been able to support his case, but none has ever been called to do so.

234.3. Witnesses to support his accounts of precursor work: On Dr Wright's case, he devised specific elements of the Bitcoin system through his academic work (at Charles Sturt University, the University of Newcastle, etc.) and through his development of his Spyder and BlackNet project. On his case, the documents he produced for his LLM, his MStat degree and his Spyder / BlackNet project specifically referenced the detail of an intended digital cash scheme. Yet he does not have any witnesses who were involved with any of the various projects.

234.4. Supposed recipients of White Paper drafts: As noted above, Dr Wright (in response to an RFI request) says that he provided pre-release drafts of the White Paper to 21 people in his own name.³⁸⁸ Of the seven for whom the Court has

³⁸⁷ Wright 1, §52 {E/1/11}.

³⁸⁸ Wright 4, §49 {E/4/21}.

accounts, only two have said that they received copies, and their accounts have serious flaws. There is no explanation of the failure to call any of the others.

234.5. Those to whom he supposedly pitched Bitcoin in 2007-2009: Dr Wright claims to have pitched his prospective cryptocurrency to some specific individuals at Pornhub in 2009.³⁸⁹ He claims to have had business meetings with Microsoft in Seattle in autumn 2008, during which the company “*demonstrated interest*” in his project and discussed him receiving stock options.³⁹⁰ Yet he has never been able to produce a witness to support these accounts or provide a list of names of either these individuals.

235. Another common feature in Dr Wright’s evidence is his repeated reliance on dead individuals as being key collaborators; for example, Dave Kleiman, Gareth Williams (the British security services agent whose body was found in a bag) and Professor Rees (discussed above). He has also cited his lawyers, both living (Simon Cohen of Ontier)³⁹¹ and dead (Amanda McGovern of Rivero Mestre)³⁹² to support aspects of his story, while seeking to maintain privilege over his dealings with them. He has even blamed the government for leaking the information that originally led to him being outed as Satoshi by WIRED and Gizmodo.³⁹³

Failure to Provide Reliable Documentary Evidence

236. None of the documentary evidence adduced by Dr Wright in this case credibly backs up his story and claims. If Dr Wright was Satoshi, then one would expect him to have produced material of the following kinds:

236.1. Satoshi would be expected to have pre-issue drafts of the White Paper and Bitcoin Source Code where the metadata are consistent with creation before their public release.

236.2. Satoshi would be expected to have at least some unpublished emails from the Vistomail and GMX accounts associated, or (failing that) to have been able to

³⁸⁹ Wright 1, §126 {E/1/24}.

³⁹⁰ Wright 1, §98 {E/1/19}. See also his statement in *Granath* in relation to these meetings that “*Bitcoin could have been owned by Microsoft, horrible as that sounds*” {O2/11/12}, internal p41.

³⁹¹ Wright 4, §19 {E/4/10}.

³⁹² Wright 3 in BTC Core, §3 {E1/4/2}.

³⁹³ {L11/194/1}.

identify some Satoshi correspondents whose names were not publicly known and obtain the material from them. By contrast, Dr Wright has failed to reveal any correspondence or information about correspondence which was not already in the public domain. For example, he never revealed the correspondence which Satoshi exchanged with Mr Bohm, despite Mr Bohm being one of the very few to whom Satoshi transferred bitcoins.³⁹⁴ Where Dr Wright has attempted to give accounts on matters outside the public domain, his accounts have been discredited, as happened with his claim in *Granath* that he sent Mr Trammell source code, which Mr Trammell has denied.³⁹⁵ He has also given inaccurate accounts in relation to Mr Malmi, Dr Back, Mr Andresen and Wei Dai, as set out above.

236.3. Satoshi would be expected to have some evidence showing his connection to one or more of the associated email addresses / accounts and his web domain. As Dr Wright has been quick to point out, payment would have had to be made with conventional payment methods. However, he has failed to provide any reliable evidence of such payments.

236.4. If, as he claims, Dr Wright had shared pre-release copies of the White Paper with 21 people, then one would expect at least some of them to have retained soft or hard copies. Yet he has not been able to provide any of these copies (in soft or hard copy), even those supposedly provided to Stefan Matthews and Don Lynam.

237. Dr Wright's failure to provide evidence linking him to the Satoshi email addresses and accounts is striking. As recounted above, he boasted loudly in April 2019 of his ability to provide this proof, then in June 2019 produced the false NAB screenshots and later (after seeing the Madden Report) had to admit their inauthenticity and give a hopeless set of excuses. There is an equally remarkable sequel to this story.

238. When Dr Wright served his Defence in this action (17 May 2021), his position was that he did not have access to the Satoshi Vistomail account.³⁹⁶ However, in Wright 4, he attempted to prove that he had had access in 2019.³⁹⁷ He did this by exhibiting videos

³⁹⁴ Bohm 1, §15 {C/10/4}.

³⁹⁵ Trammell 1, §7 {C/7/2}; *Granath* evidence at {O/11/11}, internal p38.

³⁹⁶ Defence at §83(4) {A/3/24}.

³⁹⁷ Wright 4, §§20-23 {E/4/11}.

which he claimed had been filmed on a mobile phone on 7 June 2019. He said that these showed his computer screen after he had accessed the account (although they do not show him logging in). The videos also show his passport, to prove his involvement. He does not recall which phone he was using and cannot explain why the videos were not disclosed earlier (he blames both Ontier and Travers Smith for that).

239. Mr Madden examined the videos and makes findings in Appendix PM45 to Madden 2³⁹⁸ which show them to be falsified:

239.1. On the videos, the screen has footer text in the form: “*Copyright © 1996-2009 AnonymousSpeech.com...*” Mr Madden researched web archive pages using the Wayback Machine. He found that the copyright statement in the footer was updated each year, and that this form of footer would not have appeared on a live page in 2019.³⁹⁹

239.2. Although the videos showed different areas of pages on display, none of them at any point showed the address bar of the browser (which would have allowed authenticity to be checked). Without the address bar shown, an HTML document stored locally could not be distinguished from a real website being accessed. Further, although the footage showed two different web pages and some scrolling, none of the videos showed the user navigating from one page to another, clicking live links or loading pages. Instead, footage of different pages was presented on separate videos.⁴⁰⁰ COPA says that the natural inference is that the videos were presented in this way to cover up the fact that the images have been faked.

239.3. It would have been straightforward to take a page from a web archive and to edit it so that it appeared as the pages appear on the videos (including with Dr Wright shown as user).

240. There are further extraordinary features to this story. First, Dr Wright’s account in Wright 4 that he could and did access the Satoshi Vistomail account in June 2019 is flatly at odds with his evidence in the *Kleiman* proceedings, where (a) on 2 July 2019, his legal team replied to a document production request by saying that Dr Wright no longer had

³⁹⁸ {H/241/1}.

³⁹⁹ Appendix PM45, §§18-26 {H/241/7}.

⁴⁰⁰ Appendix PM45, §§8-10 {H/241/3}.

access to the Satoshi Vistomail account;⁴⁰¹ and (b) on 18 March 2020, he testified that he had not been able to access it since before 2013.⁴⁰²

241. Secondly, if Dr Wright really had been able to access the Satoshi Vistomail account in mid-2019, one would have expected him to secure critical emails (especially those not in the public domain) as supportive evidence for his claim to be Satoshi.⁴⁰³ After all, he had been preparing his claim to be Satoshi since at least 2015 and by mid-2019 he was embroiled in litigation on the subject. The notion that Dr Wright would have had access to these emails in June 2019 but not preserved any of them by any means is risible.

Failures of Cryptographic Proof – the Sartre Blog Post and its Aftermath

242. Dr Wright’s most spectacular failure of proof was the Sartre blog post. The expectation of his entire team, including Mr MacGregor, Mr Matthews and Mr Ayre, was that on 2 May 2016 Dr Wright would issue a blog including a message signed with a key associated with one of the early blocks on the Bitcoin blockchain. That expectation was shared by Mr Andresen, Mr Matonis, the media outlets to which Dr Wright had given interviews and the media consultants with whom he had worked. Instead, the “Sartre blog” post which Dr Wright issued⁴⁰⁴ provided an over-complicated explanation of a means of verifying a cryptographic signature and presented a signature which had simply been lifted from the public blockchain. As set out above, those who had been supporting Dr Wright reacted with expressions of panic and betrayal.

243. It is common ground between the parties’ experts that the Sartre blog post proved nothing. Prof Meiklejohn explains that all the main cryptographic objects in the post “*can be derived directly from the data for the [Satoshi / Finney] Transaction and the Block 9 Generation Transaction, which due to the nature of the blockchain are available to everyone.*” She adds: “*This data is thus replayed from those transactions, which... means it provides no cryptographic evidence of the possession of the associated private key.*”⁴⁰⁵ Mr Gao accepts this point.⁴⁰⁶

⁴⁰¹ {L15/133/5}.

⁴⁰² {L16/272/192}, internal p192-193.

⁴⁰³ For example, much of Satoshi’s email communication with Mr Bohm of 2009 used the Vistomail account (e.g. email of 25 January 2009 {D/93/1}). Those emails were not in the public domain before service of evidence in these proceedings.

⁴⁰⁴ {L18/257/1}.

⁴⁰⁵ Meiklejohn §§135-137 {G/2/60}.

⁴⁰⁶ Gao 1, §308 {I/2/60}; joint expert statement at §2 {Q/3/2}.

244. Dr Wright has since sought to explain away this failure of proof by two excuses: (a) that the Sartre blog post was altered between his draft and the published version; and (b) that it was never intended to provide actual proof of his claim to be Satoshi, but rather to state his principled opposition to providing such cryptographic proof.⁴⁰⁷ As to the first of those points, his own draft of the blog post (sent on 29 April 2016) was largely the same as the published version, and his own team read it as intended to provide proof by a valid signature. As to the second, it is plain from the email correspondence from the time (summarised above) that it was intended to give such proof. Even Mr Matthews can only attempt to defend Dr Wright by saying that he was committing an act of “*sabotage*” to embarrass Mr MacGregor, which is both a bizarre explanation and conflicts with Dr Wright’s own account.⁴⁰⁸
245. The aftermath of the Sartre blog post is equally striking. Over the following 48 hours (from 2 to 4 May 2016), Dr Wright’s supporters pressed him to provide some form of objectively verifiable proof in one of various forms. As explained above, on 3 May 2016 the blog post was issued in his name entitled “*Extraordinary Claims Require Extraordinary Proof*”,⁴⁰⁹ promising over the following days to post a series of pieces to “*lay the foundations for [his] extraordinary claim*”, including “*transferring bitcoin from an early block*”. The post concluded: “*I will present what I believe to be ‘extraordinary proof’ and ask only that it be independently validated.*” However, that proof never came.
246. It was arranged that Mr Cellan-Jones and Mr Andresen would transfer Bitcoin to addresses associated with Satoshi, and that they would be sent back. Mr Cellan-Jones explains how on 4 May 2016 he sent 0.01701 Bitcoin (at a current valuation, worth around £600) to the address used in the first Bitcoin transaction with Hal Finney. This sum was never returned, and Dr Wright failed to follow up on what Mr Cellan-Jones describes as a “*simple and comprehensive way for Wright to prove that he was Satoshi*”.⁴¹⁰ As recounted above, Mr Andresen made a similar transfer, which was also never returned.
247. Dr Wright did not provide any other form of proof. In the two days between 2 and 4 May 2016, he told his team that he was taking steps to gain access to Satoshi’s PGP key to

⁴⁰⁷ Wright 1, §217-220 {E/2/37}.

⁴⁰⁸ Matthews 1, §104 {E/5/22}.

⁴⁰⁹ {L13/262/1}.

⁴¹⁰ Cellan-Jones §16, {C/5/4}.

sign a message with that (something he now says is impossible or infeasible). He dodged their questions, while trying to divert them with a short article about the Genesis Block (which anyone could have written from publicly available information).⁴¹¹ In the end, he did not provide any proof and the “big reveal” project fell apart.

248. The natural conclusion to be drawn from this remarkable sequence of events is that Dr Wright did not provide proper proof because he could not do so. The suggestion that he took a principled stand against offering cryptographic proof is contradicted by (a) the fact that he engaged in the various private signing sessions with the aim that they should be fully written up in articles and (b) the fact that his associates (not just Mr MacGregor, whom he now seeks to cast as a villain) believed that he had committed to provide such proof. The truth is that he came up with this excuse after the event.

Failures of Cryptographic Proof – Destruction of the Hard Drive and no Proof Since 2016

249. Dr Wright claims that, after 4 May 2016, he destroyed the hard drive(s) containing the private keys used in the signing sessions and that he has not had access to them since then. His accounts on this subject are inconsistent. In his evidence for these proceedings, he says he destroyed a single hard drive in around May 2016 at his home in Wimbledon and that he threw the hard drive with enough force to shatter the glass platters in the hard drive.⁴¹² As for his motive, he refers to his ASD and says that a feeling of betrayal by Mr MacGregor caused an emotional response in which he acted impulsively.⁴¹³
250. By contrast, in his evidence in the *Granath* case, he claimed that he had “*the first 12 keys and a number of key slices*” on two drives (a hard drive and a USB stick) and that he destroyed both, one by hitting it with a hammer and one by stomping on it with his foot.⁴¹⁴ He is not only inconsistent on the method of destruction. In his *Granath* evidence, he said that his motive was to “*make sure that judges and courts understand that Bitcoin is not encrypted and it can be seized, frozen and accessed*”. He said that he believed that destroying the drives had been the only way to prove this. This account of a principled motivation which he still held in September 2022 is very different from the account of an action on impulse triggered by a feeling of betrayal by Mr MacGregor.

⁴¹¹ See email of 4 May 2016 at {L13/331/1}.

⁴¹² Wright 4, §33 {E/4/15}.

⁴¹³ Wright 4, §34 {E/4/16}.

⁴¹⁴ {O2/11/29}, internal pages 108-110.

251. Dr Wright’s pleaded stance in this case is that he no longer has access to the keys associated with the early blocks in the Bitcoin blockchain. In *Granath* (in September 2022), he said that he could probably gain such access: “*In theory, I could probably track down Uyen [Nguyen] and get other people and do other thing that might give access, but I have not even tried to see whether I could do that*”.⁴¹⁵ He insisted that he would not do so. If, since September 2022, he has tried and failed to gain access, it is surprising that he has not given details in his statements. If he claims that he has not tried, or has chosen not to access the keys, that is simply implausible, not least in view of the pressure which Mr Ayre applied in his email of September 2023.⁴¹⁶

Failures of Cryptographic Proof – Overview of the Signing Sessions

252. Dr Wright has never publicly undertaken a signing session or publicly posted a signature that would prove his possession of any of the keys associated with Satoshi. What he instead sought to do was conduct such sessions behind closed doors, with selected individuals who signed non-disclosure agreements (Mr Matonis, Mr Andresen and a few journalists). As Prof Meiklejohn concludes: “*In my view, the evidence provided in the signing sessions cannot be considered as reliable in establishing possession of the private key(s) corresponding to the public key(s) used*”.⁴¹⁷ In the joint statement, Mr Gao agrees with almost all parts of Prof Meiklejohn’s report concerning the signing sessions, including with that conclusion paragraph.⁴¹⁸ As Prof Meiklejohn explains, the signing sessions omitted key steps which would have been required to make them reliable.

253. The flaws in the signing sessions are telling. For those with Mr Matonis and the journalists, Dr Wright used just his own laptop and adopted a method which would have been very easy to fake. The session with Mr Andresen was a little different, because he insisted on verification being performed on a computer other than Dr Wright’s own. However, Mr Andresen’s evidence in *Kleiman*, which was given with reference to earlier notes, makes clear that various steps were not taken to ensure reliability of the session. Furthermore, it is striking that Dr Wright’s evidence disagrees with Mr Andresen’s on precisely those critical points.

⁴¹⁵ {O2/11/31}, internal page 119.

⁴¹⁶ {L19/212/6}.

⁴¹⁷ Meiklejohn §131 {G/2/58}.

⁴¹⁸ Experts’ joint statement at §2 {Q/3/2}.

254. In Wright 2, Dr Wright gives a complex explanation of the signing sessions, setting out various technical measures he took. Prof Meiklejohn disagrees with a number of technical points Dr Wright makes:

254.1. Dr Wright says that the first stage in verification entails installing the Bitcoin Core software.⁴¹⁹ Prof Meiklejohn explains that that software was not needed in relation to the keys which were to be signed, because the relevant coin generation transactions for the early blocks were P2PK transactions so that they contained the full public keys.⁴²⁰

254.2. Dr Wright claims that he underwent the time-consuming exercise of downloading the entire Bitcoin blockchain as a preliminary to each signing session.⁴²¹ Prof Meiklejohn explains that this is unnecessary. For a reliable signing, all one requires are the relevant keys or addresses and message. Downloading the blockchain is time-intensive and does not bolster the security of the process.⁴²²

254.3. Dr Wright says that, for the signing sessions with Mr Matonis and the journalists, he had a single laptop but used the Windows laptop itself for signing and a virtual machine running Linux for verification. He adds that this element was “essential” for integrity of the exercise.⁴²³ Prof Meiklejohn explains that that is unnecessary and adds nothing to the reliability of the exercise, since it is only the verification setting that needs to be assured to avoid corruption falsely indicating success.⁴²⁴

254.4. Dr Wright insists that the procedure he used, with a second system or computer used for verification, avoids the risk of exposing the private key.⁴²⁵ Prof Meiklejohn disputes that this procedure has such a benefit over other methods.⁴²⁶ Importantly, she explains that one can give out a signature freely and let somebody else verify it on their computer without any risk of compromising the private key. This is important because it shows that Dr Wright adopted complex methods based on a spurious risk of key compromise, when all he needed to do

⁴¹⁹ Wright 2, §7-9 {E/2/4}.

⁴²⁰ Meiklejohn §114 {G/2/47}.

⁴²¹ Wright 2, §9 {E/2/5}.

⁴²² Meiklejohn §116 {G/2/48}.

⁴²³ Wright 2, §12 {E/2/6}.

⁴²⁴ Meiklejohn §115 {G/2/47}.

⁴²⁵ Wright 2, §21 {E/2/8}.

⁴²⁶ Meiklejohn §118 {G/2/49}.

was sign a message with the private key relating to an identified block and hand over the signature.

Failures of Cryptographic Proof – the Signing Sessions with Mr Matonis and the Journalists

255. As noted above, Dr Wright says that he used his own Windows laptop which was also running a Linux virtual machine. Bitcoin Core was installed and the whole blockchain downloaded.⁴²⁷ Dr Wright then claims that he signed a message of a speech by Jean-Paul Sartre which was stored in a file named “Sartre.txt” using the private key corresponding to the public key used in the coin generation transaction in block 9. He cites the command (starting “bitcoin-cli”) which he used.⁴²⁸ He claims that he then copied the signature across to the virtual machine and used a further command on the Bitcoin Core software to verify it.⁴²⁹
256. As Prof Meiklejohn explains, it would have been simple to write programs to (a) output a random string in response to the signature command; and (b) output “true” in response to the verification command.⁴³⁰ Dr Wright does not dispute that evidence. There is no evidence that Mr Matonis or any of the journalists took any steps to prevent the session being staged in this way. Of course, Dr Wright now insists that he did not stage it, and that he inputted the full command path at each stage. However, there is no independent assurance at all. Given Dr Wright’s claimed expertise, if he had wanted to conduct reliable proof sessions, he could have done so very simply (most obviously by just handing over a signed message on a clean USB stick). As with the Sartre blog, he adopted an over-complex process which proved nothing.
257. Prof Meiklejohn also notes that it is surprising, from a security perspective, for Dr Wright to have repeatedly connected his computer (containing these private keys) to the internet, given the ease of cold storage solutions.⁴³¹ On his account, he took *real* security risks while adopting complex steps to avoid *spurious* risks.

⁴²⁷ Wright 2, §§25 and 32 {E/2/9}.

⁴²⁸ Wright 2, §§26-28 {E/2/9}.

⁴²⁹ Wright 2, §§29-31 {E/2/9}.

⁴³⁰ Meiklejohn §124 {G/2/51}.

⁴³¹ Meiklejohn §125 {G/2/52}.

Failures of Cryptographic Proof – the Signing Session with Mr Andresen

258. The signing session with Mr Andresen was different from the others because Mr Andresen wanted the signed message to be verified on his computer and Dr Wright’s team agreed to a laptop being bought for the purpose. This session involved Dr Wright signing a message on his laptop, transferring the signature to the new laptop and verifying the signature on that laptop. So much is common to Dr Wright’s account and Mr Andresen’s (which was given in *Kleiman* by reference to notes in the form of a Reddit exchange with another person⁴³²).
259. In Wright 2, Dr Wright gives his version.⁴³³ He claims that the new laptop was set up by Mr Andresen, and that Mr Andresen installed Windows, connected to the hotel’s Wi-Fi network and downloaded Electrum software directly from the official website. Dr Wright says that when downloading Electrum, Mr Andresen verified the integrity of the software by comparing its hash value to the one provided on the website. Dr Wright then describes that, for each of block 1 and 9, he produced a signed message on his laptop; that he transferred it via USB stick to the new laptop; and that he then performed the verification with the Electrum software on the new laptop while Mr Andresen watched. Dr Wright recalls that the process initially failed, but only because the original message had been typed into Electrum incorrectly. The error was then corrected and the signature was verified.
260. Mr Andresen recalls that a hot-spot might have been used for internet access,⁴³⁴ a detail Dr Wright accepted in his *Granath* evidence.⁴³⁵ Importantly, Mr Andresen is also clear that Dr Wright downloaded and installed the software on the new laptop, including the Electrum software.⁴³⁶ Mr Andresen could not recall having verified that the Electrum software had the HTTPS security certificate from the website. In *Kleiman*, when asked whether he had verified the hash digest of the download against anything he had brought with him, Mr Andresen said that he had not done so, and he did not suggest that he had verified the hash digest by any other means.⁴³⁷ Mr Andresen recalled that the message signed was “*Gavin’s favourite number is 11 – CSW*”. The Reddit notes indicate that on

⁴³² The deposition transcripts are at {E/17/1} and {E/18/1}. The Reddit notes are at {L19/217/1}.

⁴³³ Wright 2, §§33-41 {E/2/10}.

⁴³⁴ {E/17/76}.

⁴³⁵ {O2/11/21}.

⁴³⁶ {E/17/73}: “*Craig downloaded and installed the software*”.

⁴³⁷ {E/17/76}.

the first try Mr Andresen had omitted “– CSW”, after which the verification failed, but that Dr Wright then identified the omission.⁴³⁸

261. Prof Meiklejohn addresses the possibility of this session being faked. She explains that there are a number of ways in which it would have been possible for Dr Wright to do this by use of software. These include: (a) downloading a non-genuine version of Electrum wallet software; (b) downloading genuine Electrum software but running malware on the new laptop to interfere with its operation; or (c) altering the download of Electrum or introducing malware through internet connection being compromised (e.g. through a device used to provide a hotspot.⁴³⁹ It is telling that Dr Wright’s account diverges from Mr Andresen’s on the key points of (i) who set up the laptop; (ii) who downloaded Electrum; and (iii) whether there was any verification of the Electrum software.
262. Once again, it is also important to note that a reliable private signing could have easily been performed much more simply and without any proper concern about allowing Mr Andresen access to the private keys. All that was needed was a clean USB stick. Dr Wright could have signed a message on his computer, using his private key associated with the public key for block 9. That signed message could have been passed via a clean USB stick to Mr Andresen, who could then have run the verify algorithm on his own laptop to determine if it was genuine. The adoption of Dr Wright’s complex process (involving the purchase of a new computer) in favour of that simple process speaks volumes. The proper inference is that the complex process was adopted because it could be staged.

(3) The Implausible and Inconsistent Nature of Dr Wright’s Accounts

263. There are numerous elements of Dr Wright’s narrative which are inherently implausible and/or which reveal inconsistency between accounts he has given or inconsistency between his version and provable fact. The examples are too numerous to be set out exhaustively here, but many are given in the section above addressing Dr Wright’s claim to be Satoshi. Taken together, they demonstrate the fantasy which he has put forward. A few instances are set out below, while further examples will be explored in cross-examination.

⁴³⁸ {L19/217/4}.

⁴³⁹ Meiklejohn §130 {G/2/56}.

BlackNet and Spyder Projects

264. Dr Wright has sought to tie the origins of Bitcoin to his Spyder and BlackNet projects, when in fact those projects had nothing to do with cryptocurrency. As noted above, they were projects based on IT security work to create a secured network. Dr Wright has sought retrospectively to add an extra phase to the projects, involving “*crypto credits*”.
265. In February 2019, he posted on Twitter a screenshot of an abstract from his Project BlackNet paper, with the comment: “*My stupidest mistake was going to the Australian government in 2001 and filing this shit*”. The abstract shown included language matching that in the abstract of the White Paper. However, the text included changes which had been made between the early drafts of the White Paper which Satoshi shared and its later iteration. COPA duly pleaded this point. Dr Wright replied in his Defence that he had filed Project BlackNet papers with AUSIndustry in 2001 and in 2009/10; that only the later versions included text matching the White Paper; and that his Twitter post had depicted one of those later versions. However, this account conflicts with the plain meaning of the Twitter post, which is that the document shown in the screenshot was filed in 2001.
266. As explained above, in these proceedings Dr Wright has doubled down on his account that his work on BlackNet involved creating a peer-to-peer transaction system closely similar to Bitcoin. He has sought to support it with project proposal documents. However, there are a series of problems with this story. First, as noted above, the key reliance document (ID_001379⁴⁴⁰) is not authentic to its stated date of 2002. Secondly, there is at least one apparently authentic 2002 version in disclosure, which omits the supposed “*crypto-credits*” fourth phase and all the language relating to Bitcoin concepts. Thirdly, Dr Wright’s filings with the ATO from 2009 show that even by that date Project BlackNet did not include the additional phase.⁴⁴¹ Fourthly, when one reads the forged documents such as ID_001379, the added elements are plainly incongruous. The (false) Abstract section and the (apparently genuine) Overall Objective section do not match

⁴⁴⁰ {L1/79/1}.

⁴⁴¹ As noted above, see the supposed IP sale agreement between Dr Wright and Information Defense Pty Ltd as filed with the ATO {L4/462/1}, which referred to a De Morgan R&D Plan of which there are many versions in disclosure (e.g. {L1/101/1}).

each other. The detailed budget cites the third phase as final and includes no costing for the supposed fourth phase.

Supposed Collaboration with Prof Wrightson and Dr Furche

267. Dr Wright's false account of collaboration with Prof Wrightson and Dr Furche during his MStat course at Newcastle University (NSW) is another striking example. In his "Fully Peer-to-Peer" blogpost of June 2019,⁴⁴² he said that studying at this university gave him access to people deeply versed in monetary systems, notably Prof Wrightson and Dr Furche. He says that Prof Wrightson knew about Wei Dai's work, while Dr Furche put him onto Hal Finney and Adam Back. He claims that their research group had a lot of resources and that he read their patents and papers on transfer instruments (hyperlinking a 1988 patent paper).

268. This account is riddled with falsehoods. Based on the evidence of Prof Wrightson and Dr (now Prof) Furche, they had both left the University and the research group cited had ceased working some years before Dr Wright's arrival and his claimed dealings with them.⁴⁴³ Prof Wrightson does not know of Wei Dai, while Prof Furche has never heard of Adam Back.⁴⁴⁴ Their research group at the University did not have the suggested resources, had never lodged a patent application and had no connection to the paper hyperlinked to Dr Wright's post.⁴⁴⁵ In addition, neither has any recollection of coming across Dr Wright at the University. Finally, the real Satoshi cannot have had these rewarding discussions about Wei Dai with Prof Wrightson in 2005-2009 because (as pointed out above) Satoshi did not know about Wei Dai's work until directed to it by Adam Back in August 2008.

Early Events in the History of Bitcoin

269. Patch Tuesday: In a blog post of 6 April 2019⁴⁴⁶ (and in other public statements⁴⁴⁷), Dr Wright has claimed that Microsoft Patch Tuesday (the monthly issuing of software patches) caused a shut-down of the Bitcoin network directly after the creation of the

⁴⁴² {L15/88/2}.

⁴⁴³ Furche 1, §§4-8 {C/13/2} and §§27-31 {C/13/6}; Wrightson email at {C/18/11}.

⁴⁴⁴ Furche 1, §§36-38 {C/13/7}; Wrightson email at {C/18/11}.

⁴⁴⁵ Furche 1, §§40-42 {C/13/8}; Wrightson email at {C/18/11}.

⁴⁴⁶ "Two steps forward, one step back" 6 April 2019 {L14/420/2}.

⁴⁴⁷ "Dr Craig Wright explains the origins of Bitcoin" 24 April 2019 {O4/25/25}; "Coingeek Toronto Fireside Chat" 19 June 2019 {O4/12/14}; "Satoshi's Vision" (June 2019 book) {L15/96/14}.

Genesis block (which was on 3 January 2009). He has claimed that he addressed this by building a domain in the week between 3 and 10 January 2009. The problem with this story is that, in January 2009, Microsoft Patch Tuesday was on 13 January.⁴⁴⁸

270. Upload.ae: In an email from Satoshi to Wei Dai on 22 August 2008 which has long been public,⁴⁴⁹ Satoshi told him that he could download a pre-release draft from an “upload.ae” address. Dr Wright has tried to appropriate this detail as part of his narrative, by saying repeatedly that this was a site he had and operated in Melbourne.⁴⁵⁰ In Wright 4, answering RFI questions, he says: “*I also operated a secondary server in Melbourne, known as upload.ae, to mirror some of the directories.*” In fact, upload.ae was a free file hosting service⁴⁵¹ that was owned in 2009 by one Faisal Al Khaja.⁴⁵²
271. Satoshi’s Bitcoin transactions: In his interview with GQ in late April 2019, Dr Wright was asked if he had moved any bitcoins from the early blocks linked to Satoshi. He replied: “*I haven’t moved them. I have sent them to Hal Finney and Zooko [Wilcox O’Hearn], and that was it. Full stop.*”⁴⁵³ It is well-known that Satoshi sent Bitcoin to Mr Finney, but the statement was otherwise wrong. First, Mr Wilcox-O’Hearn, who is credited with having written the first blog post about Bitcoin, did not receive any Bitcoin from Satoshi. He points out that even though he had blogged about Bitcoin, he did not actually use it until years later.⁴⁵⁴ Secondly, Satoshi sent 100 bitcoin, unsolicited, to Nicholas Bohm.⁴⁵⁵ That was not a matter of public knowledge before exchange of evidence in these proceedings, which explains Dr Wright’s omission. Satoshi also sent 32.51 and 50 Bitcoin to Mike Hearn on 18 April 2009.⁴⁵⁶
272. Bitcoin described as a cryptocurrency: Dr Wright insists that Bitcoin is not a cryptocurrency and that it is wrong to describe it as such. He pleads that point in his Defence⁴⁵⁷ and he makes it in his first statement in the BTC Core Claim.⁴⁵⁸ He insisted

⁴⁴⁸ See for instance the following articles: {L4/60/1}; {L4/262/1}; {L18/316/1}.

⁴⁴⁹ {L3/195/1}.

⁴⁵⁰ See “*Coingeek Toronto Fireside Chat*” 19 June 2019 {O4/12/6}; Dr Wright’s *Kleiman* trial evidence on 22 November 2021, internal p99-100 {P/10/99}.

⁴⁵¹ {L3/191/1}.

⁴⁵² {L17/379/21}.

⁴⁵³ See transcript at {O4/23/5}.

⁴⁵⁴ Wilcox-O’Hearn §§7-8 {C/6/3}.

⁴⁵⁵ Bohm §15 {C/10/4}.

⁴⁵⁶ {D/505/08}.

⁴⁵⁷ Defence at §78 {A/3/23}.

⁴⁵⁸ Wright 1 in BTC Core at §49(6) {E1/1/13}.

upon it in his evidence in *Granath*⁴⁵⁹ and *McCormack*,⁴⁶⁰ and has made the point in postings repeatedly and with vehemence.⁴⁶¹ This is part of his effort to challenge features of Bitcoin Core and promote BSV. However, since taking this line in public, he has been confronted with the difficulty that Satoshi prominently described Bitcoin as a cryptocurrency in a post of 6 July 2010.⁴⁶² He has tried to deal with this by insisting that that post was not written by Satoshi and has blamed Martti Malmi for writing it.⁴⁶³ However, Mr Malmi gives evidence that the post was written by Satoshi, and he exhibits a previously unpublished email from Satoshi to prove it.⁴⁶⁴ It is also telling that, in submissions to the ATO in 2013 – prior to having adopted his Satoshi lie – Dr Wright repeatedly described Bitcoin as a “*cryptocurrency*”.⁴⁶⁵

273. Bitcoin’s debt to Hashcash: Dr Wright says that, before releasing the White Paper, he communicated with Adam Back (the creator of Hashcash).⁴⁶⁶ The fact that Satoshi had communications with Dr Back was in the public domain, because Satoshi’s emails to Wei Dai were published, and the email of 22 August 2008 noted that Dr Back had drawn Satoshi’s attention to Wei Dai’s work.⁴⁶⁷ However, the full content of Mr Back’s communications with Satoshi was not public knowledge before this case. In Wright 1, Dr Wright maintains that Mr Back was dismissive of Satoshi’s Bitcoin idea.⁴⁶⁸ He also says that Bitcoin’s proof-of-work system did not draw upon Mr Back’s Hashcash system and that it derived instead from the work of Tuomas Aura. He asserts that the White Paper only referenced Hashcash because he had not been able to make contact with Prof Aura.⁴⁶⁹ Dr Wright has said this before, in an article of 2019 where he said that Bitcoin was not even similar to Hashcash and that its proof-of-work “*came from the Aurora [sic] paper*”.

⁴⁵⁹ {O2/11/9}, internal p28; {O2/11/19}, internal p68.

⁴⁶⁰ {O2/12/28}, internal p106.

⁴⁶¹ See Slack posts at {L17/53/10}, {L17/53/14}, {L17/53/23}, {L17/53/24}, {L18/121/30} and {L18/121/50}.

⁴⁶² {L5/196/1}: “*Announcing version 0.3 of Bitcoin, the P2P cryptocurrency!*”

⁴⁶³ See transcript of interview with Ryan Charles on 25 January 2021 at {O4/5/14}; Dr Wright’s evidence in *Granath* {O2/11/24}, internal p90.

⁴⁶⁴ {D/369/1}.

⁴⁶⁵ See Coin-Exch Pty Ltd Response to Request for Additional Information: {L8/277/4} and {L8/277/15}.

⁴⁶⁶ Wright 1, §93-94 {E/1/19}.

⁴⁶⁷ See published copy of the email at {L3/195/1}.

⁴⁶⁸ Wright 1, §93 {E/1/19}.

⁴⁶⁹ Wright 1, §94 {E/1/19}.

274. However, Satoshi’s original post about Bitcoin stated that “*New coins are made from Hashcash style proof of work*”,⁴⁷⁰ and the White Paper itself said (under “Proof-of-Work”) that “*we will need to use a proof-of-work system similar to Adam Back’s Hashcash*”.⁴⁷¹ The idea that Satoshi would have made those statements even though Bitcoin’s proof-of-work system was not derived from that of Hashcash is implausible. Furthermore, Dr Wright’s current position contradicts both (a) what his filings with the ATO said about Bitcoin⁴⁷² and (b) what Mr O’Hagan in “*The Satoshi Affair*” recorded Dr Wright saying in 2015/16.⁴⁷³
275. Computing set-up for early Bitcoin mining: Dr Wright’s story about the early computing power involved in his claimed early Bitcoin mining is wrong at a technical level. He claims that, when mining the first blocks, his electricity consumption was very high, amounting to thousands of Australian dollars, due to running computer systems in 69 racks as well as three laptops and four desktops.⁴⁷⁴ However, Prof Meiklejohn points out that (a) it was not necessary to run such a set-up to mine Bitcoin in 2009/10 and (b) that Dr Wright could not have been running a set-up on this scale, because the added computing power on the network would have increased the difficulty level of the target hash above the levels recorded.⁴⁷⁵

Further Submissions on Dr Wright’s Credibility

276. First, Dr Wright has often sought to explain his behaviour or accounts by reference to his ASD. COPA accepts the position of the experts that the Court should not make negative findings about him based only on demeanour during cross-examination (e.g. poor eye contact, occasional displays of annoyance, not taking non-verbal cues and argumentative appearance). It should be apparent from the contents of this skeleton that COPA’s focus is on what Dr Wright has done and said, not his presentation. As Chamberlain J said in *McCormack*,⁴⁷⁶ the problem with Dr Wright’s case is not the way his story is told or in what details he omits, but rather that what he does say is riddled with falsehoods.

⁴⁷⁰ Post of 31 October 2008 {L3/278/1}.

⁴⁷¹ {L5/26/3}.

⁴⁷² {L8/277/15}.

⁴⁷³ {L13/492/24}.

⁴⁷⁴ Wright 1, §116-117 {E/1/22}.

⁴⁷⁵ Meiklejohn §74 {G/2/32}.

⁴⁷⁶ Main judgment at §109 {L17/457/24}.

277. Secondly, Dr Wright has a propensity for changing his story after some aspect of his account is debunked. The history of the *McCormack* case offers a good parallel, in that his pleading and first witness statement advanced a case of being invited to numerous conferences and the invitations being withdrawn, but then he was forced to accept that his evidence was wrong.⁴⁷⁷ The Court will also be aware of changes taking place in the *Tulip Trading* case, notably in relation to the purchase order relied upon by Dr Wright to support ownership of the 1Feex address.⁴⁷⁸ In closing submissions in the *Kleiman* case, his own advocate began by accepting Dr Wright’s frequent self-contradictions.⁴⁷⁹
278. Thirdly, both in this case and in others, Dr Wright denies any lies or wrongdoing, even when faced with the clearest evidence. He has never accepted the findings of dishonesty made against him in *Ryan*, *McCormack* and *Kleiman*. Despite the many findings by the ATO that he forged documents, and despite Clayton Utz having resigned as his lawyers because of his forgeries, and despite the agreed evidence of manipulation of his documents in *Kleiman*, *Granath* and these proceedings, he recently insisted in his fifth statement in the *Tulip Trading* case that he had never falsified a document.⁴⁸⁰
279. Fourthly, he has sought to blame many others for the forgeries which have been found: disgruntled former employees; Ira Kleiman; COPA members and/or BTC Core; Ms Nguyen; the pseudonymous Reddit correspondent. In most cases, the motivation for them to plant forged documents is opaque and involves an elaborate sting operation. As noted above, Dr Wright’s story also involves repeated and implausible attempts to blame his former lawyers, especially for supposedly serious failures to disclosure documents sooner on his behalf. These aspects of his narrative are telling for his credibility.
280. Fifthly, Dr Wright’s cover stories are often simply incredible. Some good examples are the following: (a) the story he told in the *Kleiman* case of putting over 1 million Bitcoin beyond his reach and waiting on the prospect of a mysterious “*bonded courier*” bringing decryption keys in 2020 (vividly recounted in Judge Reinhart’s judgment⁴⁸¹); (b) the

⁴⁷⁷ Main judgment at §§93-94 {L17/457/21}. Note that this submission does not depend on the findings of Chamberlain J on any issues in dispute in the case. It relies solely on the judgment as a record of what happened in the case.

⁴⁷⁸ See Elliss 1 in *Tulip Trading*, at §§47-50 {S1/1.24/17}; and Elliss 4 in *Tulip Trading*, at §10 {S1/1.27/3}.

⁴⁷⁹ {L17/333/113}: “he said at some times black and at some times he said white in front of you. All right? Black and white. But so there it is. It’s a pile of black / sometimes white contradictions.”

⁴⁸⁰ See statement at §60 {S1/1.13/20}.

⁴⁸¹ {L15/207/19}. Again, COPA does not need to rely upon the Judge’s findings, but merely on the judgment as a record of Dr Wright’s story (which the Judge summarised in a one-word sentence: “*Inconceivable*”).

view that he was outed as Satoshi to WIRED and Gizmodo by the Australian government; (c) his attempt to explain away his extensive, word-for-word plagiarism of long passages of Ms Pearson's work as merely a matter of common words being reused or removing reference to other authors' work to save space;⁴⁸² (d) his account of Ontier advising him that the Overleaf files did not need to be, and could not be, disclosed despite their being (on his case) very clearly relevant (the account later rejected by Ontier).⁴⁸³

Relief Claimed

281. Whilst this trial is primarily concerned with determining the factual Identity Issue, COPA in its claim seeks specific relief. This relief comes in two forms: (a) declarations that Dr Wright is not the author of and does not own copyright in the White Paper; and (b) injunctive relief to prevent Dr Wright from maintaining his false claim and asserting it.⁴⁸⁴ COPA sets out its broad submissions here, but it would intend to expand upon them at a form of order hearing.
282. The first two declarations claimed, namely that Dr Wright is not Satoshi and that Dr Wright is therefore not the owner of the copyright in the White Paper, are both sought for the UK and for all signatories to the Berne Convention. The third declaration, that any use of the White Paper would not infringe copyright owned by Dr Wright, is only sought for the UK. The reason for this difference is that infringement can have differing tests, even within Berne Convention countries, and so to avoid complications that third declaration is only sought for the UK. COPA also seeks dissemination of judgment, which in the usual way will be addressed at the form of order hearing.
283. Dr Wright's Defence denies that the declarations should be granted and raises a quasi-jurisdictional objection.⁴⁸⁵ Of course, the latter objection cannot stand, as no challenge to jurisdiction was ever made. Meanwhile, none of his evidence addresses the merits of granting the declarations in the event that he is found not to be Satoshi. As regards the injunctions sought, Dr Wright's Defence threatened an application to strike out the claim, but Dr Wright never followed through on that threat.⁴⁸⁶ The sole substantial defence

⁴⁸² See Wright 1 in the Tulip Trading case, at §§97-98 {S1/1.9/28}.

⁴⁸³ {M/2/691}.

⁴⁸⁴ See Re-Re-Re-Amended Particulars of Claim, §§68-71 {A/2/21}.

⁴⁸⁵ Re-Amended Defence, at §§88-91 {A/3/28}.

⁴⁸⁶ Re-Amended Defence, at §93 {A/3/28}.

raised to the injunctions is that they would infringe Dr Wright's Article 10 right to free expression.

Legal Principles for Declaratory Relief

284. The legal principles for declaratory relief in the present context are set out in *Copinger and Skone James on Copyright (18th ed.)* at §21-231. See also more generally White Book 2023 Notes at §40.20.2. Declaratory relief is discretionary and the Court will be concerned to establish that there is some utility to granting it. Declarations of non-infringement may be granted where there is a genuine commercial reason for seeking the declaration.

Justification for Declaratory Relief

285. There is a need for each of the three declarations to be granted. The first declaration sought (that Dr Wright is not the author of the White Paper) is required so that the order determines the Identity Issue. The second declaration (that he is not the owner of the copyright in the White Paper) is needed because it will provide the actual defence to any claim to copyright infringement, since without title Dr Wright cannot sue. The third declaration (that any use by COPA of the White Paper would not infringe any copyright owned by Dr Wright) is needed to avoid any claims of infringement being levelled at COPA or its Represented Parties by any other means. The granting of these declarations would allow those bound by the judgment to rely upon their effects as against Dr Wright and his privies.

286. The utility of the declarations sought is equally clear. As set out above, Dr Wright has gone to great effort to assert his claims, including through a campaign of litigation. COPA was compelled to bring this action after its members faced threats of claims for copyright infringement. Before COPA issued these proceedings, Dr Wright had only brought a comparable claim against Cobra (persons unknown, against whom he obtained judgment in default), in addition to his various defamation claims. Since COPA commenced this action, he has brought the various claims outlined above.

287. The effect of his claim against Cobra was that the bitcoin.org domain name no longer allows downloading of the Bitcoin (BTC) software, as the blockchain itself contains the White Paper.

Legal Principles for Injunctive Relief

288. The following principles apply to the discretion to grant injunctive relief in the context of infringement of IP rights. Any relief should be fair, equitable and not unnecessarily complicated or costly. It should be effective, proportionate and dissuasive, and applied in such a manner as to avoid the creation of barriers to legitimate trade and to provide for safeguards against their abuse: *Merck v Merck Sharp & Dohme Corp* [2017] EWCA Civ 1834 at §307. These principles should be taken into account in relation to the granting of an injunction restraining someone from claiming or seeking to enforce IP rights in circumstances where declaration of non-infringement has been granted.
289. The granting of any injunction must be proportionate and have regard to any other competing considerations, including any Article 10 rights of the other party under the European Convention on Human Rights: see *Merck v Merck Sharp & Dohme Corp* at §310. Specifically, section 12 of the Human Rights Act 1998 (“HRA”) requires the Court to have regard to the significance of the right to freedom of expression.
290. The normal position in IP cases is that, where there has been an infringement, an injunction usually follows, absent clear undertakings or some other reason why that is not going to happen: see *Cantor Gaming v Gameaccount Global Limited* [2007] ECC 24 at §101-106. That conclusion was based on a consideration of the cases cited below.
291. The approach in copyright cases was set out by the Master of the Rolls, Lord Woolf, giving the judgment of the Court of Appeal in *Phonographic Performance Ltd v Maitra* [1998] FSR 749 at 771:
- “... where a person establishes infringement of copyright and a threat to continue infringement, an injunction will in the ordinary case be granted without restriction. ... But the court, when granting an injunction, is still required to exercise a discretion and in so doing there could be circumstances where restriction or refusal of an injunction would be warranted.”
292. In relation to patents, the Court of Appeal in *Coflexip SA v Stolt Comex Seaway MS Ltd* [2001] RPC 182 put the position as follows at §6-7:
- “... whenever a court at the end of a trial grants permanent injunctive relief, the purpose should be to give effect to its judgment on liability ... The injunction granted should protect the plaintiff from a continuation of the infringements of his rights by the threatened activities of the defendant. But the injunction must also be fair to the defendant.”

“... Normally, when a defendant has infringed, the court will assume it is not a one-off activity and will grant an injunction to stop repetition. This course is not inevitable. In a few cases courts have concluded that even though infringement has occurred, no future threat exists. In such cases, injunctive relief has been refused ...”

293. In *Cantor Gaming*, Daniel Alexander QC (sitting as a Deputy High Court Judge) said that the same principles of injunctions (set out in *PPL v Saibal* and *Coflexip*) must apply where a person establishes that there has been a breach of contract which prohibits an act akin to an infringement of an IP right: §104. COPA submits that a comparable approach must also apply when a party establishes non-infringement and the need for a declaration to resolve the issue.

294. The Court may grant an injunction in support of a declaration of non-infringement, as was decided in *Samsung Electronics (UK) Ltd v Apple Inc* [2013] FSR 134 at §§70-75. There, the Court of Appeal upheld the granting of a publicity injunction requiring Apple to publish on its website and in the press an order that there had been no infringement. As to both jurisdiction and the applicable test, Sir Robin Jacob said this at §75:

“I have no doubt that the court has jurisdiction to grant a publicity order in favour of a non-infringer who has been granted a declaration of non-infringement. A declaration is a discretionary, equitable, remedy. The injunction is an adjunct to the declaration. It will not always be appropriate to grant it. Whether or not it is depends on all the circumstances of the case – as I said earlier where there is a real need to dispel commercial uncertainty. It is that test I propose to apply here.”

295. The jurisdictional basis for the injunction was s.37(1) of the Senior Courts Act 1981, providing that an injunction may be granted “*in all cases where it appears to the court to be just and convenient.*” The situations in which such injunctions can be granted are not confined to exclusive categories by judicial decision, and the Court may grant an injunction in a novel situation to avoid injustice: see *Mercedes-Benz AG v Leiduck* [1996] AC 284 at 308 (cited in *Samsung* at §73).

296. In deciding whether to grant injunctive relief in a case such as the present, the Court will balance the competing interests. These will include any effects of refusal of the injunction on activity which would harm legitimate business activities. See *Heythrop Zoological Gardens v Captive Animals Protection Society* [2017] FSR 242 at §§56-60 (a case addressing the balancing exercise on an interim injunction basis, where the threshold for an order impinging on Article 10 rights is higher by virtue of s.12(3) of the HRA).

297. The time at which the question of granting a final injunction is to be determined is after the Court has determined the matter on the merits (i.e. at the form of order hearing).⁴⁸⁷ The likelihood of repetition is an important factor in determining whether a final injunction should be granted.⁴⁸⁸

Justification for Injunctive Relief

298. The full argument on the justification for injunctive relief will need to be heard at the form of order hearing. That is because the justification for the granting of this relief will need to be considered in light of the nature and extent of the findings in the judgment. However, COPA's broad position is as follows.

299. 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.

299.1. First, he has made highly aggressive threats, including to bankrupt Bitcoin developers, have them imprisoned and (in one unpleasant post accompanied with a photograph) to have them "*defenestrated*" (see Mr Lee's evidence at §§17-18).

299.2. Secondly, he has carried through on such threats with a campaign of litigation which is evidently well-resourced and has involved numerous claims against private individuals.

299.3. Thirdly, this campaign has (predictably) had highly undesirable effects in inhibiting legitimate activities of cryptocurrency development (see Mr Lee's evidence at §§19-24).

299.4. Fourthly, Dr Wright and Mr Ayre have made very clear that they intend to pursue their self-styled crusade as far as they possibly can. See for instance (a) the evidence of their tweets addressed in Dr Wright's *McCormack* evidence (e.g. Mr Ayre posing alongside Dr Wright and lawyers with the slogan, "*Craig and I polishing our musket's at today's Troll Hunting meeting in London*"),⁴⁸⁹ and (b) Dr Wright's posts which breached the embargo in *McCormack* (including that he

⁴⁸⁷ See *Copinger* at §21-236.

⁴⁸⁸ *Ibid* at §21.238.

⁴⁸⁹ {O2/12/33}, internal p126.

would “*spend 4 million to make an enemy pay I*”).⁴⁹⁰ A series of aggressive “*troll hunting*” tweets by Mr Ayre can be found in the *Granath* hearing bundle.⁴⁹¹

299.5. Fifthly, the benefit of an injunction is that it can be used to protect those who would otherwise gain no direct benefit from purely declaratory orders. Those bound by the decision (including privies of the parties) will have the benefit of issue estoppels, but that is cold comfort to the many who are not so bound (including current and future market participants).

299.6. Sixthly, there is a public interest in bringing to an end the extraordinary use of Court resources and legal costs expended on Dr Wright’s lawsuits deriving from his claim to be Satoshi. Prior to this trial, COPA believes that 54 days of Court time has been taken up across Dr Wright’s various Court actions in this jurisdiction (this is based on judgments and orders recording such).⁴⁹² That figure does not include this trial (24 days), nor any pre-reading time or any judgment writing time. On any view, Dr Wright has occupied a vast amount of Court time and resources with a claim which is entirely bogus.

Conclusion

300. Dr Wright’s claim to be Satoshi Nakamoto and author of the White Paper is false. This case should be the end of the road for Dr Wright’s abusive and knowingly false claims. COPA therefore asks the Court to make the necessary declarations, and to grant relief to bring an end to his unjustified threats against the developer and wider cryptocurrency community.

**JONATHAN HOUGH KC
JONATHAN MOSS
TRISTAN SHERLIKER**

⁴⁹⁰ *McCormack* judgment on consequential orders at §11 {L18/85/3}.

⁴⁹¹ {S2/2.1/4}.

⁴⁹² *COPA* 12 days; *Coinbase/Payward/BTC Core* 3 days; *Cobra* 3 days; *Granath* 4 days; *Tulip Trading* 17 days; *Tulip Trading Appeal* 2 days; *Roger Ver* 1 day; and *McCormack* 12 days.