

**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”)**

---

**CLOSING SUBMISSIONS OF COPA**

---

*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.*

**JONATHAN HOUGH KC**  
**JONATHAN MOSS**  
**TRISTAN SHERLIKER**

**8 March 2024**

**Instructed by Bird & Bird LLP**

Pre-ample: Closing Submissions .....	5
Introduction.....	7
Housekeeping.....	8
Summary of COPA’s Position .....	9
The Factual Background .....	11
Digital Cash before Bitcoin .....	11
Satoshi’s Release of Bitcoin .....	11
Satoshi’s initial communications and release of the Bitcoin White Paper .....	11
Release of the Bitcoin Source Code and creation of the early blocks .....	13
Satoshi’s later communications and his departure.....	13
Dr Wright and his Life up to 2011 .....	14
The ATO Investigations and Decisions .....	16
The Tulip Trust .....	21
The Bailout of Dr Wright and the Outing / “Doxing” in Late 2015 .....	23
The Background Work Leading to the “Big Reveal” .....	28
The EITC Agreement of February 2016.....	32
The “Signing Sessions” of March and April 2016.....	35
The Sartre Blog Post of 2 May 2016 and its Aftermath .....	37
Dr Wright’s Work with nChain and Calvin Ayre.....	40
Dr Wright’s Threats to Assert IP Rights.....	41
Dr Wright’s Other Litigation .....	42
Events since September 2023 .....	44
What is COPA?.....	45
Relevant Procedural History .....	46
Procedural chronology for the COPA Claim.....	46
Dr Wright’s Disclosure .....	49
Overview of the Reliance Documents .....	54
Overview of Cryptocurrency Technology .....	56
Introduction.....	56
Digital Signatures.....	56
Transacting in Bitcoin.....	57
Transaction Ordering .....	58
Blockchain Forks .....	58
Storage and Use of Bitcoin .....	59
Security of Digital Signatures.....	59
Public keys Associated with Satoshi.....	61
The Evidence at Trial.....	61

COPA’s Fact Evidence .....	63
COPA’s Hearsay Evidence .....	70
Dr Wright’s Fact Evidence .....	72
The evidence of Dr Wright’s witnesses that he could be Satoshi.....	73
The prism of hindsight .....	73
Witnesses whose Honesty is Challenged.....	77
Dr Wright.....	78
Mr Matthews.....	82
Mr Jenkins.....	84
Dr Wright’s Hearsay Evidence .....	86
Forensic Document Examination / LaTeX Code Experts.....	87
Status of the document forensic evidence.....	89
Cryptocurrency Experts .....	94
ASD Experts .....	98
Submissions on the Law Relevant to Resolution of the Identity Issue.....	99
Burden and Standard of Proof.....	99
Pleading and Proof of Fraud .....	100
Evidence – Recollections of Witnesses and Documentary Evidence.....	101
Points on Expert Evidence .....	101
Drawing of Inferences (including from absence of witnesses).....	102
Evidence on Character and Credibility .....	102
Hearsay Evidence – Admissibility and Weight .....	103
Admissibility of Public Reports and of Judgments in Other Proceedings.....	103
Dr Wright’s Claim to be Satoshi.....	103
Project BlackNet.....	104
Lasseter’s and Vodafone.....	105
Dr Wright’s Employment at BDO .....	106
Dr Wright’s LLM Dissertation .....	107
Dr Wright’s MStat Degree.....	109
Dr Wright’s Claims about Writing the Bitcoin code .....	109
Drafting of the White Paper.....	112
Creation of the Genesis Block, Release of the Source Code and the First Transaction ....	116
Dr Wright Leaving the Satoshi Persona.....	117
Overview of COPA’s Case .....	119
(1) Dr Wright’s Use of False and Forged Documents .....	119
Examples from the Schedules of Forgeries .....	122

(1) MYOB records [ID_004077, ID_004078 and ID_004079] - Appendix PM7 {H/47/1}	122
(2) Project BlackNet document [ID_001379] – Appendix PM8 {H/60/1}	124
(3) NAB Records [ID_003455] (with attachments) – Appendix PM17 {H/78/1}	125
(4) Spoofed Email [ID_001546] – Appendix PM21 {H/104/1}	125
(5) Bitcoin.exe [ID_000739] – Appendix PM12 {H/68/1}	126
(6) Timecoin ODT [ID_000254] – Appendix PM2 {H/17/1}	127
(7) LLM Dissertation Proposal [ID_000217] – Appendix PM25 {H/118/1}	128
(8) BDO Quill minutes [ID_004013] – Appendix PM5 {H/31/1}	128
(9) Backdated Draft of the White Paper [ID_000536] – Appendix PM3 {H/20/1}	129
(10) King2.rtf [ID_004695] – PM46 {H/278/4}	130
Dr Wright’s Excuses and Changes of Story	130
Change of Story Case Study: the NAB Screenshots	140
Chain of Custody Schedule	142
The Ontier MYOB Email forgery	143
Changes from his RFI evidence response in Wright 4	146
The New Documents	148
The BDO Drive Documents	148
The Overleaf LaTeX files	152
(2) Dr Wright’s Failures to Provide Proof of his Claim	152
Failure to Produce Supportive Witnesses	153
The Reliance on Don Lynam’s Hearsay Evidence	156
The Timecoin Paper	159
Failure to Provide Reliable Documentary Evidence	161
Failures of Cryptographic Proof – the Sartre Blog Post and its Aftermath	164
Failures of Cryptographic Proof – Destruction of the Hard Drive and no Proof Since 2016	166
Failures of Cryptographic Proof – Overview of the Signing Sessions	167
Failures of Cryptographic Proof – the Signing Sessions with Mr Matonis and the Journalists	169
Failures of Cryptographic Proof – the Signing Session with Mr Andresen	170
The Andresen Signing Session Reconsidered	172
Failure to Demonstrate the Technical Ability of Satoshi Nakamoto	175
(3) The Implausible and Inconsistent Nature of Dr Wright’s Accounts	176
Dr Wright and Mr Matthews	176
The evidence given by Mr Matthews in support of Dr Wright	176
Inconsistencies between Mr Matthews and Dr Wright	178
Mr Matthews on the Sartre blog post	179

Signing sessions / Sartre blog inconsistencies .....	180
Mr Matthews and arranging further proof after the Sartre blog failure.....	180
The Satoshi PGP Key.....	182
Dr Wright’s case in his pleading and in Wright 4 (RFI response).....	182
Dr Wright’s account in Wright 11 .....	183
Dr Wright’s position in cross-examination.....	184
Summary of the position.....	187
Dr Wright Blaming his Lawyers.....	189
BlackNet and Spyder Projects .....	190
Supposed Collaboration with Prof Wrightson and Dr Furche.....	191
Accounts of Collaboration with Professor Rees and Gareth William .....	192
Early Events in the History of Bitcoin.....	194
Papa Neema .....	199
The White Paper LaTeX Files .....	200
Dr Wright’s Patch Tuesday Story and Explanations .....	201
Accounts given by Dr Wright about Patch Tuesday.....	202
Cross-examination of Dr Wright on Patch Tuesday .....	202
Inconsistencies and flaws in Dr Wright’s accounts .....	203
List of Individuals Blamed by Dr Wright in his Evidence .....	205
Dr Wright’s principal villains .....	206
Lawyers and other professionals involved in Dr Wright’s litigation.....	207
Dr Wright’s own friends, family and co-workers.....	208
Miscellaneous individuals and computer software .....	210
Witnesses in this case.....	212
The Argument based on the Real Satoshi not having Come Forward.....	213
Further Submissions on Dr Wright’s Credibility.....	215
Relief Claimed .....	217
Legal Principles for Declaratory Relief.....	218
Justification for Declaratory Relief.....	218
Legal Principles for Injunctive Relief.....	219
Justification for Injunctive Relief .....	222
Conclusion .....	225

## **Pre-amble: Closing Submissions**

1. These Closing Submissions are written by way of expanding on COPA's opening Skeleton Argument. The original wording from the opening Skeleton Argument remains in black, with the additions shown in red. The paragraph numbering has therefore changed. Where a section can now be ignored, this is indicated.
2. Following the evidence in this trial, it is clearer than ever – clear beyond doubt – that Dr Wright is not Satoshi Nakamoto. He did not write the Bitcoin White Paper, produce the Bitcoin Code or implement the Bitcoin system. The Identity Issue should be resolved in favour of COPA and the Developer defendants to the BTC Core Claim.
3. Dr Wright has been shown to have lied on an extraordinary scale, and it is difficult to think of a precedent for what he has done. He has invented an entire biographical history, producing one tranche after another of forged documents to support it. Even when the extent of his dishonesty and forgery was exposed to him in cross-examination, he doubled down, forging further documents during the trial, blaming a litany of characters, asserting implausible technical excuses and suggesting a vast and ever-growing conspiracy to frame him, all in an effort to evade his own responsibility. His developing excuses became comical at times, but as was made clear in opening Dr Wright's conduct is no laughing matter. He used his time in the witness box to defame, blame and attack anyone he could identify to defend his position, including even his own expert witnesses and a series of law firms previously engaged by him. In short, he has attempted a very serious fraud upon the Court. To give fair warning, COPA will ask after judgment that the papers be referred to the Director of Public Prosecutions for consideration of prosecution for the offences of perjury and perverting the course of justice.
4. Attached to these Closing Submissions are the following Appendices:
  - 4.1. Appendix A is COPA's Consolidated Schedule of Dr Wright's Forgeries (the "**Forgery Schedule**"). It consists of four parts: (i) the forgeries pleaded in the Particulars of Claim; (ii) the set of 20 "core" forgeries from Dr Wright's original disclosure pleaded by COPA in its first Schedule of Forgeries; (iii) the 20 further forgeries from Dr Wright's additional documents pleaded by COPA in its Schedule of Further Forgeries; and (iv) the forgery committed during trial (the MYOB Ontier Email). For each forgery, the document sets out the text from the

existing pleading, followed by a section in red summarising Dr Wright's explanation and COPA's rebuttals. It is hoped that this will provide an easy guide for the Court in making its decisions on the forgery allegations.

- 4.2. Appendix B is a Schedule of Transcript References, which is in table format with comments provided. It is a long document, which includes all the most significant evidence with short explanatory notes. It is not intended to be read in its entirety but used as a reference tool for carrying out searches for words or terms.
5. As in the opening Skeleton Argument, this document contains short submissions on relief. However, as the Court will appreciate, the main argument on the scope of relief, and in particular any injunctive relief, will need to be carried out at the form of order hearing. That is because the arguments for injunctive relief will need to be considered in light of the Court's full findings.
6. Looking briefly ahead to the injunctive relief that COPA will be seeking, all that this trial has done is day by day to strengthen the case for such relief. Dr Wright has threatened and pursued enormous damages claims against numerous individuals. In this trial, it has been shown that these claims are based on a fiction. To defend that fiction, Dr Wright has committed perjury and forgery to an extraordinary extent. Every time he was caught in a lie, he met the charge with more lies, leading ultimately to numerous absurd conspiracy theories.
7. Two final and vivid emblems of this conduct were Dr Wright's final forgeries: (a) the editing of the White Paper LaTeX files in November / December 2023, as illustrated by the Developers' animation; and (b) his production of the fake MYOB Ontier email during trial to challenge the honest account of his former solicitors and defend his own false evidence. On reflection, it may seem a mystery that he thought he could get away with these final forgeries, but the same may be said of many of his dishonest acts. Time and again, he has told a lie or falsified a document with the arrogant presumption that he would not be caught. He has now been found out.
8. COPA wishes to make clear at the outset that it makes no criticism of the way in which Dr Wright's solicitors and counsel have conducted the trial. They have done so properly, representing Dr Wright's interests very ably within the limits of professional ethics and their duty to the Court.

## **Introduction**

9. 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.<sup>1</sup> 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.
10. 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 Claim<sup>2</sup>).
11. 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.
12. 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,

---

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}.



including the BTC Core Claim (in which Dr Wright claims damages from numerous Bitcoin developers and COPA itself for infringement of database rights in the Bitcoin blockchain and copyright in both the White Paper and File Format).

13. 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*”.<sup>3</sup> 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**

14. **This section can be ignored save for the point below about Wright 11 {CSW/1} and one further point arising out of submissions made during trial.**
15. 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).<sup>4</sup> 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.<sup>5</sup> 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.<sup>6</sup>
16. **As the Court accepted in its ruling on Day 2 of trial, much of the content of Wright 11 is irrelevant and inadmissible, and the statement as a whole is seriously non-compliant with**

---

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.

the rules. COPA maintains its detailed objections to Wright 11 as set out in its Schedule of Objections {CSW/6/1}. Whilst it remains before the Court on a *de bene esse* basis, only the parts relied upon by COPA and the Developers or put to witnesses should be admitted.

17. 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.
18. There is one further point of housekeeping arising from submissions at trial. It was agreed between the parties, and fairly pointed out by Dr Wright's counsel on several occasions, that it was not appropriate or necessary for Dr Wright to be taken to every document or challenged on every finding of the experts.<sup>7</sup> In fact, Dr Wright was taken to each and every pleaded forgery allegation and given an opportunity at trial to respond, both to factual points against him and the relevant expert analysis, given the seriousness of the allegations. Nevertheless, it is correct that in many cases the documents (including expert reports) speak for themselves, particularly where they demonstrate falsehoods in Dr Wright's witness statements.

### **Summary of COPA's Position**

19. 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. Following the evidence, COPA can now add that Dr Wright added to and embellished upon his lies during the trial, as well as forging at least one further document during trial. COPA would also have had challenges to raise to the 47 documents (mainly handwritten) which were "found" in his home on the weekend during Dr Wright's cross-examination. However, there has been no application to rely on them and the Court will therefore not have to consider them.

---

<sup>7</sup> See {Day5/180:2} – intervention by Lord Grabiner KC.

20. 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).
21. In this skeleton, COPA presents its case in three parts:
  - 21.1. 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.
  - 21.2. 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.
  - 21.3. 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**

22. 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.
23. **COPA now adds to the below further matters which have emerged or been confirmed during the evidence at trial.**

### **Digital Cash before Bitcoin**

24. 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,<sup>8</sup> while public discussion of Hashcash in the late 1990s used the expression “*block chain*” in the context of data structures.<sup>9</sup>

### **Satoshi’s Release of Bitcoin**

#### *Satoshi’s initial communications and release of the Bitcoin White Paper*

25. 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 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

---

<sup>8</sup> See US Patent 4074066, 1976: “*Message verification and transmission error detection by block chaining*” (Ehram et al.).

<sup>9</sup> See for example: <http://mailing-list-archive.cryptoanarchy.wiki/archive/1997/12/e080a2180e912b9b129e8be3e4d114421b0c9bc11217ac2e40b3b8f112305572>

on the “upload.ae” site and asking to check a reference to his paper on Hashcash.<sup>10</sup> Dr Back replied, informing Satoshi about Wei Dai’s B-Money Paper.<sup>11</sup> Satoshi then wrote to Wei Dai to check the reference for that paper.<sup>12</sup> 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.

26. On 31 October 2008, Satoshi released the White Paper by sending an email to the “metzdowd cryptography mailing list” (“**the Metzdowd List**”) (a group of individuals interested in cryptography) and directing them to a link on the “bitcoin.org” site, where the document was hosted.<sup>13</sup> 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,<sup>14</sup> and published under the MIT License.<sup>15</sup>
27. 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”.
28. A number of email addresses have been associated with Satoshi. These have included: [satoshi@vistomail.com](mailto:satoshi@vistomail.com); [satoshin@gmx.com](mailto:satoshin@gmx.com); and [satoshi@anonymousspeech.com](mailto: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.
29. Over the period from 31 October 2008 to January 2009, Satoshi wrote a series of emails to the Metzdowd List. In one, dated 8 November 2008, Satoshi explained that the code had been written before the White Paper.<sup>16</sup> In another, dated 14 November 2008, Satoshi 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*

---

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

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

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

13 The email to the Metzdowd 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}.

14 As noted above, the White Paper as released on 24 March 2009 is ID\_000865 and may be found at {L5/26/1}.

15 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.

16 {L3/290/2}.

*half while coding [Bitcoin]*”, adding that the source code for the system was coming soon but was available on request in the meantime.<sup>17</sup>

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

30. 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 Metzdown List.<sup>18</sup> 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*

31. 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.
32. 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 bear this out.<sup>19</sup> Meanwhile, on 13 December 2010, Satoshi updated nearly all the Bitcoin

---

17 {L3/306/1}.

18 {L4/63/1}.

19 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.

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.<sup>20</sup>

33. 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.<sup>21</sup>

### Dr Wright and his Life up to 2011

34. 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.<sup>22</sup> He was born and raised in Australia, and spent most of his life there until late 2015.
35. In the early to mid-1990s, he worked at OzEmail (an ISP in Australia) as a corporate account manager.<sup>23</sup> In 1997-1998, he held a post as IT security consultant for the Australian Stock Exchange, where he developed IT security systems.<sup>24</sup>
36. From 1997 to 2003 he worked primarily through DeMorgan Information Security Systems Ltd (“**DeMorgan**”), an IT security consultancy business that he founded.<sup>25</sup> In 1998, DeMorgan was engaged by Lasseter’s Online Casino.<sup>26</sup> 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.<sup>27</sup> From 1998 to

---

20 {L7/220/1}.

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

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

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

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

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

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

27 Wright 1, §39 {E/1/9}.

2002, DeMorgan worked with Vodafone on IT security project work which involved implementing a firewall system.<sup>28</sup> Whilst working with Vodafone, he met Rob Jenkins.<sup>29</sup>

37. Although Dr Wright took great umbrage at the moniker being put to him, his working history is as “the IT security guy”.<sup>30</sup> However competent he may have been at that job, he was not a visionary working at the cutting edge of designing digital payment systems. As noted below, his claims of creating early versions of the Bitcoin system in timestamp servers for Lasseter’s were not supported by any documents or by the evidence of Mr Archbold.
38. 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.<sup>31</sup>
39. 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.<sup>32</sup> 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.<sup>33</sup>
40. 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.<sup>34</sup> 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.<sup>35</sup> From 2007 to 2008,

---

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

29 Wright 1, §45, 46 {E/1/10}.

30 {Day5/177:1} - {Day5/178:1}.

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

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

33 Wright1, §49 {E/1/11}.

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

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



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.

41. Dr Wright's actual activities from 2007 to early 2009 did not give him a lot of time to work on developing a revolutionary new means of exchange and speculation. He had a full-time job for almost the entire time. He was working on his LLM (including assignments and a 90-page dissertation), an MStat course and a third master's degree. He was working towards a series of IT security qualifications. He posted 269 blog articles in 2008 alone. He prepared several chapters for a book on IT compliance, as well as working on other books. With David Kleiman and Shyaam Sundhar, he completed a long paper on overwriting hard drive data, which he said in a blog "*ate 18 months of my life*".<sup>36</sup>
42. Despite his life and his professional and academic interests being extensively documented in the blog posts and papers referred to above, there is no evidence of him doing any work or study on digital cash or even digital payment systems over this period.
43. Dr Wright was made redundant from BDO in November or December 2008, with his formal employment ending in January 2009.<sup>37</sup> After that redundancy, he actively put himself forward for work entirely focussed on IT security, and on 22 January 2009 he published a blog "A Return to Consulting", in which he put himself forward as an expert in IT security and audit.<sup>38</sup> In 2009, he started the companies Information Defense Pty Ltd and Integrys Pty Ltd. Over the following years, he founded a series of other companies.<sup>39</sup> It was also from 2009 that Dr Wright found himself the 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.<sup>40</sup>

#### The ATO Investigations and Decisions

44. 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

---

36 See: {Day6/35:25} - {Day6/38:11}.

37 Wright 1, §61 {E/1/13}.

38 See {Day6/38:12} - {Day6/41:19} and {L9/97/1} (the blog).

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

40 Wright 1, §129-130 {E/1/25}.

estimated that 94% of the income he had received in the previous two years had come from tax refunds to his companies.<sup>41</sup> This forms the backdrop for Dr Wright in 2015 needing money and receiving a bailout which involved him staking a claim to be Satoshi.

45. 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).
46. 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 Integrys Pty Ltd) for sums totalling AU\$ 2,235,000.<sup>42</sup> 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.<sup>43</sup> 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.
47. 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.<sup>44</sup> Dr Wright submitted notices of objection, which were rejected by the ATO, including on the basis of failure to substantiate the IP sales.<sup>45</sup> He applied for review to the Administrative Appeal Tribunal. The result was that the ATO agreed to lift the administrative penalty and to

---

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

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

43 {L4/462/1}.

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

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

allow various expense deductions,<sup>46</sup> but it does not appear that the CGT issue was specifically addressed.

48. 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.
49. 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.<sup>47</sup> 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.<sup>48</sup>
50. In cross-examination, Dr Wright claimed that the ATO private ruling was based on material he had provided to them between 2009-10 and that it positively showed that he had been mining Bitcoin then.<sup>49</sup> That is a total fabrication, as the ATO private ruling was in response to a request of June 2013 and based on assumed facts as set out in the request.<sup>50</sup> There is no evidence at all that Dr Wright told the ATO before 2013 that he had been mining Bitcoin in 2009/10, as set out in the request at {CSW/67.1/2} (which makes clear that Dr Wright's mining claim was an assumed fact put forward by him in 2013) and as also made clear in the ruling.
51. 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

---

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

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

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

49 {Day7/58:25}.

50 {L8/309/2}: The ruling states: "This ruling is based on the facts stated in the description of the scheme that is set out below. If your circumstances are materially different from these facts, this ruling has no effect and you cannot rely on it." It is also clear from the remaining sections of the ruling that it is based on a set of facts as presented and assumed, not on facts found or derived from prior audit work.

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 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.

52. 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.<sup>51</sup>
53. 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.<sup>52</sup> 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.
  - 53.1. 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.
  - 53.2. 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

---

51 See ATO Decision at {L16/456/1}; Preliminary GAAR Submission dated 29 August 2014 {L9/274/1}.  
52 {L11/354/1}.

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 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.<sup>53</sup> In cross-examination, Dr Wright attempted to maintain the fiction that he had engaged Prof Rees for consulting services without any of his family being aware. Dr Wright sought to evade the question when it was put to him that Prof Rees was in a nursing home, in poor health and not using a computer when Dr Wright had supposedly made a Bitcoin transaction with him.<sup>54</sup> It is also telling that Mr Yousuf, a director of C01N, had never heard of Prof Rees, who had supposedly provided valuable and costly consulting services to the company.<sup>55</sup>

54. 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,<sup>56</sup> Denariuz Pty Ltd,<sup>57</sup> Zuhl Pty Ltd<sup>58</sup> and Integryrs Pty Ltd.<sup>59</sup> 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.<sup>60</sup> 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.

---

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

54 See {Day7/61:15} - {Day7/65:20}.

55 {Day9/135:5}.

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

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

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

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

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

55. 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.<sup>61</sup> 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*”,<sup>62</sup> though he later accepted backdating the invoices.<sup>63</sup>
56. 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 apparently false copies of emails with the ATO.<sup>64</sup> 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.*” **There is a striking similarity between what the ATO found to have happened and Dr Wright’s forgery of the MYOB Ontier Email during the present trial.**
57. **Under cross-examination, Dr Wright tried weakly to explain away the ATO’s findings by saying that “*people sent in false information and fabricated documents to them*”,<sup>65</sup> which was no answer because the problem was a conflict between emails held by ATO officials and versions submitted by Dr Wright. He tried to explain away the fact that his own solicitors (Clayton Utz) lost confidence in him by saying that Mr Sommer had not shared that view, but that was a hopeless excuse given that Mr Sommer wrote the email expressing his serious concern about Dr Wright’s conduct, as well as writing and signing the letter confirming the firm ceasing to act.<sup>66</sup>**

### The Tulip Trust

58. The supposed Tulip Trust, which formed part of Dr Wright’s story in the tax claims (and whose existence was doubted by the ATO<sup>67</sup>), features in Dr Wright’s narrative in these proceedings as well. His evidence is that he placed in this trust a number of assets,

---

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

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

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

64 See email from Clayton Utz to Ramona Watts, forwarded to Dr Wright on 4 July 2015 {L10/66/1}. **See also letter from the firm to Dr Wright dated 6 July 2015 {L10/68/1}.**

65 {Day7/98:10}.

66 {Day7/98:6} - {Day7/102:3}.

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

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.<sup>68</sup> 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.<sup>69</sup>

59. In cross-examination, Dr Wright's account of the Tulip Trust was hopelessly confused and contradictory. It was addressed in particular from {Day6/179:2} - {Day6/182:9} and {Day7/8:5} - {Day7/54:12}. It became apparent from the course of Dr Wright's evidence that the Tulip Trust is an invention, the details of which have been refashioned successively for the ATO investigation, the Kleiman proceedings, the Granath proceedings and the present case.
60. A stark example of Dr Wright's dishonesty in this respect is that, in seeking to defend previous statements that Dave Kleiman had never been a trustee of the supposed Tulip Trust, he told the Court in this case that he had sworn a declaration in the Kleiman proceedings containing a series of details which were unknown to him and which he later supposedly discovered to be untrue: see {Day7/15:25} - {Day7/26:4}. He even claimed that he had been compelled by a US magistrate to make positive statements of fact despite being in ignorance: {Day7/21:11}. He even claimed that he had sworn that he himself was a trustee while believing that there was no way he could be: {Day7/18:25} and {Day7/24:1} - {Day7/25:9}.
61. 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 2011<sup>70</sup> and 17 October 2014<sup>71</sup> 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.<sup>72</sup>

---

68 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.

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

70 In disclosure at {L7/382/1}.

71 In disclosure at {L9/218/1}.

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

62. 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.<sup>73</sup> 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, including Bitcoin in an address known as 16cou.<sup>74</sup> 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*”.<sup>75</sup>

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

63. 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.<sup>76</sup> By email dated 3 February 2014,<sup>77</sup> 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.<sup>78</sup> Dr Wright says that nothing came of the introduction at that stage.<sup>79</sup>
64. It was also in February 2014 that Dr Wright began to advance his public claim to be Satoshi Nakamoto. This began with communications to the Kleiman family, which were probably sent to enlist their support for his dealings with the ATO. It appears that, having made claims about mining large amounts of Bitcoin in the early days of the Bitcoin system in order to provide a basis for the complex transactions underlying his tax concession claims (transactions the ATO later found to be fictitious), Dr Wright decided to claim that he had been involved in the earliest development of the Bitcoin system. At that stage, he placed Dave Kleiman at the heart of the story, no doubt because Mr Kleiman had featured heavily in his ATO claims as a conveniently-deceased collaborator and party to transactions.

---

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

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

75 {L17/382/46}.

76 Wright 1, §149 {E/1/28}.

77 {L8/340/1}.

78 Wright 1, §151 {E/1/28}.

79 Wright 1, §150-152 {E/1/28}.



65. On 11 February 2014 he emailed Louis Kleiman, Dave Kleiman’s father, to tell him that Dave (along with himself) was one of the three people behind Bitcoin.<sup>80</sup> Pausing there, there is the rather obvious point that this email contradicts what Dr Wright now says about he alone having written the Bitcoin White Paper, produced the Bitcoin Code and put the system into operation. It was also at odds with the great (and effective) lengths to which Satoshi Nakamoto went to conceal his identity. Dr Wright’s strategy of seeking to enlist the Kleiman family backfired spectacularly, as they went on to bring the US claim based on the premise of Dr Wright having been in a partnership with Dave Kleiman to create the Bitcoin system and develop other projects.
66. Dr Wright’s account of this email went through a series of contortions. In his Kleiman deposition of 4 April 2019,<sup>81</sup> he claimed to have typed the email and said that the third person was a person whose name could not be revealed for reasons of the national security of the USA. He said that he did not know if this “third man” was alive, nor whether they were a member of the US government.<sup>82</sup> After the US Court had ruled that the questions should be answered, Dr Wright was questioned again in a deposition on 16 March 2020,<sup>83</sup> at which point he said that he had not written the email and that it had been typed by his assistant under instructions from somebody else in his business (perhaps Uyen Nguyen). He tried to explain away his previous answer that he had typed the email by saying that he had typed the first sentence while preparing a commentary document for his lawyers. He then said that there were three key people behind Bitcoin but, contrary to the plain meaning of the email, Dave Kleiman was not one of them. He said that they were himself, his uncle Don Lynam and Gareth Williams, the deceased UK security services agent.
67. In cross-examination at this trial, Dr Wright’s account became incoherent as he tried to reconcile his previous versions. In a rare display of candour (from which he quickly backtracked), he said that in his first US Court deposition: “*I was being difficult at the time, so I was trying to waffle as much as possible.*” He claimed that the purpose of the email was to make Louis Kleiman feel proud of his son, but could not explain how he achieved that by an email which he had said meant that Dr Wright, Don Lynam and

---

80 {L8/347/2}.

81 {L14/409/126} and following.

82 It is a touch worthy of Graham Greene that the third man was supposedly a mysterious spy of fluid identity.

83 {L16/267/36} Internal transcript page 140 and following.

Gareth Williams had invented Bitcoin. When asked to identify the person he had mentioned in his first deposition whose identity was a matter of US national security and who might or might not be alive and/or a member of the US government, he said (absurdly) “*My uncle for a start, but other people as well*”, adding “*What I do know is, he has been a member of the US Government, as in, he was seconded from the Australian military to work in America.*”.<sup>84</sup>

68. At about the same time as Dr Wright began to advance his claim to the Kleiman family that he had been involved in the invention of Bitcoin, he made a crude attempt to lay an evidential trail for the claim. An item was posted on his blog with the text: “*Bitcoin: Well... e-gold is down the toilet. Good idea, but again centralised authority. The Beta of Bitcoin is live tomorrow. This is decentralised... We try it until it works. Some good coders on this. The paper rocks.*” This item was given the date 10 January 2009. However, a trail of WayBack Machine captures<sup>85</sup> makes clear that it was added between 12 December 2013 and 18 February 2014: {Day7/66:8} to {Day7/70:25}. Dr Wright agreed that this item had been added to his blog, but denied responsibility and suggested that disgruntled former employees working with Ira Kleiman had done the deed: {Day7/71:15} to {Day7/72:25}. This excuse makes no sense, since Dr Wright’s dispute with the Kleiman family had not begun by February 2014 and since the backdated blog post supported *his* version of events. Dr Wright also claimed that a replacement of that blog post which was made between June 2014 and October 2015 and which teasingly began “Bitcoin – AKA bloody nose you be...” had also been placed by someone other than him: {Day7/75:8} to {Day7/76:8}. His story therefore involved allegations of repeated misuse of his blog by his enemies over a period of at least several months which he never spotted, but which happened to accord precisely with the claims he was making at the time.
69. 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.<sup>86</sup> By late April

---

84 See: {Day6/123:21} - {Day6/133:4}, and {Day6/132:5} in particular

85 For example, {L9/89/1}

86 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}.

2015, the men were discussing investment in Dr Wright's businesses.<sup>87</sup> 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.<sup>88</sup> 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.<sup>89</sup>

70. At this point, Dr Wright desperately needed to be bailed out. Mr Matthews gave evidence that, by June 2015, Dr. Wright's financial condition was in such distress that Dr. Wright had had to dispense with practically all the staff from his businesses.<sup>90</sup> Dr Wright owed his lawyers, Clayton Utz, millions of dollars and evidently could not make payment. When Mr Ayre arranged for Mr MacGregor and Mr Matthews to travel to Australia, Dr Wright's wife had to make special arrangements for people to come into the office so that "*it may at least look like we are still doing business.*"<sup>91</sup> Dr Wright had a strong incentive to tell these potential backers anything that would encourage them to provide him with financial support, including that he had invented the Bitcoin system, thus making his subsequent work all the more valuable.
71. 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,<sup>92</sup> which was immediately superseded by a second version.<sup>93</sup> The stated purpose was for DeMorgan Ltd to receive funding for its research projects and tax obligations in light of the ATO issues.<sup>94</sup> The Term Sheet had the following provisions (in summary):
- 71.1. 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.*"

---

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

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

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

90 {Day11/124:13}.

91 See email chain of 23 June 2015 at {L9/491/1}.

92 {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}.

93 {L10/34/1}.

94 Wright 1, §153 {E/1/28}.

- 71.2. 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.
- 71.3. 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.
- 71.4. 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*”.
72. 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.<sup>95</sup>
73. By late November / early December 2015, reporters at WIRED and Gizmodo were making enquiries about the possibility that Dr Wright might be Satoshi.<sup>96</sup> On 8 December 2015, the two magazines published articles on the subject, identifying him as Satoshi and referring to some pieces of evidence.<sup>97</sup> 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 articles were published, the Australian Federal Police raided Dr Wright’s home and business premises in connection with the ongoing ATO investigations.<sup>98</sup> 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.

---

95 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}.

96 Wright 1, §161 {E/1/30}.

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

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

74. It is not known who “outed” Dr Wright to the media, but emails sent that day (including from Ira Kleiman<sup>99</sup> and Robert MacGregor<sup>100</sup>) suggest that some thought it could have been Dr Wright himself.
75. 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).<sup>101</sup> 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.<sup>102</sup> 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*”.<sup>103</sup> Gizmodo published an equivalent article the same day.<sup>104</sup>
76. 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).<sup>105</sup>

### The Background Work Leading to the “Big Reveal”

77. The EITC Agreement and the “Big Reveal” of 2016 need to be considered against the background of what Dr Wright was saying and doing from late 2015 through to early 2016 behind the scenes. Dr Wright’s narrative throughout cross-examination was one of forced compliance, as he was dragged along by Mr MacGregor, one of the key villains in Dr Wright’s rogues’ gallery. The documents, however, tell a very different story. Dr Wright’s account is so starkly at odds with the contemporaneous emails that in cross-examination he sought for the first time to deny that a whole series of them were genuine.

---

99 {L11/198/1}.

100 {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}).

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

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

103 {L11/218/1}.

104 {L11/220/1}.

105 {L13/491/2}.

78. The emails make clear that, by September 2015, plans were well underway for a book based on Dr Wright’s life story, including him being Satoshi. In an email dated 10 September 2015,<sup>106</sup> Dr Wright actively laid out how the book would cover his creation of Bitcoin, and Calvin Ayre commented in reply that “*a few warts makes a better story :-)*”.
79. Dr Wright denied the authenticity of this and a series of later emails from September to November 2015 on the basis that his contributions were from an email address [cwright@tyche.co.uk](mailto:cwright@tyche.co.uk) and he claimed never to have been employed by Tyche Consulting. As set out in more detail below, Dr Wright plainly was employed by Tyche Consulting in late 2015, and indeed that employment was crucial to his securing residency in the UK. However, the detail of the emails makes perfectly clear that they were from him.
80. It is not hard to see why Dr Wright has sought to deny these emails. In order to give credence to his story that he was reluctant to be revealed as Satoshi Nakamoto and provide proper cryptographic proof, he has since maintained repeatedly that he was only reluctantly persuaded to this course after the outing by WIRED and Gizmodo in December 2015. He even attested to this version in the Reply in the UK proceedings *Wright v Granath*.<sup>107</sup>
81. It should also be noted that Dr Wright has been eager to avoid discussion of the involvement and knowledge of his billionaire backer, Mr Ayre. On those topics, he became taciturn and tried to avoid going into detail. For instance, he tried to deny Mr Ayre’s involvement in his own corporate bailout in mid-2015, even though the emails show Mr Ayre working out all the financial details.<sup>108</sup> He also attempted bluntly to deny that Mr Ayre had ever funded his litigation, before being forced to concede that Mr Ayre had given him a large loan to fund his McCormack claim.<sup>109</sup> It is telling that Dr Wright seems keen to keep Mr Ayre out of the story, although he was and remains a central participant.

---

106 {L10/339}

107 {L17/164/22} at para. 35.2.

108 For the denial, see {Day7/84:9} and following. For a survey of some key emails showing Mr Ayre’s involvement from the very beginning of the bailout, see {Day7/85:1} - {Day7/87:11}.

109 {Day4/10:6} - {Day4/12:20}. Dr Wright denied that a large loan amounts to litigation funding, which would no doubt come as a surprise to every litigation funder in the market.

82. Continuing with the emails in late 2015, there was discussion about producing a “proof package” to support a public presentation of him as Satoshi Nakamoto. In an email of 21 October 2015,<sup>110</sup> Mr MacGregor told Dr Wright that he had had calls with a literary agent in New York and how they needed a one-page synopsis. This email asked the following questions of Dr Wright:

*“What I’m hoping that this group can contribute over the next week are a couple of dozen key bullet points that I will then fold into this approach document. What we need to prepare is the hook – why would a publisher care about another bitcoin-related (this is how they will see this unless we position it) book, when everything to date has failed? This will be something we would prepare for the agent and it will be provided under NDA, but nonetheless we will not put anything in this that would identify the players or our SN. When did the project begin? Why? With whom? Where? What was the background leading up to it? Were there prior attempts that failed? Some of the human aspects and conflicts will be important, as well... knowledge of / interactions with DPR and others and related sites that rose to prominence in association? What security measures were taken to preserve SN’s anonymity? Why? Background on the origins of the pseudonym itself. Interactions with the inevitable shady groups and interesting characters. Inception of the super-computer and why. Why there? How did you convince them? Etcetera, etcetera.”*

The email from Mr MacGregor then turned to the “proof package”:

*“Finally, we’ll need to consider the “proof package” to establish SN’s identity. There will be the package that will be required by non-technical audiences (notes, etc. that document and evidence creation), but also some decisions as to how to definitively establish SN’s pedigree technically. Some of SN’s wallets are publicly known, correct? Craig, I will need you to walk me through how this could be leveraged if and when the time comes. Could SN activate and move a coin within one of these wallets? What would be sufficient proof from a technical perspective in your view?”*

83. Dr Wright then answered the above questions by way of an email from his wife.<sup>111</sup> That response included Dr Wright’s claim to have been influenced by Wei Dai’s work since the late 1990s (a claim which Dr Wright has since repeated but which, as set out below, could not be true for the real Satoshi Nakamoto). Ms Watts’ email attached a timeline, which also featured elements of the story Dr Wright has told since then.<sup>112</sup>

---

110 {L10/424/2} and over the page to {L10/424/3}.

111 {L10/424/1}.

112 {L10/425}, named “Timeline.docx”.

84. In an email dated 24 November 2015,<sup>113</sup> from Mr MacGregor to Dr Wright (copying Mr Ayre and Mr Matthews amongst others), he said that he had met Baker McKenzie that morning, and again, referred to the “proof packet” being needed at item 5:

*“(5) We’re going to need to create a “proof packet” before too much longer. I’ve been thinking about this and have a couple of ideas. Activating the SN wallets goes a long way, but all it really proves is that someone is in control of SN’s private keys, which could, obviously, have been transferred or acquired otherwise. The keys, plus the documentation substantiating and documenting the original pre-publication research will be enough for 99% of the world, but we will want everything in a data room quite soon for assessment and forensic analysis if possible. Ideally, we identify a very, very credible blockchain “insider” (I’m sure you already know the shortlist directly, Craig) and then bring him/her under NDA and then into the data room. We need at least one extremely credible third party that can have examined the data room, the research, and spoken with Craig, so that in addition to the packet we have the voice of a trusted community member substantiating when the time comes.”*

85. Dr Wright denied the authenticity of this email too, in the following exchange:<sup>114</sup>

*“Q. Well, this one refers, at item (5), to Mr MacGregor proposing creation of a proof package -- proof packet rather, including establishing control of Satoshi Nakamoto’s private keys and so on. Was that being discussed by that stage, 24 November 2015?”*

*A. God, no. There’s no way on earth I’d give over my damn private keys to someone.*

*Q. No, but was that being discussed by Mr MacGregor at that stage?”*

*A. I don’t know what he was discussing. I mean, honestly, if I’m not the person receiving it and it’s a thing set up as Craig Wright and his company, no idea.”*

86. Dr Wright responded to Mr MacGregor’s email of 24 November 2015 within 24 hours,<sup>115</sup> giving the names of some people who could be used for the signing sessions. These included “Adam Black” (which appears twice and is a mistake Dr Wright made elsewhere, clearly getting Dr Back’s name wrong). This message also said that “*Stefan has copies of the Bitmessage and also pgp keys*”. No such Bitmessage or PGP keys have been put forward as supportive evidence.<sup>116</sup>

---

113 {L11/55/2}.

114 {Day7/108:22} - {Day7/109:8}.

115 {L11/55/1}.

116 No doubt the reason that Bitmessage keys were not tendered as evidence in these proceedings is that Dr Wright had come unstuck in the Kleiman proceedings, after being confronted with the origins of Bitmessage. That was first proposed at the end of 2012, in a white paper that is in every respect a clear homage to the work Satoshi Nakamoto (and not the other way around): see {L8/49/2}. Satoshi’s real PGP keys are addressed below.



87. As noted above, Dr Wright disavows all these emails, because they do not fit with his narrative of Mr MacGregor forcing him reluctantly into the “Big Reveal” process after the WIRED and Gizmodo articles had been published. However, it is clear from their contents that they are genuine emails, and Dr Wright’s one reason for rejecting them (i.e. that he was never employed by Tyche Consulting) is plainly false.
88. Mr Matthews similarly accused Mr MacGregor of bullying Dr Wright and forcing him to participate in the public revelation of his claim to be Satoshi Nakamoto. As explained below, Mr Matthews’ account is also unreliable, since (contrary to his repeated statements) the emails tell a story of Mr MacGregor working co-operatively with both Mr Matthews and Dr Wright through early 2016. However, it is telling that Mr Matthews did not disavow the emails which Dr Wright rejects and that Mr Matthews insisted that Dr Wright was employed by Tyche Consulting.<sup>117</sup>
89. Mr Matthews went still further, offering a detailed narrative of the reasons for, documents relating to, and terms of Dr Wright's engagement with Tyche, even confirming Dr Wright’s signature on the contract of employment.<sup>118</sup> In another example, Mr Matthews carefully looked over an email (which had been refuted by Dr Wright when it was presented to him),<sup>119</sup> and not only accepted it to be genuine but confirmed the subject matter of the references being made, and volunteered significant details corroborating of the content of those emails against oral discussions he had with Dr Wright. These included the anchoring details that Dr Wright made a particular request for Mr Matthews to call his ex-wife asking if she had photographs of the “server racks in the farm” – a call which Mr Matthews remembered making.<sup>120</sup>

#### The EITC Agreement of February 2016

90. On 7 January 2016, Mr Matthews arranged for an Implementation Deed<sup>121</sup> to be produced, setting out the manner in which the June 2015 Term Sheet terms would be carried into 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

---

117 {Day11/145:4-24}.

118 {Day11/145:2} - {Day11/148/24}.

119 {L13/338/1}.

120 {Day12/61:22} - {Day12/63/8}.

121 {L11/285/1}.

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.

91. On 17 February 2016, Dr Wright duly entered into a contract entitled "*Life Story Rights and Services Agreement*" ("**the EITC Agreement**").<sup>122</sup> Under its terms:

91.1. 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).

91.2. 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.

91.3. 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*".

91.4. 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*".

92. 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

---

122 {L11/342/1}.

which he “*identified certain documents relating to his authorship of the White Paper*”.<sup>123</sup> 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.<sup>124</sup>

93. 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.<sup>125</sup> 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).<sup>126</sup> 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.
94. 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,<sup>127</sup> 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).<sup>128</sup>
95. Dr Wright’s account in cross-examination, was that the “Life Story” originally sold in June 2015 was the story about his companies and the development of their IP.<sup>129</sup> On any objective view, that is nonsense and the sequence of documents speak for themselves. Nobody would pay the advance agreed upon for exclusive rights to the biography of a competent IT security professional who had a series of companies under investigation by the ATO (which were ultimately wound up as a result). In any event, the EITC

---

123 {A/3/11}, at §31C.

124 Wright 4, §56-59 {E/4/23}.

125 Wright 1, §183 {E/1/33}.

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

127 {L14/10/1}.

128 {L16/382/1}.

129 {Day7/95:2} and following pages.

Agreement which was produced to give effect to the original heads of terms undermines this version. On its terms, it was focussed on Dr Wright's supposed creation of Bitcoin. It was later discharged because he had not proven his claim to be Satoshi.<sup>130</sup> And it led to the work of Andrew O'Hagan, who focussed his efforts on Dr Wright's claim to be Satoshi and who published the product of his labours in "the Satoshi Affair".<sup>131</sup>

96. Following the EITC Agreement being executed, plans moved on apace for the "Big Reveal". Dr Wright underwent intensive media training in March 2016 as he and his backers geared up for the event.<sup>132</sup>

#### The "Signing Sessions" of March and April 2016

97. 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 have been a dry run for demonstrations to be carried out for ~~two of the early developers of Bitcoin,~~<sup>133</sup> Jon Matonis and Gavin Andresen (both subject to NDAs).<sup>134</sup> 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.<sup>135</sup>
98. Jon Matonis met Dr Wright in mid-March 2016 in a hotel in Covent Garden, as arranged by Mr MacGregor and Mr Matthews.<sup>136</sup> Dr Wright then met Mr Andresen in London on or about 7 April 2016, having briefly corresponded by email.<sup>137</sup> 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.<sup>138</sup> Dr Wright claims to have signed messages using the keys associated with blocks 1 and 9.<sup>139</sup> As noted below in relation to the signing sessions, there are some differences between Dr Wright's recollection and that of Mr Andresen in

---

130 This was a point that Mr Matthews appeared to concede {Day11/164:24} and following.

131 {L18/256/1}.

132 See for instance the record of the training session of 18 March 2016 at {L11/401/1}.

133 The original reference to Jon Matonis as an early Bitcoin developer was in error and has been corrected.

134 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.

135 Wright 1, §189 {E/1/34}.

136 Wright 1, §192 {E/1/34}.

137 Wright 1, §196-197 {E/1/34}.

138 Wright 1, §204 {E/1/35}.

139 Wright 1, §206 {E/1/36}.

his *Kleiman* deposition (the latter given with reference to some notes<sup>140</sup>). Based on the agreed expert evidence, these are important to whether the session was genuine.

99. 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.<sup>141</sup> 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.<sup>142</sup> Dr Wright was then interviewed by Stuart McGurk GQ, with the reporter being accompanied by a cryptologist, Dr Nicolas Courtois.<sup>143</sup> Dr Wright says he cannot “*recall the demonstrations exactly*” that were made to the journalists.<sup>144</sup> However, he does say that he did at least demonstrate possession of the private key associated with block 9 in all his signing sessions.<sup>145</sup>
100. These signing sessions with the journalists were arranged by Mr MacGregor and Mr Matthews together. In his first witness statement, Mr Matthews had denied his involvement in public proof sessions,<sup>146</sup> but then had to qualify his position after being shown the series of emails where he was shown to be making arrangements. He admitted that he had performed a series of tasks of setting up the public sessions and making them go smoothly, but denied that these involved “arranging” the sessions.<sup>147</sup>
101. By mid-to-late April 2016, there was a plan in place for Dr Wright to sign a message with one of the keys linked to early Bitcoin blocks associated with Satoshi, and for him to post that signed message on his blog as part of the Big Reveal.<sup>148</sup> Mr Matthews accepted, grudgingly, that there was such a plan in place.<sup>149</sup> After some pressing, he accepted that, as he understood it at the time, the draft blog post was supposed to be providing a cryptographic proof.<sup>150</sup>

---

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

141 Wright 1, §211 {E/1/36}.

142 Wright 1, §212 {E/1/36}.

143 Wright 1, §214 {E/1/37}.

144 Wright 2, §23 {E/2/8}.

145 Wright 2, §24, 32 and 40 {E/2/9}.

146 {E/5/21} at [99].

147 {Day12/18:21} - {Day12/19:20}.

148 See email of 26 April 2016 at {L12/363/1}.

149 {Day12/17:22} - {Day12/18:15}.

150 {Day12/22:5} - {Day12/22:8}.

102. Mr Matthews tried in cross-examination to say that he was just going along with Mr MacGregor and that there was a conceptual divide between Mr MacGregor and Dr Wright. However, as set out above, the emails from that time tell a different story and show nothing of the supposed aggression which Dr Wright and Mr Matthews attempt to attribute to Mr MacGregor. Mr Matthews accepted this but said that the large number of emails did not represent the true picture of the relationships.<sup>151</sup>

#### The Sartre Blog Post of 2 May 2016 and its Aftermath

103. 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*”.<sup>152</sup> 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.<sup>153</sup> 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).<sup>154</sup>
104. 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.<sup>155</sup> The Economist immediately published a piece saying that his proof had come under fire and that it had requested a corrected version.<sup>156</sup> 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.<sup>157</sup> 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.<sup>158</sup> 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.<sup>159</sup>

---

151 See {Day11/167/14} and following; {Day12/19/21} and following.

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

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

154 See: {L13/205/11}; {L18/330/4}.

155 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”.

156 {L13/206/1}.

157 Wright 1, §219 {E/1/37}.

158 Wright 1, §220-221 {E/1/37}.

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

105. 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.<sup>160</sup> The email traffic shows that Mr Matonis and Mr Andresen reacted with a sense of betrayal.<sup>161</sup>
106. In cross-examination, Dr Wright for the first time disavowed his part in the emails which followed the debacle of the Sartre blog post. He claimed that, because the emails attributed to him came from an email address at nCrypt, they could not be relied upon. He said that “*my email at nCrypt was actually taken over and I was excluded from it*”.<sup>162</sup> As with his unheralded disowning of the emails from him at a Tyche Consulting address, it is easy to see why he disputed the authenticity of these emails. They tell a story of him reacting to the discrediting of the Sartre blog post by claiming that the wrong copy had been uploaded, whereas he now says that the blog post had never been intended to provide cryptographic proof that he was Satoshi. The emails also tell a story of him committing to provide further proof in various forms and then failing to make good on those promises.
107. It is convenient for Dr Wright now to disown these emails. However, as explained below, it is also wildly implausible. The other participants in the emails (including Mr Matthews and Mr Andresen) have accepted them as genuine, and the idea that some enemy of Dr Wright took over his email and made false communications with Mr Matthews and Mr MacGregor on 2 to 4 May 2016 (when the three men were speaking regularly) without anyone finding out is quite absurd. Furthermore, Dr Wright disclosed all these emails without suggesting that any of them was unreliable. Finally, and remarkably, the very email which Dr Wright told the Court was not from him and had been sent by an impostor (the email of 2 May 2016 at {L13/97}) was and remains nominated as one of Dr Wright’s primary reliance documents ({ID\_002261}). It was also a document which Dr Wright

---

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

161 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}.

162 {Day8/15:12}.

reviewed for his first witness statement<sup>163</sup> and which he did not think to mention featured false emails from someone impersonating him.

108. According to Dr Wright, he had a meeting that afternoon (2 May 2016) 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.<sup>164</sup> 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*".<sup>165</sup> 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.<sup>166</sup> Moreover, contemporaneous emails show that Dr Wright was aware of this plan and at least initially appeared to support it.<sup>167</sup>
109. 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.<sup>168</sup> 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.<sup>169</sup> She wrote: "*Ok Satoshi. Your writing is REALLY impressive.*" She also mentioned that Dr Wright had emailed to suggest a modest addition to the blog post, making clear that he had read Mr MacGregor's post as well and had approved it, subject to the addition.

---

163 Under the ID number {ID\_002274}. See: {E/1/40} at item 4.

164 Wright 1, §223 {E/1/38}.

165 Wright 1, §223-224 {E/1/38}.

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

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

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

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



110. Under cross-examination, Dr Wright disowned these emails, claiming that his wife's nCrypt email had been taken over just as his had been.<sup>170</sup> As noted above, and as further explained below, it is simply incredible that (a) this happened while remaining undiscovered at the time, despite this group of people being in contact face to face and by telephone regularly over these days and (b) Dr Wright never thought to mention in his statements or in extensive correspondence about disclosure that a whole series of relevant emails over this critical period which appear to come from him and his wife were written by an impostor.
111. 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.<sup>171</sup> Mr Matthews describes Dr Wright speaking over the phone to Mr Andresen 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.<sup>172</sup> 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.<sup>173</sup>
112. 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*".<sup>174</sup> 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

113. 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

---

170 {Day8/31:23}.

171 Wright 1, §231 {E/1/39}.

172 Matthews 1, §108 {E/5/23}.

173 {L13/360/1} and {L13/361/1}.

174 {L13/409/1}.

of the nChain Group of companies.<sup>175</sup> 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.

114. In his campaign of litigation, Dr Wright has received substantial financial support from Calvin Ayre, who has an interest in the nChain Group.<sup>176</sup> Mr Ayre has also promoted Dr Wright's claim to be Satoshi, including through the content of his Coingeek website and through social media.<sup>177</sup>

#### Dr Wright's Threats to Assert IP Rights

115. 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*".<sup>178</sup> 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.<sup>179</sup>
116. 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.
117. 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).<sup>180</sup>

---

175 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).

176 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}.

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

178 "*Forking and Passing Off...*" {L16/225/1}.

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

180 Lee 1 at {C/12/1}.

## Dr Wright's Other Litigation

118. 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.
119. 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 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.<sup>181</sup> 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.<sup>182</sup>
120. In an interlocutory judgment of 27 August 2019<sup>183</sup> 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*".<sup>184</sup> 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.<sup>185</sup> 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

---

181 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}.

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

183 {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.

184 {L15/207/27}.

185 {L15/207/20}.

how he first regained and then lost access to the private keys which were used in the “signing sessions”.

121. 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.<sup>186</sup> 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.<sup>187</sup>
122. Dr Wright was found by Chamberlain J to have advanced a deliberately false case, then sought to explain it away with further falsehoods.<sup>188</sup> 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.
123. 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*”.<sup>189</sup> 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.
124. 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

---

186 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}).

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

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

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

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,<sup>190</sup> 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”.<sup>191</sup> 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”.<sup>192</sup>

125. 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 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

126. 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”.<sup>193</sup> Mr Ager-Hanssen added that he was “convinced that Dr Craig Wright is NOT Satoshi”.<sup>194</sup> 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.
127. 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

---

190 {L18/66/1}.

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

192 {L18/66/20}.

193 {P2/111/44}.

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

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.<sup>195</sup> The mock trial exercise was revealed by Mr Ager-Hanssen, and it has since been admitted by Dr Wright, Mr Matthews and Mr Ali.<sup>196</sup>

128. 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 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.<sup>197</sup>
129. 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.
130. COPA should re-emphasise that it has had nothing to do with Mr Ager-Hanssen, contrary to the conspiracy theories of Dr Wright. COPA has relied on material publicly available due to his disclosures, but COPA and its lawyers have not otherwise approached him, worked with him or sought material from him. This is not said to disparage Mr Ager-Hanssen, but simply to make clear that COPA has no relationship with him and never has had.

### **What is COPA?**

131. 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.<sup>198</sup> COPA

---

195 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}.

196 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}.

197 See {L20/195/1}.

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

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).

132. Both in Wright 11 and during his cross-examination, Dr Wright has used the opportunity afforded by court proceedings (protected from the risk of a defamation claim) to attack COPA and its members. His wild allegations, unsupported by evidence, have been spread by Mr Ayre’s website, Coingeek, and by the cultish followers of Dr Wright’s alternative cryptocurrency, BSV. They have no relevance to the Identity Issue. However, they are relevant to the relief COPA seeks, since they show Dr Wright’s propensity to use Court proceedings as a vehicle to attack anyone who rejects his claims.

### **Relevant Procedural History**

#### Procedural chronology for the COPA Claim

133. 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:
- 133.1. 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).
- 133.2. 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 to disbar COPA from relying on any documents disclosed in the *Kleiman* litigation. Both were rejected by HH Judge Matthews in December 2021.<sup>199</sup>
- 133.3. A CCMC took place before Master Clark in September 2022 at which the directions timetable was set.<sup>200</sup>
- 133.4. 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

---

199 See judgment at {B/23/1}.

200 See CCMC order at {B/7/1}.

initially 100 documents in the list served on 4 April 2023<sup>201</sup> and Dr Wright later added a further seven documents on 2 June 2023.<sup>202</sup> Since then, Dr Wright has provided many further tranches of disclosure (now 21 tranches in total).

- 133.5. 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.<sup>203</sup> 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.
- 133.6. On 28 July 2023, the parties exchanged most of their principal witness statements and hearsay notices (with short extensions agreed for a few more).
- 133.7. On 1 September 2023, COPA served its expert report on forensic document examination from Patrick Madden (the “**Madden Report**”).<sup>204</sup> 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.
- 133.8. At a hearing in mid-September 2023, the Court addressed a number of applications.<sup>205</sup> The most substantial was an application by COPA for Dr Wright to answer the Consolidated RFI (served in late June 2023). Dr Wright was 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.
- 133.9. 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.<sup>206</sup> The Court permitted the amendments, subject to COPA's case in this regard being limited to 50 forged documents (beyond those originally pleaded)

---

201 See: {M/1/712}.

202 See: {M/1/842}.

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

204 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.

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

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



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.<sup>207</sup>

- 133.10. 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).<sup>208</sup> 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.
- 133.11. 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.<sup>209</sup> 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.
- 133.12. Since the PTR, the parties have exchanged reply evidence. They have served further reports from experts in forensic documents examination and LaTeX software.<sup>210</sup> The experts have produced joint statements, reaching near complete agreement. COPA has pleaded the additional 20 forgeries in a Schedule.
- 133.13. On Day 1 of trial (5 February 2024), the Court permitted Dr Wright to rely upon a number of additional documents which had been referenced in and/or deployed with Wright 11. As a result, and with the permission of the Court, COPA served a further report from Mr Madden.<sup>211</sup>

---

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

208 {G/3/1}.

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

210 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.

211 Madden 5 {G/9/1}.

- 133.14. During trial, COPA also served a further report of Prof. Meiklejohn<sup>212</sup> answering some points Dr Wright had made in cross-examination relevant to the signing sessions, and (in relation to the Overleaf metadata) a further report from Mr Rosendahl.<sup>213</sup> These were admitted into evidence by agreement.
- 133.15. On 29 February 2024, COPA served on Dr Wright the further Schedule of Forgery During Trial as well as Madden 6 dealing with the forged MYOB Ontier Email.<sup>214</sup> The former was agreed as a pleading amendment and deemed annexed to the Particulars of Claim, while the latter was admitted into evidence by agreement.<sup>215</sup>

### Dr Wright's Disclosure

134. Dr Wright was ordered to give disclosure against a long list of issues.<sup>216</sup> 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.
135. 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.<sup>217</sup> 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.<sup>218</sup>
136. 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.<sup>219</sup> 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,

---

212 Meiklejohn 2 {G/10/1}.

213 Rosendahl 2 {G/8/1}.

214 Madden 6 is at {G/11/1}.

215 {Day18/145:21} - {Day18/147:5}

216 See DRD at {K/1/1}.

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

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

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

he only served a list identifying himself as the custodian for most documents.<sup>220</sup> 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.<sup>221</sup> He maintained until early September 2023 that this was proper compliance, before finally agreeing to provide information on intermediate custodians.

137. Following his cross-examination, it is now clear that this Chain of Custody document is deficient, even on Dr Wright's own case. In a remarkable passage of evidence at {Day3/16:5} and following, Dr Wright cast doubt on the whole corpus of his reliance documents and their provenance.
138. Even on his own case, Dr Wright's disclosure exercise has been wholly inadequate.<sup>222</sup> 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.
139. By the start of trial, Dr Wright's disclosure had reached VOL023, his twenty-third volume of disclosure. This was supplemented during trial with (a) further Overleaf disclosure (402 documents) on 16 February 2024 and (b) 47 hard copy documents "lying around the house" found during Dr Wright's cross-examination and disclosed on 22 February 2024. The latter documents, on which Dr Wright has not even tried to rely, are mostly manuscript documents and they do not advance Dr Wright's case. COPA suspects that the reason for the late provision of this material is to give Dr Wright an excuse to offer to his supporters for the Identity Issue being resolved against him.
140. 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

---

220 See letter at {M/1/778}.

221 See letter at {M/1/943}.

222 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}.

documents. Thirdly, he claimed to have a store of LaTeX files on an online editor, Overleaf, including LaTeX drafts of the White Paper.

141. Dr Wright has accepted at least one of Mr Madden’s findings, namely that one important document (ID\_003455<sup>223</sup>) 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.<sup>224</sup>
142. 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 2023<sup>225</sup> and later explained in a letter from Shoosmiths of 11 October 2023.<sup>226</sup> 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 evidence of the parties’ experts that the BDO Drive was subject to extensive manipulation and backdating in mid-September 2023.
143. 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.<sup>227</sup> 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

---

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

224 See letter at {M/2/205}.

225 {P2/116/3}.

226 {M/2/245}.

227 See Schedule at {K/11/1}.

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.<sup>228</sup>

144. The “discovery” of the Overleaf LaTeX documents supposedly came in late November 2023 and was announced in Shoosmiths’ letter of 27 November 2023.<sup>229</sup> 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.<sup>230</sup>
145. 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 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.<sup>231</sup>
146. 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

---

228 See Exhibit CSW5 at {F/148/2}.

229 {M/2/540}.

230 See Shoosmiths’ letter of 18 December 2023 {M/2/687}.

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

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.<sup>232</sup> 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.

147. 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 agree<sup>233</sup> 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.
148. 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 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.
149. 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),<sup>234</sup> 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

---

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

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

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

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.

150. 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**

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

151.1. 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).<sup>235</sup>

151.2. 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.

151.3. 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.

---

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

- 151.4. 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.<sup>236</sup>
- 151.5. 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).
152. As noted above, the Additional Documents added as Reliance Documents since the PTR include the following categories:
- 152.1. The 97 documents from the BDO Drive: These are categorised in Section 2 of Madden 3<sup>237</sup> and further addressed both there and Appendix PM46 to Madden 4.<sup>238</sup> 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.
- 152.2. Certain LaTeX documents stored in (one of) Dr Wright’s Overleaf accounts:<sup>239</sup> As noted above, the expert evidence debunks Dr Wright’s claim that these were precursor versions of the White Paper.
- 152.3. 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.

---

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

237 {G/5/8}.

238 {H/278/1}.

239 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}.



## Overview of Cryptocurrency Technology

### Introduction

153. Bitcoin was the first cryptocurrency, originating in 2009.<sup>240</sup> 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.<sup>241</sup> 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.<sup>242</sup>
154. Bitcoin is a peer-to-peer system, meaning users can transfer payments between themselves without an intermediary or central authority.<sup>243</sup> 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.<sup>244</sup>

### Digital Signatures

155. 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.<sup>245</sup> A digital signature acts to verify the signing of a given message and involves three algorithms: KeyGen, Sign and Verify.<sup>246</sup> There are several standardised digital signature schemes, with the one being used in Bitcoin known as ECDSA (Elliptic Curve Digital Signature Algorithm).<sup>247</sup> The curve used in Bitcoin is secp256k1, and ECDSA signatures are usually encoded and expressed as 64 alphanumeric characters.

---

240 Meiklejohn, at §21(a) {G/2/9}.

241 {G/2/9}.

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

243 Meiklejohn §24 {G/2/9}.

244 Meiklejohn §25 {G/2/10}.

245 Meiklejohn §31 {G/2/11}.

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

247 Meiklejohn §34 {G/2/13}.

## Transacting in Bitcoin

156. 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.<sup>248</sup> 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).<sup>249</sup>
157. 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.<sup>250</sup> 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.
158. A transaction contains, in its simplest form, an input corresponding to the sender and one output corresponding to the recipient.<sup>251</sup> 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 contains the rest of the information detailing the transaction.<sup>252</sup> 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.<sup>253</sup>
159. 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.<sup>254</sup> To prevent double spending, Bitcoin tracks which transaction outputs are unspent and allows only those unspent outputs to spend the coins they receive.<sup>255</sup>

---

248 Meiklejohn §36 {G/2/13}.

249 Meiklejohn §38 {G/2/14}.

250 Meiklejohn §39 {G/2/14}.

251 Meiklejohn §43 {G/2/15}.

252 Ibid.

253 Meiklejohn §44 {G/2/15}.

254 Ibid.

255 Ibid.

## Transaction Ordering

160. 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.<sup>256</sup> This is the role of the Bitcoin blockchain, which acts as a ledger of all valid transactions propagated through the network.
161. 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.<sup>257</sup> 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.<sup>258</sup>
162. 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.<sup>259</sup> 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.<sup>260</sup> The difficulty level itself changes according to the expected time to produce blocks divided by the actual time, meaning that difficulty increase or decrease depending on the collective computation power.<sup>261</sup>

## Blockchain Forks

163. 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.<sup>262</sup> A backwards-incompatible change is known as a hard fork, which creates two different blockchains diverging at a single block.<sup>263</sup> The most popular cryptocurrency based on the White Paper and Genesis Block is Bitcoin. Further hard

---

256 Meiklejohn §58 {G/2/20}.

257 Meiklejohn §59 {G/2/21}.

258 Ibid.

259 Meiklejohn §69 {G/2/28}.

260 Meiklejohn §71 {G/2/29}.

261 Ibid.

262 Meiklejohn §76 {G/2/33}.

263 Meiklejohn §78 {G/2/34}.

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

164. 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.<sup>264</sup> 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.<sup>265</sup> 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).<sup>266</sup>
165. 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.<sup>267</sup> 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 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.<sup>268</sup>

### Security of Digital Signatures

166. 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.<sup>269</sup> 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

---

264 Meiklejohn §87 {G/2/37}.

265 Meiklejohn §89 {G/2/38}.

266 Meiklejohn §90, 91 {G/2/39}.

267 Meiklejohn §94 {G/2/40}.

268 Meiklejohn §95 {G/2/41}.

269 Meiklejohn §97 {G/2/41}.

“replay attack”). It is for this reason that a user must be asked to sign a new message.<sup>270</sup> This explanation is significant for the topic of the Sartre message.

167. 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.<sup>271</sup> 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:

167.1. Unique message – The message to be signed must not have been signed before for that public key.<sup>272</sup>

167.2. 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.<sup>273</sup>

167.3. 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.<sup>274</sup>

167.4. 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.<sup>275</sup>

167.5. 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).<sup>276</sup>

---

270 Meiklejohn §99-100 {G/2/42}.

271 Meiklejohn §102 {G/2/42}.

272 Meiklejohn §103(a) {G/2/43}.

273 Meiklejohn §103(b) {G/2/43}.

274 Meiklejohn §103(c) {G/2/43}.

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

276 Meiklejohn §103(e) {G/2/44}.

## Public keys Associated with Satoshi

168. 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.<sup>277</sup> 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.<sup>278</sup>

## The Evidence at Trial

169. The trial schedule was provisionally set in the PTR order<sup>279</sup> 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 indicated<sup>280</sup> 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.

170. **The *actual* trial timetable was considerably different due to:**

170.1. **Dr Wright having to be in the witness box for longer due to the admission of new documents and the need to recall him twice;**

170.2. **Dr Wright deciding to abandon both of his own forensic document examination experts after cross-examining Mr Madden;**

170.3. **Dr Wright deciding that he would not cross-examine the majority of COPA's fact witnesses<sup>281</sup>; and**

---

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

278 Meiklejohn §110 {G/2/46}.

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

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

281 **This included, in respect of Prof John MacFarlane, not notifying COPA of the intention not to call him until the morning of the day he was due to give evidence.**

- 170.4. Dr Wright’s counsel’s cross-examination of Mr Madden lasting a little over half a day, rather than the three days they had requested and been allowed at the PTR.
171. Whilst it was always envisaged that Dr Wright’s evidence might need to take longer than the six days originally scheduled, other developments during trial saw Dr Wright making serious allegations against witnesses which were then not put them. For example:
- 171.1. He accused Rory Cellan-Jones of being “very biased”, “incredibly biased”, “very pro-BTC” and wanting a “cypherpunk Satoshi”.<sup>282</sup> This accusation is nonsense. What Mr Cellan-Jones’ book reveals is a journalist who was sceptical of all cryptocurrencies (including all implementations of Bitcoin), not at all a person in the pocket of “Bitcoin Core”.<sup>283</sup> After he had used the witness box to make these accusations, Dr Wright chose not to cross-examine Mr Cellan-Jones and his lawyers agreed not to rely on their client’s allegations.
- 171.2. He made even more scandalous remarks about Martti Malmi, accusing him of setting up assassination markets and funding terrorism through Silk Road.<sup>284</sup> Mr Malmi, unlike Mr Cellan-Jones, did go in the witness box. Dr Wright’s lawyers (quite properly) did not put his scandalous allegations to Mr Malmi.
- 171.3. He claimed that both his own forensic documents experts were incompetent, absurdly describing Dr Placks as just “a psychologist” (despite his qualifications all being in computer science and document forensics) as well as questioning their independence.<sup>285</sup> He repeatedly took issue with Mr Madden’s independence, competence and the correctness of his findings, despite those findings having nearly always been agreed by his own experts. In most cases, the findings were not challenged in cross-examination.
- 171.4. Even more egregiously, he accused Mr Rosendahl of being “part of the BTC Core Group”, having “developed code with them” and “been at conferences with them”. He said that this expert had significant investments with BTC Core and

---

282 {Day8/60:17} and following.

283 See for instance Mr Cellan-Jones’ reflections in his book “Always On”, exhibited to his statement: {L18/409/26}; {L18/409/34}.

284 {Day6/165:8} - {Day6/167:8}.

285 {Day2/128:4} and following; {Day3/1:25} and following.

would lose most of his savings if Dr Wright won the case.<sup>286</sup> Mr Rosendahl said that there was not an atom of truth in these allegations, adding: “I wish I had any savings to lose”.<sup>287</sup> Dr Wright’s counsel (again, quite properly) did not put his allegations to this expert.

172. In short, Dr Wright abused the privilege given witnesses by the English legal system to publicise lies and false allegations. He has been visibly supported in this effort by a billionaire, who has used his website as a megaphone to repeat Dr Wright’s false allegations. Meanwhile, witnesses who are entirely independent of COPA and have no particular axe to grind have endured the experience of having their reputations attacked, without (in most cases) having the opportunity to answer them.
173. It is trite that Dr Wright failing to challenge COPA’s witnesses means that their evidence must be accepted. However, in this case there are further consequences of their not having been challenged. Dr Wright’s accusations against them must be taken to have been without foundation. And, where their versions contradict his account, their evidence must be taken to be true and his false.

#### COPA’s Fact Evidence

174. 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. **As noted above (and detailed further below), Dr Wright gave up the opportunity to cross-examine most of COPA’s remaining witnesses during trial.**
  - 174.1. 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.<sup>288</sup> **This evidence was unchallenged.**
  - 174.2. 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

---

286 {Day5/138:6} and following.

287 {Day17/8:1} and following.

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



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. Mr Malmi was subject to cross-examination on Day 13. He was a clear and conscientious witness who gave good evidence that was consistent with the contemporaneous documents. These documents, of course, included ones not before seen and which Dr Wright had never mentioned before finding out about them. The attempts to suggest that Mr Malmi had had contact with Dr Wright beyond what he had himself acknowledged failed miserably.<sup>289</sup>

- 174.3. 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.<sup>290</sup> 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. This evidence was unchallenged. Dr Wright clearly did not want the embarrassment of his LLM dissertation being further exposed for the work of plagiarism that it is. Furthermore, by failing to challenge Ms Pearson, Dr Wright must be taken to accept her evidence that the contents of her articles which he copied were her original ideas. His own evidence that those ideas were attributable to others should therefore be rejected. In addition, his statements that her key paper was a blog post, which explained it not being referenced, must be accepted to be false.<sup>291</sup>

---

289 See: {Day13/6:19} - {Day13/11:21}.

290 {D/490/2}.

291 {Day6/27:8}

- 174.4. 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)<sup>292</sup> 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). **This evidence was unchallenged. Dr Wright evidently realised that it could not sensibly be challenged, so he instead claimed that the document and its section which referred to EdDSA dated from after July 2011, even though it is clear from the context that he originally intended to present this as a development note from before the inception of the Bitcoin system.**
- 174.5. 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. **This evidence was unchallenged. As set out above, Mr Cellan-Jones was subject to an unjustified personal attack by Dr Wright.**
- 174.6. 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. **This evidence was barely challenged, and Mr Wilcox-O’Hearn was a clear and conscientious witness. He also revealed how passionate he was about Satoshi Nakamoto, referring to him as his “hero” and saying with some force that if, as alleged by Dr Wright, he had received bitcoin from his hero, he would certainly have remembered it.**<sup>293</sup> He was also very clear that he had not

---

292 {L1/115/1}.

293 {Day14/80:14}.

downloaded the Bitcoin source code for a number of years, explaining that he did not even use Windows at the time (the bitcoin software having been Windows-only until at least 2010).<sup>294</sup> Whilst he wanted the system to work, he thought it might be a glorious failure.<sup>295</sup> When it was put to him that he must have become more actively involved earlier, he replied disarmingly: “*You underestimate my laziness and procrastination.*”<sup>296</sup> It is thus clear that Dr Wright’s claims to have sent Bitcoin to Mr Wilcox O’Hearn were failed guesswork, based on the public information that he was the first person to have blogged about bitcoin, shortly after its release.

- 174.7. 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. **This evidence was unchallenged. Dr Wright must therefore be taken to concede that his claim that code was shared with Mr Trammell was unfounded and false.**
- 174.8. 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. **This evidence was unchallenged.**
- 174.9. 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

---

294 See for instance {Day14/75:1}.

295 {Day14/78:14}.

296 {Day14/81:2}.

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. **Dr Back gave clear and cogent evidence, backed up by contemporaneous documents. The attempts by Mr Orr KC to press Dr Back to agree with Dr Wright that the proof-of-work in Bitcoin owed no meaningful debt to Hashcash were valiant but hopeless.<sup>297</sup> It was also striking how clearly superior Dr Back was to Dr Wright in terms of technical knowledge about the Bitcoin system and code and the ability to parse and convey that information. Dr Back was challenged on his independence, but this attack was baseless.**

- 174.10. 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 authenticated<sup>298</sup> and which is used as a control copy. **This evidence was unchallenged.**
- 174.11. 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).<sup>299</sup> 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. **This evidence was unchallenged.**
- 174.12. 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

---

297 See for example the exchange from {Day13/45:2} - {Day13/53:22}.

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

299 {L7/471/1}.

claims to be Satoshi, giving examples of how Dr Wright wishes to people to lose their families and be subject to criminal law sanctions (including reference to the death penalty). This evidence was largely unchallenged. It is remarkable how short a time Mr Lee was in the witness box, given that his evidence is the primary evidence from COPA as to the need for the declaratory and injunctive relief. None of his evidence that goes to relief was challenged. Instead, there were some inconsequential fishing questions about his and Block's role within COPA and about why Meta left COPA. The latter point went nowhere because, as Mr Lee, explained, Meta's leaving was explained by the company having divested itself of its sole cryptocurrency project (Libra) months ago.<sup>300</sup>

174.13. 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. Mr Hinnant gave clear and honest evidence. He was dismissive of Dr Wright's story of having built a customised time library which he called "Chrono" based on a physics simulation engine called Project Chrono. The story was "technically so outrageous that it's... literally unbelievable". It presupposed Dr Wright having gone to great effort to create a time library out of a package with an entirely different function, with the practical results that the code might well not compile at all or might not work as intended.<sup>301</sup>

174.14. 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. This evidence was unchallenged. During Dr Wright's oral evidence, he suggested that Professor MacFarlane's account was untrue in respect of the inclusion of certain lines of source code in his software (the same lines which appear in the relevant pleaded forgeries)<sup>302</sup>. Professor Macfarlane

---

300 {Day12/113:7}.

301 See for example {Day14/43:2} - {Day14/45:1}.

302 {Day5/107:15} - {Day5/108:24}.

corrected this statement, by providing a second witness statement<sup>303</sup> setting out further detail on precisely how to download and review every release of pandoc by using a computer script, and how to identify the precise date and releases in which the code was included. That evidence, too, was unchallenged. Again, Dr Wright must therefore be taken to concede that the claim he made were unfounded and false.

- 174.15. 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. This evidence was unchallenged and Dr Wright accepted Mr Loretan’s evidence during cross-examination.<sup>304</sup>
- 174.16. 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. Mr Hearn’s evidence was clear, and the attempts to challenge him on his recollections of the meeting in Wild Honey with Dr Wright and Mr Matthews failed.<sup>305</sup> Mr Hearn was frank about what he could and could not remember, and he convincingly refuted the suggestion that his questions had any bearing on supposed new inventions of Dr Wright.<sup>306</sup>
- 174.17. 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. This evidence was unchallenged.

---

303 {C/24.3/1}

304 {Day5/106:10-20}.

305 See in particular {Day14/21:13} - {Day14/23:20}.

306 See in particular: {Day14/12:17} and {Day14/23:1}. The latter answer in particular shows how far Mr Hearn’s questions were from any supposed new inventions by Dr Wright.

- 174.18. 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. **This evidence was unchallenged and Dr Wright accepted Prof Gerlach’s evidence during cross-examination.**<sup>307</sup>
175. 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

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

- 176.1. 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.
- 176.2. 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.<sup>308</sup> Mr Stathakis and Ms Li explain in some detail that this form of Quill notepad was not available until 2012. **This evidence was challenged by Dr Wright, who claimed to know more about the printing of this notepad than those at the manufacturer who were responsible for it.**<sup>309</sup> **Dr Wright had to maintain his story that the BDO Minutes written on the Quill notepad must be genuine to 2007, so he was driven to claim that he knew through unidentified family connections that the notepad had been made earlier. He produced no witness or document to support this account, which must be**

---

307 {Day7/165:15} - {Day7/166:3}

308 ID\_004013 {L2/159/1}.

309 See: {Day3/106:6} - {Day3/108:16}; {Day 3/112:18} - {Day3/114:2}.

rejected as baseless. It is perhaps the best example of Dr Wright denying an obvious truth when trapped in a lie.

- 176.3. 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. A second hearsay statement from Mr Furche which answers false statements about him in Wright 11: {C/31/1}. As explained further below, Dr Wright was driven to accept the accounts of Mr Furche and Prof Wrightson, while weakly conceding that his previous confident statements about his dealings with them might be mistaken.
- 176.4. 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}.
- 176.5. Extracts from the Lynn Wright deposition transcripts from the *Kleiman* proceedings {C/27/1}. In cross-examination, Dr Wright sought to discredit this evidence, because Lynn Wright told the US Court that Dr Wright had never mentioned Bitcoin to her and had only once mentioned digital currency (evidence which conflicts directly with Dr Wright’s own). He attempted this by saying that she had not been fit to give evidence due to a medical procedure and treatment, and also that she had never been asked about her fitness, implying that this caused her to lose her memory on the points it did not accord with his.<sup>310</sup> This attempt was distasteful and was not justified, given that she confirmed at the start of her evidence that she was fit to testify<sup>311</sup> and given that her testimony in the transcript reads as clear and coherent.
- 176.6. 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

---

310 {Day2/97:15} - {Day2/98:4}.

311 {L16/116/8}.



on the assets of Wright International Investments Limited. It is significant because Dr Wright claims to have shared a copy of the Bitcoin White Paper with Mr Chesher before its release,<sup>312</sup> while Mr Chesher says that he did not meet Dr Wright until 2010.<sup>313</sup>

176.7. 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}. Wei Dai also explains that he has never worked in academia, contrary to Dr Wright's description of him.

### Dr Wright's Fact Evidence

177. 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.
178. After COPA's opening Skeleton Argument had been written, Dr Wright served a further three statements: Wright 13<sup>314</sup> in support of his application to rely on further documents; Wright 14<sup>315</sup> providing chain of custody information for the White Paper LaTeX files; and Wright 15<sup>316</sup> concerning the MYOB Ontier email.

---

312 {E/4/21} at para. 49m.

313 {C/26/2}, para. 6.

314 {E/32/1}

315 {E/33/1}

316 {E/34/1}

179. 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. COPA now also challenges the honesty of Mr Jenkins, in light of what happened during his re-examination. Dr Wright, Mr Matthews and Mr Jenkins are dealt with in a new section below.

*The evidence of Dr Wright's witnesses that he could be Satoshi*

180. A refrain common to a number of Dr Wright's witnesses was that, based on what they had seen, they believed he had the technical skill or expertise to have invented the Bitcoin system. In the main, this was evidence from witnesses who did not claim great technical expertise themselves and who knew of Dr Wright's abilities in the field of IT security and audit. Setting aside the doubts which Dr Wright's evidence has raised about his ability in C++ coding, this evidence from the witnesses has no probative value in relation to the Identity Issue. When asked, the witnesses had no knowledge of the abilities or experience of any of the other individuals identified as possible candidates to be Satoshi.<sup>317</sup>

*The prism of hindsight*

181. Another common feature of the evidence of many of Dr Wright's witnesses is that they are looking back on events knowing that their friend, colleague or family member has claimed to have invented the Bitcoin system. This led them to draw connections between Dr Wright's background and the attributes or work of Satoshi, whether that be an interest in Japanese culture or a commonplace concern that IT security logs should be secure against alteration. These were classic features of hindsight and of observation bias.

---

317 The Court may recall a selection of the following being put to these witnesses: Hal Finney, Nick Szabo, Dr Vili Lehdonvirta, Michael Clear, Neal King, Vladimir Oksman, Charles Bry, Shinichi Mochizuki, Gavin Andresen, Jed McCaleb, Adam Back, Ross Ulbricht, Len Sassaman. These all come from the Wikipedia page for Satoshi Nakamoto: [https://en.wikipedia.org/wiki/Satoshi\\_Nakamoto#Possible\\_identities](https://en.wikipedia.org/wiki/Satoshi_Nakamoto#Possible_identities).

182. Dr Wright's witnesses are as follows:

- 182.1. 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. Ms DeMorgan gave honest evidence, but it was of no probative value. In both her statement and the blog post on which she based it, the key reason she drew a connection between her brother and Satoshi Nakamoto was that as a teenager he had dressed as a ninja in the local park.<sup>318</sup> Nothing in her evidence gave any credence to Dr Wright's claim, and she did not support his assertion that he shared a pre-release copy of the Bitcoin White Paper with her.<sup>319</sup>
- 182.2. 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. Mr Bridges gave honest evidence, but it was of no probative value. Although his statement drew parallels between the Bitcoin system and Dr Wright's work with him, on examination these were of no significance.<sup>320</sup> He did not support Dr Wright's claim to have shared a pre-release copy of the Bitcoin White Paper with him.<sup>321</sup>
- 182.3. 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

---

318 See for instance {Day10/9:2}.

319 {E/4/21}, para. 49a.

320 He drew a parallel between Dr Wright's work for Qudos and the blockchain, but only on the basis that both featured a record of all transactions and good traceability, not based on any technical features in common: {Day11/5:19} and following. He drew a parallel between an idea pitched by Dr Wright and the blockchain, but it turned out that the only parallel was that Dr Wright was proposing a payment platform with security features: {Day11/13:7} and following.

321 {E/4/21}, para. 49.p. Furthermore, it is telling that disclosure has been given of nearly 100 emails and papers sent by Dr Wright to Mr Bridges ({ID\_006367} - {ID\_006463}), none of which addresses Bitcoin or prior digital currency systems: {Day11/6:22} and following. It is also notable that, when Dr Wright spoke to Mr Bridges about the Bitcoin pizza payment of 2010, he did not mention having created the Bitcoin system, even though he now says that he had shared the Bitcoin White Paper with Mr Bridges before its release: {Day11/15:7} and following.

statement addressing the mock cross-examination and messages he exchanged with Mr Ager-Hanssen. **Mr Matthews' evidence is dealt with below.**

- 182.4. 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. **Mr Pang accepted that his memory of both conversations from 15 years previously was “hazy” and had been improved by discussions with lawyers which had involved Dr Wright.<sup>322</sup> The account of the Lego conversation is so strange and implausible that it cannot be right, and Dr Pang could only explain it by saying that Dr Wright had a tendency to “say things that are nonsensical or funny”, such as that he had eaten “Babe” from the engaging family film about a charismatic pig. Furthermore, the real Satoshi did not use the word “blockchain” in the White Paper (although it was a term that had been mentioned in relation to HashCash).**
- 182.5. 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. **Mr Archbold gave honest evidence, but his recollections were simply of Dr Wright being a competent IT security professional. He was candid that he only believed that Dr Wright could “possibly” be Satoshi and that this belief was based on hindsight.<sup>323</sup> He did not support Dr Wright’s claim to have shared a pre-release copy of the Bitcoin White Paper with him.<sup>324</sup>**
- 182.6. 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

---

322 {Day9/25:11}; {Day9/28:10}; {Day9/32:5} and following; {Day9/37:2} and following.

323 {Day10/29:6} and following.

324 {E/4/21}, para. 49n.

at some time in or after 2009, and that Dr Wright later (in 2013) told them that it had been mining Bitcoin. Max Lynam’s evidence gave no support to Dr Wright’s claim. The communications he actually had with Dr Wright in 2008 which we have in disclosure say nothing about a digital currency project or anything like it.<sup>325</sup> Mr Lynam agreed that the only work or projects about which those communications spoke concerned IT security and digital forensics.<sup>326</sup> As for the code run for Dr Wright by Don Lynam in 2009, Max Lynam acknowledged that it was an “*unknown bit of code*”; that he did not know what it was doing; and that at the time he connected it to Dr Wright’s “*White Hat*” ethical hacking work (IT security work, which is quite different from the Bitcoin system).<sup>327</sup> He said that there was no secrecy surrounding the running of this code (as there surely would have been if it was for Satoshi, who was trying to maintain a secret identity). Before a dinner which he dated to 2013, he had no idea of Dr Wright’s claim to have invented the Bitcoin system. He could not recall having been shown the Bitcoin White Paper, as Dr Wright has claimed he was. By 2013, he had only heard the word Bitcoin from the general press and he did not connect the Bitcoin system with the code which he and his father had run for Dr Wright.<sup>328</sup> It is also telling that Mr Lynam had no knowledge of documents Dr Wright later produced which suggested wrongly that he and his family had a stake in Bitcoin mined at an early stage.<sup>329</sup>

- 182.7. 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*”. Dr Jones is a consultant who spends most of her time working for NChain on their patents. Her evidence was that Dr Wright could be Satoshi due to him having made three particular inventions recorded in three patents. Even if this evidence could conceivably be relevant (which it is not), she omitted the crucial fact that Dr Wright was not the

---

325 {Day11/25:14} - {Day11/27:24}.

326 {Day11/27:24}.

327 {Day11/28:11} - {Day11/33:3}.

328 {Day11/37:19} - {Day11/38:4}.

329 See: {Day11/42:20} - {Day11/45:11}.

sole inventor even for those. Indeed, for the first patent, all the internal documents show that the inventive work was done by Mr Savannah. Given she has personally and professionally associated herself with Dr Wright, nChain and the entire Satoshi story, it is clear that her evidence was in no way independent. She accepted that she was not a patent attorney,<sup>330</sup> but had never objected to being given that title in a series of marketing events she attended on behalf of NChain. Ms Jones' evidence gave no support to Dr Wright's case, as Lord Grabiner KC accepted by objecting that questioning her about the patents which were the subject of her statement was irrelevant to the Identity Issue.<sup>331</sup>

182.8. Shoaib Yousuf {E/7/1} – Mr Yousuf 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). Mr Yousuf gave no useful evidence for the Identity Issue. All he could say was that he had rated Dr Wright highly as an expert in IT security and that he had spoken with Dr Wright about digital payment systems such as the use of Visa and Mastercard over the internet.<sup>332</sup> He gave no support to Dr Wright's claim to have shared a pre-issue copy of the Bitcoin White Paper with him.<sup>333</sup> Even after Dr Wright's claim to be Satoshi became public, Mr Yousuf was not sufficiently interested to discuss it with him.<sup>334</sup>

182.9. 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. Mr Jenkins' evidence is addressed below.

### Witnesses whose Honesty is Challenged

183. COPA says that three witnesses of Dr Wright lied under oath: Dr Wright, Mr Matthews and Mr Jenkins.

---

330 This is presumably because, as she will be aware, patent attorney is a regulated term and she has never been admitted as a UK patent attorney and is not regulated by IPREG.

331 {Day10/64:5} and following.

332 {Day9/111:1} - {Day9/112:21}.

333 {E/4/21} at para. 49i.

334 {Day9/123:7} and following.

*Dr Wright*

184. For reasons set out throughout these submissions, COPA maintains that Dr Wright has been serially dishonest. If even a few of COPA's allegations of dishonesty or forgery are made out, it would justify the Court regarding his uncorroborated evidence as an unsafe basis for any finding. In any event, his evidence cannot be relied upon unless it is supported by other evidence which is independently reliable or unless it is against his interest. Three particular and clear examples of Dr Wright's dishonesty are given here.

185. Tyche Emails: As noted above, Dr Wright denied the authenticity of emails from him at the email address [cwright@tyche.co.uk](mailto:cwright@tyche.co.uk). His account can be seen from the following exchange:<sup>335</sup>

Q. {L11/54/1}, please. This is an email dated 25 November 2015, ostensibly from you, "cwright@tyche.co.uk", to Mr MacGregor and others. Do you say that this is another non-genuine email, something you didn't write?

A. I didn't write it, no. Tyche is a British company belonging to Rob that I never worked for.

Q. So all this content saying -- referring to the original White Paper being a good start and engaging with Mr MacGregor's ideas, that's all fake content, is it?

A. I've no idea what it is.

Q. Are you aware who supposedly created these non-genuine documents, Dr Wright?

A. Probably someone at Tyche.

Q. Who are you fingering for this?

A. I've no idea.

186. As is clear from the above, Dr Wright denied that he had ever worked for Tyche Consulting Ltd. He blamed an unknown third party for faking his email, but could not say who that was or why they had done so. Furthermore, as with so many of the Tyche emails, it is implausible that this email was faked, since it is authentic to 2015 and it says precisely what one would have expected Dr Wright to say. It even includes his characteristic mistake of spelling Dr Back's name as "Black".

---

<sup>335</sup> {Day7/109:9} - {Day7/110:3}. From that point, every time he was taken to a Tyche email he denied it was from him.

187. Dr Wright’s claim never to have worked for Tyche Consulting Ltd is comprehensively undermined by the documentary record. There is a Tyche Consulting Contract bearing Dr Wright’s signature,<sup>336</sup> and when this was put to him he could only claim that his signature had been forged.<sup>337</sup> His employment with the company was recorded in the Implementation Deed of January 2016<sup>338</sup> giving effect to the Heads of Terms he had agreed in June 2015. He had already admitted that that was a genuine document, so he could only say that he had not read it and that the reference to his employment with Tyche Consulting Ltd was wrong.<sup>339</sup>
188. Contemporaneous emails show Mr Matthews and Tyche Consulting Ltd arranging Dr Wright’s salary package and demonstrate that this employment was used for Dr Wright’s visa to move to the UK as he left Australia in late 2015.<sup>340</sup> Mr Matthews confirmed that Dr Wright had indeed been employed by Tyche Consulting Ltd and that this employment was crucial for the visa<sup>341</sup>, and provided independent details about the arrangements as explained in more detail above.
189. To add yet another piece of evidence, there is also in disclosure a documentary record of a TUPE transfer of Dr Wright’s employment from Tyche Consulting Ltd to The Workshop Technologies with effect from 1 February 2016 (demonstrating that he was employed by Tyche Consulting Ltd previously).<sup>342</sup>
190. In total, Dr Wright disclosed around 20 emails from [cwright@tyche.co.uk](mailto:cwright@tyche.co.uk), without once mentioning that these were not his own emails. Furthermore, the DRD identifies this as one of his email addresses.<sup>343</sup>
191. NAB Credit Card: On 10 June 2019 Dr Wright emailed Mr Nguyen referring to a credit card number, describing it as “my old credit card” and attaching some screenshots of supposed banking records.<sup>344</sup> As explained below, COPA maintains that the screenshots are forgeries. However, the point of relevance here is how Dr Wright described the card

---

336 {L10/426/1}

337 {Day8/5:22} - {Day8/7:7}

338 {L11/285/10}

339 {Day8/6:15} - {Day8/16:10}

340 See email at {L10/385/1}.

341 {Day11/144:19} - {Day11/145:24}.

342 {L11/329/1}.

343 {K/2/25}.

344 {H/78/1}.



when asked about it. When Dr Wright was taken to this email, his immediate response was to say that it was in fact a debit card, then adding that the card had been cancelled in 2005.<sup>345</sup>

192. He evidently made these points about the card in order to back up his wider story about the email, by saying that the email could not have been putting this card forward as the credit card he had previously claimed in interviews he had used to buy the Bitcoin.org domain.
193. Again, the documents conclusively undermine Dr Wright's story. He had disclosed an NAB statement for an "NAB Low Rate Visa" card,<sup>346</sup> which makes it very clear that the card was a credit card with Available credit of \$981 and Credit Limit of \$30,000 and describes it in the small print as a "NAB Credit Card account". The statement related to the period August / September 2008, showing that the card had not been cancelled in 2005. Faced with that evidence, Dr Wright denied that the card was a credit card and suggested that payments were being received but it was not to be used for payments.<sup>347</sup> He was then confronted with another document from his disclosure; a receipt from a garden centre<sup>348</sup> for a payment actually made with a card with this number described as an "NAB visa credit card" in May 2009. He then pivoted to saying that his wife must have used the card, despite the bank having told them not to use it. See **{Day2/79:15}** to **{Day2/82:9}**.
194. The nCrypt Emails: The third stark example of Dr Wright's dishonesty is his evidence about the nCrypt emails, already mentioned above. There are a series of emails from mid-March to early May 2016, the period of the signing sessions and the Big Reveal (including the Sartre blog), in which Dr Wright was sending and receiving messages using his nCrypt email address.<sup>349</sup> As noted above, Dr Wright disclosed these emails, reviewed a number of them for the purposes of his statement (as shown by the CPR PD57AC list) and nominated one which he now disputes as a primary reliance document.

---

345 **{Day2/30:10}** - **{Day2/31:11}**.

346 **{L7/390/1}**.

347 Although payments were also being made, as can be seen on the face of the document.

348 **{L5/70/38}**.

349 See for example **{L13/67/1}**, **{L13/78/1}** and **{L13/123/1}**.

195. However, when confronted with one which he found inconvenient from 2 May 2016, he claimed that it was not genuine and that his nCrypt email address had been taken over. He went on to claim that subsequent emails from him at that address were not genuine, and that emails from his wife at an equivalent address for her were likewise the work of an impostor.
196. Quite apart from it being highly implausible that Dr Wright would have disclosed these emails and nominated one as a primary reliance document without mentioning that they were all the work of others pretending to be him and his wife, the story does not make sense on its own terms. In particular, it is incredible that the impostor would have been able to go on sending these emails day after day, while the others on the chain were seeing and speaking to each other regularly, without the ruse being discovered.
197. This was put to Dr Wright, and he gave the following incoherent explanation:<sup>350</sup>

Q. Next question. It would be pretty strange, wouldn't it, for Mr MacGregor to deliver a real message, aimed at you, to an email address that wasn't you?

A. No. This is part of what I was explaining before, Mr MacGregor came up with the idea that if he's saying that I'm sending and telling everyone that it's mine, that that's going to be evidence that I'm on board with this and thus I need to follow what he's saying. So, part of the -- the whole thing with Tyche running all of the IT and other systems for nChain was that as soon as I didn't agree, they could cut me off my own email. That was probably one of my stupidest mistakes. By deciding just to be chief science officer, I handed over the control, the CEO or CIO, of all of the IT systems to Robert, and while I wanted just to be the research guy, the problem is, as soon as I did that, other people get to control what I do.

...

Q. Mr Matthews was spending time with you those days, including in your home in Wimbledon, wasn't he?

A. That was after this, not on the 2nd, so --

Q. But on the 3rd and the 4th?

A. He came over on those days, yes. I don't recall much of it, but he did.

Q. And Mr [MacGregor], you say, was simultaneously sending him fake messages about what you were up to even though he was spending time with you?

A. Well, this isn't when Mr Matthews was with me. I'd only just come back from Paris on the 2nd. Next, what Mr Matthews did after that is a different thing.

---

350 The full exchange is at {Day8/23:1} - {Day8/26:25}.

Q. But it was an incredibly high risk strategy, on your account, wasn't it, Dr Wright, for Mr MacGregor to be sending fake emails about what you were up to to somebody who was going to be spending time with you over the following days?

A. No, he didn't actually realise Stefan would. I talked to Stefan and had him come over. I mean, I called him and said, "Please, I need to talk to you", so I don't think Robert actually wanted him to be there, and I know Rob was incredibly angry later.

198. In short, Dr Wright's story is that, at the time when he was in fact taking the position that he would not provide public proof before further steps had been taken, Mr MacGregor was sending emails to Mr Matthews and others in Dr Wright's name taking the opposite position (i.e. that he would try straight away to provide public proof in various forms). His account is Mr MacGregor was doing this over at least several days in a series of emails while he (Dr Wright) was speaking to and spending time with Mr Matthews, all without anyone finding out. The notion is absurd.

#### *Mr Matthews*

199. Mr Matthews gave dishonest evidence that he knew of Dr Wright's work on developing Bitcoin in 2008; that he received a draft of the Bitcoin White Paper from Dr Wright in August 2008; that Dr Wright offered him Bitcoin in exchange for money in early 2009; and that Dr Wright pitched a blockchain-based project to him in early 2009. In addition, his account of the "Big Reveal" is heavily skewed by his desire to cast Mr MacGregor as a bully and so divert attention from Dr Wright's failure to provide the proof everyone expected. There are several indications of Mr Matthews' dishonesty.
200. First, in his WhatsApp exchange with Mr Ager-Hanssen on 25 September 2023 {L20/183/1}, he clearly expressed the view that Dr Wright was a fake. Responding to a message describing Dr Wright as the "Biggest fake ever", Mr Matthews replied: "*Fuck. WTF is wrong with him. Well, at least we have NCH [nChain] to focus on, that's not fake.*" Under cross-examination, he made a hopeless attempt to deny the plain meaning of these words.<sup>351</sup> He also attempted to explain the email by saying that it was intended to divert Mr Ager-Hanssen, who was threatening to "destroy" him.<sup>352</sup> However, as the Court put to him, the balance of power lay with Mr Matthews,<sup>353</sup> who in the event was able to fire Mr Ager-Hanssen and have him injunctioned. If the Court accepts that Mr

---

351 {Day11/73:15} - {Day11/79:15}.

352 {Day11/79:16} - {Day11/83:23}.

353 {Day12/100:1}.

Matthews' message bore its obvious meaning and that he intended that meaning, then he cannot have believed that Dr Wright was Satoshi Nakamoto. It follows that his evidence about receiving the Bitcoin White Paper from Dr Wright in 2008 cannot be true.

201. Secondly, Mr Matthews' account of receiving the Bitcoin White Paper from Dr Wright was in any event not plausible. It is not supported by any documentary evidence, or evidence from any other witnesses. It was not told until after 2015, when doing so served Mr Matthews' financial interests. The accounts from Dr Wright and Mr Matthews conflict, with Mr Matthews saying that the paper was provided in a USB stick containing a single file, which he printed, while Dr Wright claims that he handed over a paper copy. Mr Matthews' account in his statement also conflicted with the account Mr O'Hagan took from him and recorded in "the Satoshi Affair". See generally {Day11/89:22} - {Day11/103:20}.
202. When the Court asked Mr Matthews why he dated his receipt of the White Paper to August 2008, he let down his guard and said that his anchor point in time was that the White Paper was released publicly on 31 October 2008 and he received the paper before that time. He then tried to say that he would have been aware of that anchor point because the release was public, but when pressed he admitted that the release was not well-known at the time (and on his own evidence, he took no interest in Bitcoin after reading the paper). In the end, he could only say "*that's my understanding of how to place it in the 2008 calendar*".<sup>354</sup> In short, these answers further betrayed his story as dishonest.
203. Thirdly, it is apparent that Mr Matthews had no idea that Dr Wright was claiming to be the inventor of Bitcoin when they were reconnecting in early 2014. That is evident from his email introducing Dr Wright to Mr MacGregor in February 2014.<sup>355</sup> In that email, he put Dr Wright forward as a potential partner for a business venture concerned with cryptocurrencies but did not mention his best and singular qualification as the actual creator of the original cryptocurrency. The following exchange highlighted how ridiculous that would be:<sup>356</sup>

---

354 {Day12/97:16} - {Day12/98:11}.

355 {L8/340/2}.

356 {Day11/118/4} - {Day11/118/16}.

Q. But you were introducing two people in the context of a project about cryptocurrencies and you're saying it doesn't occur to you to mention that one of them is the inventor of the whole Bitcoin cryptocurrency blockchain system?

A. I didn't want to go to that level of detail, I wanted to introduce two people and let them find out if they had a way of working together.

Q. It's not a level of detail; it's one sentence on something which you've told us had not been a matter of secrecy.

A. I did not disclose that at the time to MacGregor. Obviously MacGregor found out later.

204. Overall, Mr Matthews was considerably more careful in his lies than Dr Wright, only lying where he had to do so to sustain Dr Wright's position. In relation to the events of 2015-16, Mr Matthews' evidence was far more consistent than Dr Wright's with the contemporaneous documents. Later in these Closing Submissions is a selection of the significant differences between Mr Matthews' evidence and Dr Wright's. It does not follow from these differences that Mr Matthews was telling the truth on all the points concerned, but it is of value on some topics where it is consistent with contemporaneous documents that Dr Wright has tried to disown.

#### *Mr Jenkins*

205. When Counsel for COPA sat down after cross-examination ended, no allegation of lying was going to be made in respect of Mr Jenkins. His evidence had been that he had discussed E-Gold with Dr Wright because it was an interest of his own; that there had been some discussion of buying Bitcoin (i.e. tokens) from Dr Wright in early 2011; that he had not received a copy of the Bitcoin White Paper from Dr Wright; and that he first discovered that Dr Wright was claiming to have invented Bitcoin at the time of the public "outing" in December 2015. When it was put to him that he could only speculate on Dr Wright being Satoshi Nakamoto based on hindsight, Mr Jenkins agreed and gave a vague answer about Dr Wright being unique and shy.<sup>357</sup>
206. However, Mr Jenkins' re-examination revealed that he had been prepared to answer questions in a certain way, but had not had the chance to do so during cross-examination. The issue arose because Mr Jenkins had confirmed in *Granath* that he had not been sent the Bitcoin White Paper – contrary to what Dr Wright claimed. In re-examination he

---

357 See {Day9/91:24} and following.

was asked if he had instead *seen* it. To this, he answered, after looking down at notes in front of him, that he had seen a paper, “*something called Timecoin*”. Dr Wright has produced a number of “Timecoin” White Papers, one of which is among COPA’s pleaded forgeries and another (with different content) was attached to one of Dr Wright’s “Papa Neema” emails and is similarly inauthentic. When one of those documents was put to Mr Jenkins, he claimed that it looked like the document shown to him.<sup>358</sup>

207. Since that evidence had not featured in Mr Jenkins’ statement or in his testimony in the Granath proceedings, the Court permitted further cross-examination, in which Mr Jenkins’ new evidence unravelled. He admitted that he had referred to a note when giving the evidence, and that the note had the word “Timecoin” written on it. At first, he agreed that he “*wrote Timecoin down on that piece of paper before [his] evidence started*”. However, when it was then put to him that this was a sign of him having been primed by others to mention Timecoin, he contradicted the evidence he had given moments before, saying: “*these were notes I took during the course of this interaction rather than anything I wrote down before the interaction*”. When pressed with the contradiction, he replied that he had written some of the notes on the piece of paper before his evidence began, but insisted that Timecoin and two other notes (each of several words) were written during his cross-examination. Even when it was put to him that he had not been seen to write anything during cross-examination, he insisted that he had.<sup>359</sup>
208. In short, Mr Jenkins contradicted himself within the space of a minute about whether the word “Timecoin” was a note written before his evidence. He lied about his having written notes during his cross-examination, when it was obvious to all in court that he had not done so.
209. The natural inference to be drawn from this sequence of events is that Mr Jenkins was indeed primed to bring up a “Timecoin” White Paper, something he had not mentioned in his witness statement in these proceedings nor in his Granath testimony; and which happens to be the title of documents of Dr Wright bearing signs of forgery. In the circumstances, it is also unlikely to be a coincidence that Dr Wright in his eleventh

---

358 See {Day9/96:19} - {Day9/99:1}.

359 See {Day9/99:16} - {Day9/105:13}.

statement had for the first time specifically claimed to have shown Mr Jenkins a copy of the “Timecoin” paper.<sup>360</sup>

210. COPA therefore seeks findings that (a) Mr Jenkins was prepared by someone to slip “Timecoin” into his evidence, and his denial of that was a lie; (b) he had written a note of “Timecoin” before he gave evidence to remind him to insert it; and (c) his claim to have written it and other notes during cross-examination was a lie.
211. As noted above, there is nothing material in the balance of Mr Jenkins’ evidence which advances Dr Wright’s case on the Identity Issue. However, given the lies he was prepared to tell, COPA submits that in general his evidence cannot be believed except to the extent that it is supported by contemporaneous documents.
212. The final curiosity with Mr Jenkins’ evidence was his repeated insistence that he had been explicitly told he should not consult any documents to aid his memory. It was not clear who might have told him that, but COPA presumes it cannot have been the lawyers who took his statement. As such, it appears either that Dr Wright (or someone else associated with him) told Mr Jenkins not to go looking for documents, or alternatively that this was another story invented by Mr Jenkins to justify why he had no documents to back up his assertions.
213. Overall, there is no probative evidence given by Mr Jenkins that in any way assists Dr Wright’s case on the Identity Issue.

#### Dr Wright’s Hearsay Evidence

214. Dr Wright relies on four documents served under a CEA notice:
  - 214.1. 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. **Mr Lynam’s evidence is addressed below in the section on Dr Wright’s failures of proof.**

---

<sup>360</sup> See Wright 11 at para. 289 {CSW/1/53}.

214.2. 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.<sup>361</sup> In an email on 4 May 2016,<sup>362</sup> 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.*”<sup>363</sup> **Mr Andresen’s evidence is addressed further below in the section on Dr Wright’s failures of proof.**

214.3. 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

215. COPA has adduced four reports of Mr Madden,<sup>364</sup> and Dr Wright has adduced two reports from Dr Placks<sup>365</sup> and one from Spencer Lynch.<sup>366</sup> 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.

---

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

362 {L13/351/1}.

363 {L18/242/1}.

364 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}.

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

366 Lynch at {I/5/5}.



216. 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 are made for a further 16 documents, while Dr Placks agrees that the remaining five are unreliable.
217. 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.
218. As noted above, Madden 5 {G/9/1} deals with the new documents that Dr Wright was permitted to adduce at the start of trial, as well as some of Dr Wright's opinion evidence in Wright 11 (such as his position on DNS server records). Meanwhile, Madden 6 {G/11/1} deals with the forged MYOB Ontier Email created and sent to Shoosmiths during this trial.
219. As for the LaTeX experts (Mr Rosendahl and Mr Lynch), they agree that:<sup>367</sup>
- 219.1. 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).
- 219.2. 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.

---

367 Joint Report at {Q/5/1}.

- 219.3. Reverse engineering the White Paper into LaTeX source code to make something superficially similar is not too difficult.
- 219.4. 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.

*Status of the document forensic evidence*

220. While it is remarkable that Dr Wright chose to dispense with the evidence of both his forensic document examination experts, the reason is not difficult to see. In the end, their expert reports were almost universally adverse to Dr Wright. Dr Placks agreed with the great majority of Mr Madden’s findings of document manipulation, while Mr Lynch reached complete agreement with Mr Madden. If these experts had been called, they would have endorsed Mr Madden’s evidence. In particular, it is evident that they would have rejected Dr Wright’s bogus technical explanations for signs of document manipulation (e.g. the effects of Citrix environments, use of normal.dotm templates and x-copy commands), since they both agreed with Mr Madden in their respective joint reports that Dr Wright’s recent witness statements did not alter any of their findings.
221. Dr Wright was so keen to get away from their evidence that he attacked both in cross-examination. He said that Dr Placks was not “*terribly independent*” and not suitably qualified to give evidence on the matters covered in his reports, being a “psychologist”.<sup>368</sup> When Dr Placks’ impressive set of qualifications and experience was put to him, he denied their relevance.<sup>369</sup> He similarly accused Mr Lynch of not being suitably qualified.<sup>370</sup> He also alleged that Mr Lynch was in a position of conflict of interest both himself and for Stroz Frieberg due to “30%” of the firm’s work coming from COPA members (a wholly unsupported allegation).<sup>371</sup> He insisted that Mr Lynch was not independent.<sup>372</sup>
222. Absurdly, Dr Wright even said in response to questions from the Court that these experts were foisted on him by his lawyers (then Travers Smith), who he said rejected a series of

---

368 {Day2/128:4} and following.

369 {Day3/1:25} and following.

370 {Day3/4:14} - {Day3/6:3}.

371 {Day3/56:19} - {Day3/57:9}.

372 {Day5/150:22} - {Day5/151:6}.

requests from him to instruct other, more suitably qualified experts.<sup>373</sup> While it is not possible to test this due to privilege, it is inherently unlikely that these experienced solicitors refused reasonable requests from their client to instruct supposedly better qualified experts.

223. As for the legal consequences of Dr Wright's decision not to call Dr Placks and Mr Lynch, COPA submits as follows:

223.1. By virtue of COPA calling Mr Madden and Mr Rosendahl, the joint statements those experts completed with their opposite numbers are in evidence, and as Lord Grabiner KC stated can be taken as read.<sup>374</sup> Accordingly, the Court can take the joint statements into account as evidence of the extent to which Mr Madden's views commanded the agreement of the experts then instructed for Dr Wright.

223.2. An inference can and should be drawn against Dr Wright from the failure to call Dr Placks and Mr Lynch. Specifically, it should be inferred that these experts would have adhered to the views recorded in the joint statements and agreed with Mr Madden on at least the matters with which they agreed in those documents.

223.3. Dr Wright is not entitled to rely upon the evidence of his experts to the extent that it diverges from Mr Madden's (unless it was put to Mr Madden and accepted by him). This is only an issue in respect of Dr Placks, and only for a very few documents in relation to his reports. Mr Lynch reached complete agreement with Mr Madden and Mr Rosendahl, and COPA does not detect any differences of view between their reports.

223.4. As a result of the decision, Mr Madden's is the only forensic document expert evidence before the Court and this is a matter of choice for Dr Wright. The Court should adopt the usual approach set out above that, where an issue is one of expert evidence and the evidence is all one way, that evidence should be accepted in the absence of exceptional reasons not to do so.

223.5. No weight should be given to assertions by Dr Wright about technical matters which lie properly within the realm of the forensic documents experts. Dr Wright

---

373 {Day3/6:5} and following.

374 {Day17/3/14}.

had the opportunity to put forward independent expert evidence on such matters and he chose not to do so. His own pseudo-expert evidence, which lacks any independence, cannot be used as a basis for challenging the true expert evidence.

224. An attempt was made to attack Mr Madden on the basis that solicitors from Bird & Bird had assisted in the preparation of his report. This challenge was not fair. In his first report, Mr Madden was entirely open about the form of assistance he had received and the reasons for it.<sup>375</sup> When cross-examined, he explained the process carefully and openly.<sup>376</sup> It is apparent from those explanations that all his findings were his own independent work and that he also took responsibility for completing the reports. Anyone reading the reports and their appendices would see that Mr Madden is extremely careful to identify every step of his investigative and analytical process.
225. Moreover, the attack is particularly unfair because (a) Mr Madden's technical findings were never disputed by Dr Wright's experts; (b) the great majority of his conclusions as to document alteration were agreed by Dr Wright's experts; and (c) Dr Wright chose not to call his own experts to dispute any of Mr Madden's findings or conclusions. In those circumstances, any suggestion that the assistance given by Bird & Bird somehow undermined the evidential value of Mr Madden's report would be wholly without merit.
226. As for the substantive cross-examination of Mr Madden, it was of very limited scope. Mr Orr KC put a number of Dr Wright's theories about how his computing environment supposedly explained some signs of document manipulation, which Mr Madden rejected. Otherwise, only the following specific documents were addressed:
- 226.1. BDO Minutes {ID\_004013};
  - 226.2. JSTOR article {ID\_004019};
  - 226.3. MStats Assignment {ID\_000073};
  - 226.4. POISSONC.odt {ID\_000260};
  - 226.5. MYOB Records {ID\_004077};

---

375 {G/1/14}, para. 33a.

376 {Day16/114:1} - {Day16:123:4}.

226.6. BDO Drive; and

226.7. Abacus Emails {ID\_001414}.

227. The unfairness of the attack on Mr Madden can be seen from the way in which he was challenged when he was explaining how gaps can arise in domain name service records and the gaps simply show an absence of information for the period: see {Day16/97:2} and following. He mentioned that he operated a couple of domains himself and had seen this phenomenon in practice. It was then put to him that he should have put this in his report, to which he said that he did not think it necessary to add, given all the points he had made in support of his opinion. There was then the following exchange:<sup>377</sup>

*Q. That doesn't answer my question. Was the matters that you are now disclosing --*

*A. It's --*

*Q. -- relevant to your opinion?*

*A. It's -- well, it's an example of my opinion. My opinion is formed independently of the information I've just shared. That would demonstrate it, but it is of a domain that is unrelated to Abacus Offshore.*

*Q. Mr Madden, you're aware that, as a result of you not including this information in your report it's unable to be tested, isn't it?*

*A. When you say "unable to be tested"?*

*Q. By my client or indeed anyone else involved in this litigation.*

*A. Well, if -- if you're saying "tested" as a legal term, then that will be that, but, you know, anyone can --*

*Q. Tested and verified?*

*A. Anyone can go onto the website and look it up, but yeah.*

*Q. Mr Madden, you're just making this up as you're going along, aren't you?*

*A. No.*

*Q. You see, what your answer doesn't address, which is the point that Stroz Friedberg made, namely that this information is showing changes?*

*A. Wrong. I would invite you to ask them to clarify the point. The service, these companies, they don't receive a -- a catalogue of this sort of information, they collect it themselves. If they do not collect it, their records incomplete. They state it quite*

---

377 {Day16/97:24} - {Day16/99:6}.

*clearly in the FAQ that their records are not complete. It is an unsafe assumption to say that just because they polled it on 3 April 2015 and received this information back, that that is when it was the first time.*

228. In the above exchange, which related to Madden 5 (a report Mr Madden had had to produce under pressure of time during trial, as a result of Dr Wright’s late disclosure), Dr Wright’s counsel:
- 228.1. complained about Mr Madden having not disclosed the DNS checks he had carried out on his own server, although they had been mentioned in response to an open question as an example of a point fully set out in the report;
  - 228.2. put to him a report from Stroz Friedberg, an hour before announcing that the expert from that firm would not be called; and
  - 228.3. accused him of making up his evidence, without a reasonable basis for the accusation.
229. Mr Madden dealt with this personal attack on his integrity with grace, but it exemplifies the weakness of Dr Wright’s position where Mr Madden’s expert reasoning and conclusions commanded the support of Dr Wright’s own experts. Dr Wright’s counsel were left with only the option to put their client’s assertions to the expert and to launch unjustified attacks on him.
230. As for Mr Rosendahl, his evidence was also unchallenged by any opposing expert evidence. The cross-examination of this expert only highlighted the frankly ridiculous story put forward by Dr Wright of how he had created the Bitcoin White Paper in LaTeX, but in doing so had to “customise” certain aspects of the LaTeX code to allow the creation of the version we recognise as the Bitcoin White Paper. It was repeatedly put to him that features of the White Paper which he concluded showed clear signs of not having been written in LaTeX could in theory (as a matter of “technical possibility”) have been produced by specially customised code.<sup>378</sup>
231. In re-examination, Mr Rosendahl pointed out that, including the creation of the diagrams, that he thought it would have taken around eight hours to write the Bitcoin White Paper

---

378 {Day17/11:3} - {Day17/20:10}.

in Open Office.<sup>379</sup> This is in comparison to the effort to do what Dr Wright claims he did in creating his own bespoke version of the LaTeX open-source software to produce the necessary effects. Mr Rosendahl explained in that regard that:

231.1. It would have taken several months of work for one individual to make the necessary changes to the TeX engine and, in his view, only very few in the world would have the requisite technical skills to do that; and

231.2. After doing that work, the person would need to create a bespoke version of the Times New Roman font, which would take a matter of further weeks for someone with the requisite technical knowledge.<sup>380</sup>

Quite apart from the fact that there is no evidence of Dr Wright having the level of technical skill with LaTeX envisaged (and strong evidence to the contrary, given his fumbleings with LaTeX vividly demonstrated in the animations created by the Developers), it is absurd to suppose that, while working on the Bitcoin White Paper and the Bitcoin Code and holding down a full-time job at BDO, Dr Wright spent several months doing entirely unnecessary work to produce the Bitcoin White Paper in LaTeX while giving the impression that it was written in OpenOffice.

### Cryptocurrency Experts

232. 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}.

233. 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,<sup>381</sup> Dr Wright is not permitted to rely on these parts of Mr Gao's report which deal with his assertion that

---

379 {Day17/33:24} - {Day17/34:6}.

380 See the exchange in re-examination at {Day17/33:14} - {Day17/35:16}.

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

BSV is the superior implementation of Bitcoin and/or the alleged fidelity of BSV to the suggested intentions of Satoshi.<sup>382</sup>

234. 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.<sup>383</sup>

235. Mr Gao’s articles and posts demonstrate an extraordinary lack of independence and objectivity. In his recent self-published book, he treats Dr Wright as a messianic figure, misunderstood by the World.<sup>384</sup>

*“Being the world’s most highly certificated cybersecurity expert, Wright knew how to secure the system.*

*Having a Master of Laws, Wright understood how the system he created would interact with real society, including the legal and political systems.*

*It all bears the marks of a deliberate Divine preparation for this creation, for where in the world can you find another person with all these necessary qualifications?”*

236. In his blog posts and articles, Mr Gao committed his personal credibility to the position that Dr Wright is Satoshi Nakamoto and made clear his strong desire to see Dr Wright prevail in this litigation. Under cross-examination, he admitted that attitude:<sup>385</sup>

*Q. And you were saying that you cared that Dr Wright should win, didn't you?*

*A. Yeah, because the result would affect the kind of Bitcoin I believe should be advanced.*

*Mr Gao also accepted that he had staked his personal reputation on the case.<sup>386</sup>*

*Q. But through these articles, and through your book, you have staked your personal credibility on this position, haven't you?*

---

382 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}.

383 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}.

384 {L20/121/67}.

385 {Day18/67:10}.

386 {Day18/74:16}.



*A. Yes.*

237. His lack of independence extended to a personal hostility to COPA, claiming that its approach in these proceedings is to trick the court,<sup>387</sup> and disputing its stated motivation for bringing this claim. Finally, and tellingly, he maintained in that there was no error of judgment in him continuing to post such articles after he had been instructed as an expert, and even in the run-up to trial.<sup>388</sup>
238. Given Mr Gao’s manifest lack of independence, his expert evidence should be treated with great caution where it diverges from that of Prof Meiklejohn. However, on the most important matters of the signing sessions and the technical aspects of cryptographic proof (including technical features within the Sartre blog), he could not dispute Prof Meiklejohn’s evidence.
239. One feature of his evidence which demonstrated his lack of independence was his attempt to make arguments about the meaning of the Sartre blog post. While accepting that it was not the cryptographic proof which Dr Wright’s backers, the journalists, Mr Andresen and Mr Matonis expected it to be, Mr Gao sought to argue that it was apparent from the words of the post that it was not offering such proof. Since the matters of technical content are not in dispute, the meaning of the blog post is not a matter for expert evidence. In any event, no weight should be given to Mr Gao’s efforts to argue for a particular interpretation of the post.
240. Finally, the vast majority of Mr Gao’s report addresses the idea that BSV is the “true version” of Bitcoin as envisioned in the Bitcoin White Paper. The Court at the PTR ruled this evidence inadmissible. It does not advance Dr Wright’s case because, even if BSV were somehow more faithful to Satoshi’s original conception of Bitcoin, that would not support Dr Wright’s claim to be Satoshi. Nothing would stop anyone creating a fork of the Bitcoin blockchain that could be said to be the most faithful to its original conception.<sup>389</sup>
241. 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

---

387 **{Day18/66:10}** and blog at **{L19/264/1}**.

388 **{Day18/75:20}**.

389 Indeed, following that line of argument through to its logical (but absurd) conclusion, someone reverting to the original protocol as released in 2009 would have the best claim to be Satoshi.

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,<sup>390</sup> which are actually of quite limited importance to the issues in the case.

242. During his cross-examination Mr Gao accepted the following points:

242.1. All that is needed for a digital signature to be verifiable and avoid a replay attack is that the verifier has ensured that a known, new message is being used. It does not improve security for the person signing to add anything to the message.<sup>391</sup> So, there was no good reason for Dr Wright to add “CSW” to the message chosen by Mr Andresen in the signing session with him.

242.2. All that is required for a simple and subversion-proof signing session is for someone to sign a new message (chosen by the verifier), and send the signature or put it onto a USB and hand that over. The verifier can then run verification software against the relevant public key and the known message on their own computer, even without connecting to the internet. This could be done in a matter of minutes.<sup>392</sup>

242.3. A public proof of possession of a private key may be given by signing an obviously new message with the key and publishing the digital signature. Anyone can then verify the signature for themselves. There is no risk of the private key being compromised (i.e. found out) by this process.<sup>393</sup>

242.4. There were straightforward means for all the signing sessions to be spoofed, including both with the journalists, the one with Mr Matonis and the one with Mr Andresen. Moreover, this could have been done in such a way that no clear warning was visible.<sup>394</sup>

242.5. It was not necessary to spend the time and effort to download the Bitcoin Core software or the entire blockchain in order to conduct the signing sessions, and

---

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

391 {Day18/5:17}.

392 {Day18/7:13} - {Day18/9:24}.

393 {Day18/11:3} - {Day18/12:1}.

394 {Day18/17:3} - {Day18/33:1} – this whole section discusses Mr Gao’s agreement with the technical steps set out in Ms Meiklejohn’s evidence about how the signing sessions could be subverted.

doing so did not confer any benefit in terms of security or preventing subversion.<sup>395</sup>

- 242.6. The Sartre blog was “*clearly not a genuine proof*” of possession of any private key.<sup>396</sup>

### ASD Experts

243. 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.
244. 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 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.
245. The adjustments were provided. In the end, Dr Wright did not display signs of emotional dysregulation and did not need the more regular breaks that were on offer to him. However, his vulnerable status was mentioned when he repeatedly made reference to privileged communications despite warnings about doing so. It should be stressed that the ASD expert evidence does not suggest that Dr Wright is incapable of understanding the concept of legal professional privilege. Dr Wright himself lays claim to advanced legal training, and there is no reason why he should be unable to understand or apply the concept that relying on communications with solicitors whose main purpose was legal advice or litigation may lead to a loss of privilege.

---

395 {Day18/38:6} - {Day18/41:8}.

396 {Day18/45:4}

246. When assessing Dr Wright’s evidence, the Court will no doubt take account of the expert evidence on the effects of his ASD. However, COPA should stress that its many challenges to Dr Wright’s credibility are not based on aspects of his demeanour or manner of giving evidence: they are based on the content of what he said, which can be shown to be straightforwardly false in so many respects.

### **Submissions on the Law Relevant to Resolution of the Identity Issue**

#### **Burden and Standard of Proof**

247. 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.
248. 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.
249. 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 (20<sup>th</sup> 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.”*

250. 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

251. 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.”*

252. 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

253. 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

254. 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.

255. 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)

256. 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

257. 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

258. 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

259. 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

260. 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.



261. 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.<sup>397</sup> 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++.<sup>398</sup> 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*”.<sup>399</sup>
262. When pressed about the fact that Dr Wright could not have been writing C++ when aged 8 to 11 (given that C++ wasn’t released until 1983 when he was 13 years old), Dr Wright did not give the obvious excuse that he might have made an error with the dates. He claimed to have been writing in precursor languages (not the account in his statement) and that he was merely “simplifying” his story so that people understand. Dr Wright then declined to cross-examine Professor Stroustrup, whose evidence had caused Dr Wright to change his story. Had Professor Stroustrup been called, he could have disputed Dr Wright’s substitute account, which is obviously why he chose to not cross-examine him.<sup>400</sup>

### Project BlackNet

264. Dr Wright claims that he began his journey with working at OzEmail on the implementation of a payment protocol known as Millicent.<sup>401</sup> 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.<sup>402</sup> 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.<sup>403</sup> 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.

---

397 Wright 1, §11 {E/1/4}.

398 Wright 1, §25 {E/1/7}.

399 Wright 1, §26 {E/1/4}.

400 See {5/161/19} - {5/163/13}.

401 Wright 1, §29 {E/1/7}.

402 Wright 1, §31 {E/1/8}.

403 Wright 1, §32 {E/1/8}.

265. 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”,<sup>404</sup> 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.*”<sup>405</sup> 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 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).
266. Cross-examination of Dr Wright merely confirmed that Project Blacknet had nothing to do with Bitcoin. Dr Wright’s attempts to tie Blacknet to being “premiered on crypto credits”, suffer from the flaw that none of the authentic Blacknet documents says anything about such crypto credits.<sup>406</sup>
267. As for the forged versions of Project Blacknet, these are addressed in more detail in the section of the Forgery Schedule concerned with {ID\_001379} (p76 of the Forgery Schedule). It is clear that the supposed extra “Stage 4” of the project has been added to try and retrospectively make Dr Wright’s Project Blacknet appear to be tied to cryptocurrency concepts.

#### Lasseter’s and Vodafone

268. 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.<sup>407</sup> It was his time at Lasseter’s that he says “*planted the seeds that would later germinate into the idea of Bitcoin*”.<sup>408</sup> Similarly, Dr Wright charts his further career development working at Vodafone as being significant

---

404 {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}.

405 {L1/80/5}.

406 {Day5/171:17} - {Day5/173:5}.

407 Wright 1, §39 {E/1/9}.

408 Wright 1, §42{E/1/10}.

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.<sup>409</sup>

269. 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.
270. Under cross-examination Dr Wright sought to distance himself from his various CVs, all of which painted a picture of him being a competent IT security professional. He blamed this on the fact that they were either written by others or tailored for certain jobs. However, even on his own account the various alternative CVs all concerned work in IT security, computer audits or digital forensics.<sup>410</sup> In any event, the overriding point is that he cannot point to reliable contemporaneous documents showing what he claims was his special expertise and interest in digital cash and transaction systems.

#### Dr Wright's Employment at BDO

271. 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.<sup>411</sup> Dr Wright says that, in 2007, he introduced Mr Granger to what would become Bitcoin, though without that name.<sup>412</sup> He also claims he discussed Bitcoin with Neville Sinclair.

---

409 Wright 1, §45-47 {E/1/9}.

410 See for instance {Day5/174:10}.

411 Wright 1, §50 {E/1/11}.

412 Wright 1, §52.

He has said on other occasions that he tried to interest BDO in investing in his nascent cryptocurrency project.

272. 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.<sup>413</sup> 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.<sup>414</sup>
273. **As set out in the Forgery Schedule, the Quill notepad dates from years after Dr Wright claims to have used it in 2007. He was left claiming that he knew more about the history of the product than those responsible for producing it (Mr Stathakis and Ms Li) who had looked into the issue and given a detailed account. His purported reason for this privileged knowledge was because he and unspecified family members supposedly worked for the production company or its predecessor. His answers on this issue became farcical.**<sup>415</sup>

#### Dr Wright's LLM Dissertation

274. 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.<sup>416</sup> He says that he analysed online payments and the cost issues plaguing online intermediaries, which “*informed [his] vision for Bitcoin*”.<sup>417</sup>
275. 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

---

413 Transcript at {E/19/3}.

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

415 {Day3/107:19} - {Day3/110:10}.

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

417 Wright 1, §58 {E/1/12}.

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.<sup>418</sup> In August 2019, Dr Wright posted a copy of the falsified proposal document on both the SSRN website<sup>419</sup> and his Slack channel,<sup>420</sup> as well as emailing a copy with the subject line “FYI. The start of bitcoin”.<sup>421</sup>

276. 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,<sup>422</sup> but perhaps the most obvious acknowledgements are missing. Large sections are plagiarised from the work of Ms Hilary Pearson, representing wholesale copyright infringement.<sup>423</sup>
277. 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.
278. As noted above, Dr Wright’s actual LLM dissertation (unlike the forged LLM proposal document) does not contain any concepts or language from the Bitcoin White Paper. Dr Wright could not safely insert fake content into the actual dissertation, since it had been filed and might be obtained. As set out in the Forgery Schedule, within the section on {ID\_000217} (at p28), Dr Wright’s self-contradictory account about his receipt of documents from the University only add evidence of his dishonesty concerning the dissertation. As to the plagiarism charge, in cross-examination he had to admit the substantial sections of Ms Pearson’s work which he had copied, and his desperate attempts to deny the charge of plagiarism with stories of an unnamed editor’s incompetence were hopeless. It is clear that he lied about this matter in his first statement

---

418 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}.

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

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

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

422 {L18/373/16}.

423 See {D/490/2}.

in the Tulip Trading case, lies which were all the more serious for being told in the context of an *ex parte* application. See generally: {Day6/23:5} - {Day6/35:24}.

### Dr Wright's MStat Degree

279. 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.<sup>424</sup> In a blog post about this course,<sup>425</sup> 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 assignment<sup>426</sup> completed by him for a tutor, Richard Gerlach, in October 2005 which contains text matching that in the White Paper.
280. In fact, the statistics assignment is a forgery, apparently based on a genuine document in disclosure.<sup>427</sup> The genuine document<sup>428</sup> addresses statistics questions and does not have any connection to Bitcoin. Prof Gerlach has given a statement in which he points to anomalous features in the forged document (thus giving independent support for Mr Madden's forensic findings). **Dr Wright chose not to cross-examine Prof Gerlach, so his evidence should be taken to be uncontested.** 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 ultimately accepted their evidence (or almost all of it).**

### Dr Wright's Claims about Writing the Bitcoin code

281. Dr Wright says he began working on the source code in 2007 using C++.<sup>429</sup> He says he initially engaged in web testing and then progressed to coding a minimum viable product prototype.<sup>430</sup> 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.<sup>431</sup>

---

424 Wright 1, §95-96 {E/1/19}.

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

426 ID\_000073 {L1/323/1}.

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

428 ID\_000077 {L1/337/1}.

429 Wright 1, §70 {E/1/14}.

430 Wright 1, §72 {E/1/15}.

431 Wright 1, §73 {E/1/16}.

He says he created a repository on SourceForge to provide a centralized location for Bitcoin source code.<sup>432</sup>

282. 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.<sup>433</sup> 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.<sup>434</sup> 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.<sup>435</sup> Mr Turner has never given evidence for Dr Wright.
283. 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).
284. When this scatter plot was put to Dr Wright, he claimed that he was working these hours, citing current supposed Audible listening times between 2am and 6.30am and boasting of listening to Audible on average 8.3 hours per day, seven days a week.<sup>436</sup> None of this is more than his assertion, and it is not credible. In particular, it is highly improbable that, having in December 2008 taken redundancy to dedicate himself to work on Bitcoin full-time (as he says he did), he made almost all his communications at these peculiar times of day. He could give no particular reason for such a bizarre working pattern.

---

432 Wright 1, §75 {E/1/16}.

433 Wright 1, §76 {E/1/16}.

434 Wright 1, §78 {E/1/16}.

435 Wright 1, §79 {E/1/16}.

436 {Day6/177:19} - {Day6/179:1}.

285. 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.<sup>437</sup> The latter appears to be an edited version of the Bitcoin source code dating from November 2008, which is publicly available.<sup>438</sup> 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.<sup>439</sup>
286. Dr Wright says that the first email account he set up was the Satoshi GMX account in around December 2007,<sup>440</sup> 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.<sup>441</sup>
287. Dr Wright’s counsel challenged Mr Malmi in cross-examination to suggest there were other, undisclosed, emails or communications between him and Satoshi from before May 2009. Mr Malmi denied that and was firm that their first communication was in May 2009.<sup>442</sup> This line of questioning descended into speculative suggestions of earlier communications between Satoshi and Mr Malmi (under the name of Trickstern) on the anti-state.com forum. There are two short answers to this speculative questioning. First, Mr Malmi denied it in evidence which was clear, consistent and credible. He was able to link the timing of his first communications with Satoshi to a move of house in late April / early May 2009.<sup>443</sup> Second, Mr Malmi only registered on the anti-state.com forum (in the name of Trickstern) on 9 April 2009 – so still two months after Dr Wright claims that Satoshi and Mr Malmi first communicated.<sup>444</sup>

---

437 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}.

438 See {L20/206/1}.

439 {L4/15/1}.

440 Wright 1, §81 {E/1/16}.

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

442 {Day13/6:19} - {Day13/6:24}.

443 {Day13/8:12} - {Day13/9:12}.

444 <https://web.archive.org/web/20100103145828/http://anti-state.com/forum/index.php?action=viewprofile;user=Trickstern>



## Drafting of the White Paper

288. In Wright 1, Dr Wright claims to have started writing the White Paper by hand, between March 2007 and May 2008.<sup>445</sup> He then claims to have started the drafting process using voice recognition software known as Dragon.<sup>446</sup> 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.<sup>447</sup> **It is important to note that not once in any of his other proceedings, prior to raising LaTeX in this case in October 2023, did Dr Wright ever claim that the Bitcoin White Paper was produced with LaTeX.**
289. 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.<sup>448</sup> There are 21 people on that list, of whom five are witnesses in this case and two are the subject of hearsay notices.<sup>449</sup> Only two of the 21 have ever corroborated Dr Wright's account in this respect – 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.
290. From March 2008 to May 2008 Dr Wright says that the draft started to look like the version that is now publicly known.<sup>450</sup> Dr Wright also gave an account in the *Kleiman* proceedings of writing the White Paper which he has avowed for these proceedings.<sup>451</sup> 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.<sup>452</sup> 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).<sup>453</sup>

---

445 Wright 1, §86 {E/1/17}.

446 Ibid.

447 Wright 1, §87 {E/1/18}.

448 Wright 4, §49 {E/4/20}.

449 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.

450 Wright 1, §88 {E/1/17}.

451 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}.

452 Wright 4, §6(c) {E/4/5}.

453 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.

291. 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.<sup>454</sup> According to Dr Wright, Mr Kleiman provided edits to the draft.<sup>455</sup> 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.<sup>456</sup> This email was among the trove of documents leaked to Wired and Gizmodo in late 2015<sup>457</sup> and it is among the forgeries originally pleaded in COPA’s Particulars of Claim.<sup>458</sup>
292. 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.<sup>459</sup> Then in August 2008 he says he reached out to Wei Dai and Adam Back under the Satoshi pseudonym. He sent them a link to upload.ae where he had uploaded the draft.<sup>460</sup> Both 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).
293. **In his first statement, Dr Wright insisted that, when he (as Satoshi) approached Dr Back with his Bitcoin concept, Dr Back was “quite dismissive” and “stated that digital cash had been attempted before and was bound to fail”. That evidence was shown to be false by Dr Back’s statement, which exhibited his previously-unpublished emails with Satoshi. Those emails showed that Dr Back was supportive, and showed Satoshi expressing gratitude. Dr Wright doubled down on his lie, first trying to deny the plain meaning of**

---

454 Wright 1, §89 {E/1/18}.

455 Ibid.

456 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}.

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

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

459 Wright 1, §90 {E/1/18}.

460 Wright 1, §91 {E/1/18}.

the emails, and then pivoting to say: “he hasn’t included all of the emails, and he also hasn’t included the extensive communications that himself and I had on Twitter and direct messages”. Needless to say, Dr Wright did not have any of those “extensive communications”. Dr Back’s evidence is that he has provided all of the emails he had with Satoshi,<sup>461</sup> and Dr Wright’s counsel did not challenge him on that evidence.

294. When it was put to Dr Wright that he was inventing the supposed additional communications with Dr Back, he launched a remarkable attack upon Dr Back (a respected computer scientist of good character):<sup>462</sup>

*“Q. He says in his witness statement of these emails, that was the extent of it, and that he's provided a copy of his email correspondence.*

*A. This morning, yesterday and the day before, he also promoted to people that Bitcoin will go up in price and that if you buy now you'll get rich. He has never promoted an actual solution. The only thing that he does every single day on his feeds and promotion is to tell people to buy into a Ponzi, "if you buy BTC, it will go to the moon and you will get rich", that is a quote from one of his things. Technically, that's actually a breach of the financial services legislation, and telling people to buy into a risky asset is not only highly irresponsible, but also criminal. So, where he is saying these things, the only thing he says is about "get rich quick, buy into this, it has to go to a million".*

*Q. Dr Wright, how was that an answer to any of my questions?*

*A. Well, if you're going to be dishonest in selling to people and getting people to buy into a highly speculative asset ... he told people online –*

*Q. Pause there. Pause there. None of this is an answer to any of my questions, is it?*

*A. Actually, yes, it is –*

*Q. These are just allegations against people you don't like, aren't they, Dr Wright?*

*A. No, actually, on his Twitter, where he said, "Sell your house, take out a mortgage, put all the money into Bitcoin because you can't lose it" –"*

295. The above exchange is a good example of how Dr Wright sought to divert from questions and did so making baseless and disgraceful allegations against others. Dr Wright’s counsel (quite properly) did not put any of those allegations to Dr Back, demonstrating that there is no supportive evidence for them.

---

461 Back, §9 {C/9/3}.

462 {Day6/68:6} - {Day6/69:20}.

296. 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.<sup>463</sup> 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*”.<sup>464</sup> However, the few communications he has provided with Microsoft<sup>465</sup> 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.
297. Dr Wright was taken through those communications in cross-examination.<sup>466</sup> He first tried to deny the plain fact that they showed him looking for a regular job in a click fraud team, not pitching a digital currency project. Then he changed tack, asserting that there were other communications with Microsoft which would have supported his account but which he no longer had. Apart from this being pure assertion, it is at odds with the emails we do have, which present a reasonably full picture of a set of communications about a regular job interview process.
298. He then claims to have implemented the core of the Bitcoin system in Hoyts, a cinema chain in Australia, and for QCSU, a bank.<sup>467</sup> However, in his dealings with the ATO, he said that he had dealt with Hoyts as a client “*in his security role*”<sup>468</sup> and that he managed the company’s firewalls.<sup>469</sup> Meanwhile, his work for Qudos Bank (formerly known as QCSU) was done through BDO, where he did straightforward IT security and audit work.
299. 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.<sup>470</sup> The evidence he has deployed to demonstrate purchase of that site has been demonstrated to be forged.

---

463 Wright 1, §96 {E/1/19}.

464 Wright 1, §98{E/1/19}.

465 See {L3/247/1} and {L3/249/1}.

466 {Day6/88:13} - {Day6/97:9}.

467 Wright 1, §96 and 98 {E/1/19}.

468 {L8/408/5}.

469 {L7/431/133}.

470 Wright 1, §100 {E/1/20}.

300. Dr Wright asserts that the essential elements of the code were already in place by the time of the upload.<sup>471</sup> Dr Wright then mentions that he engaged with Hal Finney and Mike Hearn as Satoshi<sup>472</sup> These are also known contacts of Satoshi derived from with emails in the public domain.<sup>473</sup>

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

301. Dr Wright says that he manually crafted the Genesis Block rather than mining it<sup>474</sup> 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.<sup>475</sup> He says that he chose this headline, which referred to the bank bailouts after the 2008 crash, because he strongly disagreed with the policy.<sup>476</sup> Dr Wright was not in the UK at this time, but claims to have had access to The Times through a university portal.<sup>477</sup> 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.<sup>478</sup>

302. 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.<sup>479</sup> **When confronted with this point in cross-examination, Dr Wright could only refer to an unspecified blog by himself and say that the public key to the Genesis Block (identified by Prof Meiklejohn) is only something that “looks like a public key”. He then claimed that neither of the experts in cryptocurrency technology was qualified to opine on the point because they were not cryptographers.**<sup>480</sup>

---

471 Ibid.

472 Wright 1, §105 {E/1/21}.

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

474 Wright 1, §108 {E/1/21}.

475 Wright 1, §110 {E/1/21}.

476 Wright 1, §110-111 {E/1/21}.

477 Wright 1, §110 {E/1/21}.

478 Wright 1, §112 {E/1/22}.

479 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}.

480 {Day7/54:13} - {Day7/57:4}.

303. Dr Wright asserts that in the “*early days*” the only individuals involved in mining were himself, and his family (including Don and Max Lynam).<sup>481</sup> 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.<sup>482</sup> He claims that the considerable electricity associated with mining amounted to thousands of dollars, but that he was willing to go to this expense to set the Bitcoin Blockchain in motion.<sup>483</sup> 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.<sup>484</sup> 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

304. 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.<sup>485</sup> 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.<sup>486</sup> He says that he also granted Mr Andresen access to the Bitcoin code on SourceForge, though only on a lower-level administrator basis.<sup>487</sup>

305. 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 Dr Wladimir van der Laan transferred the Bitcoin code from SourceForge to GitHub.<sup>488</sup> There is no evidence that Dr 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

---

481 Wright 1, §115 {E/1/22}.

482 Wright 1, §116 {E/1/22}.

483 Wright 1, §117 {E/1/22}.

484 Wright 1, §121 {E/1/23}.

485 Wright 1, §127-130 {E/1/24}.

486 Wright 1, §131-132 {E/1/25}.

487 Wright 1, §133 {E/1/25}.

488 Wright 1, §134 {E/1/26}.

database, and (as noted above) it is clear from contemporaneous emails that Satoshi was perfectly content with the move to GitHub.

306. Dr Wright's story about being frozen out and denied administrative privileges by Mr Malmi and others when the new server was set was undermined when Mr Malmi pointed out that (a) Satoshi would have only needed to ask to get credentials if they had wanted them, and (b) that Satoshi never requested such credentials. This latter point is unsurprising, as at that point Satoshi clearly knew they were going to leave the scene.<sup>489</sup>
307. Dr Wright attempted to maintain his position that Mr Andresen made the move to GitHub against Satoshi's wishes, but all the communications show that Satoshi approved of increasing use of GitHub. Furthermore, his insistence that he (as Satoshi) wanted to maintain eternal control of the Bitcoin source code is starkly at odds with the fact that Satoshi (a) handed over project management to Mr Andresen (including telling him that he should feel free to disable or delete SourceForge forums) and then (b) in the parting email of April 2011 urged Mr Andresen to make Bitcoin more an open source project and give more credit to developers.<sup>490</sup> Dr Wright also doggedly maintained that Dr van der Laan had been involved in making the move to GitHub, without a shred of evidence.
308. 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 did this by putting in trust all these assets, including bitcoin he claims to have mined since 2009.<sup>491</sup> He claims that 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.
309. 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).<sup>492</sup> 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

---

489 {Day13/31:1} - {Day13/31:11}.

490 {Day6/167:22} - {Day6/177:7}.

491 Wright 1, §138-140 {E/1/26}.

492 Wright 1, §187 {E/1/33}.

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**

310. 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**

311. 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 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. **Mr Madden's fifth and sixth reports show Dr Wright's pattern of forgery continuing up to and during trial.**

312. 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.

313. 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.
314. The documents found by Mr Madden to have been altered include:
  - 314.1. 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*).
  - 314.2. 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)).
  - 314.3. 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)).

- 314.4. 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 PM43<sup>493</sup>).
  - 314.5. 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.
  - 314.6. The “Papa Neema” emails and their contents, which were deployed through Wright 11 shortly before trial in combination with a byzantine account of how they came to be received.<sup>494</sup>
  - 314.7. The MYOB Ontier email, backdated and planted by Dr Wright on the email system of one set of solicitors (Ontier) before being sent to another set (Shoosmiths) to advance a dishonest case.<sup>495</sup>
315. Mr Madden also found numerous indicators of tampering. By way of example only:
- 315.1. Internal metadata timestamps contradicted by the face dating, apparent dating or external provided metadata timestamps.
  - 315.2. Metadata containing references to fonts and schemas which did not exist at the supposed time of creation of the document.
  - 315.3. 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).
  - 315.4. The presence of touchup textedit tags showing later editing of the document.
  - 315.5. 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.).

---

493 {H/219/1}.

494 Madden 5 at {G/9/29} - {G/9/49}.

495 Madden 6 at {G/11/1}.

- 315.6. Edit times and overlaps in editing times that were either impossible or very difficult to square with anything like normal user behaviour.
- 315.7. Emails apparently sent from domain names which did not exist at the supposed time of sending.
316. 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.
317. *Appendix A – the Forgery Schedule – gives further details of Dr Wright’s excuses in relation to the findings of forgery in the 10 documents set out below, and of COPA’s answers to all those excuses. Those details are not repeated here, and reference should be made to the Forgery Schedule when addressing COPA’s case on the specific pleaded forgeries. Text (in red) is only added in the following section where necessary to understand the current position.*

#### Examples from the Schedules of Forgeries

*(1) MYOB records [ID\_004077, ID\_004078 and ID\_004079] - Appendix PM7 {H/47/1}*

318. 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.<sup>496</sup> In their first joint expert statement, Dr Placks agrees with this conclusion.<sup>497</sup>
319. Dr Wright has *suggested 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.

---

<sup>496</sup> See {H/47/33} at §§58-65 and the logs at {H/53/1} and {H/55/1}.  
<sup>497</sup> {Q/2/9}.

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).<sup>498</sup>

320. Dr Wright’s account of these documents developed in Wright 11 and at trial, as set out in Appendix 1 - the Forgery Schedule. He maintained that the entries in the security logs for 6 and 7 March 2020 reflected entries had made on a local version of MYOB to record the contents of an QIF file he had had somebody extract from the online version. Meanwhile, he said that the screenshots had been taken before 6 March 2020 by his solicitors, Ontier, from a live version of MYOB to which they had been given login access in late 2019. He thus maintained that the entries he had made had not affected the records shown by the screenshots.
321. This convoluted story was shown to be false when Ontier told the parties and the Court that they had been provided with login details on 9 March 2020 and had taken the screenshots in the days that followed, a position further supported by the point that a related screenshot which showed the date of capture was taken on 9 March 2020. Dr Wright then forged the MYOB Ontier email, as set out below, in a last desperate attempt to back up his story.
322. 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).<sup>499</sup> 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 person(s) using the email addresses of Dr Wright and his current wife (Ramona Ang).<sup>500</sup> This finding is agreed by Dr Placks in the first joint statement.<sup>501</sup>
323. Dr Wright tried to answer this point in Wright 11 by claiming that both Mr Madden and Dr Placks had failed to understand how MYOB works, and that Mr Madden’s findings of entries being associated with very recent versions of MYOB software were explained

---

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

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

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

501 {Q/2/9}.

by system updates. This evidence did not account for all Mr Madden’s findings, because (for example) he had found clear evidence of backdating of entries by simply producing a log showing entries in the order in which they had been committed to the database. Mr Madden explained this clearly in his fifth report, produced during trial.<sup>502</sup> Dr Wright’s account was also plainly flawed on its own terms, since if system updates caused previous entries misleadingly to be associated with the most recent version of software, all entries would naturally show the same version. When cross-examined on these points, Dr Wright insisted upon his version, asserting features of MYOB for which he had no supportive evidence.<sup>503</sup> Quite apart from all the expert evidence ranged against him, it would be very surprising if accounting software caused such misleading and confusing entries to be committed to logs as he suggests MYOB routinely does.

(2) *Project BlackNet document [ID\_001379] – Appendix PM8 {H/60/1}*

324. 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.
325. The following features have been found in the BlackNet documents in disclosure:
- 325.1. 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 **internal** 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.
- 325.2. 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.

---

502 {G/9/4} - {G/9/10}.

503 {Day15/20:16} - {Day15/43:25}.

325.3. 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.

326. 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.

*(3) NAB Records [ID\_003455] (with attachments) – Appendix PM17 {H/78/1}*

327. 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.<sup>504</sup>

328. 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.<sup>505</sup> Following the service of the Madden Report, Dr Wright admitted that these bank records are not authentic,<sup>506</sup> 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. **This excuse is addressed further in the Forgery Schedule.**

*(4) Spoofed Email [ID\_001546] – Appendix PM21 {H/104/1}*

329. 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

---

504 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}.

505 {Q/2/9}.

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

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.<sup>507</sup> 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.<sup>508</sup>

330. **Dr Wright has admitted that this document is a forgery, but has denied his responsibility for it. That denial is addressed in the Forgery Schedule.**

*(5) Bitcoin.exe [ID\_000739] – Appendix PM12 {H/68/1}*

331. 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.
332. 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.
333. **Dr Wright has admitted that this document is a forgery, but has denied his responsibility for it. That denial is addressed in the Forgery Schedule.**

---

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

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

(6) *Timecoin ODT [ID\_000254] – Appendix PM2 {H/17/I}*

334. 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:
- 334.1. 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.
  - 334.2. 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.
  - 334.3. 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.
  - 334.4. 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.
  - 334.5. In various places, the document omits formulae which feature in the published White Paper but which would corrupt on conversion from PDF to Word.
  - 334.6. There are irregularities in line breaks and structuring of tables which similarly appear to be artefacts of conversion from a PDF original.



334.7. 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}*

335. 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,<sup>509</sup> which corresponds in time to the period of the email and the postings.

336. 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 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}*

337. 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*<sup>510</sup>) to support his account of proposing a Bitcoin project to Mr Granger and others at BDO. Dr Wright’s Chain of Custody Schedule<sup>511</sup> 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

---

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

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

511 {K/11/1}.

notepad, is that the first version of this pad was produced in March 2012.<sup>512</sup> They provided a sample proof of the version (MS1), which Mr Madden and Mr Placks have authenticated.<sup>513</sup>

*(9) Backdated Draft of the White Paper [ID\_000536] – Appendix PM3 {H/20/1}*

338. 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:<sup>514</sup>

338.1. The metadata timestamp for creation (on 24 January 2008) precisely matches that for the control copy of the White Paper<sup>515</sup> (to the day, minute and second), though one year earlier. This is either a clear sign of backdating or the most extraordinary coincidence.

338.2. 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.<sup>516</sup> This makes it implausible that the document is a preliminary draft dating to May 2008.

338.3. 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.<sup>517</sup>

338.4. 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.

338.5. Metadata showed reference to Dr Wright's details at nChain (which of course he did not join for many years).

---

512 {C/16/2}.

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

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

515 The control copy is ID\_000865.

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

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

338.6. Font files were embedded that included 2017 copyright notices.

338.7. 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}*

339. 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.<sup>518</sup> 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.<sup>519</sup> 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 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.

340. In cross-examination, Dr Wright accepted Mr Madden’s findings and that this was a forgery. He denied responsibility, claiming that, in the supposed hack of his systems by Mr Ager-Hanssen in September 2023, false versions of this document had been seeded in both InfoDef09.raw and BDOPC.raw.<sup>520</sup> As set out further in the Forgery Schedule, that account is incoherent and implausible.

Dr Wright’s Excuses and Changes of Story

341. 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

---

518 Madden 3, §§86-91 {G/5/34}.

519 See Appendix PM46, §12 {H/278/4}.

520 {Day5/76:15} - {Day5/78:19}.

Wright 9 to Wright 12), he has at great length sought to present his complex operating systems as explaining signs of apparent document alteration.

342. The Court will note that this pattern of making up excuses after being caught out continued throughout his cross-examination. Even his third trip to the witness box involved an elaborate and incredible conspiracy theory to account for his last forgery of the MYOB Ontier Email.

343. 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* evidence<sup>521</sup>)

“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 10<sup>522</sup>)

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.

344. In cross-examination, Dr Wright came up with a series of excuses for documents exhibiting signs of forgery. These are addressed in detail in the Forgery Schedule, but the main responses can be classified as follows:

344.1. False technical excuses / techno-babble – When confronted with signs of forgery revealed by the experts' analysis, Dr Wright frequently fell back on false technical excuses, notably (a) that use of normal.dotm templates on a shared Citrix environment would cause anachronistic artefacts (such as later-dated Grammarly timestamps, Mathtype references, fonts and MS schemas) to become inserted into

---

521 Transcript for 14 September 2022, internal p71 {O2/11/19}.  
522 Wright 10, §6 {E/31/2}.

files simply as a result of their being opened, without there being any user interaction to cause timestamps to update; (b) that use of a shared Citrix environment, possibly in combination with the xcopy command, could cause different documents to merge (so accounting, for instance, for hidden remnant text showing that material referring to the existing Bitcoin system had been edited out). Dr Wright has provided no evidence that the ordinary use of a Citrix environment causes documents to be affected in these ways, and indeed one would expect the many blue-chip companies which use Citrix to be horrified if it did.

Mr Madden has given clear evidence disputing Dr Wright's points, both in Madden 4<sup>523</sup> and in his oral evidence.<sup>524</sup> Dr Placks and Mr Lynch agreed with Mr Madden on these issues in their respective joint reports.<sup>525</sup> Even the report of Mr Bryant which Dr Wright applied to adduce at a late stage during trial (before promptly abandoning the attempt) did not support Dr Wright's account on the matters above. But quite apart from the substantive weakness of his excuses, Dr Wright's answers betrayed a consistent effort to "*blind with (computer) science*" (as Butcher J memorably described Dr Wright's time in the witness box in an earlier case<sup>526</sup>). Many of his answers were extremely fragmented and scattered references to computer systems seemingly at random. The conclusion that these were efforts to obfuscate becomes all the clearer when one considers his inability to explain basic aspects of C++ code and of the Bitcoin source code when under cross-examination by Mr Gunning KC for the Developers on Day 8.

- 344.2. Deliberate forgery by others – As set out below, there is a long list of those whom Dr Wright blamed for his disclosed documents bearing signs of forgery. In a number of cases he came up with conspiracy theories involving forgery by disgruntled former employees (who had unspecified grudges), Ira Kleiman, Uyen Nguyen, Christen Ager-Hanssen, Bitcoin developers, etc. As set out in the Forgery Schedule, these theories were uniformly unsupported by any evidence. Many were also implausible and failed to account for the document appearing to

---

523 See Madden 4, paras. 155 to 162 {G/6/51} - {G/6/55}. COPA would encourage the Court to read those few pages as a definitive answer to most of Dr Wright's technical excuses.

524 See in particular {Day16/35:19} - {Day16/38:11}; {Day16/125:7} - {Day16/125:18}.

525 {Q/4/6}, para. 8; {Q/6/3}, para. 9.

526 *Ang v Reliantco* [2020] EWHC 3242 (Comm) at para. 49 {L17/52/15}.

support Dr Wright's case. A few memorable examples are (i) the supposed forgery of the NAB records attached to the email at {ID\_003455} by an unnamed Reddit user just after Dr Wright had given interviews saying he had precisely such records; (ii) the supposed forgery of the Kleiman email {ID\_000465} in order to add a single paragraph which made no real difference; (iii) somebody supposedly forging a version of the Tominaga Nakamoto article and posting it online by 2016 in order to discredit an account first given by Dr Wright in an interview of 2019.

344.3. Accidental alteration by others – A common refrain of Dr Wright's in evidence was that documents could not be treated as reliable because they had been sourced from "staff laptops" and could have been edited by any number of unnamed employees over time. On Day 3, he gave a soliloquy that he was not relying on his primary reliance documents as authentic originals (to prove supposed precursor work to the Bitcoin White Paper, for instance) but as proof of his ingenuity and creativity: {Day3/16:5} and following. Later the same day, he went so far as to say that none of his documents was really from 2008 in a strict sense, "because they have all been accessed and all used" since then: {Day3/53:14} and following. Quite apart from this being a remarkable retreat from his original position that he could prove his claim to be Satoshi by authentic evidence of precursor work, it does not account for all the signs of deliberate editing and backdating to fake a documentary record to support his claim. Furthermore, for many of the documents, it is not plausible that staff engaged in work in recent years would be making use of Dr Wright's scrappy notes and postgraduate degree work from 15 years previously.

344.4. Not working linearly – Dr Wright repeatedly cited his supposedly "non-linear" working patterns to explain away evidence that documents had been derived from versions later than their supposed dates. For instance, where his supposed precursor work from early 2008 or before was found to contain text from the March 2009 version of the Bitcoin White Paper that did not feature in the August and October 2008 versions, he claimed that this was a result of eccentric "non-linear" writing methods. It is striking that in each case, these signs of backdating (based on the content of the documents) co-existed with entirely distinct forensic signs of backdating (based on expert analysis), requiring Dr Wright to deploy

multiple excuses in tandem. See for example the entries in the Forgery Schedule for {ID\_000073}, {ID\_000254} and {ID\_000536}.

345. 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.<sup>527</sup>
346. 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.
347. 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).
348. 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.

---

<sup>527</sup> 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.

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.

349. 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 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 Lynch<sup>528</sup> and Dr Placks,<sup>529</sup> as well as by Mr Madden.<sup>530</sup> **Further answers to these excuses are given above.**
350. 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.
351. 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*".<sup>531</sup>

---

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

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

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

531 See RFI Response 66 at {A/13/23}.



352. When Dr Wright gave that response about the operating systems being irrelevant, it was on 11 September 2023. So that was *after* service of Madden 1 and the week before Dr Wright’s supposed search which yielded the BDO Drive. Accordingly, it is apparent that Dr Wright had not at that stage come up with his excuse that his operating systems accounted for the defects identified in Madden 1. If Dr Wright really did have the expertise in digital forensics which he claims, then even an initial read of Madden 1 and its first few appendices would have alerted him to the findings which he now says are explained away by features of his computing environment. For example, Mr Madden’s first Appendix PM1 {H/1/1} is just 22 pages long and illustrates practically all the types of forensic finding which Dr Wright now seeks to attribute to his operating systems, and others besides.
353. His answer about the operating systems being irrelevant stands in stark opposition to what has become a central leitmotif of his defence to the first set of forgeries (i.e. those set out in Part 2 of the Forgery Schedule, addressed now in Appendix B to Wright 11).<sup>532</sup> In his oral evidence alone, Dr Wright invoked operating systems on no fewer than 102 occasions (referring variously to Windows, Linux, CentOS, Apple, Citrix, Virtual Machines and other “operating systems” in general).
354. There are further objections to Dr Wright’s attempts to attribute signs of document manipulation to the unusual effects of his operating systems.
- 354.1. He has never adduced any independent expert evidence, or clear documentary evidence, to support his assertions about the effects of his systems. Despite having Mr Madden’s report since 1 September 2023, he never found a single independent expert to support his position. This cannot be ascribed to a lack of resources of money or expertise, given the lawyers and experts he went on to recruit. Nor can it be ascribed to a reticence about introducing new evidence shortly before trial, given the applications he went on to make. Nor can it be ascribed to a lack of determination on Dr Wright’s part: anyone who could find the time to produce the mammoth Wright 11 (as well as 13 other statements since October 2023) had the time to identify experts.

---

<sup>532</sup> If the main common ‘defence’ to the first forgeries was his computing environment, then the main ‘defence’ to the later forgeries was that he was hacked.

- 354.2. There is also no factual basis for his computer environment claims beyond his own unsupported assertions. There is no supporting evidence of the precise set of systems he used, for what periods or the numbers of users. Nor is there any supporting evidence that he used any of the special versions of software that he claimed (such as Grammarly Enterprise<sup>533</sup> and Dragon Dictate Legal<sup>534</sup>). Nor is there any evidence of the forms of template supposedly used in his nChain and other computer systems which supposedly accounted for anachronistic artefacts being attached to earlier documents. Again, the absence of such evidence cannot be put down to a lack of will, inventiveness or resources.
- 354.3. Dr Wright's accounts often also involve computing environments being used in very unusual ways. For instance, he sought to account for very long edit times (which Mr Madden anyway never used as a freestanding reason for finding a document inauthentic<sup>535</sup>) by saying that he would leave Citrix sessions open for extraordinarily long periods, sometimes of more than a year in length. He suggested that numerous documents would have been opened by unnamed staff members on shared environments without their editing the documents (or even, on his account, having the ability to do so).
355. The English Courts use independent expert evidence for a very good reason. This is a case where, if Dr Wright had wanted his excuses to carry any weight, he need to find an expert who agreed with him. None could be found, and as noted above it is safe to assume that every effort was made and no expense spared.
356. Another attempt made on Dr Wright's behalf to blunt the force of the expert findings concerned the material available to the experts. Right at the start of Mr Madden's cross-examination, it was put to him that he would have been able to produce more extensive or decisive conclusions if he had had access to the computing environment on which electronic documents were produced (as well as the documents themselves). This was not a good point because, as Mr Madden had said in his reports and confirmed in re-examination, he only made the findings of inauthenticity which he could safely make on

---

533 Note that a Slack post he made attaching his fake LLM dissertation proposal in 2019 showed that he was then using the Standard version of Grammarly, not the Enterprise version, as he admitted: {Day3/66:22}.

534 Dr Wright insisted that he used Dragon Dictate Legal, which he claimed had a different logo from the Dragon Dictate logo shown on the computer screen photographs supposedly sent to him by "Papa Neema": Wright 11 at para. 278 {CSW/1/51}. But even that was wrong: {P1/20/13} and {G/9/48}.

535 Madden 1, Appendix PM24, para. 35 {H/116/12}; Madden 2, para. 47b {G/3/19}.

the material he had. Access to the computing environments would only have helped him make further findings of anomalies (as his work on the BDO Drive showed).<sup>536</sup>

357. Moreover, this line of attack was also strikingly hypocritical. From the time he began his work, Mr Madden began asking, through Bird & Bird, for such access. His request was made by letter of 18 May 2023.<sup>537</sup> This was refused in Travers Smith’s letter of 12 July 2023,<sup>538</sup> and that position was maintained thereafter. There is no basis at all for Dr Wright to complain that Mr Madden’s work was done without access to the original forensic images which he refused to provide when requested.
358. Further, the Travers Smith response needs to be considered in the context of two possible scenarios. If Dr Wright had told his lawyers that his computing environment might account for anomalies in his documents, then it would have been wrong for them to dispute the value of access to original forensic images (as they did in the letter of 12 July 2023). If, however, Dr Wright had not mentioned that his computing environment might be significant (and especially if he endorsed the position taken in the letter), then it is clear that he did not then think that it could account for anomalies in the documents.
359. Another startling feature of this case is the period of time over which Dr Wright’s forgeries have been produced.
- 359.1. 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 Trading Ltd documents to bear signs of having been forged in 2014/15.<sup>539</sup> There is full documentary evidence showing that Dr Wright purchased Tulip Trading Ltd as an “aged shelf company” in late 2014 from Abacus Seychelles.<sup>540</sup>

---

536 See for example {G/3/8} - {G/3/9} at paras 11-14.

537 {M/1/805} at para. 11.6 {M/1/810}.

538 {M/1/951} at paras. 23ff {M/1/956}.

539 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.

540 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}.

Meanwhile, a series of documents were produced, each bearing signs of alteration, to suggest that the company had been in his hands since 2011.

- 359.2. 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.
- 359.3. 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.<sup>541</sup>
- 359.4. 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.
- 359.5. He then produced the forged MYOB Ontier Email in the middle of trial, placing his counsel in the most embarrassing position on 26 February 2024 as they explained what had happened.

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 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.

---

541 See: {H/219/2}.

*Change of Story Case Study: the NAB Screenshots*

360. 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.

361. As noted above, when Satoshi was operating, the email address [satoshi@vistomail.com](mailto: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.<sup>542</sup> On 12 April 2019, in an article entitled “*Evidence and law*” he wrote that “*Bitcoin was birthed using a credit card payment*”.<sup>543</sup> 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*”,<sup>544</sup> finishing the article by saying he would provide that evidence and would do so by using the “*courts and law*.”<sup>545</sup> In this article, Dr Wright was telling the world that he would prove his creation of Bitcoin, not through signing with a private key<sup>546</sup> 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.”<sup>547</sup>

“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.”<sup>548</sup>

362. 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.<sup>549</sup> These two screenshots appear to be NAB banking

---

542 Wright 4, §13 {E/4/8}.

543 {L14/451/2}.

544 {L14/451/5}.

545 Ibid.

546 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.

547 {O4/25/34}.

548 {O4/25/36}.

549 {L15/100/1}.

records showing two transactions: AU\$ 687 to Anonymous Speech; and an AU\$ 8 transaction fee (both dated 30 August 2008).<sup>550</sup> 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.*”

363. 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*”.<sup>551</sup> Ms McGovern has passed away, so that the account cannot be checked with her.
364. 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,<sup>552</sup> and he adds in Wright 4<sup>553</sup> 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.
365. 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.

---

550 {L15/101/1}.

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

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

553 Wright 4, §16 {E/4/10}.

Further analysis of Dr Wright’s account, including his answers under cross-examination, is set out in the section of the Forgery Schedule concerning {ID\_003455} (p83).

### *Chain of Custody Schedule*

366. As pointed out above, the Chain of Custody Schedule of 13 October 2023<sup>554</sup> 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.<sup>555</sup> For example:

366.1. Bond Percolation in Timecoin (ID\_000525):<sup>556</sup> 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.

366.2. LLM Proposal (ID\_000217):<sup>557</sup> 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.

366.3. Project BlackNet (ID\_001379):<sup>558</sup> 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

---

554 {K/11/1}.

555 {H/219/1}.

556 See PM43, §§17-35 {H/219/7}.

557 See PM43, §§36-53 {H/219/16}.

558 See PM43, §§62-68 {H/219/27}.

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 Ontier MYOB Email forgery*

367. Dr Wright’s forgery of Ontier MYOB Email is the latest in time, and it is probably the most serious, since it was perpetrated during trial in a direct effort to deceive the Court and accuse reputable solicitors of a falsehood. The forgery is addressed in detail in Part 4 of the Forgery Schedule, and that content is not repeated here.
368. What is worth setting out here is the reality of what Dr Wright’s excuses mean in practical terms. When one reflects on his evidence under cross-examination and compares that evidence against the documentary evidence, what emerges is his most ridiculous cover story of all.
369. Dr Wright’s version of events requires the following to have happened:
- 369.1. On 2 December 2019, he forwards an email to Simon Cohen of Ontier which concerns documents related to Information Defense. Mr Cohen replies by asking what this relates to. Dr Wright then writes two separate replies in short order: (a) first (at 14:52) an email referring to MYOB data which has no obvious relevance to the previous emails and which actually provides no login details {X/56/2}; and (b) second (at 15:56) an email which is relevant to the rest of the chain and concerns Information Defense (i.e. the one COPA says is real) (the “**Ontier Version**”) {X/59/1}.
- 369.2. The second of those December 2019 emails remains on Ontier’s system until February 2024 and is ultimately accessible to the firm when they come to investigate at that time. For some reason, the first of them is lost and not accessed when Ontier come to investigate in February 2024.
- 369.3. At some point before 18 February 2024, somebody opposed to Dr Wright (let’s call them the “Bad Actor”) gets hold of a native version of the first of those emails (the one talking about MYOB log in details). Dr Wright has no idea who this Bad Actor could be, since hundreds of people have had access to his emails.



- 369.4. On 18 February 2024, Dr Wright decides to forward to his wife (Ramona Watts), and she decides (independently) to send to Shoosmiths, a copy of the email from 2 December 2019 talking about MYOB log in details (the “**Ramona Version**” – {X/56/2}). (The email was forwarded by him at 11:39, so the decision must have been made some time before then.) Very unluckily for Dr Wright, the Ramona Version email contains forensic signs of having been created on 18 February 2024 (the ESTMPSA timestamp format and the encoded timestamp for the image file) which the only expert evidence indicates could not be explained in the way he says.<sup>559</sup> The time stamp in the image file, usually created when the email starts being composed, is 10:17 on 18 February 2024.
- 369.5. At 11:06 on 18 February 2024, the Bad Actor sends to Ontier a spoofed version of the 2 December 2019 email concerning MYOB login details (the “**18 February 2024 Received Version**”) {X/58/1}. Assuming that the timing of this in relation to Ms Watts’ email is not a gigantic coincidence, what must have happened is as follows. The Bad Actor must have discovered (through an undiscovered bug in Dr Wright’s house) that the Ramona Version was about to be sent to Shoosmiths. The Bad Actor must have discovered this even before Dr Wright had sent the Ramona Version to Ms Watts. The Bad Actor must have spotted their chance, sprung into action and spoofed a copy of the original version of the Ramona Version email, doing so in such a way that it appeared to come from Dr Wright (something the only expert evidence indicates is at least exceptionally difficult, if not impossible, on the forensic materials). The Bad Actor must have managed to complete the spoofing in time to send the email at 11:06 (when it arrived on Ontier’s systems).
- 369.6. Tragically falling into the Bad Actor’s trap, Dr Wright forwards the Ramona Version email to Ms Watts at 11:39 and Ms Watts forwards it on to Shoosmiths at 12:56.
- 369.7. In the days that follow, the Bad Actor waits as, despite their resourcefulness and despite Dr Wright having fallen for the trap, it seems likely that the trap may

---

559 Madden 6 {G/11/14}.

have no effect. Shoosmiths do not raise any queries with Ontier and the MYOB issue goes unmentioned.

- 369.8. On the morning of Friday 23 February 2024, during COPA’s cross-examination of Dr Wright, the topic of the original MYOB screenshot documents is revisited. Dr Wright confidently says in his cross-examination that he has the emails to prove that Ontier received the MYOB login details in late 2019. That response drives Shoosmiths (whilst Dr Wright is still in the witness box) to raise a question with Ontier by emailing them the Ramona Version to check it {X/57/2}. The Bad Actor must have either foreseen COPA’s cross-examination and what followed or must have been very lucky.
- 369.9. The Bad Actor’s spoofed 18 February 2024 Received Version email is discovered by Ontier and everything falls into place, as Ontier inform Shoosmiths that they do have that email with a date header of 2 December 2019, but that the email metadata shows it was sent to Mr Cohen (who has left Ontier some time ago now) on 18 February 2024 {X/57/1}.
- 369.10. At this point the Bad Actor’s luck transcends good fortune, and Dr Wright’s misfortune is compounded, because (despite maintaining meticulous records in all other respects) Ontier must also have lost the original true MYOB email that Dr Wright originally sent on 2 December 2019, as that is apparently nowhere to be found.
- 369.11. On 26 February 2024, Lord Grabiner KC runs in detail through the set of newly disclosed emails, including the 18 February 2024 Received Version, having accepted that privilege has been waived. There is no mention in Court of this 18 February 2024 Received Version having been spoofed. It is to be assumed that Dr Wright tragically failed to mention that to his counsel, as no doubt they would otherwise have noted the point in their presentation to the Court.
- 369.12. On 29 February 2024, Dr Wright prepares Wright 15 {E/34/1}. He forgets to mention, in spite of his claims to be a leading IT security expert, that the 18 February 2024 Received Version is a fake email which must have been planted by this unknown Bad Actor. Instead, he spends his time arguing that the

“received-spf: none...” entry in the Ontier Version email (which he later accepts in cross-examination is a real email) suggests that that is a spoofed email.

370. The second possible story is that Dr Wright faked an email (the Ramona Version) to back up his story and had it sent to Shoosmiths. Having read Madden 6, he flailed around for a cover story and initially came up with (in Wright 15) one which involved denying the authenticity of the Ontier Version email, relying on server DNS records he had changed the day before. Then he either changed his mind or got confused when being cross-examined about which email he wanted to claim was fake. Ultimately, he was forced to claim that an unknown Bad Actor (from a cast of hundreds) spoofed an email with the same content as one he says is genuine in order for him to say that he has been set up.
371. Simply setting out these competing versions makes clear how absurd was the account to which Dr Wright was ultimately driven

*Changes from his RFI evidence response in Wright 4*

372. Dr Wright has made a significant number of changes to his story between Wright 4 (which was served in response to the Consolidated RFI) and his eventual oral evidence.
- 372.1. **In Wright 4 at §8:** *“I believe that there is also an encrypted image on the drive “Samsung T1 USB SSD”, the decryption keys for which I cannot find (the “Encrypted Image”)”.*<sup>560</sup> This must have been a reference to the InfoDef09.raw image, which was within an encrypted zip file. When asked for those keys, Dr Wright’s solicitors explained that Dr Wright had been “hacked”. When pressed for detail, they said that he had been hacked “at least 10” times,<sup>561</sup> but would provide no more detail for reasons of proportionality. In fact, the actual “encrypted image” had been deleted from the drive by Dr Wright not three weeks earlier, but it was recoverable on the Samsung Drive as a deleted file. Mr Madden recovered it and found it was actually just a previous copy of BDOPC.raw, containing mistakes that Dr Wright had later cleaned up before disclosure (including ChatGPT responses and all the other indications of forgery uncovered by Mr Madden).

---

560 {E/4/7}

561 {M/2/866} It is also very important to note that there is not a single piece of evidence to show that Dr Wright has been hacked even once, never mind over ten times.

- 372.2. **Wright 4 at §9-12**<sup>562</sup> – Dr Wright stated that in the *Kleiman* proceedings he was making only “generic” references to versions of the White Paper. However, in that litigation he clearly identified “*The handwritten first draft*”, “*the first typed version*”, “*the third version of about 10 pages.*”<sup>563</sup> The response was an attempt by Dr Wright to avoid providing clear particulars, and so to avoid tying himself down to a particular story. It is at odds with Dr Wright’s oral evidence at trial, which was that “*the original handwritten document is [in disclosure], and it’s been seen by multiple people*”.<sup>564</sup> None of these people have ever given evidence to that effect (Mr Matthews of course saying that his version was on a USB and not a handwritten document).
- 372.3. **Wright 4 at §16:** In October 2023, Dr Wright claimed not to remember the payment method allegedly used for purchase of the bitcoin.org domain name. Under cross-examination, in response to being faced with COPA’s pleaded forgery allegation,<sup>565</sup> Dr Wright claimed to have used “*a card associated with a WebMoney account*”,<sup>566</sup> and claimed now to remember a much more precise level of detail than was given in his written evidence. It was an obvious fiction made up on the spot, Dr Wright having forgotten what he had said in a previous statement.
- 372.4. **Wright 4 at §25-26:**<sup>567</sup> In his oral evidence, Dr Wright sought to distance himself from the SSRN upload of the Bitcoin White Paper, stating that “*I don’t know what’s on the website*” and “*It is on SSRN because staff members at nChain who manage the SSRN site loaded it.*”<sup>568</sup> This is at odds with Dr Wright’s answer to COPA’s RFI in Wright 4 at paras. 25-26,<sup>569</sup> in which he repeatedly took responsibility for the upload: “*I uploaded*”, “*I tried to upload*”, “*I uploaded to SSRN*”. The explanation at trial, that others were responsible for the uploads without Dr Wright’s knowledge, should be rejected as a dishonest attempt to distance himself from one of COPA’s original pleaded forgeries.

---

562 {E/4/7-8}.

563 Request 7 {E/4/7}.

564 {Day 5/15:16-17}.

565 {ID\_003455}, NAB banking screenshots.

566 {Day 2/45:15} - {Day2/47:11}.

567 {E/4/13-14}.

568 {Day3/171:18} - {Day3/172:11}.

569 {E/4/13-14}.

372.5. **Wright 4 at §33-35:** In response to a question to provide detail of how he destroyed a hard drive allegedly required for accessing Satoshi Nakamoto’s private keys, Dr Wright responded that he “*threw it to the ground with enough force to shatter the glass platters in the hard drive,*”<sup>570</sup> and that “*This was not a calculated action but a reaction influenced heavily by my emotional state.*”<sup>571</sup> This is at odds with Dr Wright’s previous accounts (in the Granath proceedings) of having stomped on the hard drive, as a calculated measure to prove a point. Under cross-examination in this trial, Dr Wright flailed around in an effort to reconcile the differences in his accounts of how he destroyed the drive(s) and whether it was an act on impulse or a carefully thought-out action.<sup>572</sup> He also contradicted his account in the Granath proceedings in another respect, by saying that since 2019 he had known that he could not regain access to the private keys (whereas in Granath he claimed not to know whether that was possible).<sup>573</sup>

### The New Documents

373. 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 Forgery Schedule contains further details of the findings of forgery in relation to the BDO Drive, a number of key documents on that drive and the LaTeX files.**

### *The BDO Drive Documents*

374. 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.<sup>574</sup> He claims that the BDO Drive (which was an image located on

---

570 {E/4/15} at 33.

571 {E/4/16} at 35.

572 {Day8/79:3} - {Day8/84:25}.

573 {Day8/85:1} - {Day8/87:8}.

574 Wright 5, §§7-9 {E/20/4}.

a Samsung Drive) was hidden, encrypted and password protected.<sup>575</sup> 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.

375. Mr Madden has found widespread forgery in the BDO Drive. In summary, Madden 4<sup>576</sup> makes the following findings:

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

375.2. 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.

375.3. 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.

375.4. 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

---

<sup>575</sup> Wright 5, §20 {E/20/7}.

<sup>576</sup> {G/6/1}.

modifying “Bitcoin” to “Timecoin” and altering references to 2009 and 2016 dates.

- 375.5. 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.

376. In addition, as set out in COPA’s skeleton argument for the PTR, Madden 3<sup>577</sup> 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 PM46<sup>578</sup> to Madden 4.
377. **One particular excuse given by Dr Wright for these findings deserves special mention. He sought to explain away the appearance of <chrono> and lines of code characteristic of the <chrono> time library in C++ code documents which he claimed to have written before the time when the <chrono> time library was standardised for C++ (a time fixed by the undisputed evidence of Mr Hinnant). In Wright 11, Dr Wright claimed that he had produced his own customised time library called “chrono” before the standard library was released. He said that he had derived this from Project Chrono, which is a physics**

---

577 {G/5/1}.

578 {H/278/1}.

simulation library. Mr Hinnant comprehensively refuted that explanation in his second statement.<sup>579</sup>

378. In cross-examination, it was put to Mr Hinnant that it would have been “*technically possible*” for a person to create a time library in the way suggested by Dr Wright and to come up with namespaces later used in `<chrono>`. Mr Hinnant accepted that it would be technically possible, but that it would result in undefined behaviour. Mr Orr KC then put the critical question to Mr Hinnant and received the following important answers:<sup>580</sup>

*Q. And so in summary, it is right, isn't it, that from a technical perspective, there was nothing to prevent a C++ programmer doing what Dr Wright says he did?*

*A. It is possible. It is -- does result in undefined behaviour, and it is highly, highly unlikely.*

*Q. You say it's highly unlikely because it's something that you regard as unconventional?*

*A. I say it's highly unlikely because telling me that you started with Project Chrono and ended up with `std::chrono` is -- is absurd from a technical perspective. It's like saying I started with a P51 Mustang fighter plane to create a Ford Mustang car.*

379. In re-examination, when asked to elaborate on his reasons for that view, Mr Hinnant answered:

*A. That opinion is based on the knowledge that Project Chrono has no similarity whatsoever to `std::chrono` besides the name "chrono". It's -- it's a statement that is technically so outrageous that it's -- it's literally unbelievable. I cannot believe it. The -- the mere fact that somebody says that they derived a date time library from a physics library indicates to me that they don't have the technical expertise to even write chrono from scratch, because it would actually take more work to write chrono from scratch than to derive it from a completely unrelated piece of software. Chrono did in fact derive from other libraries. It derived from the Boost.DateTime authored by Jeff Garland. And Jeff Garland and I worked on chrono together in the 2007/2008 time frame -- well, in the 2008 time frame, I'm sorry. In 2007, we were working together, but it wasn't called chrono at that point, it was called Boost.DateTime. (emphasis added)*

380. When asked what would be the effect on the code and its functioning of Dr Wright's (supposed) programming amounting to undefined behaviour, Mr Hinnant said:

*A. When a compiler encounters undefined behaviour, it is not required to admit a diagnostic, it may admit a diagnostic or it may not. It may take the code and do exactly*

---

579 {C/24.2/1}.

580 {Day14/34:4} - {Day14/34:15}



*what the programmer intends, or it may take the code and completely modify it so that it does something different and unrelated. Literally anything can happen when the compiler comes upon undefined behaviour.*

381. So, Dr Wright's explanation assumes that (a) he went to great effort to create a customized time library drawing from a physics simulation library, even though it would have been much easier to start from scratch; (b) he happened to use terms and namespaces that would later appear in the real <chrono> standard library; (c) he went to all this effort even though (as he must have known if he was a competent programmer) his programming would amount to undefined behaviour and might fail to achieve any of his intended results. Not only is this an inconceivable story and an evident lie, but it also shows either a lack of basic technical expertise or an arrogant presumption that nobody else would notice the obvious flaws in the story.

#### *The Overleaf LaTeX files*

382. 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.
383. 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.
384. 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**

385. 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

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

386. 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:<sup>581</sup>

“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)<sup>582</sup>

387. 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.<sup>583</sup>

“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.<sup>584</sup> At the time of that boast, he was well into the current proceedings (it was the time of the CCMC in the COPA Claim).

388. 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

---

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

582 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.

583 {O2/12/37} at internal p140.

584 {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.

389. 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:

389.1. 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.<sup>585</sup> 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.

389.2. 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.

389.3. 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.

389.4. 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.<sup>586</sup> Of the seven for whom the Court has

---

585 Wright 1, §52 {E/1/11}.

586 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.

- 389.5. 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.<sup>587</sup> 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.<sup>588</sup> Yet he has never been able to produce a witness to support these accounts or provide a list of names of either these individuals.
- 389.6. Lynn Wright: Dr Wright’s former wife, who gave evidence in the Kleiman proceedings. As noted above, Dr Wright claimed that that evidence was wrong in important respects (notably whether he mentioned his work on Bitcoin to her), but he has given no explanation for why she is not giving evidence in this case. Mr Ager-Hanssen leaked an email from Mr Ayre to himself and Zafar Ali KC indicating that Mr Ayre was putting pressure on Ms Wright to assist Dr Wright’s case.<sup>589</sup> If so, she appears to have resisted the pressure.
- 389.7. Ms Ramona Watts: Dr Wright’s current wife was in court with him throughout the proceedings, and clearly could have given evidence given her involvement in much of the history covered in the trial (at least events since about 2013). Her evidence would have been valuable in relation to the preparations for and undertaking of the “Big Reveal” (including about the email communications of late 2015 and May 2016 which Dr Wright disavows). Any competent trial lawyer reading the statements and documentary evidence for this case would have identified her as a potentially important witness.
390. 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

---

587 Wright 1, §126 {E/1/24}.

588 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.

589 {L5/469/6}: Emails from Mr Ayre dated 7 August 2023: “*Lynn has upside if she co-operates and helps us win... she has downside... getting funding cut and kicked out of my place, if she does not co-operate. She needs this explained to her...*”; “*Ya... she would be suicidal if she refuses to help given that I am supporting her right now on the condition that she help Craig.*”

(discussed above). He has also cited his lawyers, both living (Simon Cohen of Ontier)<sup>590</sup> and dead (Amanda McGovern of Rivero Mestre)<sup>591</sup> 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.<sup>592</sup>

### The Reliance on Don Lynam's Hearsay Evidence

391. Mr Don Lynam is Dr Wright's uncle. He is elderly and in poor health, and has recently suffered bereavement. By a hearsay notice,<sup>593</sup> Dr Wright relies on the transcript of a deposition by him from the *Kleiman* proceedings {E/16/1}. In Dr Wright's opening skeleton argument, this is described as supplying evidence of his "*knowledge of, and involvement in, early work on Bitcoin, including their review of precursors or drafts of the White Paper and running nodes for initial testing of the Bitcoin software and code*".<sup>594</sup>
392. Very little of the deposition of Mr Don Lynam is conceivably relevant to this Identity Issue before this court. That is largely because Ira Kleiman brought his claim on the premise that Dr Wright had been involved in creating the Bitcoin system (as Dr Wright had told the Kleiman family in 2014). As a result, nobody in that case had any wish or incentive to test Mr Lynam's statement that he saw a copy of the Bitcoin White Paper. Much of the questioning was directed to whether Dave Kleiman was involved in the creation of Bitcoin.
393. In his deposition, Mr Don Lynam gave an account of being close to Dr Wright and regularly discussing his work in the mid-2000s. He was asked by Dr Wright's lawyer if he was familiar with the Bitcoin White Paper, to which he answered that he had "*received the advance and pretty rough copy of it in 2008*", adding that Dr Wright had sent him a copy for his review. When asked what the paper was about, he said that he could not be sure of the heading but that it was about a "*digital monetary system*". He added that it was the precursor "*because it had the same content as the paper that came out, or very similar content*."<sup>595</sup> In response to a leading question from Dr Wright's lawyer, he

---

590 Wright 4, §19 {E/4/10}.

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

592 {L11/194/1}.

593 {E/15/3}

594 {R/14/8}

595 {E/16/26} - {E/16/27}.

confirmed that he had run a node for Dr Wright after the release of the Bitcoin system and that doing so had caused his brand-new computer to become very hot and noisy, adding to his electricity bill.<sup>596</sup> When cross-examined by Mr Kleiman’s lawyer, Mr Lynam said that he could not remember how he had received the paper.<sup>597</sup> He said that he had not attempted to edit it.<sup>598</sup>

394. The material in disclosure paints a different picture. An email in May 2008 provides a family update about Dr Wright’s LLM qualification.<sup>599</sup> Another, from December 2008,<sup>600</sup> is titled “*Pop’s Service Records*” and provides another update about Dr Wright’s newest qualifications with a note that “*the farm is going well*”. Neither of these mentions anything relating to Bitcoin at all. The emails do not suggest any relationship of regular contact and sharing research, but a distant relationship of occasional updates.
395. There is nothing further until 2019, when Mr Don Lynam was being asked to supply an account for the Kleiman case. Mr Lynam wrote to Dr Wright,<sup>601</sup> making clear that Dr Wright had “*advised*” Mr Lynam of what the evidence was to be: “*Memory is a bit foggy of my playing to link as part of the network in the way that you advised*”. Mr Lynam at that stage was unsure of the year Dr Wright supposedly told him of his invention (“*since you emailed me in 2007/8/9 about your new currency invention*”).
396. Dr Wright responded to the effect that he may be able to assist Mr Lynam to trace the coins represented by any early Bitcoin mining. Shortly afterwards, Dr Wright’s lawyers evidently suggested the same thing, because Mr Lynam later wrote: “*The lady lawyer said that they were valuable now as motivation to search*”.<sup>602</sup>
397. Following this prompting and the promise of value, Mr Lynam gradually improved his account to prepare for his deposition. By 10 September 2019, he began describing more detail in an email, offering a narrative to Dr Wright for comment (“*Is this all some sort of fantasy in my mind or did this really happen? My recollection (or dream??) is that you set me up to mine Bitcoin...*”).<sup>603</sup> According to what he later said in his deposition, he

---

596 {E/16/34} - {E/16/36}.

597 {E/16/65}

598 {E/16/64}

599 {L2/491/1}

600 {L3/321/1}

601 {L15/209/2}

602 {L15/322/3}

603 {L15/322/3}

“went back researching” for references to Mr Kleiman on the internet;<sup>604</sup> he bought books about Satoshi Nakamoto;<sup>605</sup> he discussed his deposition with Dr Wright’s mother and joined Twitter for the first time specifically to follow what was happening with Dr Wright.<sup>606</sup> He continued researching even up to the week before his deposition.<sup>607</sup>

398. By the time of his deposition, then, Mr Don Lynam (then aged nearly 80 years) no longer had difficulty recalling the dates and events. As noted above, he was no longer unsure as to whether the year of Dr Wright discussing his supposed invention was 2007, 2008 or 2009.

399. Had Mr Lynam been called to give evidence in this case, it would have been possible to investigate why his memory worked in reverse, becoming clearer as the weeks progressed even though months earlier the details had seemed “foggy”, a “dream”, “some sort of fantasy”. There is good reason to doubt the accuracy of what he had come to believe, having been “advised” by Dr Wright of the facts he was required to state, “motivated” to search for what could be “valuable” to him, and pointed by Dr Wright’s mother to follow the social media narrative that Dr Wright was posting during that time.

400. As for the one point on which Dr Wright really seeks to place heavy reliance (i.e. Mr Don Lynam’s supposed sight of a draft of the Bitcoin White Paper), Mr Don Lynam and Dr Wright diverge on the detail. In particular, Dr Wright has insisted at various times that his uncle actively edited the draft, as a result of which he (Dr Wright) considered his uncle a central contributor to Bitcoin. By contrast, in his *Kleiman* deposition, Mr Don Lynam said that it was “way above [him] technically”<sup>608</sup> and that he had not edited it, stressing that he had actively decided not to edit it.<sup>609</sup> In summary, and with the relevant quotations:

400.1. In his deposition in the Kleiman proceedings, Dr Wright said that “*Dave helped me edit part of the White Paper, as with other people, including Doug [Don] Lynam, some of my other family...*”<sup>610</sup>

---

604 {E/16/32-33} at 33 line 21

605 {E/16/79} at line 11

606 {E/16/81}

607 {E/16/75} - {E/16/76}

608 {E/16/26}

609 {E/16/61} and the following pages.

610 {L16/267/22} at internal p85, l.12.

- 400.2. By contrast, Mr Don Lynam said that he “*did not attempt to edit the paper*” and that if someone said that he had edited it, “*that would be incorrect*”.<sup>611</sup>
- 400.3. Mr Don Lynam also made clear that he did not have “*any technical input into establishing or operating*” the Bitcoin system.<sup>612</sup> This is starkly in contrast to Dr Wright’s story that Mr Don Lynam was “*one of the three people behind Bitcoin*” – a contorted story discussed above.<sup>613</sup>
401. It is also difficult to reconcile Mr Don Lynam’s evidence of being made fully aware of Dr Wright’s digital currency project and the evidence given by his son Max Lynam, which (as discussed above) was that he first became aware of the project several years later and that he was only aware of the family running an “*unknown bit of code*” for Dr Wright (which he said was not unusual in their family).
402. Finally, the detail given by Mr Don Lynam of his new computer becoming hot and noisy (and costing more in electricity) as a result of running the Bitcoin code is not plausible, given the expert evidence about the early Bitcoin mining. However, it does chime with Dr Wright’s false understanding of early Bitcoin mining.

### The Timecoin Paper

403. In his original reliance documents, Dr Wright included many supposed versions of the Bitcoin White Paper, including a purported precursor draft with the title “Timecoin” {ID\_000254} (which supposedly dated from 2008). That document is a forgery, for reasons given in the Forgery Schedule at Appendix A.
404. During his evidence at trial, Dr Wright repeatedly sought to use the “Timecoin” moniker in relation to his work developing Bitcoin. Part of the motivation appears to have been to explain away his witnesses’ inability to remember being given a document referencing “Bitcoin”.
405. In Wright 11, Dr Wright told the story of receiving emails from a lawyer, Denis Mayaka, under the alias “Papa Neema”. That story is addressed below. In a remarkable feature of the story, Dr Wright claimed that Mr Mayaka had responded to his request for documents relating to the formation of two Seychelles companies by sending him on 10

---

611 {E/16/62} at line 21 to {E/16/64} at line 7

612 {E/16/64}

613 {Day6/129:7} - {Day6/132:22}



September 2023: (a) some invoices relating to those companies; and (b) a “Timecoin” paper, “TimeDoc2.pdf” {CSW/31/1} ({ID\_006565}), which supposedly dated from April 2009 and presented a development of Bitcoin on behalf of Information Defense (one of Dr Wright’s companies). This is remarkable for at least three reasons. First, there was no reason for Mr Mayaka (a company formation agent) to have a copy of the Timecoin paper. Secondly, Dr Wright had not asked for this document or anything like it. Thirdly, by a striking coincidence, this document (which was not in his original disclosure) came to Dr Wright by two means in mid-September 2023; once from “Papa Neema” on 10 September 2023 and a second time through his happy discovery of the Samsung Drive on 15 September 2023 (which as Mr Madden found contained a hash-identical document<sup>614</sup>). Dr Wright had no good explanation<sup>615</sup> for that coincidence.<sup>615</sup>

406. In Wright 11, Dr Wright claimed that he had sent this document to a series of individuals, including Mr Bridges, Mr Jenkins, Mr Matthews and various unnamed others at QSCU, Centrebet and Hoyts.<sup>616</sup> In a direct contradiction of Wright 4, he said that he had not sent the original Bitcoin White Paper to Mr Bridges or Mr Jenkins. The only person who gave any support to this account was Mr Jenkins, who said that he had been shown (not sent) a copy of such a document. As submitted above, he had never mentioned this in his Granath evidence or his witness statement, and it became clear that he had been primed to add the reference to his evidence.
407. The Timecoin paper supposedly supplied by Papa Neema (and on the Samsung Drive) was light on metadata but contained features that led Mr Madden to doubt its authenticity, including (a) the fact that diagrams had been embedded as low resolution picture images, consistent with having been copied in as screenshots from a public source; and (b) irregular metadata timestamps which were of a date (31 October 2017) associated with the 2023 editing process that created BDOPC.raw.<sup>617</sup> Furthermore, the content of the Timecoin paper is very odd. It has an abstract which is very similar to that of the Bitcoin White Paper, including detailing proof-of-work and outpacing, but the body of the paper then includes a mix of copied and paraphrased sections of the Bitcoin White Paper while missing out the sections on proof-of-work and outpacing. Some incongruous IT security

---

614 Madden 5, para. 104 {G/9/34}.

615 {Day15/57:16} and following.

616 Wright 11 at para. 289 {CSW/1/53}.

617 Madden 5, paras. 104-126 {G/9/34} and following.

features (including Tripwire) are then bolted on to tie the document to Dr Wright's areas of expertise.<sup>618</sup> It bears all the signs of a forgery prepared in haste to suggest Dr Wright developing the Bitcoin project in early 2009.

#### Failure to Provide Reliable Documentary Evidence

408. 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:

408.1. 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.

408.2. 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 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.<sup>619</sup> 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.<sup>620</sup> He has also given inaccurate accounts in relation to Mr Malmi, Dr Back, Mr Andresen and Wei Dai, as set out above.

408.3. 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.

---

618 See cross-examination at {Day15/63:16} - {Day15/91:8}.

619 Bohm 1, §15 {C/10/4}.

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

- 408.4. 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.
409. 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.
410. 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.<sup>621</sup> However, in Wright 4, he attempted to prove that he had had access in 2019.<sup>622</sup> He did this by exhibiting videos 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).
411. Mr Madden examined the videos and makes findings in Appendix PM45 to Madden 2<sup>623</sup> which show them to be falsified:
- 411.1. 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.<sup>624</sup>
- 411.2. 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

---

621 Defence at §83(4) {A/3/24}.

622 Wright 4, §§20-23 {E/4/11}.

623 {H/241/1}.

624 Appendix PM45, §§18-26 {H/241/7}.

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.<sup>625</sup> 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.

- 411.3. 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).
412. 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 access to the Satoshi Vistomail account;<sup>626</sup> and (b) on 18 March 2020, he testified that he had not been able to access it since before 2013.<sup>627</sup>
413. 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.<sup>628</sup> 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.
414. **When the above was put to Dr Wright in cross-examination, he had no coherent answer. He asserted that Mr Madden had done the wrong research and that in fact footers in Vistomail did not update as he suggested.<sup>629</sup> This assertion has not been supported with any evidence. Also, as the Court will recall, Dr Wright first blamed the lack of live navigation between windows on the supposed difficulty of recording footage with a**

---

625 Appendix PM45, §§8-10 {H/241/3}.

626 {L15/133/5}.

627 {L16/272/192}, internal p192-193.

628 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.

629 {Day2/49:10} and following.

phone in one hand and operating a computer mouse with the other.<sup>630</sup> That was always a silly explanation, but it was firmly refuted when another video was played showing him operating the mouse while filming.<sup>631</sup>

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

415. 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 issued<sup>632</sup> 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.
416. 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.”*<sup>633</sup> Mr Gao accepts this point.<sup>634</sup>
417. 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.<sup>635</sup> 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

---

630 {Day2/52:9} - {Day2/52:24}

631 {Day2/85:2} - {Day2/85:21}

632 {L18/257/1}.

633 Meiklejohn §§135-137 {G/2/60}.

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

635 Wright 1, §217-220 {E/2/37}.

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.<sup>636</sup>

418. 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*”,<sup>637</sup> 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.
419. 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*”.<sup>638</sup> As recounted above, Mr Andresen made a similar transfer, which was also never returned.
420. 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 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).<sup>639</sup> In the end, he did not provide any proof and the “big reveal” project fell apart.

---

636 Matthews 1, §104 {E/5/22}.

637 {L13/262/1}.

638 Cellan-Jones §16, {C/5/4}.

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

421. 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

422. 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.<sup>640</sup> 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.<sup>641</sup>

423. 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.<sup>642</sup> 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. **As noted above, Dr Wright’s attempts in his evidence at trial to make these two different accounts reconcile were unimpressive.**<sup>643</sup>

424. 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

---

640 Wright 4, §33 {E/4/15}.

641 Wright 4, §34 {E/4/16}.

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

643 See {Day8/79:3} - {Day8/84:25}.

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*”.<sup>644</sup> 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.<sup>645</sup> **As noted above, when cross-examined about this, he claimed to have discovered in 2019 that he could not access the keys, which conflicted with his evidence in Granath, and then he proceeded to deny the conflict.**<sup>646</sup>

### Failures of Cryptographic Proof – Overview of the Signing Sessions

425. 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*”.<sup>647</sup> 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.<sup>648</sup> As Prof Meiklejohn explains, the signing sessions omitted key steps which would have been required to make them reliable. **As explained above, all these matters remained common ground between the experts in their oral evidence.**

426. 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

---

644 {O2/11/31}, internal page 119.

645 {L19/212/6}.

646 See {Day8/85:1} - {Day8/87:8}

647 Meiklejohn §131 {G/2/58}.

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



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.

427. 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:

427.1. Dr Wright says that the first stage in verification entails installing the Bitcoin Core software.<sup>649</sup> 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.<sup>650</sup>

427.2. Dr Wright claims that he underwent the time-consuming exercise of downloading the entire Bitcoin blockchain as a preliminary to each signing session.<sup>651</sup> 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.<sup>652</sup>  
**As noted above, this is agreed by Mr Gao.**

427.3. 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.<sup>653</sup> 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.<sup>654</sup>  
**Again, there is no dispute about this between the experts.**

427.4. 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.<sup>655</sup> Prof

---

649 Wright 2, §7-9 {E/2/4}.

650 Meiklejohn §114 {G/2/47}.

651 Wright 2, §9 {E/2/5}.

652 Meiklejohn §116 {G/2/48}.

653 Wright 2, §12 {E/2/6}.

654 Meiklejohn §115 {G/2/47}.

655 Wright 2, §21 {E/2/8}.

Meiklejohn disputes that this procedure has such a benefit over other methods.<sup>656</sup> 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. **As noted above, Mr Gao agreed in his evidence.** 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 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

428. 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.<sup>657</sup> 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.<sup>658</sup> 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.<sup>659</sup>
429. 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.<sup>660</sup> **Mr Gao agrees with her on these matters.** 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). **Mr Gao readily agreed that that would have been simple, reliable and a process involving no risk of compromising the private key.** As with the Sartre blog, he adopted an over-complex process which proved nothing.

---

656 Meiklejohn §118 {G/2/49}.

657 Wright 2, §§25 and 32 {E/2/9}.

658 Wright 2, §§26-28 {E/2/9}.

659 Wright 2, §§29-31 {E/2/9}.

660 Meiklejohn §124 {G/2/51}.

430. 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.<sup>661</sup> On his account, he took *real* security risks while adopting complex steps to avoid *spurious* risks.
431. In opening submissions, Dr Wright relied upon hearsay attributed to Mr Matonis in a press release of 28 April 2016 (i.e. before the debacle of the Sartre Blog post) suggesting that he was persuaded by the signing session he attended.<sup>662</sup> This multiple hearsay statement was not even submitted under a CEA notice. In any event, he has not given evidence and we have no account from him about steps taken to ensure that the session he attended was reliable. The agreed expert evidence is that it could very easily have been faked. And it is telling that Mr Andresen was initially persuaded by the signing session he attended, but later came to believe that it could well have been spoofed.

#### Failures of Cryptographic Proof – the Signing Session with Mr Andresen

432. 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 person<sup>663</sup>).
433. In Wright 2, Dr Wright gives his version.<sup>664</sup> 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.

---

661 Meiklejohn §125 {G/2/52}.

662 See {L12/492/1}.

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

664 Wright 2, §§33-41 {E/2/10}.

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.

434. Mr Andresen recalls that a hot-spot might have been used for internet access,<sup>665</sup> a detail Dr Wright accepted in his *Granath* evidence.<sup>666</sup> Importantly, Mr Andresen is also clear that Dr Wright downloaded and installed the software on the new laptop, including the Electrum software.<sup>667</sup> 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.<sup>668</sup> Mr Andresen recalled that the message signed was “*Gavin’s favourite number is 11 – CSW*”. The Reddit notes indicate that on the first try Mr Andresen had omitted “*– CSW*”, after which the verification failed, but that Dr Wright then identified the omission.<sup>669</sup>
435. In his evidence at trial, Dr Wright sought to bring his account into line with Mr Andresen’s. He said that he could not remember which of them had downloaded what, but tried to insist that Mr Andresen had been watching his every move.<sup>670</sup> He admitted that Mr Andresen may well have been right in his recollection of the message and how the verification initially failed.<sup>671</sup>
436. 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).<sup>672</sup> It is telling that Dr Wright’s account diverges from

---

665 {E/17/76}.

666 {O2/11/21}.

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

668 {E/17/76}.

669 {L19/217/4}.

670 {Day8/68:12}.

671 {Day8/72:16}.

672 Meiklejohn §130 {G/2/56}.

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.

437. 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.

#### The Andresen Signing Session Reconsidered

438. It is important to bear in mind the circumstances in which Mr Andresen arrived at and participated in the signing session that took place on 7 April 2016. His flight to London departed from Boston at 21:35 on 6 April 2016<sup>673</sup> (02:35 GMT on 7 April 2016), arriving in London around 6.5 hours later (at around 09:10 GMT). According to his deposition in the Kleiman proceedings he "*can't sleep on airplanes very well.*"<sup>674</sup> He arrived at the Firmdale Hotel in Covent Garden at around 11:00 GMT.<sup>675</sup> In his Kleiman deposition, Mr Andresen repeated that at this point he was "*very tired*" as it was a red-eye flight.<sup>676</sup>
439. After landing, Mr Andresen got 1-2 hours of sleep<sup>677</sup>. According to the schedule that was prepared for the day, he then met Mr Matthews and Mr MacGregor for lunch at 1pm (13:00 GMT).<sup>678</sup>
440. Following the lunch meeting, it appears there was an "introduction" session with Mr Matthews and Mr MacGregor, following which Mr Andresen and Dr Wright met in person for the first time.<sup>679</sup> According to Mr Matthews they spoke for around 1-1.5

---

673 {L12/24.6/1}.

674 {E/17/240} internal lines 22-23. Mr Matthews also highlights in his first witness statement that Mr Andresen is "*afraid of flying*" {E/5/18} at paragraph 88, which may have made the trip to London a stressful experience.

675 {E/17/68} internal lines 15-17.

676 {E/17/68} internal lines 21-22.

677 {E/17/240} internal lines 17-23.

678 {L12/24.6/2}.

679 {L12/24.6/2}.

hours<sup>680</sup> on a number of topics, including “*eight or ten different aspects of the Bitcoin code*”.<sup>681</sup> According to the account he gave to Andrew O’Hagan for *The Satoshi Affair*, Mr Andresen “*was so jet-lagged at one point... that [he] had to stop [Dr Wright] from diving deep into a mathematical proof [Dr Wright had] worked out related to how blocks are validated in bitcoin.*”<sup>682</sup>

441. The meeting moved towards the signing session itself, although Mr Andresen describes the session as “*one continuous meeting*” in the hotel room.<sup>683</sup> According to the account given in *The Satoshi Affair*, at around 5.30pm, Dr Wright logged onto his laptop in order to sign a message with Satoshi’s private key.<sup>684</sup> Mr Andresen wished to perform verification using his own laptop, and produced a “*brand new sealed in the package USB stick*” which he expected Dr Wright to “*take and produce some digital signatures that [he] could verify on [his (i.e. Mr Andresen’s)] laptop.*” However, Dr Wright did not agree to do this.
442. There was then a discussion that lasted around 15-20 minutes,<sup>685</sup> following which a new laptop was “*procured*” by an assistant, which Mr Matthews has said was purchased from Curry’s on Oxford Street.<sup>686</sup> The distance between the Firmdale Hotel and Curry’s on Oxford Street is 11 minutes each way by foot. It is therefore reasonable to assume that it was some time after 6pm by the time the assistant returned with the laptop, and the signing session continued.
443. By Mr Andresen’s account, the process of convincing him that Wright had taken an early block and signed a message using its private key, took “*some—many hours, I don’t recall how many hours, but it took much longer than – than expected*”.<sup>687</sup>
444. Even if the assistant returned with the laptop promptly, and the signing session completed very shortly after they returned (say 7pm), this would be 16.5 hours after Mr Andresen’s flight had departed Boston (which itself was at the end of day on 6 April Boston time – 9:35pm). Assuming that Mr Andresen had woken at, say, 9am on the day of his flight,

---

680 {O3/1/26}.

681 {E/5/19} para 91.

682 {L13/53.7/1}

683 {E/17/74} at internal lines 8-9.

684 {L13/491/64}.

685 {O3/1/26}.

686 {Day12/79:7}.

687 {E17/75} internal lines 2-4.

and allowing for the time difference, by 7pm London time on 7 April (the earliest time at which the alleged signing can have been completed), Mr Andresen would have been through a 29-hour period since waking up on 6 April with only 3-4 hours of sleep. By his own account, by the time that Dr Wright allegedly signed the message, Mr Andresen was “*exhausted*”.<sup>688</sup>

445. As for the technical possibility of Mr Andresen’s session being hacked or interfered with in some way, both Professor Meiklejohn and Mr Gao agreed this was all technically possible and in fact relatively straightforward. Professor Meiklejohn also clarified how easy it was for this to be done, noting as the final answer in her cross-examination, the following:<sup>689</sup>

*Q. And I suggest that you have consistently understated the inherent difficulty of actually subverting the Andresen signing session in your reports.*

*A. That is completely inaccurate.*

*Q. The fact is that, in reality, it would have been extremely difficult to subvert the process.*

*A. I can think of literally hundreds of people who could compromise the router in a matter of minutes, and from there, the entire process would be almost trivial from a computer science perspective.*

446. In his evidence,<sup>690</sup> Dr Wright tried to argue that any attempt to subvert the signing session would either have been obstructed because of the blockchain having been downloaded or have given rise to a clear red warning highlighting the use of a spoof website. Professor Meiklejohn addressed and rejected this evidence in her second report: **{G/10/1}**. Mr Gao accepted in cross-examination that the downloading of the blockchain would not have provided any special protection against spoofing<sup>691</sup> and that there were various very feasible ways to subvert the process, at least some of which would not result in any clear warning notice.<sup>692</sup>

---

688 **{E17/78}** internal lines 1-4.

689 **{Day18/138:9}** - **{Day18/138:18}**.

690 **{Day8/69:10}** and following.

691 **{Day18/41:9}**.

692 **{Day18/25:8}** - **{Day18/34:5}**.

## Failure to Demonstrate the Technical Ability of Satoshi Nakamoto

447. In opening, Dr Wright’s counsel made much of his vaunted expertise. However, even if he were found to be a highly able computer scientist who in 2008 had an interest in digital currency and all the skills to create the Bitcoin Code, that would not prove that he is Satoshi Nakamoto or even materially advance his claim. After all, there are many others who could make the same claim, several of whom have given evidence for COPA in this trial.
448. In any event, when Dr Wright’s expertise was put under the microscope, it was found to be wanting. Under cross-examination by the Developers’ counsel on Day 8,<sup>693</sup> he showed (a) a lack of understanding of the CheckBlock function in the Bitcoin Code; (b) an ignorance of the CheckBlockHeader function and when it came into use; and (c) an inability to explain what an “unsigned integer” is, despite it featuring many times in the Bitcoin Code. It is understood that the Developer defendants will address these matters in more detail in their Closing Submissions. Furthermore, on his second visit to the witness box, Dr Wright showed himself unable properly to explain Merkle trees, wrongly describing them as a form of binary search tree.<sup>694</sup>
449. The witnesses also had a number of comments which cast serious doubt on Dr Wright’s technical expertise:
- 449.1. Dr Back pointed out that he found that Dr Wright’s commentary on Twitter in 2012-14 appeared incorrect and he had to mute him.<sup>695</sup>
- 449.2. Mr Hearn asked questions about the Bitcoin System at the Wild Honey dinner which Dr Wright struggled to answer (needing to be protected by Mr Matthews under the pretence of nChain’s patents being revealed by a discussion of foundational features of Bitcoin).<sup>696</sup>
- 449.3. As noted above, Mr Hinnant explained that Dr Wright’s story of creating a customised “chrono” time library from the Chrono physics library was technically absurd.

---

693 {Day8/120:15} - {Day8/145:1}

694 {Day15/176:24} - {Day15/188:2}

695 {Day13/69:10} - {Day13/70:11}.

696 {Day14/12:9} - {Day14/13:4}.



450. Similarly, Dr Wright’s boasts of his many patents are also not relevant. However, what information we do have on them from the documentary evidence raises serious questions about his inventive work. Of the supposed treasure trove of nChain patents, only six contained him as sole inventor, and none of those was relied upon by Dr Jones in her evidence praising his abilities.
451. Dr Wright’s academic qualifications likewise would be of little or no significance even if they were of great distinction. In fact, his evidence reveals a person who actively pursues multiple postgraduate degrees at any one time, but without actually assembling a starry academic record. The Court will recall that he boasted of working towards five PhDs at present, but then could only give the first names of some of his supervisors and found it hard to give the surname of any. He later changed his story to say that he was actually only doing two PhDs, along with three DBAs.<sup>697</sup>

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

452. 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.

#### **Dr Wright and Mr Matthews**

453. Mr Matthews was the principal supportive witness for Dr Wright; the only witness to give evidence of having discussed the Bitcoin project with him before its release, and the only one to give evidence of the “Big Reveal” and the Sartre Blog debacle. It is therefore significant that there were substantial inconsistencies between Dr Wright and Mr Matthews.

#### *The evidence given by Mr Matthews in support of Dr Wright*

454. The main point of evidence on which Dr Wright relies from Mr Matthews is that he allegedly discussed his Bitcoin project with Mr Matthews in late 2008 and early 2009,

---

697 {Day6/45:25} - {Day6/48:7}.

and specifically that he shared a draft of the Bitcoin White Paper with Mr Matthews in August 2008. As set out above, COPA submits that this evidence is a fiction. In summary:

- 454.1. The story is unsupported by any documentary or other evidence.<sup>698</sup>
  - 454.2. The story was not told until after 2015, when doing so accorded with Mr Matthews' and nChain's motives. Since then, it has featured in an nChain information memorandum, a press release for Mr Matthews' Squire Mining company and an interview given by Mr Matthews, as well as in the Satoshi Affair by Andrew O'Hagan. It is plainly an important "origin myth" for nChain.
  - 454.3. As explained above, Mr Matthews' and Dr Wright's accounts conflict on the detail of the story. Mr Matthews said that he was handed a USB stick,<sup>699</sup> that he had to print the document himself, and that "*I read it straight away when I printed it.*"<sup>700</sup> Faced with Dr Wright's conflicting account of having handed over a paper copy which then sat unread on Mr Matthews' desk for months, Mr Matthews said that "*wasn't what actually occurred.*"<sup>701</sup>
  - 454.4. Mr Matthews' account was also materially inconsistent with the account told to Mr Andrew O'Hagan, who interviewed him for the book that nChain commissioned to promote Dr Wright's claim. Mr O'Hagan writes that Mr Matthews said that he was given a document "*written by someone called Satoshi Nakamoto*" and that he had been busy and not read it for a while.<sup>702</sup> Mr Matthews now says that that is wrong on two counts: it definitely did not bear the name Satoshi Nakamoto and he read it without delay.
455. As to Mr Matthews' story of Dr Wright's work with Centrebet having a connection to Bitcoin, the only work he ever carried out was standard IT security work; nobody else at Centrebet has ever spoken about him doing any other type of work; and the only

---

698 {Day11/97:7} - {Day11/98:16}.

699 {Day11/89:22} - {Day11/90:10}, {Day11/98:17} - {Day11/99:9}.

700 {Day11/101:21}.

701 {Day11/97:4}.

702 {L13/491/11}.

document purporting to support the claim is a supposed pitch document (not taken forward) which has been debunked as unreliable by Mr Madden.<sup>703</sup>

*Inconsistencies between Mr Matthews and Dr Wright*

456. Mr Matthews also contradicted Dr Wright's account on a number of other material points of fact, as follows:

456.1. The two differed about the initial meetings between him, Mr Ayre and Dr Wright from April 2015. Meetings which were said by Dr Wright to be about sale and purchase of bitcoin<sup>704</sup> were said by Mr Matthews to concern possible investments in Dr Wright's businesses. Mr Matthews confirmed that Dr Wright's account was "*not true*".<sup>705</sup>

456.2. In relation to the purchase of life story rights, Mr Matthews accepted that nChain (under its previous name) was in discussions to purchase the life story of Dr Wright for significant sums of money and that "*the life story rights were referring to Dr Wright's involvement in the creation of Bitcoin,*"<sup>706</sup> an account contrary to that of Dr Wright who emphasises "*academic research and ... patents*" and the "*enduring legacy of nChain*", and said that his "*background as Satoshi was to be kept confidential*".<sup>707</sup>

456.3. Mr Matthews' account, and Dr Wright's account in these proceedings, of their discussing digital currency since 2005 and Bitcoin from August 2008, is also significantly at odds with the account given by Dr Wright by email in 2015 - that "*Stefan knows my history with Bitcoin from March 2009 on*".<sup>708</sup>

456.4. In relation to Dr Wright's purported reluctance to be outed as Satoshi Nakamoto, Mr Matthews accepted that from the start of their dealings in mid-2015 Dr Wright was "*comfortable with the concept*" of a book being published on the topic, and "*It was always understood that it would occur at some point in*

---

703 {Day11/88:25} - {Day11/89:17}; {Day11:107:8}.

704 {Day7/81:21} and following.

705 Compare {Day7/80:11} - {Day7/82:18} and {Day11/125:21} - {Day11/126:7}.

706 {Day11/136:24}.

707 {E/1/29}.

708 {Day12/1:24} - {Day12/3:4}; {L9/467/2}.

time”.<sup>709</sup> By contrast, Dr Wright insisted that he was only reluctantly forced to that view after the WIRED and Gizmodo articles were published in December 2015.

- 456.5. As noted above, contrary to Dr Wright’s vehement denials that he was ever an employee of, or associated with the company Tyche (in response to emails from his address at tyche.co.uk which are now inconvenient to him), Mr Matthews not only agreed readily that Dr Wright was employed by Tyche, but offered a detailed narrative of the reasons, documents, and terms of his engagement, even confirming Dr Wright’s signature on the contract of employment.<sup>710</sup>

*Mr Matthews on the Sartre blog post*

457. Contrary to Dr Wright’s evidence that no right-minded person would interpret his Jean-Paul Sartre “signing” blog post as intended to supply cryptographic proof:

457.1. Mr Matthews (who supported and provided direct input into the blog post) confirmed that providing cryptographic proof of Dr Wright’s alleged identity as Satoshi Nakamoto was precisely the intent behind the post.<sup>711</sup>

457.2. That was also the clear and consistent media message supplied to the media, as also confirmed by Mr Matthews.<sup>712</sup>

457.3. The reaction at the time, from Mr MacGregor, Mr Ayre and Mr Matthews was that the signature had “fallen apart” - to which Dr Wright provided an excuse not that the blog was intentionally misleading, but that “*the wrong copy was uploaded*”.<sup>713</sup> This was such a serious and obvious problem for Dr Wright’s evidence that it led him to come up with the story that the email (from his nCrypt email address) had been sent by an impostor.

457.4. Mr Matthews at first “*felt that incorrect information had been provided*” (in Dr Wright’s draft) which he considered to be in error.<sup>714</sup>

---

709 {Day11/144:4} - {Day11/144:24}.

710 {Day11/145:2} - {Day11/148:24}.

711 {Day12/25:11}.

712 {Day12/27:2}.

713 {Day12/28:10-15}.

714 {Day12/33:1}.

- 457.5. The day after the signature, Dr Wright spoke to Mr Matthews “*a dozen times*”, and sent an email offering further cryptographic evidence, indicating that he would promptly provide signed messages from blocks 1 and 9.<sup>715</sup> By contrast, Dr Wright maintains that he was not prepared to do that at the time.
- 457.6. Mr Matthews accepted that Dr Wright’s account in these proceedings was inconsistent with the events at the time;<sup>716</sup> and that Dr Wright’s account has materially changed; and that the only person who has advanced an alternative story is Dr Wright himself.<sup>717</sup>

*Signing sessions / Sartre blog inconsistencies*

458. As noted above, Mr Matthews claimed in his written evidence<sup>718</sup> that he had “*no involvement in arranging the public proof sessions*”, a claim falsified by the emails in evidence, which show him actively involved and working collaboratively with Mr MacGregor.<sup>719</sup> He claimed only “peripheral” involvement in discussions of the Sartre blog post, whereas the emails show that he reviewed at least one version and apparently did some editing work on it.<sup>720</sup>

*Mr Matthews and arranging further proof after the Sartre blog failure*

459. Mr Matthews also made arrangements, and laid the groundwork, for a further level of proof which would involve the movement of partial bitcoins from Mr Matonis and Mr Andresen to an address associated with early block, then to be returned to them. That would have constituted “*excellent on-chain evidence*” (per Mr Andresen)<sup>721</sup>, but about this Mr Matthews, Dr Wright, and the contemporaneous documents tell three divergent stories:

---

715 {Day12/29:25} - {Day12/30:10}.

716 {Day12/34:4}.

717 {Day12/44:13}.

718 {E/5/21}.

719 {Day12/18:21} and following.

720 {Day12/41:7} and following.

721 {L13/208.6/1}.

- 459.1. Dr Wright’s evidence was that he had no knowledge at the time that arrangements were being made to transfer coins in this way, and that he found out only after the event.<sup>722</sup>
- 459.2. By contrast, the documents indicate that at the time Dr Wright’s commitment to that public on-chain proof was communicated from Mr Matthews to Mr Andresen.<sup>723</sup>
- 459.3. Mr Matthews’ account falls between both stools. In his oral evidence, he confirmed that Dr Wright did agree, and that this agreement was given following discussions with Dr Wright directly and by phone. His written evidence had been to the contrary. He accepted that was false, seeking to excuse it on the basis that Dr Wright had initially consented, and then withdrawn that consent.<sup>724</sup> This account is even more divergent from Dr Wright’s: quite apart from him having no knowledge at all, Mr Matthews’ revised evidence is that Dr Wright had continuing involvement in evolving discussions through which he considered and reconsidered his consent.
460. These inconsistencies are important. Dr Wright now seeks to maintain that he did not provide proof of possession of the private keys between 2 and 4 May 2016 because he was taking a consistent stand on principle. If it is true, as the emails demonstrate, and as Mr Matthews has been driven to accept, that Dr Wright kept offering to supply proof and failing to make good on his offers, then that supports COPA’s case that he was trying to hold his backers at bay while being unable to provide the proof they required.
461. In support of his denial of knowledge, Dr Wright on several occasions retreated to refuting the authenticity of yet more emails from his own disclosure:
- 461.1. In one example, Dr Wright went to pains to take issue with emails purportedly from Mr Mayaka to him concerning “authority” to use certain keys.<sup>725</sup> Mr Matthews, who had also been involved in those discussions, accepted the same emails, remembered the specific discussions taking place with Dr Wright, and

---

722 {Day8/54:2}.

723 {Day12/53:7}.

724 {Day12/54:17} - {Day12/55:19}.

725 {Day8/34:7} - {Day12/36:5}.

even volunteered himself that they were consistent with his discussions and the arrangements he was in fact making at the time, for Dr Wright to make use of the keys.<sup>726</sup>

- 461.2. In another example, an email<sup>727</sup> was disowned by Dr Wright on the basis that “*I didn’t have nCrypt at this time.*”<sup>728</sup> As noted above, Mr Matthews looked over the email carefully and grounded it against corroborating details of his conversations with Dr Wright and their resulting actions.

### The Satoshi PGP Key

462. It is well known that Satoshi Nakamoto had a PGP key and that the public key in the pair has been available on the bitcoin.org website. The earliest available archive of the page of the website dates from 2011, and for reference purposes the key begins “mQGIB EJ...” {H/318/2}. As Prof Meiklejohn explains in her report, that key is well known to the Bitcoin community: {G/2/45}, para. 107 (footnote 29), referring to her exhibit at {H/200/2}. As explained below, the private key is one which can be used to sign a message (allowing verification with a public key) or to encrypt a message (allowing decryption with a public key). One of the means by which a person could provide evidence supporting a claim to be Satoshi would be to sign a message with the private PGP key.<sup>729</sup>
463. Dr Wright has provided a complex and evolving set of excuses as to why he has not signed a message with the private key in this pair. His failure to use the key and his excuses for not doing so are telling.

### *Dr Wright’s case in his pleading and in Wright 4 (RFI response)*

464. In paragraph 83(2) of Dr Wright’s Re-Re-Amended Defence, he responded to COPA’s contention that, if he were Satoshi, he could demonstrate control with Satoshi’s private key. He stated that: “*It is not clear from paragraph 61.1 [of the Particulars of Claim] what “private key” is referred to. There has been a public discussion of a key created in 2011 after Dr Wright ‘retired’ his Satoshi Nakamoto persona. The key was created by a*

---

726 {Day12/55:20} - {Day12/57:8}.

727 {L13/338/1}.

728 {Day8/53:21} - {Day8/54:1}.

729 For simplicity, we refer to the common parlance of a "PGP Key" in the singular. As was clear from the evidence, the "key" encompasses multiple keys (subkeys) with different purposes, a point which became important in view of Dr Wright's responses under Cross-examination.

*person or persons unknown. Therefore, control, command or ownership of that key has no probative value as to the identity of Satoshi Nakamoto.*<sup>730</sup>

465. In Wright 4, he said that the reference in the Re-Re-Amended Defence to a key created by unknown persons in 2011 was “a reference to the PGP encryption key at [https://web.archive.org/web/20110228054007/bitcoin.org/satoshi\\_nakamoto.asc](https://web.archive.org/web/20110228054007/bitcoin.org/satoshi_nakamoto.asc).” He added: “This was generated by Vistomail when I set-up the Sakura account in 2008. I subsequently shared this with a number of individuals, including Marti Malmi, so that they could send code updates to me. It was only published in 2011 by an unknown party (I suspect Marti Malmi), after I stopped the active use of the Satoshi Nakamoto pseudonym”.<sup>731</sup>
466. Dr Wright also said that he had a PGP key linked to his GMX account on Vistomail and that the key resided on Vistomail’s server.<sup>732</sup> A server PGP key is typically generated as a pair consisting of public and private keys. The private key is used for decryption and is kept secure. According to Dr Wright, the PGP key in question was generated internally by Vistomail and used for domain and server management functions – but he said that he had not himself created it. It was, he claimed, an integral component of the services provided by Vistomail, including its application to Dr Wright’s Sakura account for domain and email management. On his account, the key was not specific to any individual but to a server at Vistomail. As a system-specific key, its primary role was securing various server operations, such as data encryption and user authentication.<sup>733</sup> The PGP key came into existence when the Sakura account transitioned to a paid subscription in 2008 (Dr Wright believed around October 2008).<sup>734</sup>

#### *Dr Wright’s account in Wright 11*

467. Dr Wright embellished his story in Wright 11, claiming that Satoshi’s public PGP key was a server key for software encryption and was never an identity key.<sup>735</sup> The only use that Dr Wright said he had made of it as Satoshi was with Mr Malmi in decrypting

---

<sup>730</sup> {A/3/24}.

<sup>731</sup> Wright 4, §104 {E/4/34}; see also Wright 9, §34 {E/26/12}.

<sup>732</sup> Wright 4, §22, §24(e) {E/4/11} to {E/4/13}.

<sup>733</sup> Wright 4, §105 {E/4/35}.

<sup>734</sup> Wright 4, §107 {E/4/35}; see also Wright 9, §34 {E/26/12}.

<sup>735</sup> Wright 11, §233 and §234 {CSW/1/44}.



material associated with the Bitcoin site.<sup>736</sup> At no point had Dr Wright ever signed a message with that key.<sup>737</sup> (Of course, COPA agrees that Dr Wright has never signed a message with the key, but not for the reasons Dr Wright gives.)

468. Dr Wright's reiterated his position that the PGP key was associated with the Vistomail site. The key was a server key associated with the system. Encryption and signing were separate processes and should not reuse the same key.<sup>738</sup> He concluded: "*the PGP key is not a signing key*".<sup>739</sup>

#### *Dr Wright's position in cross-examination*

469. Dr Wright said that the well-known PGP key attributed to Satoshi, the public key for which has been hosted on the Bitcoin.org website, was first posted online in 2011. There was, he claimed, an unknown earlier version associated with the site which was no longer available.<sup>740</sup> He claimed that key on the web page captured by the Way Back Machine<sup>741</sup> is a key loaded by Martti Malmi in February 2011 on to the site, replacing the other one.<sup>742</sup> That key (MQGiBEkJ) had been promoted from 2011, after Dr Wright claimed to have left the Satoshi persona.<sup>743</sup>
470. When asked whether the key referred to at paragraph 83(2) of his Defence as having been created in 2011 was the MQGiBEkJ key, Dr Wright responded confusingly: "*No, actually, not in the way you're talking... what I'm stating is that the key that had been used for Gavin, Martti and others, as an encryption and decryption key was loaded as if it was a signing key. They're different things.*"<sup>744</sup> When asked again, Dr Wright answered: "Do you understand that private keys and public keys are separate? 83(2) is answering a question about a private key."<sup>745</sup> When asked by the Judge to answer the question of whether the key referred to at 82(3) was the key that that the court had just been looking

---

<sup>736</sup> Wright 11, §238 {CSW/1/45}, commenting on para 10 of Malmi 1 {C/2/3}.

<sup>737</sup> Wright 11, §238 and §241 {CSW/1/45}.

<sup>738</sup> Wright 11, §239 {CSW/1/45}.

<sup>739</sup> Wright 11, §243 {CSW/1/46}.

<sup>740</sup> {Day8/36/10}.

<sup>741</sup> [https://web.archive.org/web/20110228054007/bitcoin.org/satoshi\\_nakamoto.asc](https://web.archive.org/web/20110228054007/bitcoin.org/satoshi_nakamoto.asc)

<sup>742</sup> {Day8/36/19}.

<sup>743</sup> {Day8/37/6}.

<sup>744</sup> {Day8/37/21}.

<sup>745</sup> {Day8/38/9}.

at, Dr Wright gave a further confusing answer: “No. In 82(2) [sic] is referencing a private key. That’s referencing a public key.”<sup>746</sup>

471. Dr Wright was then asked whether 83(2) was referring to the private key, which is the pair of the MQGiBEkJ public key looked at a few moments ago. He again sought to confuse: “What I’m saying, again, is the difference between a signing and encryption key. The encryption key is related to that one, and the private key would be the same, but you can update algorithms, etc, in these.”<sup>747</sup>
472. It was then put to Dr Wright that the plain meaning of para 83(2) was that the MQGiBEkJ public key was nothing to do with Satoshi and had been created by person or persons unknown. He replied that that was incorrect: “...the key was a decryption key used in the Vistomail site. So, the creation basically is in a function within Vistomail. So, by using Vistomail, I create a key that I don’t have the private key for. That allows me to receive files and decrypt them on the platform. So where I’m saying I don’t have any of that, that’s because it’s in Vistomail, which is now shut down. It wasn’t used as a signing key.”<sup>748</sup> Dr Wright went on: “Now, it was never a public key, because I’d sent it privately only to a few people.”<sup>749</sup> These answers marked an obvious departure from the account given in his pleading.
473. Dr Wright was then asked about an email sent by Satoshi (via GMX email, not Vistomail) to Martti Malmi on 6 December 2010 {L6/477/1} which contained the same public key looked at earlier (i.e. the MQGiBEkJ key hosted on bitcoin.org from 2011 or earlier).<sup>750</sup> He gave another confusing answer: “Not one that was originally there. It’s the one that Martti loaded.” On being asked whether the figures and numbers were the same as between the key in the email and the key from the 2011 web capture looked at earlier, Dr Wright failed to answer and just repeated: “It is not the original one.”<sup>751</sup>
474. Dr Wright was then referred to a public post by Satoshi on 25 July 2010 (“For future reference here’s my public key. It’s the same one that’s been up there since the bitcoin.org site first went up in 2008”): {L19/111/2}. He was asked if he accepted that

---

<sup>746</sup> {Day8/38/18}.

<sup>747</sup> {L6/477/1}.

<sup>748</sup> {Day8/39/22} to {Day8/40/2}.

<sup>749</sup> {Day8/40/3}.

<sup>750</sup> {Day8/40/21}.

<sup>751</sup> {Day8/41/3}; see also {Day8/47/17} to {Day8/48/18}.

in July 2010 Satoshi was informing people that the public PGP key had been up on the bitcoin.org site in fact since 2008. Dr Wright replied: “*Not that one, no.*”<sup>752</sup> Again, the contemporaneous documents cut across Dr Wright’s evidence.

475. Dr Wright was then asked about the findings of Mr Madden that the MQGiBEkJ public key contained metadata dating it to a first upload on 30 October 2008 (precisely consistent with Satoshi’s post): Madden 4, para. 144ff {G/6/46}. Dr Wright denied that there was any evidence for this conclusion.<sup>753</sup> When Mr Madden later gave evidence, Dr Wright’s Counsel never challenged him on these findings.
476. On being taken to Mr Madden’s report showing the GPG output of the key containing an internal date stamp of 30 October 2008, Dr Wright stated that the date, etc was just typed in.<sup>754</sup> In response to questions from the Judge, he went on: “*I’m saying that that date was set back to the beginning of the project... by myself. ... Because that’s when the project started... I do this sort of thing all the time.*”<sup>755</sup>
477. Dr Wright was also asked whether he accepted that Mr Madden’s GPG output of the MQGiBEkJ public key shows distinct signature packets showing that it can be used both as a signing key and an encryption key. After commencing with an initial denial, Dr Wright accepted that “*you can use PGP in that way, but that is bad practice*”. Upon being pressed as to whether he accepted that the GPG output in Mr Madden’s report showed that this key had always had the functions of signature key and encryption key and could be used for both, based on the signature packets, Dr Wright did not accept that it always had, since he said he could update the algorithms.<sup>756</sup> In response to further cross-examination for the Developers about GPG output for the key provided by Mr Madden, he again admitted that the key could be used as a signing key but denied that that was its proper function, despite being shown clearly that the primary sub-key was indeed a signing key.<sup>757</sup>

---

<sup>752</sup> {Day8/42/1}.

<sup>753</sup> {Day8/43/9} to {Day8/43/24}. See also {Day8/48/19}

<sup>754</sup> {Day8/44/15}.

<sup>755</sup> {Day8/45/3} to {Day8/45/17}.

<sup>756</sup> {Day8/45/18} to {Day8/46/18}.

<sup>757</sup> {Day8/162/3} to {Day8/172:2}

### *Summary of the position*

478. Drawing the threads together, the position is now clear:
- 478.1. First, the real Satoshi made their public PGP key widely available when the Bitcoin.org website went live in 2008. That is evident not only from the Satoshi public post of 25 July 2010<sup>758</sup> but also from the Wayback capture of the Bitcoin.org website of 31 January 2009,<sup>759</sup> which shows a link to Satoshi's PGP key; and Mr Madden's unchallenged findings that the internal and external metadata of the key dates it to 30 October 2008.
  - 478.2. Secondly, the PGP key encompasses multiple keys, and is equally capable of use for signing functions and encryption functions alike.
  - 478.3. Thirdly, if Dr Wright were Satoshi he ought to have been able in May 2016 to sign using the PGP key. Indeed, at times he told his team that he might be able to do so.
  - 478.4. Fourthly, Satoshi's 6 December 2010 e-mail to Martti Malmi providing him with the PGP key was not available before 28 June 2023, when Mr Malmi's first witness statement in these proceedings was served.
  - 478.5. Fifthly, in ignorance of that email, Dr Wright plainly thought that he could invent an account to explain away his inability to use the private PGP key (whether for signing or encryption).
479. Bearing in mind that background, Dr Wright's story changed as the evidence has been presented to him.
- 479.1. In his pleading and original evidence, Dr Wright never once mentioned the story about backdating the output and adding functions to the key. As usual, it was a significant point of detail that, if true, would have come out earlier.
  - 479.2. Dr Wright has said that he shared the PGP key with a number of individuals, but it was only published in 2011 by an unknown party;<sup>760</sup> and it was never a public

---

<sup>758</sup> {L19/111/2}

<sup>759</sup> {L4/466/3}.

<sup>760</sup> Wright 4, §104 {E/4/34}; see also Wright 9, §34.

key because he had sent it privately only to a few people.<sup>761</sup> Quite apart from the misuse of the technical term “public key”, that is at odds with the contemporaneous documents showing that Satoshi published their PGP key in 2008/2009.

- 479.3. Despite Dr Wright’s denial that it meant this, the originally pleaded version of Dr Wright’s story was clearly that the publicly known Satoshi PGP key was no such thing, but was *created* by persons unknown and made public in 2011. That contention did not survive disclosure of the previously unpublished Mr Malmi e-mail showing that Satoshi had provided the identical public key to Mr Malmi in December 2010.
- 479.4. Dr Wright was then forced to shift to a newly concocted story in Wright 4; namely, that the key was generated by his Vistomail server in 2008, but was an encryption key and not a signing key. (He ultimately appears to have accepted that the key could be used for either purpose, but tried to maintain that it was bad practice to use it as a signing key.)
- 479.5. Under cross-examination Dr Wright displayed notable reluctance to accept even the obvious truth that the key sent to Mr Malmi in December 2010 and the key known from the 28 February 2011 Wayback capture were identical on their face. It is unclear why Dr Wright should have been unwilling to admit this, given that following Wright 4 he was no longer contending that the known 2011 key was a new creation. He also contended that there was an earlier version of the PGP key associated with the Bitcoin.org website, which is not true (as evident from Satoshi’s post and the Madden analysis).<sup>762</sup>
- 479.6. Faced with the finding in Madden 4 that the known Satoshi PGP key dated from 30 October 2008, Dr Wright initially denied that there was any evidence of that. Faced with the internal time stamp data in the GPG key output, Dr Wright then said that he had manually backdated the key to the start of the project (“*I do this sort of thing all the time*”). However, as already noted Mr Madden’s report had identified two independent sources for dating the key to 30 October 2008.

---

<sup>761</sup> {Day8/40/3}.

<sup>762</sup> {Day8/36/10}.

Furthermore, Dr Wright's claim to have manually backdated the PGP key is at odds with his oft-repeated assertion that the PGP key pair was automatically generated by the Vistomail server, not by him personally.

- 479.7. Dr Wright's insistence that PGP keys are either for encryption or signing is simply wrong, and he eventually acquiesced on that point. It is unclear whether his false evidence on this point was due to a failure to understand how PGP keys work or just because he was willing to lie on the subject hoping to not get caught.

#### Dr Wright Blaming his Lawyers

480. On numerous occasions during his evidence, Dr Wright blamed his lawyers for conduct such as failing to select an appropriate expert, failing to advise him properly on disclosure and failing to inform COPA and the Developers that material being disclosed was forged or otherwise unreliable. Despite warnings about waiver of privilege from counsel on both sides and the Court, he persisted in this conduct. His conduct strongly suggests that this is a deliberate tactic to shut down difficult issues.
481. Some instances of privilege being waived were agreed and material was supplied by Dr Wright's lawyers during trial. In other cases, they concluded that they could resist the argument that privilege had been waived. COPA ultimately decided not to press for disclosure of a number of categories of material where it considered that privilege had been waived. A significant factor in that decision was that there were by that time more than enough examples of Dr Wright falsely blaming his lawyers for supposed mistakes or conduct. The incident of the MYOB Ontier Email is the clearest example, but far from being the only one. Other examples are (a) Dr Wright's false claim that Ontier advised him that he could not deploy the White Paper LaTeX files because of disclosure date ranges; and (b) Dr Wright's false claim that the entire period of his editing of the White Paper LaTeX files represented one or more demonstrations to Shoosmiths.
482. The legal principle that no adverse inference may be drawn from a party maintaining privilege does not bar the Court from considering the plausibility of a story, nor does it confer an automatic benefit of doubt. Put another way, it is not assumed in favour of the party maintaining privilege that, had they waived privilege, a document from their lawyers would have supported their position. Accordingly, in each case where Dr Wright has given an account and then been stopped from going further because of a claim to

privilege, the Court should consider whether the account is inherently credible and consistent with the other evidence.

483. It is, for example, inherently implausible that Dr Wright was sitting on documents forged by Ira Kleiman, disgruntled ex-employees, Uyen Nguyen, Gwern, Bitcoin developers, Mr MacGregor, etc., and yet this fact was never conveyed to COPA or any other parties until he started proffering these excuses in Wright 11 and/or in cross-examination. His excuse of knowing of these forgeries and manipulated documents in his disclosure does not gain some hallowed protected status because he asserts privilege. The Court needs to look at the plausibility of that story regardless and ask whether it is credible that Dr Wright's competent and well-resourced legal teams were notified of these toxic forgeries among his disclosure documents but failed to highlight them as unreliable, so exposing their client to a risk of false allegations.

#### BlackNet and Spyder Projects

484. 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*".
485. 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.
486. 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\_001379<sup>763</sup>) 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.<sup>764</sup> 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 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

487. 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,<sup>765</sup> 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).
488. 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.<sup>766</sup> Prof Wrightson does not know of Wei Dai, while Prof Furche has never heard of Adam Back.<sup>767</sup> 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.<sup>768</sup> In addition, neither has any recollection of coming across Dr Wright at the University. Finally, the real Satoshi cannot have had these

---

763 {L1/79/1}.

764 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}).

765 {L15/88/2}.

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

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

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



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.

489. As recorded above, Dr Wright's attempts to answer the evidence of Prof Wrightson and Mr Furche were a rare example of his invention running dry: {Day6/77:11} to {Day6/88:5}. He was left accepting what they said but claiming to be poor at remembering people and his dealings with them (*"when it comes to people, I'm terrible"*<sup>769</sup>). However, if one re-reads his *"Fully Peer-to-Peer"* article and compares it against the admissions he has now made, the only explanation for the series of contradictions is that Dr Wright has been caught in a series of lies. He claimed that these academics played an important part in his work leading to his development of the Bitcoin system, but he has now been compelled to accept that his account was a fiction.

#### Accounts of Collaboration with Professor Rees and Gareth William

490. One of the most distasteful aspects of Dr Wright's lies is the abuse of those who are dead. Professor Rees was a famous cryptographer whose name Dr Wright co-opted to try and embellish his story by association. He cited Professor Rees as influencing his work in his vanity tract, *"Satoshi's Vision"*. He also deployed Professor Rees' name in his R&D tax offset claims. As explained above, the ATO enquiries established that his declared dealings with Professor Rees could not be true.<sup>770</sup>
491. Something similar was done by Dr Wright in his lies about being associated with the dead security services officer, Gareth Williams. Dr Wright told the Court that he had already cited Mr Williams' name to the ATO before he died on 16 August 2010.<sup>771</sup> However, this is not credible because the ATO proceedings concerning Dr Wright's Bitcoin claims did not start until 2013. There is no evidence of any ATO enquiry in 2010 or earlier in which Dr Wright could conceivably have deployed Mr Williams' name. Furthermore, the ATO proceedings in which Bitcoin-related issues arose concerned nine of Dr Wright's companies, of which the oldest had a registration date of 8 March 2011, so after Mr Williams' death.

---

769 {Day6/86:1}.

770 {Day7/60:1} - {Day7/64:21}.

771 {Day6/115:6}.

492. In the Kleiman proceedings, Dr Wright claimed to have engaged in a video conference with Mr Kleiman that was attended by Mr Williams in early 2011. When it was pointed out that Mr Williams had died before then, Dr Wright’s answer was that he had “got the dates wrong”.<sup>772</sup> However, that response is difficult to square with his evidence in the Kleiman proceedings, in which he dated the video call to a time when he was supposedly just about to go to Venezuela, a trip he has elsewhere dated to January 2011 (including in “Satoshi’s Vision”). He also said that, when he made that call, he was supposedly erasing his connection with Satoshi, which also dates it to early 2011.
493. Dr Wright’s account of this call in the Kleiman proceedings throws up another, and even more serious, inconsistency in his accounts. In his deposition of 28 June 2019, the following exchange took place about the call:<sup>773</sup>

“Q. How did that have to do with you erasing your connection to Satoshi?”

A. We had a communication before I left to go to Venezuela, where Dave and Mr. Williams were all on the line. Mr. Williams had helped me in the early days when I was creating Bitcoin. And no one else, other than Dave and Mr. Williams, knew at that point that I was definitively Satoshi or what I've done.” (emphasis added)

That evidence is, of course, inconsistent with Dr Wright’s evidence in these proceedings, which was that by early 2011 numerous people knew that he had created Bitcoin (Mr Matthews, the 20 other people he named in Wright 4 as recipients of the Bitcoin White Paper, the ATO, etc.).

494. Finally on this subject, there is not a single reliable document that shows Dr Wright had met, let alone knew and worked with, either Professor Rees or Gareth Williams. There is not a single witness who attests to any connection between Dr Wright and either of those men. Dr Wright’s stories of collaboration with these two men on the development and implementation of Bitcoin are pure fiction.

---

<sup>772</sup> Dr Wright’s story around Gareth Williams was returned to a number of times, but the best overall picture of this fabrication is from {Day6/114:22} onwards.

<sup>773</sup> {L15/125/102}.

## Early Events in the History of Bitcoin

477. Patch Tuesday: In a blog post of 6 April 2019<sup>774</sup> (and in other public statements<sup>775</sup>), 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 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.<sup>776</sup> **Dr Wright’s attempt to explain away this clear error is important and is addressed in a separate section below.**
478. Upload.ae: In an email from Satoshi to Wei Dai on 22 August 2008 which has long been public,<sup>777</sup> 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.<sup>778</sup> 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 service<sup>779</sup> that was owned in 2009 by one Faisal Al Khaja.<sup>780</sup> **In cross-examination, Dr Wright tried to reconcile his account with the records by accepting that he did not own or operate the domain but had a sub-domain on the site.<sup>781</sup> However, that is not consistent with the account given in his RFI response (of actually operating upload.ae) and it does not explain why he falsely linked upload.ae to Melbourne.**
479. 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*

---

774 “Two steps forward, one step back” 6 April 2019 {L14/420/2}.

775 “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}.

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

777 {L3/195/1}.

778 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}.

779 {L3/191/1}.

780 {L17/379/21}.

781 {Day6/102:1} - {Day6/104:20}.

*O’Hearn*], and that was it. Full stop.”<sup>782</sup> It is well-known that Satoshi sent Bitcoin to Mr Finney, but the statement was otherwise wrong.

479.1. 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.<sup>783</sup> In his evidence, Dr Wright doubled down on his lie.<sup>784</sup> As noted above, the attempt by Dr Wright’s counsel to dispute Mr Wilcox-O’Hearn’s recollection on this point signally failed.

479.2. Secondly, Satoshi sent 100 bitcoin, unsolicited, to Nicholas Bohm.<sup>785</sup> That was not a matter of public knowledge before exchange of evidence in these proceedings, which explains Dr Wright’s omission. It must be Dr Wright’s case that he just forgot about Mr Bohm. If he really did send Bitcoin to very few people in his identity as Satoshi, that is unlikely.

479.3. Thirdly, Satoshi also sent 32.51 and 50 Bitcoin to Mike Hearn on 18 April 2009.<sup>786</sup> Again, it must be Dr Wright’s case that this slipped his mind.

479.4. Fourthly, under cross-examination, Dr Wright sought to add to his story by saying that, in addition to the transfers he had mentioned to GQ, he had (as Satoshi) made transfers of Bitcoin to “*probably about a hundred*” other people but with the Bitcoin coming technically from his company, Information Defense. No doubt this struck him as a good way to explain away people having received Bitcoin from Satoshi whose names he had not given to GQ. He was then asked to name some of this group of about a hundred people, and he failed to do so. The Court pressed: “*Not even one?*” And Dr Wright could not give even one name.<sup>787</sup>

480. Dr Wright was asked in the Consolidated RFI about whether or not he had transferred Bitcoin to any individuals. In his initial RFI response, he said that he did not recall the

---

782 See transcript at {O4/23/5}.

783 Wilcox-O’Hearn §§7-8 {C/6/3}.

784 {Day7/157:20}.

785 Bohm §15 {C/10/4}.

786 {D/505/08}.

787 {Day7/156:19} - {Day7/159:14}.

details or recipients (save for referring to Wright 1, para. 121, which mentioned only Mr Finney, Mike Hearn and Gavin Andresen) and that these were relatively trivial ones.<sup>788</sup> That answer now stands in stark contrast to his recollection that he made transfers to about a hundred people (although he cannot name any). Furthermore, he cannot evade this contradiction by saying that his RFI answer referred to his few transactions from himself while his answer in oral evidence referred to his many transfers from Information Defense, since he specifically said in his oral evidence that the transfers to Mr Hearn and Mr Andresen were from Information Defense.<sup>789</sup>

481. 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 Defence<sup>790</sup> and he makes it in his first statement in the BTC Core Claim.<sup>791</sup> He insisted upon it in his evidence in *Granath*<sup>792</sup> and *McCormack*,<sup>793</sup> and has made the point in postings repeatedly and with vehemence.<sup>794</sup> 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.<sup>795</sup> 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.<sup>796</sup> However, Mr Malmi gives evidence that the post was written by Satoshi, and he exhibits a previously unpublished email from Satoshi to prove it.<sup>797</sup> 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*”.<sup>798</sup>
482. **When cross-examined on this subject, Dr Wright insisted that Mr Malmi had written the post of 6 July 2010 describing Bitcoin as a cryptocurrency. He maintained that position even when confronted with Satoshi’s email to Mr Malmi earlier on 6 July 2010, stating: “I still need to post the announcement message on the forum and mailing list. Here’s**

---

788 {A/13/23}.

789 {Day7/157:8}.

790 Defence at §78 {A/3/23}.

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

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

793 {O2/12/28}, internal p106.

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

795 {L5/196/1}; “Announcing version 0.3 of Bitcoin, the P2P cryptocurrency!”

796 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.

797 {D/369/1}.

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

*what I've prepared: 'Announcing version 0.3 of Bitcoin, the P2P cryptocurrency'* (emphasis added). Denying the obvious meaning of the words, Dr Wright said: "I took what Mr Malmi originally wrote and prepared that". He added: "if you go back into his other emails, you will find that he originally wrote some of this stuff for the page."<sup>799</sup>

483. A little later, Dr Wright was taken back to all Mr Malmi's relevant earlier emails, which showed Satoshi first raising the term "cryptocurrency" with Mr Malmi and the latter just approving it. Pivoting once again, Dr Wright insisted that Mr Malmi had somehow already put a reference to "cryptocurrency" on the web page before the post of 6 July 2010 and said that this could be proved by looking at WayBack Machine captures.<sup>800</sup> By this stage, he had talked himself into a position of clear self-contradiction, since his evidence in the *Granath* proceedings was very specifically that Mr Malmi (not Satoshi) had written the post which was dated 6 July 2010,<sup>801</sup> i.e. the post which the email exhibited by Mr Malmi showed had been prepared by Satoshi.
484. As for the fact that his own documents presented to the ATO described Bitcoin as a cryptocurrency, Dr Wright characteristically blamed others for this supposed deviation from his cardinal principle, saying that it was the fault of his EA ignoring a firm instruction not to use the term.<sup>802</sup>
485. Bitcoin's debt to Hashcash: Dr Wright says that, before releasing the White Paper, he communicated with Adam Back (the creator of Hashcash).<sup>803</sup> 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.<sup>804</sup> 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.<sup>805</sup> 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

---

799 {Day6/150:2} - {Day6/155:9}.

800 {Day7/4:22} - {Day7/7:18}.

801 See the Granath transcript at {O2/11/24}, internal p90, lines 4ff. For the avoidance of any doubt, the document referred to in that exchange is p271 of the Granath bundle, and that in turn may be found at {S2/2.1/41}. It is the post dated 6 July 2010, which Satoshi's email said Satoshi had prepared.

802 {Day6/75:19} and following.

803 Wright 1, §93-94 {E/1/19}.

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

805 Wright 1, §93 {E/1/19}.

Paper only referenced Hashcash because he had not been able to make contact with Prof Aura.<sup>806</sup> 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*”.<sup>807</sup>

486. However, Satoshi’s original post about Bitcoin stated that “*New coins are made from Hashcash style proof of work*”,<sup>808</sup> 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*”.<sup>809</sup> 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 Bitcoin<sup>810</sup> and (b) what Mr O’Hagan in “*The Satoshi Affair*” recorded Dr Wright saying in 2015/16.<sup>811</sup>
487. Dr Wright’s attempts to defend his position on this topic were, again, convoluted and misconceived. He denied the plain meaning of Satoshi’s words, saying that they only meant that both Hashcash and Bitcoin used proof-of-work, not that Bitcoin or its proof-of-work features had any similarity with Hashcash.<sup>812</sup> He insisted that Mr O’Hagan had misquoted him in acknowledging the debt Bitcoin owed to Hashcash.<sup>813</sup> He blamed the terminology in his ATO filing on his former EA.<sup>814</sup>
488. In addition to all these internal contradictions, there is the problem that, as Prof Meiklejohn explains in her report<sup>815</sup> and as Dr Back himself explained carefully under cross-examination (discussed above), the form of proof-of-work used in Bitcoin is very similar to that in Hashcash.
489. 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,

---

806 Wright 1, §94 {E/1/19}.

807 {L15/482/2}.

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

809 {L5/26/3}.

810 {L8/277/15}.

811 {L13/492/24}.

812 {Day6/71:7} and following.

813 {Day6/73:4} and following.

814 {Day6/75:1} and following.

815 Meiklejohn 1, para. 63 at {G/2/23}

amounting to thousands of Australian dollars, due to running computer systems in 69 racks as well as three laptops and four desktops.<sup>816</sup> 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.<sup>817</sup>

490. Dr Wright said that the reference to 69 racks of computers was an error for 69 computers in racks. He insisted on his story of incurring electricity costs of AU\$11,000 per month in his early Bitcoin operation, but said that this was explained by his having to operate the system and verify transactions as well as carrying out hashing operations.<sup>818</sup> As noted above, Prof Meiklejohn rejected Dr Wright's evidence, and she was not cross-examined on the point. Mr Gao could not dispute her figures and he acknowledged that hashing consumes more power than verifying transactions. He likewise could not dispute that Dr Wright's computing set up would have alone overwhelmed the network if even half of its power was dedicated to the power-intensive task of hashing.<sup>819</sup>
491. Being legally trained: Dr Wright's story involves placing his LLM work (both the forged proposal and his actual, albeit irrelevant, LLM dissertation) at the heart of the development of Bitcoin. He claims that his understanding of the legal issues helped him develop Bitcoin. This is in contrast to the real Satoshi writing firmly, "I am not a lawyer"<sup>820</sup> in an email to Mike Hearn on 27 April 2009.

### Papa Neema

492. Papa Neema is another concoction of Dr Wright. In Wright 11, paras. 269-297, Dr Wright told an elaborate story which included him having received emails from Denis Mayaka on 10 and 29 September 2023. He claimed that Mr Mayaka had used, not his professional email address, but a Gmail one: [papa.neema@gmail.com](mailto:papa.neema@gmail.com). He said that, on 10 September 2023, "Papa Neema" sent files said to be tied to Dr Wright's companies in 2009 to 2012.<sup>821</sup> These included alleged invoices from Abacus Seychelles and a version

---

816 Wright 1, §116-117 {E/1/22}.

817 Meiklejohn §74 {G/2/32}.

818 {Day6/146:15} - {Day6/150:1}. Dr Wright has also failed to provide an evidence for the \$11,000 electricity bills, see {Day8/174:10} - {Day8/175:4} and {Day8/179:19}.

819 {Day18/56:21} - {Day18/61:2}.

820 {L18/436}.

821 {CSW/25/1}.



of the “Timecoin” paper discussed above. He also said that “Papa Neema” separately sent photographs of a computer monitor with images of the invoices on them.

493. There are a series of indications that these emails were sent by Dr Wright to himself, as further detailed in Madden 5, from para. 87 {G/9/29}.

493.1. First, the time zone setting of the emails (both those dated 10 and those dated 29 September) was +0100, which was consistent with the UK but not with Mr Mayaka’s residence (Nairobi, Kenya). Faced with that inconvenient fact, Dr Wright claimed that Mr Mayaka set his computer clock to London time because he worked with British clients. That is an obvious lie: it makes no sense for someone to do that.<sup>822</sup>

493.2. Secondly, there are a series of dubious features to the Timecoin document supposedly sent by Papa Neema, as set out above (including the fact that Papa Neema just happened to send it to Dr Wright five days before he found the Samsung Drive containing a hash-identical copy of this previously “lost” document).

493.3. Thirdly, there were further suspicious features associated with the Abacus invoices, including that four documents created on different dates across two years (with different templates) had file titles with the same spelling mistake (“Invoice” for “Invoice”).

493.4. Fourthly, there are a series of indications that the computer monitor screen on the photographs sent by “Papa Neema” was Dr Wright’s, including that the tabs shown referenced his documents (at least one from the BDO Drive) and his favoured software products.

#### The White Paper LaTeX Files

494. As set out above and in the Forgery Schedule at Appendix A, the Bitcoin White Paper was written in OpenOffice 2.4, and not in LaTeX as Dr Wright claims. The White Paper LaTeX files are forgeries. The process by which the forgery was accomplished is addressed in more detail in the Developers’ submissions, which COPA adopts.

---

822 {Day15/49:23} - {Day15/50:17}.

495. We now know that Dr Wright’s acts of forgery were captured on Overleaf’s project history, including over 20 hours of painstaking edits. He claimed that this work had been done to demonstrate to Shoosmiths how adjustments could be made in LaTeX.<sup>823</sup> However, that made no sense and did not square with the information from Shoosmiths about the brief occasions when demonstrations were performed.<sup>824</sup>
496. Dr Wright was forced to concede that the White Paper LaTeX files which he had disclosed on 20 December 2023 would not compile into a replica of the Bitcoin White Paper. When it was pointed out to Dr Wright that the account in Field 1 about these LaTeX files reproducing the Bitcoin White Paper (a statement he endorsed in Wright 6<sup>825</sup>) was therefore wrong, Dr Wright blamed a mixture of his own bad explanation and Ms Field’s lack of technical expertise as to why this false statement had been put before the Court.<sup>826</sup>
497. We also know that Dr Wright knowingly deleted files on Overleaf. This was confirmed in Shoosmiths’ letter of 20 February 2024.<sup>827</sup> Dr Wright also confirmed it in cross-examination.<sup>828</sup> However, when he made his application at the PTR, Dr Wright did not mention the fact that no original files existed, that files had been deleted or that files had been extensively edited. Indeed, the Maths (OLD) project was not referred to in any correspondence or witness statement, but was disclosed inadvertently (as stated by Shoosmiths in correspondence on 1 February 2024).<sup>829</sup> Had that not happened, the truth about the history and extent of the edits would not have been found.

#### Dr Wright’s Patch Tuesday Story and Explanations

498. It is well known that an unexplained gap exists between Satoshi’s creation of the Genesis Block on 3 January 2009 and the mining of Block 1 on 9 January 2009. Dr Wright’s evolving attempts to fill the gap reveal a series of contradictory, unconvincing attempts to explain away a tell-tale flaw in his Satoshi origin story.

---

823 {Day15/137:3}.

824 {M/3/15}

825 At §4, {E/21/3}.

826 {Day15/143:14} - {Day15/146:12}.

827 {M1/2/210}.

828 {Day15/152:2} - {Day15/153:22}.

829 {M1/2/153}.

499. Patch Tuesday (occurring on the second, and sometimes on the fourth, Tuesday of each month) is the day when Microsoft rolls out updates to address security vulnerabilities and other issues in its software.

*Accounts given by Dr Wright about Patch Tuesday*

500. Dr Wright gave a series of accounts of events in the early life of Bitcoin in interviews and articles. In an interview, article and a chapter of “Satoshi’s Vision”, he told a story of the Bitcoin system crashing between 3 January and 9 January 2009 as a result of the occurrence of Patch Tuesday. He said that, after this happened, he had had to build a domain to prevent problems recurring. See: (a) transcript of interview of 24 April 2019;<sup>830</sup> (b) blog post of 6 April 2019, “*Two Steps Forward One Step Back*”;<sup>831</sup> and (c) Satoshi’s Vision at p14-15.<sup>832</sup>

*Cross-examination of Dr Wright on Patch Tuesday*

501. Commenting on the statement in the transcript of his April 2019 video interview<sup>833</sup> “*Before the 10<sup>th</sup> of January, I had to build a domain*”, Dr Wright said that it should have been “*rebuild*”<sup>834</sup> and that he “*already had a domain.*”<sup>835</sup> However, he repeated his account that the problem which afflicted his network occurred between 3 and 10 January 2009.<sup>836</sup>
502. It was then put to him that Patch Tuesday in January 2009 had taken place on Tuesday 13 January. Dr Wright replied that he did not know whether or not that was true, but he said that he had a WSUS server that would implement patches on a schedule set by him.<sup>837</sup>
503. On being challenged that Microsoft’s Patch Tuesday update notification for 13 January 2009 covered both Windows Update (WU) and Windows Server Update Services

---

830 {L17/108/13}, lower half.

831 {L14/420/2}.

832 {L15/95/14}.

833 “*Dr Craig Wright explains the origins of Bitcoin*” 24 April 2019 {O4/25/25}.

834 It is unclear whether Dr Wright was questioning the accuracy of the transcript or purporting to correct an error in what he said during the interview. Either way, it is evident from the video recording itself that he said ‘build’ {L15/16/1} (00:45:12).

835 {Day6:135/16}.

836 {Day6/136:13}.

837 {Day6/137:3} and following.

(WSUS),<sup>838</sup> Dr Wright developed his story further, saying that he was a member of the Microsoft Developer Network (“*not one of the every day plebs out there*”) and had access to pre-release material after internal testing and beta testing by Microsoft.<sup>839</sup> He described members of the MSDN programme as “*test guinea pigs first, it’s like a beta programme...*”<sup>840</sup> Dr Wright stated that “*Patch Tuesday*” was a generic reference to Microsoft’s updates, even if a WSUS server was pulling patches on its own schedule.<sup>841</sup>

#### *Inconsistencies and flaws in Dr Wright’s accounts*

504. As can be seen, Dr Wright’s story on Patch Tuesday has changed every time its flaws have been pointed out to him. He began by saying that “Patch Tuesday” (a recognised term for an event affecting MS users generally on a designated Tuesday each month), which he described as a “*horrible invention*” had crashed the systems. When confronted with the point that the dates did not work, he said that as a WSUS user he scheduled his own updates. When confronted with the point that the update notification for 13 January 2009 affected WSUS users, he claimed to be a member of the MSDN.
505. There are myriad problems and inconsistencies with Dr Wright’s evolving account of events.
- 505.1. **No WSUS server (6 April 2019 blogpost).** The first version of the Patch Tuesday story in Dr Wright’s blogpost of 6 April 2019 made no mention of a WSUS server: “*The original machines were a group of workstations and not a domain.*” Furthermore, the explanation for the simultaneous shutdown implied separately patched machines, not a cluster of machines with updates managed locally by a WSUS server: “*I had configured all of the machines with the same time zones, even those in different countries. They all shut down to patch at the same time.*”
- 505.2. **WSUS in response to Patch Tuesday (24 April 2019 interview).** In the 24 April 2019 interview Dr Wright appears to describe building a domain in response to the problems said to have been caused by “*Microsoft making all*

---

838 {L4/60/2}.

839 {Day6:138/21} - {Day6:139/11}.

840 {Day6:140/2}.

841 {Day6:136/21}, {Day6:137/5}.

*machines turn off at once*". Similarly, in his 19 June 2019 interview Dr Wright described how he was running "*a bunch of standalone Windows XP machines*". He described how in response to the Patch Tuesday shutdown he "*set up ... WSUS servers. ... I had to set up a full domain just to keep these Windows XP machines running so that we could say that they didn't actually all shut down at the same time. And I had to have rolling intervals*".

- 505.3. **WSUS from the start (Wright 11).** In contrast, in Wright 11<sup>842</sup> Dr Wright stated that his servers were set up with WSUS from the start, that the Bitcoin nodes were running as a service and with updates from Microsoft during the week some did not restart.
- 505.4. **WSUS integration in response to Patch Tuesday (Initial cross-examination).** Dr Wright's initial position in cross-examination was that he responded to the supposed Bitcoin shutdown by integrating his Windows XP machines with his existing WSUS server. "*No, I already had a domain. I hadn't had the Windows XP machines on the domain. So what we're talking about there is, I had a domain but I needed to integrate these systems.*"<sup>843</sup>
- 505.5. **WSUS from the start plus MSDN pre-release updates (Later cross-examination).** In order to explain how Microsoft's Patch Tuesday updates could have shut down the Bitcoin machines over a week earlier than 13 January 2009, Dr Wright's position then became that the machines were already on a WSUS server<sup>844</sup> distributing pre-release Microsoft updates according to a schedule under Dr Wright's control<sup>845</sup>.
- 505.6. **Patch Tuesday just a name?** Seeking to explain his anachronistic references to Patch Tuesday having caused disruption in the first week, Dr Wright's response in cross-examination was that Patch Tuesday is a generic industry term for Microsoft updates regardless of when a local WSUS server may be configured to distribute them: "*It's called Patch Tuesday even when it happens*

---

842 {CSW/1/200} at paras. 1158 and 1159.

843 {Day6/135:16}.

844 {Day6/136:17} - {Day6/136:23}; {Day6/137:5} - {Day6/137:6}.

845 {Day6/138:21} - {Day6/140:6}.

*on a Friday”<sup>846</sup>. However, in his 19 June 2019 video interview Dr Wright said: “Anyone remember Patch Tuesday? So that was another reason Bitcoin before the current Blockchain turned off, apart from crashing, literally on that Tuesday night everything updated, turned off and restarted...”<sup>847</sup>*

- 505.7. Finally there is a contradiction between Dr Wright’s reply evidence that “*I needed to travel between locations to ensure the servers were running correctly, and in the first week, this was not possible*” and his statement in the 19 June 2019 video interview that he was driving back and forth to Bagnoo in that week in order to fix the problems.<sup>848</sup>
506. It is quite clear that, not only can Dr Wright not get his story straight, but that he has changed it several times as each excuse is debunked. There is also no evidence of him being on the Microsoft Developer Network, nor any proof that even if he was, these updates would have been applied to him within that network. It is therefore a good example of Dr Wright trying to bolster his origin story by attempting to add in supposedly complementary detail to what was a known public event (the lack of mining between 3 to 9 January). However, the detail he added was wrong. The real Satoshi would know what actually happened and have a cogent reason for it.

### **List of Individuals Blamed by Dr Wright in his Evidence**

507. In his evidence, Dr Wright gave a very large number of excuses for signs of forgery in his documents and for apparent inconsistencies and falsehoods in his own accounts. These involved making accusations of malicious and dishonest acts, errors and incompetence against an ever-increasing cast of characters. By contrast, Dr Wright denied even the clearest evidence of his own falsehoods. The only times he came close to making any admissions were a couple of occasions when he admitted to having given misleadingly incomplete evidence in the Kleiman proceedings.<sup>849</sup>
508. The following is a list of the individuals he has blamed for hostile acts, errors and incompetence. It is given here to illustrate the remarkable set of findings which would

---

846 {Day6:137/1}.

847 “Coingeek Toronto Fireside Chat” 19 June 2019 {O4/12/14}.

848 “Coingeek Toronto Fireside Chat” 19 June 2019 {O4/12/14}.

849 See for example, {Day2/56:6} - {Day2/56:21}.

be required to endorse Dr Wright's version of events. In each case, the allegations made against these individuals by Dr Wright are baseless and unsupported.

### Dr Wright's principal villains

509. Dr Wright repeatedly cited three individuals as being responsible for hostile acts against him, often involving elaborate conspiracies, sophisticated hacking of computer systems and the forgery and planting of documents. On Dr Wright's account, they rarely acted alone, and were often aided and abetted by unknown co-conspirators. These were:

509.1. **Ira Kleiman**, for working with others to plant falsified evidence on Dr Wright, such that Dr Wright was, he says, later compelled in litigation to disclose it (e.g. {Day2/21:13} - {Day2/25:8}, {Day4/46:18} - {Day4/51:11}, among many other examples). Mr Kleiman is said to be assisted by various others including "Gwern...working with Ira Kleiman to out me in 2015" {Day 2/21:14}. The motivation for their desire to reveal Dr Wright as Satoshi Nakamoto a few months before he was going to be revealed anyway is obscure.

509.2. **Christen Ager-Hanssen**, for a range of activities including spiking Dr Wright's drinks {Day 4/155:3}, compromising Dr Wright's computer {Day 4/155:10}, perpetrating a hack which accounted for all anomalies in the BDO Drive materials {Day5/68:4}, seeking to divert documents from Mr Mayaka (aka Papa Neema) {Day 5/149:19}, and even (perhaps) bugging Dr Wright's home. According to Dr Wright, Mr Ager-Hanssen has been assisted by a band of others including:

509.2.1. one or more **unknown hackers**<sup>850</sup> with a Linux laptop {Day 5/68:4};

509.2.2. **Some Really Tall Guy** who is supposedly ex-CIA and who pressurised witnesses {Day 5/112:3};

509.2.3. **Some Other Guy** who is said to be ex-Mossad and who also pressurised witnesses {Day 5/112:4};

---

<sup>850</sup> This was one of a number of instances of 'hackers' being blamed by Dr Wright. The Court is invited to treat those claims with even greater skepticism given that, on Dr Wright's own account, he is a highly qualified IT security professional.

- 509.2.4. **Maze Cyber**, a hacker group which was supposedly somehow involved in the attempt to divert material from Mr Mayaka {**Day 4/155:16**}.
- 509.2.5. **Zafar Ali KC**, and **Ted Loveday**, “*who set up the fake trial thing*” and pressured witnesses (at least pressuring Mr Matthews to drop his evidence) {**Day5/110:12**}.
- 509.3. **Greg Maxwell**, a defendant in the BTC Core case, who is said to operate under numerous aliases and to be responsible for planting evidence, presenting misleading technical explanations, giving misleading factual explanations, and colluding with others against Dr Wright’s interests (including Ira Kleiman).

#### Lawyers and other professionals involved in Dr Wright’s litigation

510. Dr Wright has also cited a series of various professional advisers in his excuses, often accusing them of incompetence or worse (expert witnesses are addressed in another section):
- 510.1. “**Jonny the Sikh**”, who is said to have been told about false NAB records being planted on Dr Wright {**Day2/35:10**}.
- 510.2. **Amanda McGovern**, his previous attorney in Florida, who supposedly received the false NAB records from the mysterious Reddit user, and has since died {**Day2/29:13**} - {**Day2/38:3**}.
- 510.3. **Ontier**, who are said to have (a) “accidentally released privileged documents” without identifying them as privileged {**Day2/39:11**}; (b) given him defective advice about disclosure of White Paper LaTeX files; (c) given false information about when they received MYOB login information; (d) failed to identify numerous documents in Dr Wright’s disclosure as forgeries or unreliable, despite that being clear from their internal Relativity platform, from chain of custody information given to them by Dr Wright or otherwise from Dr Wright’s instructions.
- 510.4. **Travers Smith**, for coming under a conflict due to accepting instructions from Mr Ager-Hanssen against Dr Wright’s wishes and interests {**Day4/157:12**} and



for rejecting all experts identified by Dr Wright as suitably qualified **{Day5/56:13}**.

- 510.5. **Wikborg Rein**, Dr Wright's lawyers from Norway who nominated a list of primary reliance documents on Dr Wright's behalf in the Kleiman proceedings notwithstanding that Dr Wright knew some to be forgeries: **{Day4/90:1}** to **{Day4/96:5}**.
- 510.6. One or more **unidentified solicitors at Ontier** for persistently mishandling documents, giving rise to signs of manipulation: **{Day3/65:2}** - **{Day3/65:9}**.
- 510.7. A **young trainee solicitor at Ontier**, who was particularly responsible for bad advice about disclosure of Overleaf materials and who has "*since been let go*" **{Day5/131:17}**.
- 510.8. **Shoosmiths**, for choosing Stroz Friedberg as expert witnesses despite their supposedly evident conflict of interest **{Day5/57:4}**.
- 510.9. **AlixPartners**, for failing to notice the encrypted content on the Samsung Drive, applying stickers incorrectly to the drive, etc. **{Day5/34:1}** to **{Day5/35:13}**.
- 510.10. The lawyers who drafted various trust deeds which contributed to the confusing tale of the Tulip Trust, including **Diane Pinder of Lloyds Solicitors and Bakers** (presumably, Baker McKenzie whose name appears on the Implementation Deed) **{Day4/102:11}**.

#### Dr Wright's own friends, family and co-workers

- 511. Dr Wright has also named family members, friends and colleagues in his excuses, often piling blame upon them:
  - 511.1. His ex-wife **Lynn Wright**, who (on Dr Wright's account) gave false evidence in the Kleiman proceedings, as a result of being "*on a lot of medication...heavily sedated...on opioids*" **{Day2/97:18}**, having wrongly stated that she was fit to give evidence **{Day2/118:3}**.

- 511.2. **Jamie Wilson**, former CFO of one of Dr Wright’s companies “FASV”, and who “ended up helping Ira Kleiman” {Day4/85:4} to {Day4/86:2}, and who “was actually doctoring my signature” {Day4/88:5}.
- 511.3. **Sebastian Ploetzender**, who was responsible for posting blogs / uploads by Dr Wright and was thus said to be responsible for any inconsistencies in evidence arising from them: {Day2/141:2}; {Day4/26:24}; {Day3/96:3}.
- 511.4. “**Andy**”, another person responsible for Dr Wright’s blogs/uploads: {Day2/141:2}; {Day3/96:3}; {Day4/26:24}.
- 511.5. Dr Wright’s “**EA**” who supposedly “had access to my email” and submitted documents to the ATO with mis-descriptions against his authority: {Day6/75:19}.
- 511.6. The editor of Dr Wright’s LLM Thesis, an unnamed “**woman in Australia**” who “didn’t use EndNote” {Day6/29:21} and removed references, leading to Dr Wright’s work appearing to be plagiarised.
- 511.7. The **people who operate his Twitter account** for him (“My Twitter isn’t just myself” {Day 2/18:1}).
- 511.8. **Disgruntled former employees** in Dr Wright’s companies, who were seeking to help Ira Kleiman and his case, including in leaking / falsifying documents (e.g. {Day4/46:18} to {Day4/51:11}) and **ex-staff members** who had “intentionally tried to sabotage my company” {Day2/39:24}. These may or may not have been references to the same groups of individuals.
- 511.9. “**A variety of staff**” to whom his documents were “accessible” and whose actions in opening and/or editing documents accounted for signs of inauthenticity / forgery (e.g. {Day2/58:22}). These included:
- 511.9.1. “**Somebody**” at **nChain** who had “written a disk”, thus accounting for a chain of custody anomaly {Day2/117:3}.
- 511.9.2. “**Someone**” who “updated or not saved the document the same way” while “the server has had a partial image” (said to lead to Dr

Wright's documents accidentally splicing together content from different time periods without his knowledge): {Day2/137:3}; {Day2/140:2}.

- 511.9.3. **"Someone...at a later date"** who *"has opened up the document probably with MathType server"*, giving rise to an artefact in a document {Day2/143:22}.
- 511.9.4. **"Someone"** who had made a post on his behalf and added incorrect content (*"added something I don't want because of the cryptocurrency bit"*) {Day2/142:23}.
- 511.9.5. **"A team of individuals"** at DeMorgan {Day4/32:16} who were responsible for preparing a later Code2Flow document which looked identical to a supposed 2008 predecessor, but none of whom was giving evidence {Day4/37:14}.
- 511.9.6. **"Someone"** who *"opened [the Code2Flow document] with Adobe Distiller"* with the result that it acquired a metadata reference to a 2016 version of Adobe XMP Core {Day4/42:17}.
- 511.9.7. **An ex-staff member who had access** to "my wife's email, my wife's personal email, my email, several other staff members' emails, and other emails that it should not have had" and who was responsible for a spoofed email being in Dr Wright's disclosure {Day4/64:7}.

#### Miscellaneous individuals and computer software

512. Dr Wright has also pointed to a series of other individuals and pieces of computer software in his excuses:

- 512.1. **Someone who was not Dr Wright** but posted a browser speed test screenshot to Dr Wright's Slack, in Dr Wright's name and against his profile photograph, using an IP address geolocated to Dr Wright's home, and with "*Craig*" written on it at the top: {Day3:54/13} - {Day3/56:17}.
- 512.2. The **Australian Tax Office**, who were trying to bankrupt Dr Wright, and also the individual **Christopher McArdle**, who was trying to seek a judgment

against him (and whose actions resulted in Dr Wright's assets being moved through various companies and obscure trust structures: {Day4/97:3}).

- 512.3. **“Third parties on the Internet”** who sent information to the Australian Tax Office, leading to Dr Wright being compelled to disclose that information in litigation: {Day4/67:6}.
- 512.4. The **“anonymous Reddit person”** who was supposedly responsible for planning the false NAB records on Dr Wright and his lawyers {Day2/31:9}.
- 512.5. **Mr Arthur van Pelt** (a podcaster and blogger who has written articles over the years explaining flaws in Dr Wright's claim to be Satoshi), for supposedly leaking information from this case that was, Dr Wright suggested, not in the public domain {Day19/55:5}.<sup>851</sup>
- 512.6. **Dr Nicholas Courtois**, *“an academic who was basically a fraud”* who participated in the GQ interview in May 2016 {Day7/155:16}.
- 512.7. **The BBC**, for misleadingly editing and then losing footage, which *“suits their purposes”* {Day8/60:9}.
- 512.8. **“Grinder, or whatever”** which *“will embed documents this way”* and was thus responsible for embedded pictures which appeared to be artefacts of conversion from a later version of Word {Day2/111:4}.
- 512.9. **“Printers”**, which supposedly had the effect of making numerals appear smaller / misaligned in Dr Wright's Tominaga Nakamoto article (*“Printers do that”*) {Day2/23:16}.
- 512.10. **“A system”** which *“changes something by itself”*, accounting for metadata references to anachronistic artefacts in Dr Wright's LLM proposal {Day3/59:19}.
- 512.11. **EndNote** Software which *“didn't handle blogs terribly well”* and so (in combination with human error by the Australian female editor) helped to

---

<sup>851</sup> Mr Van Pelt has tweeted screenshots of documents from the case, but (to the best of COPA's knowledge) he has only ever done so after they have been publicly released.

account for signs of forgery in Dr Wright's LLM dissertation (even though Ms Pearson's paper was not a blog at all) {Day6/29:21} - {Day6/30:20}.

- 512.12. **Xcopy, Citrix, symbolic links, Normal.dotm** templates, **Microsoft** software, **VMWare, LaTeX compilers and packages, pandoc**, and various other software packages referred to extensively throughout Dr Wright's evidence to explain forensic signs which the experts by agreement considered showed document manipulation.

### Witnesses in this case

513. In addition to the other individuals identified above, Dr Wright took aim at all the expert witnesses in this case (even the adulatory Mr Gao, whom he claimed did not have expertise to opine on the signing sessions). He also attacked a number of COPA's fact witnesses. The main targets were as follows:

- 513.1. **Professor Meiklejohn**, a respected cryptographer and cryptocurrency expert, whose expertise he challenged, saying that she "*studies sociology*" and has not "*studied cryptography in any real depth*" {Day7/56:17}.
- 513.2. **Mr Madden**, for failing to notice that "*printers...do that*" {Day 2/23:24}, for "*extraordinarily bad analysis*" {Day2/115:23}; for having done "*not a single IT security, IT forensics, or other certification, course or training*" {Day2/128:18}; for being "*completely biased*" {Day3/111:17} to {Day3/112:1}; and for countless other perceived failings throughout Dr Wright's evidence.
- 513.3. **Mr Rosendahl**, who was said to be biased and to have extensive links to BTC Core developers and investments in cryptocurrency ({Day5/137:22} - {Day5/138:12}), as well as alleged to be wrong in the application of his expertise throughout Dr Wright's evidence on the LaTeX files.
- 513.4. His own expert **Dr Placks**, for incompetence, being "*a psychologist*" having "*no qualifications in information security*" {Day 2/128:6}, with a reprise on Day 3 {Day3/1:25} - {Day3/4:6} and an accusation of him being entirely "*unskilled*" {Day3/112:4} (and continuing in the same vein throughout Dr Wright's evidence).

- 513.5. His own expert **Mr Lynch**, on the basis that he was not qualified or experienced and “*doesn’t even meet the basic level for the US Government certification framework*” {Day3/5:14} - {Day3/6:3}.
- 513.6. **Stroz Friedberg**, for misunderstanding Dr Wright’s various computing environments ({Day5/48:8} and {Day5/55:7}), working under a conflict of interest and having unacceptable connections with COPA members {Day5/57:4}.
- 513.7. **Mr Statakis and Ms Li of Quill**, for (on Dr Wright’s account) misrepresenting their knowledge of their business and in particular Ms Li’s personal knowledge of the design, proof, and manufacture of the Quill notepad on which Dr Wright claims to have written years before it was put into production {Day3/106:11} - {Day3/114:11}. Dr Wright claims that Ms Li had “*no involvement*” at all {Day3/114:7}.
- 513.8. **Mr Rory Cellan-Jones**, an otherwise highly-respected science and technology journalist, for being “*very biased... incredibly biased*” {Day8/60:24}.

### **The Argument based on the Real Satoshi not having Come Forward**

514. Dr Wright, in his opening skeleton and opening oral submissions, sought to rely on the fact that it was surprising that nobody else had come forward claiming to be Satoshi. The very fact that Dr Wright placed such reliance on this argument demonstrates his lack of reliable and probative evidence to support his claim and a desire to divert attention from the serious flaws in the “proof” he has offered over the years.
515. It is wrong to say that there is an absence of other people claiming to be Satoshi. As noted above, there have been many other claims to copyright in the Bitcoin White Paper. As the Court will know from its own inbox, even during this trial there has been a stream of communications to the parties and the Court by people saying that they are Satoshi. It may be objected that these are cranks. But in truth the only difference between their claims and Dr Wright’s false claim is that he has had more persistence, a penchant for forgery and the financial backing of a billionaire.
516. In any event, the fact that the real Satoshi Nakamoto has not come forward is hardly surprising. The person (or persons) went to great efforts to disguise their identity

between 2008 and early 2011, both by not giving away contextual clues in communications and by using anonymous, untraceable means of communication. The surprise is not that the real Satoshi has failed to come forward, but that Dr Wright can seriously claim to have made all those efforts to secure anonymity while revealing his identity to numerous people while not even asking them to keep it secret.

517. Quite apart from all the signs that the real Satoshi wanted to remain anonymous from the start, they would have even more incentive to do so now. If they are still alive, they would appear to be sitting on a trove of Bitcoin worth billions of pounds / dollars (potentially up to US\$80 billion, based on Bitcoin's current price and estimates of the Bitcoin mined by Satoshi), which would comfortably place them among the world's 20 richest people. For the real Satoshi to come forward now would put them in an intense spotlight – not just by the media, but by tax authorities and regulatory authorities. It would also expose them to pressure from criminals, since they would immediately be known to have a vast fortune which could be transferred to another person without the protective measures a bank would adopt.
518. There is no reason why the real Satoshi would reverse their decision to remain anonymous based on Dr Wright having made his false claim prominently. Assuming that the real Satoshi has chosen for their own reasons to remain in the shadows, yet another false claimant would not be expected to change their approach.
519. The related argument might be made that Dr Wright would not have made his claim at the risk of having it discredited by the real Satoshi. However, this case has revealed Dr Wright repeatedly taking risks with his lies and forgeries, and being caught out time and again. The idea that in 2015-16 he decided that staking a claim to be Satoshi was a risk worth taking after the real Satoshi's identity had remained a mystery for several years is hardly surprising in that context.
520. Furthermore, in the setting of the Tulip Trust disputes, Dr Wright has previously been outed as a liar by claiming to own the 16cou address, with that address among others then being used to sign the message "*Craig Wright is a liar and a fraud*" after the ATO communication was made public.<sup>852</sup> This is a good illustration of Dr Wright being

---

852 {L/17/382/46}.

prepared to take a risk of staking a false claim which could immediately be discredited by the real owner of the address.

### **Further Submissions on Dr Wright's Credibility**

521. 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*,<sup>853</sup> 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. COPA submits that Dr Wright's evidence should be assessed in the same way in this case – focusing on the content of what he said and testing it against the facts, other evidence and inherent probabilities.
522. 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.<sup>854</sup> 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.<sup>855</sup> In closing submissions in the *Kleiman* case, his own advocate began by accepting Dr Wright's frequent self-contradictions.<sup>856</sup> This case demonstrates similar changes and convolutions of account. One obvious example is the developing history of the MYOB documents, with each new development involving a further forgery, ending with the forged MYOB Ontier Email made during trial.

---

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

854 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.

855 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}.

856 {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."



523. 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.<sup>857</sup> **Dr Wright was given repeated chances in this case to confess and come clean, including at the end of his final trip to the witness box. Not only did he decline that opportunity, but he went on a rant (which makes no sense when read in the transcript) about Google Takeout and faking times in Outlook.**<sup>858</sup>
524. 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.
525. 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 judgment<sup>859</sup>); (b) the 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;<sup>860</sup> (d) his account of Ontier advising him

---

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

858 {Day19/49:13}.

859 {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*").

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

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).<sup>861</sup>

526. Sixthly, Dr Wright during his cross-examination repeated variations on a theme of COPA's members and the Developer defendants conspiring against him, in particular supposedly seeking to steal "his" patents (which on any view are in fact patents owned by nChain) and other intellectual property. There is no truth in these accusations, and Dr Wright had no evidence for any of them. He also accused COPA, the Developer defendants and their fact witnesses of trying to pursue a particular implementation of Bitcoin. That point ignores the fact that COPA's fact witnesses take different views about how the Bitcoin system ought to operate and develop (a point which emerged clearly in Mr Hearn's evidence). They are hardly a cohesive group, as illustrated by Mr Wilcox-O-Hearn having blocked Dr Back on Twitter.

### **Relief Claimed**

527. 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.<sup>862</sup> COPA sets out its broad submissions here, but it would intend to expand upon them at a form of order hearing.
528. 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.

---

<sup>861</sup> {M/2/691}.

<sup>862</sup> See Re-Re-Re-Amended Particulars of Claim, §§68-71 {A/2/21}.

529. Dr Wright's Defence denies that the declarations should be granted and raises a quasi-jurisdictional objection.<sup>863</sup> 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.<sup>864</sup> The sole substantial defence raised to the injunctions is that they would infringe Dr Wright's Article 10 right to free expression.

#### Legal Principles for Declaratory Relief

530. The legal principles for declaratory relief in the present context are set out in *Copinger and Skone James on Copyright (18<sup>th</sup> 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

531. 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.

532. 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

---

<sup>863</sup> Re-Amended Defence, at §§88-91 {A/3/28}.

<sup>864</sup> Re-Amended Defence, at §93 {A/3/28}.

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.

533. 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

534. 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.
535. 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.
536. 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.
537. 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.”

538. 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 ...”

539. 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.

540. 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.”

541. 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).

542. 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).
543. 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).<sup>865</sup> The likelihood of repetition is an important factor in determining whether a final injunction should be granted.<sup>866</sup>
544. **The Court of Appeal has recently emphasised how serious it is to abuse the court process by advancing false claims. In *Flitcraft Limited v Price* [2024] EWCA Civ 136 the Master of the Rolls commented as follows:**

*“85. I agree with both judgments. I would only add one point, just in case the heinous nature of what Mr Price and Mr Middleton have done is lost in the meticulous detail of the two main judgments above. It appears from what the judge found that (a) Mr Price deliberately instigated a false claim in the High Court founded on an allegation that he was the proprietor of the patents, when he was not, and (b) Mr Middleton deliberately supported that false claim. The court takes a very serious view of dishonest conduct of this kind. It undermines the integrity of the justice system.*

*86. Whilst Summers was a different kind of case on the facts as has been pointed out, the following part of what Lord Clarke said in Summers at [53] was relevant here:*

*As to costs, in the ordinary way one would expect the judge to penalise the dishonest and fraudulent claimant in costs. It is entirely appropriate ... to order the claimant to pay the costs of any part of the process which have been caused by his fraud or dishonesty and moreover to do so by making orders for costs on an indemnity basis. Such cost orders may often be in substantial sums perhaps leaving the claimant out of pocket. It seems to the court that the prospect of such orders is likely to be a real deterrent.*

*87. That was why the judge was right to order Mr Price to pay Flitcraft's costs on the indemnity basis, and to penalise Supawall in costs for Mr Middleton's false evidence.*

---

<sup>865</sup> See *Copinger* at §21-236.

<sup>866</sup> *Ibid* at §21.238.

*The court will take every appropriate step to deter those who contemplate bringing false claims, and thereby practising an intolerable deception on the court itself.*

545. In *Flitcraft*, the “intolerable deception on the court” was a claim to be the proprietor of a patent. In that case, it was Mr Price who advanced this deception, but he was in fact the original proprietor (having subsequently lost his right through bankruptcy).

#### Justification for Injunctive Relief

546. 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.

547. Whilst the conduct in *Flitcraft* was described by the Master of the Rolls as heinous, the dishonesty and other conduct of Dr Wright (including his threats and pursuit of aggressive litigation based on false premises) is many orders of magnitude worse. The Court should therefore take every appropriate step to stop this from happening again.

548. 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.

548.1. 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).

548.2. 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.

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

548.4. 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*");<sup>867</sup> and (b) Dr Wright's posts which breached the embargo in *McCormack* (including that he would "*spend 4 million to make an enemy pay I*").<sup>868</sup> A series of aggressive "*troll hunting*" tweets by Mr Ayre can be found in the *Granath* hearing bundle.<sup>869</sup>

548.5. 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).

548.6. 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).<sup>870</sup> 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.

549. Furthermore, in these proceedings Dr Wright has abused the Court process at various levels. There is abuse at a high level, in that his claim is based on a central lie. However, he has also abused the court process at every step on the way, as set out below.

549.1. He has disclosed large numbers of false documents which appear to support his claim. In some cases, he has now admitted that they are fakes, but even those were not identified as such when disclosure was given.

549.2. He committed repeated and serious failures of disclosure, and kept up a stream of very late disclosure (including the box of manuscript documents provided during trial). While late disclosure is not itself out of the norm, the pattern in

---

867 {O2/12/33}, internal p126.

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

869 {S2/2.1/4}.

870 *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.



this case is egregious, in particular the fact that much of the late disclosure was due to forgery being committed during the proceedings.

- 549.3. He sought to avoid providing information and material, including in response to RFIs, requests for chain of custody information and requests for access to computing equipment and Overleaf materials. In many instances, the information that he was ultimately required to provide proved crucial in exposing one or more forgeries.
- 549.4. Relatedly, he refused to answer questions by saying that they were irrelevant, but then later on maintained that they were of the utmost importance. A clear example of is his refusal to answer the RFI Request about operating systems he used. Compare that to how much importance he later placed on his Citrix environment and Virtual Machines.<sup>871</sup> Another example is him refusing Mr Madden's requests to give access to forensic images of the sources of his documents and then (through counsel) challenging Mr Madden for not examining such images.
- 549.5. He forged the Ontier MYOB Email in the middle of trial.
550. Finally, Dr Wright sought to use the witness box as a podium to trumpet his views about the Bitcoin system, even when they had no relevance to the question being asked. For example, the final question in the cross-examination by Mr Gunning KC when Dr Wright had been recalled, and Dr Wright's answer, were as follows:

*Q. Dr Wright, your claim to be Satoshi Nakamoto is a fraudulent claim, isn't it?*

*A. No, not at all. In fact, I wouldn't need to actually claim to be Satoshi, I have now proveably scaled beyond anything Silicon Valley can do. We have created a system that's doing 1.1 million transactions a second live, my Lord. That exceeds the capability of Oracle, it exceeds the capability of Microsoft, who are now talking to us, it exceeds any -- and they will argue centralised, except it's distributed. No Oracle database, as a centralised system, can do a million transactions a second, my Lord. That's actually running, and we now have governments involved in that, and none of them care that I'm Satoshi or not. What they care about is we have a distributed blockchain that is scaling to 1.1 million plus transactions a second continuously.*

---

871 {A/13/23}.

551. It is clear that Dr Wright will go on using legal proceedings as a tool to threaten his opponents and as a megaphone for his views. A particularly unattractive aspect of his conduct has been that he at first sought to do this by bringing claims against individuals like Mr McCormack and Mr Granath, who were unlikely to have the means to defend his claims adequately. Mr Ayre even boasted of this strategy: “*judge only needs one troll to pass judgment... no need to sue everyone... just waiting for a volunteer to bankrupt themselves trying to prove a negative*” (13 April 2019, right after his “troll-hunting” meeting with Dr Wright and his defamation lawyers in London).<sup>872</sup> He only brought his principal proceedings against well-funded opponents after COPA called him out by bringing this action.

### **Conclusion**

552. 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.<sup>873</sup>

**JONATHAN HOUGH KC  
JONATHAN MOSS  
TRISTAN SHERLIKER**

---

<sup>872</sup> See the collection of Mr Ayre’s tweets in the Granath hearing bundle at {S2/2.1/4} - {S/2.1/14}.

<sup>873</sup> Whilst their names do not appear on these Closing Submissions, it would not have been possible to prepare them without the help of numerous individuals within the COPA legal team, and their contribution has been vital.