Neutral Citation Number: [2024] EWHC 1198 (Ch)

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

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

The Rolls Building
7 Rolls Buildings
Fetter Lane
London EC4A 1NL

Date: 20th May 2024

Before:

MR. JUSTICE MELLOR

- - - - - - - - - - - - - - - - - - - -

Between:

CRYPTO OPEN PATENT ALLIANCE

Claimant in IL-2021-000019

(the "COPA Claim")

and

CRAIG STEVEN WRIGHT

Defendant in the COPA Claim

And Between:

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

Claimants in IL-2022-000069 (the "BTC Core Claim")

and

(1) BTC CORE
(2) WLADIMIR JASPER VAN DER LAAN
(3) JONAS SCHNELLI
(4) PIETER WUILLE
(5) MARCO PATRICK FALKE
(6) SAMUEL DOBSON
(7) MICHAEL ROHAN FORD
(8) CORY FIELDS
(9) GEORGE MICHAEL DOMBROWSKI (a.k.a 'Luke Dashjr')
(10) MATTHEW GREGORY CORALLO

(11) PETER TODD
(12) GREGORY FULTON MAXWELL
(13) ERIC LOMBROZO
(14) JOHN NEWBERY
(15) PETER JOHN BUSHNELL
(16) BLOCK, INC.
(17) SPIRAL BTC, INC.
(18) SQUAREUP EUROPE LTD
(19) BLOCKSTREAM CORPORATION INC.
(20) CHAINCODE LABS, INC
(21) COINBASE GLOBAL INC.
(22) CB PAYMENTS, LTD
(23) COINBASE EUROPE LIMITED
(24) COINBASE INC.
(25) CRYPTO OPEN PATENT ALLIANCE
(26) SQUAREUP INTERNATIONAL LIMITED

Defendants in the BTC Core Claim

- - - - - - - - - - - - - - - - - - -

- - - - - - - - - - - - - - - - - - -

JONATHAN HOUGH KC, JONATHAN MOSS (instructed by Bird & Bird LLP) and TRISTAN SHERLIKER (of Bird & Bird LLP) appeared for COPA.

LORD GRABINER KC, CRAIG ORR KC, MEHDI BAIOU, TIMOTHY GOLDFARB and RICHARD GREENBERG (instructed by Shoosmiths LLP) appeared for Dr Wright.

ALEX GUNNING KC and BETH COLLETT (instructed by Macfarlanes LLP) appeared for the Developers in the BTC Core Claim (Defendants 2-12, 14 & 15).

TERENCE BERGIN KC and JACK CASTLE (instructed by Harcus Parker LLP) made brief submissions on behalf of the Claimants in the BTC Core Claim.

Hearing Dates: 5th-9th, 12th-16th, 19th-23rd, 26th-29th February, 12th-14th March 2024

- - - - - - - - - - - - - - - - - - -

APPROVED JUDGMENT

- - - - - - - - - - - - - - - - - - -

I direct that pursuant to CPR PD 39A para 6.1 no official shorthand note shall be taken of this Judgment and that copies of this version as handed down may be treated as authentic.

This judgment was handed down remotely by circulation to the parties' representatives by email. It will also be released for publication on the National Archives and other websites. The date and time for hand-down is deemed to be Monday 20th May 2024 at 10.30am.

THE HON MR JUSTICE MELLOR

MR JUSTICE MELLOR:

SUMMARY

1. Dr Craig Steven Wright ('Dr Wright') claims to be Satoshi Nakamoto i.e. he claims to be the person who adopted that pseudonym, who wrote and published the first version of the Bitcoin White Paper on 31 October 2008, who wrote and released the first version of the Bitcoin Source Code and who created the Bitcoin system. Dr Wright also claims to be a person with a unique intellect, with numerous degrees and PhDs in a wide range of subjects, the unique combination of which led him (so it is said) to devise the Bitcoin system.

2. Thus, Dr Wright presents himself as an extremely clever person. However, in my judgment, he is not nearly as clever as he thinks he is. In both his written evidence and in days of oral evidence under cross-examination, I am entirely satisfied that Dr Wright lied to the Court extensively and repeatedly. Most of his lies related to the documents he had forged which purported to support his claim. All his lies and forged documents were in support of his biggest lie: his claim to be Satoshi Nakamoto.

3. Many of Dr Wright's lies contained a grain of truth (which is sometimes said to be the mark of an accomplished liar), but there were many which did not and were outright lies. As soon as one lie was exposed, Dr Wright resorted to further lies and evasions. The final destination frequently turned out to be either Dr Wright blaming some other (often unidentified) person for his predicament or what can only be described as technobabble delivered by him in the witness box. Although as a person with expertise in IT security, Dr Wright must have thought his forgeries would provide convincing evidence to support his claim to be Satoshi or some other point of detail and would go undetected, the evidence shows, as I explain below and in the Appendix, that most of his forgeries turned out to be clumsy. Indeed, certain of Dr Wright's responses in cross-examination effectively acknowledged that point: from my recollection at least twice he indicated if he had wanted to forge a document, he would have done a much better job.

4. If Dr Wright's evidence was true, he would be a uniquely unfortunate individual, the victim of a very large number of unfortunate coincidences, all of which went against him, and/or the victim of a number of conspiracies against him.

5. The true position is far simpler. It is, however, far from simple because Dr Wright has lied so much over so many years that, on certain points, it can be difficult to pinpoint what actually happened. Those difficulties do not detract from the fact that there is a very considerable body of evidence against Dr Wright being Satoshi. To the extent that it is said there is evidence supporting his claim, it is at best questionable or of very dubious relevance or entirely circumstantial and at worst, it is fabricated and/or based on documents I am satisfied have been forged on a grand scale by Dr Wright. These fabrications and forgeries were exposed in the evidence which I received during the Trial. For that reason, this Judgment contains considerable technical and other detail which is required to expose the true scale of his mendacious campaign to prove he was/is Satoshi Nakamoto. This detail was set out in the extensive Written Closing Submissions prepared by COPA and the Developers and further points drawn out in their oral closing arguments.

6. At the same time, it is right to record that Counsel for Dr Wright put forward the best case which could possibly be presented for Dr Wright in their written and oral closing submissions, constrained as they were by the evidence I heard in this Trial.

7. However, at the conclusion of closing submissions I felt able to and did announce the result of the Identity Issue, namely whether Dr Wright is the pseudonymous Satoshi Nakamoto i.e. the person who created Bitcoin in 2009. Having considered all the evidence and submissions presented to me during the Trial, I reached the conclusion the evidence was overwhelming. At that point, I made certain declarations (because I was satisfied they are useful and are necessary to do justice between the parties), as follows:

    7.1. First, that Dr Wright is not the author of the Bitcoin White Paper.

    7.2. Second, Dr Wright is not the person who adopted or operated under the pseudonym Satoshi Nakamoto in the period between 2008 and 2011.

    7.3. Third, Dr Wright is not the person who created the Bitcoin system.

    7.4. Fourth, Dr Wright is not the author of the initial versions of the Bitcoin Software.

8. I also indicated that any further relief would be dealt with in my written Judgment (to the extent possible). I extended time for filing any appellant's notice until 21 days after the form of order hearing to be appointed following the hand down of this Judgment. I made an Order to give effect to what I stated at the conclusion of the closing argument, which contains the above declarations and directions. Finally, I stated I would give my detailed reasons in a written Judgment which would be handed down at a later date. This is that Judgment containing my detailed reasoning.

9. I should point out that the conclusion I reached and explain in this Judgment is the product of a highly iterative process. I have had regard to a very large number of pieces of evidence. Each piece had and has to be evaluated on its merits but also in the context of what other pieces of evidence appear to show. The period between the conclusion of the evidence and receipt of the lengthy Written Closing Submissions, along with my detailed consideration of the written and oral closing arguments, allowed me to reflect on the totality of the evidence. It is true that most of the evidence has concerned COPA's allegations of forgery. Ultimately, those allegations are just one factor which I took into account in reaching my overall conclusion. It was essential to step back from all the detail, to identify the various factors which supported Dr Wright's claim to be Satoshi and those which went against it.

10. Satoshi Nakamoto was and remains a pseudonym. Although this is not of any significant weight in my overall conclusion, my personal view, having heard all the evidence in this Trial, is that it is likely that a number of people contributed to the creation of Bitcoin, albeit that there may well have been one central individual. It would therefore be accurate to refer to Satoshi as he/she/they to reflect the possibilities, but unwieldy. I will therefore refer to Satoshi simply as 'he', but it is a shorthand for he/she/they.

11. Here I summarise the competing factors, starting with the factors which are alleged to support Dr Wright's claim to be Satoshi:

    11.1. His unique combination of skills, knowledge, qualifications and interests in various concepts which combined to result in the creation of Bitcoin.

    11.2. The evidence from his business associates and family which is consistent with his claim (albeit largely circumstantial).

11.3. The evidence from the 'proof' sessions in 2016.

11.4. The very substantial body of evidence comprised in Dr Wright's own witness statements.

11.5. The *content* of his Reliance Documents which he emphasised was more significant than their metadata.

12. It is relevant to point out that all of these factors are significantly affected not only by COPA's allegations of forgery but also the evidence of a large number of witnesses called by COPA who I judge to have given entirely independent and unbiased evidence.

13. As for the factors against Dr Wright being Satoshi, I divided these into two categories:

13.1. First, the attributes and behaviour which one would expect Satoshi to exhibit and prove (on the assumption that he would set out to prove he was Satoshi – on which see below), and those he would not. Under this head, the principal points are:

13.1.1. First, Satoshi would be most unlikely to have any real difficulty in proving he was Satoshi. For example, he would be able to present some insight or knowledge from the very early materials which no-one but the creator of Bitcoin would know – perhaps something hidden in the Genesis block. Or he would have been able to transfer Bitcoin out of some of the very early blocks which are generally accepted to have been mined by Satoshi, to prove that he owned those Bitcoin. He would not have lost every private key to those early blocks.

13.1.2. Second, I do not believe that Satoshi would ever have resorted to forgery in his attempt to prove he was Satoshi. He would not have backdated documents or altered the clock on his computer(s), for the simple reason that there was and is no need for him to do so. (For completeness I add that, in the very unlikely event that he did engage in some forgery, upon that being discovered, he would own up and explain why it was he had been driven to forgery. He would not have engaged in yet more forgery or engaged in technobabble in his attempts to justify it).

13.1.3. Third, the contemporaneous materials written by Satoshi, including the White Paper, the posts and his email exchanges with individuals, convey an impression of a calm, knowledgeable, collaborative, precise person with little or no arrogance, willing to acknowledge and implement ideas and suggestions from others who had shown an interest in Bitcoin.

13.1.4. Fourth, due to his collaborative and non-confrontational nature, I consider it is most unlikely that Satoshi would ever have resorted to litigation against the Developers. Satoshi would have recognised that differences in views led to the hard forks in the Bitcoin Blockchain and moved on.

13.2. Second and by contrast, the attributes and behaviours which Dr Wright has exhibited and which were proved to my satisfaction in this Trial:

13.2.1. Dr Wright is an individual with some strong views about Bitcoin and details of its implementation. However, I was struck by the fact that all of his knowledge and supposed insights could well have been obtained by careful study of the publicly available materials relating to the early years of Bitcoin. In my judgment, in none of his evidence did he reveal any insight or knowledge unique to Satoshi.

13.2.2. Furthermore, in his evidence, Dr Wright made significant errors which Satoshi would never have made, even after this length of time. Some of these relate to Satoshi's interactions with individuals not previously made public. Others relate to technical matters which Dr Wright simply got wrong but which Satoshi would not have got wrong.

13.2.3. Dr Wright has had many years to prepare to prove that he was/is Satoshi. I have concluded (in the detailed findings I make below and in the Appendix) that, as he faced greater and more significant challenges to his claim, he took his lies and forgery to ever greater levels. I explain this in much greater detail below.

13.2.4. The picture painted by Dr Wright in his evidence was, in essence, that he was solely responsible for creating Bitcoin, that he was much cleverer than anyone else, that anyone who questioned his claim or his evidence was not qualified to do so or just didn't understand what he was saying. In my judgment, the arrogance he displayed was at odds with what comes through from Satoshi's writing. In short, in his writing and attitude Dr Wright just doesn't sound or act like Satoshi.

14. Ultimately, I consider it is likely that the real Satoshi would never have set out to prove in litigation that he actually was Satoshi and certainly not in the way that Dr Wright attempted to do so.

15. I recognise that Dr Wright will disagree with my findings and this Judgment and, true to the form he displayed on numerous occasions during his oral evidence as regards the expert evidence, he may well allege that I didn't understand his technical explanations or other aspects of the technology. There are perhaps four main points to note in response:

15.1. First, to the extent that I have made errors, the Court of Appeal is well qualified (a) to detect them and (b) to correct them.

15.2. Second, the technology involved in his case is not particularly complex or difficult to understand (compared with some of the Patent cases I have dealt with). Indeed, the more complex areas of technology in this case did not concern Bitcoin or cryptography but the evidence which exposed his forgeries.

15.3. Third, if he does make such accusations, I will remain reassured that I am in good company, along with the experts who gave evidence in this case, both those instructed by COPA and those instructed by Dr Wright's team.

15.4. Fourth, this Trial was Dr Wright's opportunity to explain everything, to make his technical explanations clear to me. He had the benefit of numerous procedural indulgences regarding disclosure and additional evidence. Furthermore, on more

than one occasion during his cross-examination, I made it clear that it was important he ensured I understood the point he was trying to make. I was left with the clear impression that he simply engaged in technobabble precisely because he was not able to put forward any coherent explanation for the forgeries which had been exposed, and yet he could not bring himself to accept that he was responsible for them.

THE STRUCTURE OF THIS JUDGMENT

16. My aim has been to assemble the facts into chronological order, so far as is possible. However, I consider it is necessary to address the facts twice. In the first run through the chronology of events below, I have only set out facts which are agreed/generally accepted to be what happened i.e. the first run is designed to set out an uncontroversial framework, including various procedural events in this action.

17. In the second run through the chronology, I consider Dr Wright's account of what he claims to have done as Satoshi, both prior to and during this action. His account is conveniently divided into the following periods of time:

    17.1. His background and experience relevant to his claim to be Satoshi.

    17.2. His claimed development of the concepts which he says combined and led him to devising Bitcoin.

    17.3. The writing and publication of the Bitcoin White Paper.

    17.4. The writing and release of the first version of the Bitcoin Source Code.

    17.5. Interactions between Satoshi and others who participated or took an interest in Bitcoin, up to the time when Satoshi withdrew from the project.

    17.6. Events between the start of Bitcoin and the emergence of Dr Wright's claim to be Satoshi.

    17.7. The lead up to and the conduct of the 'proof' sessions in 2016.

    17.8. The other litigation in which Dr Wright has been involved relating to Bitcoin.

    17.9. The COPA action.

    17.10. The actions commenced by or at the instigation of Dr Wright.

18. It would have been unwieldy if I had addressed each allegation of forgery in the course of this second run, so I decided to address them separately. That does not mean I have considered them separately from all the other evidence: far from it. Although some of the alleged forgeries can be decided simply on what the expert witnesses have said the document in question presents, it is true to say that the allegations of forgery are mutually supportive as well. So I have dealt with the detail in relation to each allegedly forged document in the Appendix. I consider them according to the date or dates ascribed to them by Dr Wright in his evidence and/or by reference to dates shown in their metadata. As one might expect, there are a considerable number of documents which are said by Dr Wright to predate the publication of the Bitcoin White Paper and/or the Bitcoin Source

Code. However, there are a number of overarching arguments affecting my consideration of those documents which I deal with in the main body of this Judgment.

19. It is once I have addressed the allegations of forgery that I can return to conduct the second chronological run.

References

20. The Trial bundles were electronic on the Opus2 platform. I have included many bundle references so that the parties can identify the document and page to which reference is made. References to the Trial bundle take the form: **{Bundle / Tab / Page}**. References to witness statements and expert reports give the name and number of the statement / report e.g. **{Wright1 [48]}**. References to the transcript take the form **{DayX/page:line}**.

AN UNCONTROVERSIAL CHRONOLOGY

21. This contains the following sections:

    21.1. A short history of Satoshi's involvement in Bitcoin.

    21.2. Uncontested aspects of Dr Wright's background and activities in Australia.

    21.3. Dr Wright's activities following his move to the UK.

    21.4. The progress of this action to this Trial.

A short history of Satoshi's involvement in Bitcoin.

22. The events from 2008 down to the date of commencement of the COPA action are based on the short chronology agreed before Trial, supplemented by some uncontroversial dates drawn from various witness statements.

    22.1. By way of background, it is generally accepted that the earliest concept of digital cash was devised by an American cryptographer called David Chaum who proposed a form of token currency in the early 1980s 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 (Dr Adam Back). Hashcash used a proof-of-work algorithm, as many modern cryptocurrencies do.

    22.2. Bitcoin is based on concepts first set out in the Bitcoin White Paper, the full title of which is: "Bitcoin: A Peer-to-Peer Electronic Cash System". It was written by Satoshi Nakamoto, which is agreed to be a pseudonym.

23. The following dates concern the period when the Satoshi pseudonym was in use:

    23.1. In August 2008, Satoshi acquired the bitcoin.org domain name, which was used to establish the bitcoin.org Website.

    23.2. On 20 August 2008, Satoshi contacted Dr Back by email, referring him to a draft of the White Paper hosted on the "upload.ae" site and asking to check a reference

to his paper on Hashcash. Dr Back replied on 21 August 2008, informing Satoshi about Wei Dai's B-Money Paper. On 22 August 2008, Satoshi then wrote to Wei Dai to check the reference for that paper. 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.

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

23.4. On 31 October 2008, Satoshi released the White Paper by posting a link to it (on the bitcoin.org website). He sent an email to the "metzdowd cryptography mailing list" ("**the Metzdowd List**") (a group of individuals interested in cryptography) directing them to the link on the "bitcoin.org" site, where the document was hosted.

23.5. On 8/9 December 2008, Satoshi uploaded the White Paper to the SourceForge Bitcoin Project.

23.6. On 3/4 January 2009 (depending on time zone), Satoshi created the first block in the Bitcoin blockchain, i.e. the Genesis Block or Block 0.

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

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

23.9. On 24 March 2009, Satoshi uploaded a further version of the White Paper to the SourceForge Bitcoin Project.

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

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

24. In the very early days of the Bitcoin system, Bitcoin had negligible value.

Uncontested aspects of Dr Wright's background and activities in Australia.

25. Dr Wright was born and raised in Australia, and spent most of his life there until 2015, when he moved to the UK. He claims to have earned more than 16 Master's degrees and

two doctoral degrees, including a PhD in Computer Science and Economics from Charles Sturt University.

26. In his evidence, Dr Wright relied on much of his employment history as giving him a unique series of stepping stones towards his claimed development of Bitcoin. I discuss those aspects below. Here I relate his employment history and introduce various people who gave evidence in support of his claim.

27. In the early to mid-1990s, he worked at OzEmail (an ISP in Australia) as a corporate account manager. In 1997-1998, he held a post as IT security consultant for the Australian Stock Exchange, where he developed IT security systems.

28. From 1997 to 2003 he worked primarily through DeMorgan Information Security Systems Ltd ("**DeMorgan**"), an IT security consultancy business that he founded. In 1998, DeMorgan was engaged by Lasseter's Online Casino. 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. From 1998 to 2002, DeMorgan worked with Vodafone on IT security project work which involved implementing a firewall system. Whilst working with Vodafone, he met Rob Jenkins ("**Mr Jenkins"**).

29. 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 **{L1/334/1}**.

30. 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 {see **Wright1 [48] {E/1/10}** plus his 2007 CV at **{L2/102/1}** and his 2015 LinkedIn profile at **{L11/130/6}**. 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 (**"Mr Matthews"**), who was then CIO of CentreBet.

31. 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. From 2007 to 2008, Dr Wright was also heavily occupied with studying for a series of IT security qualifications and with writing books and papers on IT security, regulation and audit.

32. Dr Wright was made redundant from BDO in November or December 2008, with his formal employment ending in January 2009. After that redundancy, he actively put himself forward for work 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 {see **{Day6/38:12}** - **{Day6/41:19}** and **{L9/97/1}** (the blog)}. In 2009, he started the companies Information Defense Pty Ltd and Integyrs Pty Ltd. Over the following years, he founded a series of other companies. It was also from 2009 that Dr Wright found himself the subject of investigations by the Australian Tax Office ("**ATO**"), which I have to discuss in greater detail below. Around late 2010, Dr Wright's first marriage to Lynn Wright was failing, and they separated officially in January 2011.

33. The ATO investigations continued until about 2016. In some of these, Dr Wright made claims about mining large amounts of Bitcoin in the early days of the Bitcoin system, in conjunction with Dave Kleiman, who died in 2013. On 11 February 2014, Dr Wright sent an email to Louis Kleiman, Dave Kleiman's father, to tell him that Dave (along with himself) was one of the three people behind Bitcoin.

34. This email eventually led to a claim by Ira Kleiman (Dave Kleiman's brother, but acting in his capacity as the personal representative of the estate of Dave Kleiman) and W&K Info Defense Research LLC against Dr Wright brought in the United States District Court for the Southern District of Florida (*Kleiman v Wright* (Case No. 18-cv-80176-BLOOM/Reinhart)). See further below.

35. It seems that Dr Wright reconnected with Mr Matthews by meeting up on 2nd January 2014 in Sydney. This was a social occasion, but it seems to have led to Mr Matthews introducing Dr Wright to Robert MacGregor of nTrust in Canada by email on 3 February 2014. This introduction apparently led to a short conversation between Dr Wright and Mr MacGregor but nothing came of that conversation at the time.

36. Dr Wright next contacted Mr Matthews in around April 2015 by phone. In the call, Dr Wright told Mr Matthews he had a number of issues he wanted to discuss with him about his business in Australia. Mr Matthews recalls Dr Wright being quite anxious. On his next trip to Australia in April or May 2015, Mr Matthews had a lunch meeting with Dr Wright, Mr Allan Pedersen who worked for the DeMorgan Group running research programmes and Dr Stephane Savanah, an academic with a research role also in DeMorgan. Although there are aspects of what Mr Matthews says happened on that day which are controversial, it seems that Mr Pedersen and Dr Savanah were interested in persuading Mr Matthews to invest (millions) into their research into blockchain technology and Bitcoin, whereas Dr Wright remained anxious about the issues which DeMorgan were facing in terms of R&D grants which they had applied for and the related difficulties with the Australian Tax Office. Mr Matthews says that his research on the internet after the lunch was the first time he encountered the name Satoshi Nakamoto. Mr Matthews had dinner with Dr Wright later that day. Mr Matthews says he asked 'who is Satoshi Nakamoto?' to which he says Dr Wright replied 'you already know the answer to that question', whereupon Mr Matthews says he asked for a straight answer. In his witness statement here, Mr Matthews says Dr Wright replied 'you are looking at him', whereas in his evidence in *Granath*, Mr Matthews said that Dr Wright replied with 'I am'.

37. After an apparently long explanation from Dr Wright about him being Satoshi, the conversation turned to the difficulties at DeMorgan. Dr Wright explained he wanted to protect his intellectual property, continue his research but not have anything to do with running companies, something he felt he was not good at. He wanted to push his ideas into a company which could turn them into 'valuable solutions'.

38. Mr Matthews discussed the situation with Mr Ayre, a friend of his, who suggested that they introduce Dr Wright to Mr MacGregor since his company nTrust was involved in Bitcoin and blockchain technology. This resulted in Mr Matthews and Dr Wright flying to Vancouver in late May 2015, to meet with Mr Ayre and then with Mr MacGregor. The initial encounter with Mr MacGregor did not go well, but Mr Matthews persevered which resulted in he and Mr MacGregor travelling to Sydney and spending some time in the offices of DeMorgan. Again, there are aspects of Mr Matthews' evidence on this

encounter which are controversial, but the end result was that Mr MacGregor got involved in the creation and initial funding of what Mr Matthews describes as the nCrypt project.

39. A 'first version' of a 'Heads of Terms' document was signed on 29 June 2015 **{ID_004127}**. Mr Matthews says the basic idea was to transfer the IP from the DeMorgan Group to a new company within the nCrypt group (now called the nChain group), with Dr Wright as Chief Scientist continuing his research activities. Mr Matthews says this was a rushed process because DeMorgan had to pay its solicitors, Clayton Utz, substantial fees (between 1-1.2m Au$) by 30 June 2015. The payment was organised by Mr MacGregor. A second version of the 'Heads of Terms' was signed on 30 June 2015 to remove the provision in the first version that Dr Wright and his wife would have equity in the new company.

40. Mr Matthews says that part of the plan was for Dr Wright to move to the UK (along with his family) to work as nCrypt's Chief Scientist at its base in London. He and his family made trips to London in or around September/October 2015 to find schools and to look at a property in Wimbledon leased for them by one of Mr MacGregor's companies. Their belongings were packed up and shipped to the UK, with Dr Wright and his family moving into a serviced apartment in Sydney.

41. The next set of dates concern the identification of Dr Wright as potentially being Satoshi:

    41.1. In November and early December 2015, Dr Wright faced enquiries from reporters at Wired and Gizmodo magazines concerning his potentially being identified as Satoshi.

    41.2. On 8th December 2015, Wired magazine published an article in which it indicated a belief that Dr Wright was the person behind the Satoshi pseudonym and on 9th December 2015, Gizmodo magazine published a similar article.

    41.3. In mid-December 2015, Wired and Gizmodo published further articles which sought to cast doubt on whether Dr Wright was Satoshi.

42. Mr Matthews says that around the same time, the DeMorgan offices were raided by the federal police under a warrant secured by the ATO. It seems that if the police had managed to catch up with Dr Wright, they would have detained him. Mr Matthews was flying to Manila that same day and organised a ticket for Dr Wright, on the basis that the plans were already in place for Dr Wright to move to the UK. Thus, it appears that Dr Wright managed to evade the authorities in Australia and spent a couple of days in Manila before travelling onto London.

Dr Wright's activities following his move to the UK.

43. The Wired and Gizmodo publications were followed by a series of events involving Dr Wright:

    43.1. Dr Wright entered into a 'Life Story Rights and Services Agreement' with EITC Holdings Limited ("**EITC**") (the "**EITC Agreement**"), dated 17th February 2016.

43.2. In early March 2016, Dr Wright performed two private demonstrations for Mr Andrew O'Hagan ("**Mr O'Hagen**"), during which (on Dr Wright's case) he demonstrated possession of a private key to one of the original blocks (i.e. blocks 1 to 11). COPA disputes Dr Wright's case on this demonstration.

43.3. In mid-March 2016, Dr Wright held a 'private proof session' with Mr Jon Matonis ("**Mr Matonis**"). On Dr Wright's case, he demonstrated to Mr Matonis that he had access to the private keys associated with two early blocks in the Bitcoin blockchain. COPA disputes Dr Wright's case on this demonstration.

43.4. In early April 2016, Dr Wright held a 'private proof session' with Mr Gavin Andresen ("**Mr Andresen**"), during which (on Dr Wright's case) he demonstrated to Mr Andresen that he had access to the private keys associated with two early blocks in the Bitcoin blockchain. COPA disputes Dr Wright's case on this demonstration.

43.5. In late April 2016, Dr Wright had a meeting with Mr Rory Cellan-Jones ("**Mr Cellan-Jones**") of the BBC. On Dr Wright's case, he demonstrated that he was in possession of the private key associated with block 9 of the Bitcoin blockchain. COPA disputes Dr Wright's case on this demonstration.

43.6. Also in late April 2016, Dr Wright had a meeting with Mr Ludwig Siegele ("**Mr Siegele**") of The Economist. On Dr Wright's case, he demonstrated that he was in possession of the private key associated with block 9 of the Bitcoin blockchain. COPA disputes Dr Wright's case on this demonstration.

43.7. On 29 April 2016, Dr Wright was interviewed by Mr Stuart McGurk ("**Mr McGurk**"), a reporter for GQ Magazine, and Dr Nicholas Courtois ("**Dr Courtois**") of University College London.

43.8. Those demonstrations were part of the lead-up to the 'Big Reveal', as planned by Dr Wright's team (which included a PR firm). The Big Reveal involved the following happening simultaneously on 2 May 2016:

43.8.1. Dr Wright publicly asserted his identity as Satoshi;

43.8.2. Mr Andresen and Mr Matonis made blog posts stating that they had been convinced that Dr Wright was Satoshi;

43.8.3. Articles from the BBC and The Economist were made public;

43.8.4. A post was uploaded onto the blog website hosted at www.drcraigwright.net (the "**Blog Website**") entitled "*Jean-Paul Sartre, signing and significance*" (the "**Sartre Message**"). Following the posting of the Sartre Message, online commentators posted articles commenting on the significance and probative value of the Sartre Message. There is disagreement between the parties about Mr Andresen's subsequent views on whether Dr Wright is Satoshi.

43.9. On 3 May 2016, a blog post was published on the Blog Website, which referred to Dr Wright providing "*extraordinary proof*" (the "**3 May Post**").

43.10. On 4 May 2016, on Dr Wright's evidence, he self-harmed by cutting his throat with a knife, lost consciousness and was taken to hospital in an ambulance.

44. The *Kleiman* claim was commenced on 14 February 2018. The following description of the claim is taken from the Judgment of District Judge Bloom in that case dated 18th September 2020:

> *'The Complaint alleges that Defendant and David Kleiman ("David Kleiman" or "Mr. Kleiman") were former business partners that created Bitcoin under the pseudonym Satoshi Nakamoto. Between 2008 and before David Kleiman's death in April 2013, the two allegedly worked together on Bitcoin, mining bitcoins and developing blockchain related intellectual property. Starting in 2008 through February 2011, they allegedly worked together as a partnership, and from February 2011 until Mr. Kleiman's death in 2013, they conducted their work through Plaintiff W&K Info Defense Research LLC ("W&K"). During this period, significant amounts of bitcoins allegedly were mined and acquired by Defendant and Mr. Kleiman and valuable intellectual property was developed. This lawsuit concerns a dispute over the ownership of bitcoins and Bitcoin-related intellectual property.*
> *The Complaint alleges that following David Kleiman's death, Defendant perpetrated a fraudulent scheme to seize Plaintiffs' bitcoins and their rights to certain blockchain related intellectual property. This scheme included, among other things, producing fraudulent documents and forging David Kleiman's signatures on documents to purportedly show that David Kleiman transferred to Defendant bitcoins and intellectual property rights belonging to David Kleiman and W&K before David Kleiman's death. Since then, Defendant has taken sole ownership and control over the bitcoins and related intellectual property and refuses to return any bitcoins or intellectual property to either the estate or W&K. Plaintiffs seek relief against Defendant through various causes of action: …'*

45. Dr Wright was deposed several times in that case (e.g. in June 2019) and also gave evidence at trial. At this Trial, reference was made to numerous passages in the transcripts of the evidence given by Dr Wright and other witnesses.

46. The agreed chronology then moves to 2019-2021 and I have added references to other proceedings which have touched on the Identity Issue:

46.1. On 10 February 2019, Dr Wright published on Twitter images appearing to be the front page and abstract of his BlackNet paper, in which the abstract contained language similar to that in the Bitcoin White Paper. This is the BlackNet Abstract which I deal with in section 4 of the Appendix. It is COPA's case that he falsely presented it as a precursor work. Dr Wright disputes that.

46.2. On 17 April 2019, Dr Wright sued Peter McCormack for libel, the proceedings being concerned with a series of tweets published between 29 March and 29 August 2019, plus a YouTube video published on 18 October 2019 in which it was alleged that Dr Wright was not Satoshi and his claims to be Satoshi were fraudulent. Mr McCormack initially pleaded a defence of truth, but in late 2020, he abandoned that defence. So, whether Dr Wright is or is not Satoshi was not an issue which Chamberlain J. had to determine in his trial Judgment: [2022] EWHC 2058 (QB), 1 August 2022 ("*McCormack*").

46.3. On 26 June 2019, Dr Wright sued Magnus Granath in the UK for libel (QB-2019-002311) in relation to Mr Granath's Twitter account, hodlonaut, and his tweet of 17 March 2019 'The forensics to CSW's first attempt to fraudulently 'prove' he is Satoshi. Enabled by @gavinandresen. Never forget. #CraigWrightIsAFraud'.

46.4. Mr Granath brought proceedings in his native country Norway seeking negative declarations i.e. that his statements about Dr Wright were not unlawful, Granath v Wright, (19-076844TVI-TOSL/04) ("*Granath"*). The trial was heard in October 2022 by Judge Engebrigtsen. In her written Judgment dated 20 October 2022, seen in translation, Judge Engebrigsten ruled in favour of Mr Granath and ordered Dr Wright to pay costs. Several of the witnesses who gave evidence in this Trial also gave evidence in Norway and reference was made to various passages in the transcripts of their evidence in Norway in October 2022.

46.5. On 21 August 2019, Dr Wright uploaded to the SSRN website a version of the Bitcoin White Paper, with details indicating that he was the author. It is COPA's case that he falsely presented this version as written in August 2008. Dr Wright disputes that case.

46.6. On 13 February 2020, Dr Wright published a blog entitled "*Forking and Passing Off*" in which he asserted his claim to be "the sole creator of Bitcoin" and evinced an intention to enforce claimed intellectual property rights as such.

46.7. On 19 February 2021, SCA Ontier LLP ("**Ontier"**), the solicitors then acting for Dr Wright, wrote to Bird & Bird LLP (the solicitors for COPA) indicating that Dr Wright did not consent to COPA or its members using the Bitcoin White Paper and asking that both COPA and its members remove the Bitcoin White Paper from their respective websites and social media accounts.

THIS ACTION

47. For reasons which will become apparent later, it is necessary to rehearse some of the procedural history of this action.

48. COPA commenced this action on 9th April 2021. In their original Particulars of Claim, COPA pleaded their case that Dr Wright was not Satoshi by reference to publicly available events and documents, including (1) the Sartre Message, (2) the BlackNet Abstract, (3) the '12 March 2008 email' and (4) the SSRN Submission, each of which COPA alleged to be forged. In addition, at that stage, COPA relied on various findings made in the *Kleiman* litigation (which were not relied on at Trial given the rule in *Hollington v Hewthorn*, cited below), plus one other matter derived from the *Kleiman* litigation which was alleged to go to Dr Wright's credibility: an allegation that an email purportedly from Dave Kleiman to Uyen Nguyen dated 20 December 2012 had been forged by Dr Wright. Obviously, at that stage, COPA did not know what other documents Dr Wright would rely upon as supporting his claim to be Satoshi.

49. Dr Wright pleaded a full Defence in which he asserted in some detail his positive case that he was Satoshi and provided his explanations of the matters relied upon by COPA. With the benefit of hindsight, his Defence is notable for referring largely to documents which were made public by Satoshi. Bearing in mind the number of documents Dr

Wright later disclosed as supporting his claim to be Satoshi, it is notable that the Defence did not make reference to any of them.

50. Dr Wright did not file any Counterclaim. Following service of COPA's Reply on 19th July 2021, Dr Wright issued an application seeking to strike out parts of the (by then) Amended Particulars of Claim which was heard by HHJ Paul Matthews in December 2021. He ruled that 'forgery was in issue' on the four particular documents pleaded by COPA. His Order gave permission for COPA to add a second matter derived from the Kleiman litigation: that a Deed of Trust document proffered by Dr Wright in the Kleiman case as evidencing the existence of a trust called the Tulip Trust had been backdated. At that point the case involved six allegedly forged documents.

51. The costs and case management conference was heard by Master Clark on 1st & 2nd September 2022. Her Order (sealed on 4th October 2022) set out directions down to the trial, which was subsequently listed to commence in January 2024. Of relevance are the following features of her Order:

    51.1. The Master considered and approved the Disclosure Review Document, the purpose of which was to define the scope of disclosure to be given and the searches which were to be carried out to locate relevant documents.

    51.2. The parties were ordered to give extended disclosure by 31st January 2023. In the event, extended disclosure took place on 7th March 2023. Both Dr Wright and COPA have given further disclosure at various points subsequently, a point to which I return later. It is also relevant to note that a full discovery exercise had already taken place for the *Kleiman* proceedings, and it involved Alix & Partners undertaking a comprehensive search at Dr Wright's home for any computers, hard drives etc which were to be (and were) imaged and searched for relevant documents.

    51.3. On 28th February 2023, Dr Wright was to file 'a list of documents upon which he primarily relies in relation to the factual issue of whether or not he is the author of the Bitcoin White Paper. Such list will not preclude the Defendant from relying upon other documents in support of his case and may be updated from time to time to include further documents or to exclude documents.' This list became known as Dr Wright's '**Primary Reliance Documents**'. Due to the slippage in the timetable, the list was produced on 4 April 2023, originally containing 100 documents, but updated subsequently in the light of some further disclosure Dr Wright gave to 107.

    51.4. On or before 28th March 2023, COPA was given the power to request '**Chain of Custody**' information for any of Dr Wright's Primary Reliance Documents, with the requested information to be supplied 4 weeks later. Following service of Dr Wright's list of his Primary Reliance Documents, COPA requested Chain of Custody information for all of them.

    51.5. On or before 31st March 2023, COPA was to serve a list of any disclosed documents the authenticity of which was denied or not admitted (the '**Challenged Documents**'). In the event, the list of Challenged Documents was served on 5 May 2023, (again later revised in the light of the further disclosure given by Dr Wright) which made clear that COPA was challenging authenticity in respect of

(almost) all of Dr Wright's Reliance Documents, as well as a large number of other documents in Dr Wright's disclosure.

51.6. The following procedural steps were for exchange of witness statements on 2nd June 2023, which in fact took place on 28 July 2023, followed by sequential exchange of expert evidence on forensic document analysis, with COPA's expert originally set to serve his report on 30th June 2023, Dr Wright's expert evidence on 25th August 2023 and a reply from COPA's expert on 22nd September 2023. There was also provision for expert evidence relating to relevant aspects of digital currency technology.

51.7. A point of some significance was a further direction, made by the Master at the explicit request of Dr Wright's then Counsel, for evidence of fact in reply *after* all the expert evidence had been filed. In other words, Dr Wright requested and obtained the ability to serve his evidence in reply in response to the expert evidence.

51.8. Although all the specific dates originally directed were extended, the basic sequence of the service of evidence was retained.

Case management of the docketed actions

52. In January 2023, four actions were docketed to me:

52.1. The first was the COPA action.

52.2. The second and third actions (the *Coinbase* and *Kraken* Actions) were issued on the same day by Dr Wright and associated companies against two sets of defendants which have been referred to as the Coinbase and Kraken Defendants respectively. In each of those actions, the claim is for passing off by reference to the term Bitcoin. The claimants claim to own goodwill in the term Bitcoin, underpinned by what are alleged to be important and defining characteristics including those designated in the Particulars of Claim as the 'Bitcoin Characteristics'. The cause of action in passing off is said to be sufficient to prevent third parties (including the Coinbase and Kraken Defendants) from using the term Bitcoin in relation to digital assets with tickers BTC and BCH.

52.3. The fourth action was IL-2022-000069 between Dr Wright (and two companies) and 26 Defendants (*Wright v BTC Core*), which I refer to as 'the BTC Core action'. In this action, Dr Wright claims to be the owner of certain database rights which he says subsist in three databases, namely (i) the Bitcoin Blockchain, (ii) the Bitcoin Blockchain as it stood on 1 August 2017 at 14.11 – up to and including block 478,558 and (iii) another part of the Bitcoin Blockchain made in a particular period (the details of which do not matter for present purposes). Dr Wright also says he (or one of the Claimants) owns the copyrights which subsist in the Bitcoin White Paper and in the Bitcoin File Format. The Defendants to the BTC Core claim include COPA, various other corporate entities which are members of COPA (and for that reason have not themselves played a role in this Trial) and the Developers.

53. After these cases were docketed to me, the first applications I had to deal with were at a Joint CMC listed in the Coinbase and Kraken Actions on 25th & 26th May 2023. One of the applications was by the Coinbase and Kraken Defendants seeking a stay of each of those actions pending Judgment in the COPA Action. This was a logical application for these Defendants to make since (a) whether Dr Wright was Satoshi would be determined in the COPA action and (b) they were members of COPA.

54. However, it did not seem to me to be satisfactory to make directions in those two actions without consideration of the other two. Hence, I directed a further Joint CMC, this time in all four actions, which took place on 15th June 2023. The same point occurred to Dr Wright's team very shortly before the hearing – they wrote to Dr Wright's opponents in all four actions suggesting that, since the identity issue arose in all four actions, it should be tried by way of preliminary issue. As a result, at that hearing there was considerable debate as to what should be ordered to be tried by way of preliminary issue. In the result, I ordered that the trial set in the COPA Action should be a Joint Trial of (a) the COPA Action and (b) a preliminary issue in the BTC Core Claim of the Identity Issue, namely whether Dr Wright is the pseudonymous 'Satoshi Nakamoto', i.e. the person who created Bitcoin in 2009. On agreeing to be bound by the result of that Joint Trial, the Coinbase and Kraken Defendants agreed to a stay of their actions. I also reset the timetable to trial in the COPA Action.

55. At that point, the BTC Core claim had not advanced very far, so the active defendants to that claim – the Developers – had a lot of work to do to catch up with the progress which had been made in the COPA Action. I ordered the provision to the Developers of the disclosure in the COPA Action, but further directions as to the involvement of the Developers in the Joint Trial were reserved to a later date.

56. Subsequently the action brought by Tulip Trading Ltd against the Bitcoin Association for BSV (a Swiss Verein) and fifteen individuals (being or including the Developers), BL-2021-000313, was also docketed to me.

Service of Madden1, and further applications.

57. The report of COPA's forensic documents expert, Mr Madden, was served on 1st September 2023. This was a very extensive report: with appendices it amounts to some 970 pages, but it turned out to be the first of six reports Mr Madden served in these proceedings.

58. Meanwhile, on 8 September 2023, Dr Wright served his expert evidence on Autism Spectrum Disorder ("**ASD**"), from Professor Fazel.

59. At a further CMC in mid-September 2023, I heard a number of applications, including for Dr Wright to answer a consolidated Request for Further Information relating to his Defence (the RFI having been served in June) and his application to adduce expert evidence on ASD. This resulted in my Judgment ([2023] EWHC 2408 (Ch)) and Order dated 3 October 2023 in which I set revised directions to trial. I ordered Dr Wright to answer many of the requests, and he did so in two statements: Wright2 (concerning the signing sessions); and Wright4 (concerning remaining matters), served on 23 October 2023. Pursuant to COPA's application, I also ordered Dr Wright to provide further information as to the chain of custody of his Reliance Documents.

Dr Wright's Chain of Custody information

60. In their third letter of 9 June 2023, Ontier set out the list of 107 Primary Reliance Documents. The first set of Chain of Custody information was set out in an Annex to the letter dated 8 July 2023 from Dr Wright's new solicitors, Travers Smith LLP.

61. By letter dated 13 October 2023, Dr Wright's third set of solicitors, Shoosmiths LLP (then recently instructed), wrote enclosing a second set of Chain of Custody information in a detailed spreadsheet, pursuant to paragraph 3 of my Order of 3rd October 2023. This is a document of some significance. Some entries are confusing and internally inconsistent, but the overall effect was to suggest that most of his Reliance Documents had been used or accessed by others after being produced, such that they could have been altered. It repeatedly indicated that more reliably authentic versions of Reliance Documents might be available on the "new drives". In his statement of 23 October 2023 answering the RFI requests (**Wright4**), Dr Wright also provided a schedule {CSW5 at **{F/148/2}}** addressing versions of the White Paper in disclosure in which he told a similar story of those documents being unreliable.

Further Disclosure and the Mock Trial

62. On 25 September 2023, Dr Wright's solicitors wrote to say he had further disclosure to give. It subsequently emerged that Dr Wright claimed to have discovered in mid-September 2023 two hard drives which were not previously imaged and which supposedly contained more reliable versions of documents supporting his claim.

63. At this point I introduce nChain, a UK company with which Dr Wright had been closely associated (latterly as a consultant) since 2015. The financial muscle behind nChain is said to be Mr Calvin Ayre ("**Mr Ayre**"), a Canadian billionaire, who has supported Dr Wright's claim to be Satoshi. Until late September 2023, the CEO of nChain was Mr Christen Ager-Hanssen ("**Mr Ager-Hanssen**").

64. Although the details only emerged subsequently, it turned out that, following service of Madden1, nChain had arranged for Dr Wright to undergo a mock trial exercise on 22 September 2023 in which he was cross-examined by a criminal barrister, Zafar Ali KC, on a number of his primary reliance documents. A mock judgment, apparently given by a judge who had been drafted in to help, was delivered on 24 September 2023, finding Dr Wright's Satoshi claim to be false. The day after the mock trial, Mr Ayre sent Dr Wright an email (which Mr Ager-Hanssen posted on X) making clear that Mr Ayre now believed that Dr Wright had forged documents and should confess to having done so {see the 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}**}. The mock trial exercise was revealed by Mr Ager-Hanssen, and it has since been admitted by Dr Wright, Mr Matthews and Mr Ali, albeit in differing terms {see Wright3 **{E/3/1}** and Matthews2 **{E/27/1}**. For Mr Ali's account, see Clyde & Co letter at **{M1/1/707}**}.

65. On 29 September 2023, Mr Ager-Hanssen began a series of postings on X 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*" **{P2/111/44}**. Mr Ager-

Hanssen added that he was "*convinced that Dr Craig Wright is NOT Satoshi".* 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.

66. 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 **{L20/195/1}**.

67. Following those revelations, I understand that Mr Ager-Hanssen was dismissed and left the UK. I was told that interim injunctive relief was obtained to prevent further disclosure of allegedly confidential information. He has not played any role in this Trial. Thus, he has not had any opportunity to respond to various serious allegations made against him by Dr Wright. Furthermore, COPA were anxious to stress that they have had nothing to do with Mr Ager-Hanssen, contrary to various conspiracy theories espoused by Dr Wright during his cross-examination.

The October application to plead further forgeries.

68. A further hearing took place before me on 12 October 2023, where the principal application was COPA's application to make an unspecified but large number of additional allegations of forgery. The application was based on the analysis in Madden1 as to documents he considered to be inauthentic. I heard that heavily contested application on 12th October 2023 and handed down my Judgment on the application on 24th October 2023: see [2023] EWHC 2642 (Ch). Dr Wright's team estimated that COPA were seeking to add around 400 additional allegations of forgery, based on the proposed amendments, or at least 180 based on a schedule exhibited by Mr Sherrell to his witness statement supporting the application.

69. For the reasons set out in that Judgment, I gave COPA permission to plead forgery of a total of 50 additional documents in a pleading to be served within 7 days of that Judgment, along with a schedule identifying by ID number both (a) the Reliance Documents and (b) other documents which they alleged to be forged along with all reasons relied upon in support of the allegation of forgery, cross-referenced to Madden1, and the reasons why Dr Wright was alleged to be responsible.

70. My resulting Order dated 31 October gave COPA permission to plead additional allegations of forgery against Dr Wright (as I said, limited to 50) and some further directions. All of these allegations originated from COPA's challenges to authenticity of documents disclosed by Dr Wright (i.e. the list of Challenged Documents served on 5 May 2023) but Madden1 enabled COPA to plead forgery.

71. At that stage, the principal outstanding procedural steps were service of the expert report on forensic document analysis from Dr Wright's side on 23 October 2023 and service of Dr Wright's reply fact evidence on 1st December 2023. In an attempt to reduce the burden on Dr Wright and his team in view of the impending trial date, I took the view that Dr Wright's response to the new allegations of forgery did not need to be made in a responsive pleading, but could be set out in his witness statement in reply.

Developments in the expert evidence

72. On 23 October 2023, Dr Wright's side served the first report of Dr Simon Placks on forensic document analysis. On the same day the parties exchanged expert evidence on digital currency technology (Professor Meiklejohn for COPA and Mr ZeMing Gao for Dr Wright).

73. COPA served their reply expert report (**Madden2**) on forensic document analysis on 17 November 2023. As Master Clark had directed, meetings between the respective experts took place and very helpful Joint Statements were produced, indicating what they agreed upon and where they disagreed.

74. COPA served its expert evidence on ASD on 21 November 2023 and on 30 November 2023 the ASD experts produced a helpful agreed Joint Statement.

75. On 8 December 2023, the Joint Statement from Mr Madden and Dr Placks was served. It addressed 47 of Dr Wright's Reliance Documents. The experts concluded that 32 had had their metadata manipulated to record non-contemporaneous date/time values or are unreliable on other bases. At that stage, there was disagreement between the experts as to the remaining 15 of the 47. All 28 of the Reliance Documents in COPA's list of 50 forgeries were agreed to be manipulated or unreliable. 17 of the Reliance Documents referred to in Dr Wright's witness statement were agreed to have been manipulated or to be unreliable. In addition, the experts agreed that one of the sets of MYOB data purporting to show entries in 2009-2011 disclosed by Dr Wright was created in 2020, with the other set of MYOB data (provided to Dr Placks by Dr Wright as a reaction to the problems with the earlier data) created in 2023 and then backdated. The significance of at least some of the MYOB data was that they purported to support Dr Wright's purchase of the domain name at which the Bitcoin White Paper was first published.

76. Meanwhile, however, 1st December 2023 had passed without service of any reply witness statement from Dr Wright. The reasons for this emerged at the PTR, heard on 15th December 2023, and are explained in my PTR Judgment, handed down on 20th December: see [2023] EWHC 3287 (Ch).

The Pre-Trial Review, the 'Additional Documents' & the application to adjourn

77. At the PTR, Dr Wright applied to rely on the 'Additional Documents' and to adjourn the Joint Trial, which was then due to commence on 15th January 2024 with one day of opening submissions followed by 4 days of my pre-reading before commencing the evidence the following week.

78. In their submissions at the PTR, Dr Wright's Counsel placed great emphasis on the importance of the '**Additional Documents**'. For present purposes I can deal with two categories of the Additional Documents:

    78.1. First, Dr Wright had identified 97 documents which were a selection of documents taken from two USB drives which Dr Wright said he had discovered in a drawer at his house on 15 September 2023. One of the drives, termed the Samsung USB drive, was said to contain an image of a drive which Dr Wright had used when he worked at BDO from 2004-end 2008 – the BDO Drive. This image was said to be a snapshot dating from 31st October 2007. The significance

of that date was clear – if the image did date from 31st October 2007, then 95 of the 97 documents pre-dated either the publication of the Bitcoin White Paper or the release of the Bitcoin Source Code.

78.2. The second category of documents were certain LaTeX documents stored by Dr Wright in an online Overleaf account.

79. The evidence in support of the application was a witness statement of Ms Hannah Field ("**Ms Field**"), the partner in charge of Dr Wright's case at his (then relatively newly instructed) solicitors, Shoosmiths LLP, but in his sixth witness statement, Dr Wright confirmed the content of her witness statement as true. In relation to the two categories of Additional Documents, her evidence was as follows:

79.1. Ms Field reported that Dr Wright had told her that he had not edited or amended any documents in the BDO Drive since 31st October 2007. She continued: '*If that is correct, then the 95 documents are at least very strong evidence that Dr Wright is Satoshi Nakamoto, as is clear from their nature and contents*.' She set out in Schedule 1 to her statement an explanation of the relevance of these documents based on information provided by Dr Wright which '*proceeds on the basis that the documents in the BDO Image were not modified since 31 October 2007'*. She made one qualification: she referred to a Stroz Friedberg ('**SF**') memorandum and related, as in Wright5, that there were a number of data points identified by SF which required further investigation. Dr Wright accepted these points would need to be analysed by the parties' forensic experts when considering the provenance of the hard drives.

79.2. As regards the LaTeX documents, Ms Field related two key pieces of evidence from Dr Wright. In summary, these were that:

79.2.1. The relevant LaTeX files were said to be unique, such that (so it was said) mere possession of them is evidence of authorship of the White Paper.

79.2.2. It is practically infeasible to reverse engineer the LaTeX Code from the published Bitcoin White Paper (for two reasons which she set out).

79.2.3. And she concluded:

'34. The White Paper LaTeX Files are therefore of the highest possible importance for the trial of the Identity Issue, and that issue cannot fairly be determined unless Dr Wright is entitled to rely on these documents and have his case on the significance of these documents addressed in expert evidence.'

80. Notwithstanding the serious criticisms made by COPA in their correspondence and evidence served for the PTR **{Sherrell18 and Madden3}**, I was persuaded to admit the Additional Documents. On the evidence of Ms Field and Dr Wright, I could not see how a fair trial of the Identity Issue could take place without those documents being considered.

81. The other part of Dr Wright's application was to adjourn the trial to come back in April 2024. Enquiries revealed that it could not come back in April 2024 and a full

adjournment would be likely to lead to the Joint Trial being delayed by about a year. In those circumstances, I investigated the possibility of delaying the start of the trial to enable analysis of and evidence relating to the Additional Documents to be prepared and filed, and for Dr Wright's reply evidence to be completed. In the result, I ordered the commencement of the Joint Trial to be delayed until 5th February 2024, with my pre-reading in the preceding week. This put pressure on both sides in terms of the additional preparation required, but my expectation that they could be ready for that delayed trial date proved to be correct, and I am very grateful for all the hard work which was done to enable the Joint Trial to go ahead.

82. In view of the Additional Documents, I considered it right, in my PTR Judgment, to limit COPA's existing allegations of forgery to the 20 documents listed in the Schedule appended to Bird & Bird's Third Letter of 14 December 2023. I proposed that COPA should be permitted to add a maximum of 20 further allegations of forgery relating to the Additional Documents. These were pleaded in the Claimant's Schedule of Further Forgeries dated 23 January 2024. As I shall relate, there was a yet further Schedule served by the Claimants on 28 February 2024 of Dr Wright's Forgery during Trial.

83. In my PTR Order, I also ordered Dr Wright to provide Mr Madden with a forensic image of the Samsung Drive, containing a forensic image of the BDO Drive. The content of these forensic images turned out to be important.

84. Following the PTR, the parties exchanged reply evidence. They served further reports from experts in forensic documents examination and LaTeX software **{Madden4 {G/6/1}** and **Rosendahl1 {G/7/1}** for COPA; **Lynch1 {I/5/1}** and **Placks2 {I/6/1}** for Dr Wright}. The experts produced Joint Statements, reaching near complete agreement.

85. On Day 1 of trial (5 February 2024), I permitted Dr Wright to rely upon a number of further additional documents which had been referenced in and/or deployed with Wright11. As a result, and with the permission of the Court, COPA served a further report from Mr Madden – **Madden5**.

86. During trial, COPA also served a second report of Prof. Meiklejohn 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. These were admitted into evidence by agreement.

87. On 29 February 2024, COPA served on Dr Wright the further Schedule of Forgery During Trial as well as **Madden6** dealing with the forged MYOB Ontier Email. 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.

88. The final point to make regarding the procedural history is that no complaint was made that any of the parties were not ready to start the Trial on the adjourned date of 5 February 2024.

89. To the extent that Dr Wright might be tempted to complain about the somewhat unusual procedural history of this claim and the compression of the timetable as the start of Trial approached, it may be noted that both those attributes were very largely his responsibility, both in terms of his late and very late disclosure and (in line with my findings in the Appendix) the very extensive scale of his forgery.

Disclosure

90. I mentioned that both sides produced additional disclosure at various points. On COPA's side, it is my understanding that the further (mostly voluntary) disclosure made by COPA concerned documents provided by various witnesses, of which prompt disclosure was made, together with various documents obtained from the internet. Some of those documents prove to be significant in the analysis which follows, but no complaint was or is made about the timing or content of the additional disclosure from COPA.

91. The same is not true of the additional disclosure made by Dr Wright. I think it is helpful to set out how disclosure by Dr Wright proceeded, based on a table annexed by the Developers to their Written Closing Submissions.

Date	**Name/ Volume Number**	**Number of Documents (where appropriate)**	**Summary of Contents**
7 March 2023	VOL001	4,090	Disclosure pursuant to Order of Master Clark
25 March 2023	VOL002	423	Additional documents ordered by Master Clark {B/8/3}
12 July 2023	VOL003	13	Various documents disclosed in response to Birds & Bird's questions.
28 July 2023	VOL004	16	Evidence referred to in witness statements.
11 August 2023	VOL005	3	Full versions of documents which had previously been disclosed.
14 September 2023	VOL006	92	Macfarlanes' specific disclosure requests (Gavin emails and other Kleiman docs)
27 September 2023	VOL007	8	Kleiman exhibits, Australian tax returns from 2008/2009 and bank statements.
25 October 2023	VOL008	93	The 93 new documents following the hard drive "discovery" which Dr Wright sought to rely on.
27 October 2023	VOL009	180	Further hard drive documents
27 October 2023	VOL010	3	Documents referred to in Ben Ford's statement
1 November 2023	VOL011	579	Public documents answering Bird & Bird's disclosure requests
8 November 2023	VOL012	393	Further hard drive documents
17 November 2023	VOL013	5	Bird & Bird's specific disclosure requests: 3 forensic reports and two documents related to liberty reserve
21 November 2023	VOL014	20	Documents which should have previously been disclosed but were missed in error.
28 November 2023	VOL015	352	Further hard drive documents.
28 November 2023	VOL016	10	Documents concerning dispute with ATO which were initially missed.
7 December 2023	VOL017	2	DEFAUS_01746855 (fear of the future/good senator email)
20 December 2023	Overleaf	146	Initial Overleaf disclosure
21 December 2023	VOL018	3	Documents responding to RFI (Mark Archbold/Ignatius Pang emails)
8 January 2024	Overleaf	17	Outputs
12 January 2024	VOL019	64	CSW11 documents
17 January 2024	VOL020	2 image drives	BDO Drive Images
28 January 2024	VOL021	69	CSW11 documents
29 January 2024	VOL022	12	Papa Neema documents

Date	Name/ Volume Number	Number of Documents (where appropriate)	Summary of Contents
2 February 2024	VOL023	4	Corrected documents referred to in Cerian Jones' Witness Statement
16 February 2024	Overleaf	402	Further Overleaf disclosure
22 February 2024	VOL024	47	Hard copy documents
26 February 2024	Ontier	5	Ontier Version/Ramona Version etc

92. Of these 28 tranches of disclosure, it is striking how many were given after service of **Madden1** on 1st September 2023 and how many were provided very close to and even during the Trial. It is also relevant to note that the originally stipulated set of search terms were not used when searches were made of the 2 image drives or the Overleaf documents. Furthermore, all of COPA's requests for forensic images were simply ignored (at least until my Order at the PTR, requiring the provision of a forensic image of the BDO Drive), even though Mr Madden had made it perfectly clear that forensic images would have proved useful, and no reason was given why they could not have been supplied.

93. VOL024 comprised 47 hard copy documents 'lying around the house' found during Dr Wright's cross-examination. I was told by COPA these are mostly manuscript documents and 'do not advance Dr Wright's case'. Certainly, Dr Wright did not attempt to rely on any of them and there was no application in respect of them.

THE IDENTITY ISSUE

94. The Identity Issue was and remains simple and Dr Wright's case is simple: it is that he was the creator of Bitcoin, the author of the Bitcoin White Paper and the Bitcoin Source Code and the person who adopted and operated under the pseudonym Satoshi Nakamoto. However, what he has relied upon in his attempts to prove that case has changed and morphed on a regular basis, following the service of evidence (often expert evidence) from COPA and the Developers and further tranches of disclosure from him.

95. Prior to Trial, with one exception (where Dr Wright accepted that ID_003455 was inauthentic), I did not understand Dr Wright to have abandoned his Primary Reliance Documents, even though the emphasis might have appeared to shift to the various newly disclosed documents. So, his case underwent a process of accretion.

96. The case of COPA and the Developers is equally simple and the opposite of Dr Wright's case. Thus, the Identity Issue is essentially a binary issue. It was only ever a theoretical possibility that I would find neither side had proved their case.

97. It will be seen that in the evidence I was presented with various expressions of opinion as to whether Dr Wright was (or was not) Satoshi Nakamoto and doubts on that subject. However, I must decide the Identity Issue based on the evidence which was led in this Trial and I should not and do not delegate the decision to any witness or third party. With one exception, it is fair to say that I have given these opinions very little or no weight, depending on the reasons given for holding the opinion. It is universally the case that none of the witnesses have had access to the wide range of information and evidence which has been presented to me in this Trial. The exception is concerned with an expression of opinion which conflicts with the witness' evidence in a signed witness statement – this concerns Mr Stefan Matthews.

98. Before I embark on my detailed findings, some preliminary topics must be addressed. I start with the useful reminders I was given about the applicable legal principles. Then I must set out my general views of each of the witnesses – I address the key disputes in context later.

Applicable Legal Principles

99. In their Opening Submissions, the parties addressed the legal principles which they contended were applicable to this Joint Trial. I divide them into two categories. First, there are the principles I should apply which affect my approach to the evidence and my conclusions from the evidence. I deal with these in this section of the Judgment under a series of headings. The second category concerns the relief I should grant and I address these later. In Closing Submissions, Lord Grabiner KC drew my attention to certain important principles which concern the making of findings of forgery, which were already familiar from my October Judgment.

100. As for my approach to deciding the Identity Issue itself, although there were differences in content and emphasis, I did not detect there to be any real dispute as to the applicable principles. What follows is my distillation of the parties' very helpful combined submissions. I have endeavoured to apply all these principles.

Burden and Standard of Proof

101. The general rule is that the legal burden lies upon the party who substantially asserts the affirmative of the relevant issue: *Phipson On Evidence* 19th Ed, at [6-06]. However, in deciding which party substantially asserts the affirmative, regard must be had to the substance of the issue and not merely to its grammatical form. It is also said that 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.

102. The true meaning of the general rule, therefore, is that 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. Another way to approach the same question is to posit the striking out of the particular allegation and ask which party's case would fail as a result (the legal burden being borne by that party).

103. The Joint Trial is the main trial of COPA's claim for, *inter alia*, a declaration that Dr Wright is not the author of the Bitcoin White Paper. An essential (and necessary) part of that claim is COPA's allegation that Dr Wright is indeed not the author of the Bitcoin White Paper/ Satoshi Nakamoto. Put another way, COPA's claim for that declaration would fail if its allegations as to Dr Wright's identity were struck out. It follows that COPA bears the legal burden of proving those allegations (which includes the legal burden of proving its forgery allegations).

104. It is common ground that COPA bears the burden of proving its entitlement, as a matter of law, to the declaratory (and other) relief it seeks.

105. However, the Joint Trial is also the preliminary issue trial of the Identity Issue in the BTC Core Claim. Dr Wright is in that case asserting his identity as Satoshi Nakamoto as an essential part of his claim for injunctions and a declaration. Dr Wright therefore accepts that he bears the legal burden in respect of the Identity Issue in the BTC Core Claim.

106. The result of this procedural arrangement is that (1) in the COPA Claim, in order to obtain the relief it seeks, COPA must prove, on the balance of probabilities, that Dr Wright is not Satoshi Nakamoto; but (2) in order to succeed in due course in the BTC Core Claim (and in the other cases where the parties are bound by the result of this Trial), Dr Wright must have proved in this Joint Trial that he is, on the balance of probabilities, Satoshi Nakamoto.

107. 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.

108. The standard of proof applying to all factual issues in civil proceedings is the balance of probabilities. It applies equally to allegations which amount to criminal conduct: see *Phipson on Evidence (20th ed.)* at §6-57. It is not a flexible or sliding standard. In applying the standard, a Court may where appropriate take account of the inherent probability of particularly serious allegations: see *Re H (Minors)* [1996] AC 563 at 586. However, there is no necessary connection between the seriousness of an allegation and its inherent probability, as Lord Hoffmann explained in *Re B (Children)* [2009] 1 AC 11 at §15:

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

109. 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."*

110. 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

111. 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."*

112. I was also reminded of the principles I summarised and applied back in October 2023, when allowing COPA to plead an additional 50 allegations of forgery: see [2023] EWHC 2642 (Ch) at [39]-[49].

113. In Dr Wright's closing submissions, it was stressed on his behalf that:

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

114. 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

115. 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.

116. I was naturally referred to the well-known observations of Leggatt J in *Gestmin SGPS SA v Credit Suisse (UK) Ltd* [2013] EWHC 3560 (Comm) (reported at [2020] 1 CLC 428) at [15]-[22] which have been cited in many cases and which I need not repeat. Leggatt J. concluded as follows:

> *'22. In the light of these considerations, the best approach for a judge to adopt in the trial of a commercial case is, in my view, to place little if any reliance at all on witnesses' recollections of what was said in meetings and conversations, and to base factual findings on inferences drawn from the documentary evidence and known or probable facts. This does not mean that oral testimony serves no useful purpose – though its utility is often disproportionate to its length. But its value lies largely, as I see it, in the opportunity which cross-examination affords to subject the documentary record to critical scrutiny and to gauge the personality, motivations and working practices of a witness, rather than in testimony of what the witness recalls of particular conversations and events. Above all, it is important to avoid the fallacy of supposing that, because a witness has confidence in his or her recollection and is honest, evidence based on that recollection provides any reliable guide to the truth.'*

117. In the circumstances of this case, it is important to point out that the Court must be satisfied that the purportedly contemporaneous documents are *reliable*. If any of the purportedly contemporaneous documents are alleged to be forged, these allegations add an extra layer of complexity to the assessment of the evidence.

118. I also found some recent observations of Rajah J. helpful from his Judgment in *South Tees Development Corporation v PD Teesport Ltd* [2024] EWHC 214 (Ch), a case where the numerous witnesses were recollecting/trying to recollect, against an incomplete documentary record, uses of various rights of way dating back to the 1970s and 1980s. In the context of setting out [15]-[20] of *Gestmin,* Rajah J observed:

> *'23. … Memory plays tricks on people. It is perfectly possible for an honest witness to have a firm memory of events which they believe to be true, but which in fact is not correct.*
>
> *…*
>
> *30. Although Leggatt J's words have been sometimes taken as an encouragement to place no reliance on witness recollection, particularly when there is an abundance of reliable contemporaneous documentation, the Court of Appeal has confirmed that the assessment of the credibility of a witness' evidence should be a part of a single compendious exercise of finding the facts based on all of the available evidence; see* Kogan v Martin *[2019] EWCA Civ 1645 and* Natwest Markets Plc, Mercuria Energy Europe Trading v Bilta (UK) Ltd (In Liquidation) *[2021] EWCA Civ 680 at paragraphs 50 and 51.*

> *31. Each witness's evidence has to be weighed in the context of the reliably established facts (including those which can safely be distilled from contemporaneous documentation bearing in mind that the documentation itself may be unreliable or incomplete), the motives and biases in play, the possible unreliability or corruption of human memory and the inherent probabilities. Where there is reliable contemporaneous documentation, it will be natural to place weight on that. Where documents add little to the analysis, other secure footholds in the evidence need, if possible, to be found to decide whether it is more likely than not that the witness' memory is reliable or mistaken.'*

Points on Expert Evidence

119. 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.

120. As COPA submitted, 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.

The Preparation of Expert Evidence

121. In Dr Wright's written Closing, my attention was drawn to the following legal principles regarding the preparation of expert evidence:

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

> ***"2.1** Expert evidence should be the independent product of the expert uninfluenced by the pressures of litigation.*

> ***2.2*** *Experts should assist the court by providing objective, unbiased opinions on matters within their expertise, and should not assume the role of an advocate."*

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

121.3. If an expert's report is found not to be compliant with the principles of independence or impartiality, there are a wide variety of sanctions available to the court. Typically, the court will either refuse to admit the evidence of the expert, or, more frequently, the matter will be taken into account when considering the weight to attach to that expert's evidence. {*Expert Evidence: Law and Practice*, 9-013; *Phipson on Evidence*, 33-78}.

122. Since expert evidence is usually the main and sometimes the only evidence in Patent trials, I was already very familiar with these principles. Whether they were observed in this case is a topic to which I return below.

Drawing of Inferences (including from absence of witnesses)

123. 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

124. 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

125. 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

126. 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 on Evidence* 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.

127. In this case, Dr Wright relies on numerous documents said to be or to have been contemporaneous to support his claim to be Satoshi. However, the contemporaneous documents on which Dr Wright relies are themselves said by COPA and the Developers to be suspect. In many cases, more than merely suspect: I have heard a significant amount of evidence directed to allegations that all of the most important documents on which Dr Wright relies are forgeries. For case management reasons, at earlier stages in this litigation I limited the number of forgery allegations which COPA were allowed to level against Dr Wright and his documents. However, those limits do not prevent COPA from alleging additional documents are inauthentic or unreliable.

128. It is clear that Dr Wright has a well-developed ability to persuade people of his technical acumen, when they do not fully understand what he is talking about. In other words, he can talk a good story. His ability should not come as a surprise because he has been working for over a decade to establish himself as Satoshi Nakamoto. However, when his story is exposed to detailed forensic analysis, as occurred during this trial, it is found to

be riddled with inconsistencies, but, most importantly, to be founded on a whole series of documents which I find to have been either forged or to be unreliable. The detail of my findings is set out below.

The expert evidence on Autism Spectrum Disorder.

129. At (and before) the Trial it was common ground that Dr Wright suffers from Autism Spectrum Disorder, which covers a very wide spectrum. On 8 September 2023, Dr Wright served a report from Professor Seena Fazel which suggested that some radical adjustments were required (including receipt of all questions in advance) if Dr Wright was to give evidence. Professor Fazel had formed his view based on interviews with Dr Wright but without being told that Dr Wright had given evidence and been cross-examined before. In particular, Professor Fazel was not given access to any of the videos (e.g. from the *Granath* proceedings in Norway) showing him being cross-examined without apparently any problem at all. After I had given permission to rely on that report, COPA served their report from Professor Michael Craig on 21 November 2023, who had seen the videos. The experts met and agreed a very useful Joint Statement which recommended only limited adjustments. Their agreement was the basis for the Order I made at the PTR, as follows:

> *'Pursuant to CPR PD1A, the Court shall adopt for the evidence of Dr Wright at trial the adjustments agreed upon by the parties experts in ASD, namely (a) there being clear timetabling of Dr Wright's evidence; (b) him being given access to a pen and paper; (c) him being given access to a real time transcription screen; (d) there being a lower threshold for breaks in evidence, particularly if he becomes emotionally dysregulated; and (e) follow-up questions being relatively shorter in the event of Dr Wright becoming emotionally dysregulated.'*

THE EVIDENCE OF FACT

Dr Wright's witnesses of fact

130. Here I introduce and make certain overall findings about the witnesses relied upon by Dr Wright, all of whom were cross-examined. I have to discuss the evidence given by Dr Wright, Stefan Matthews and Robert Jenkins in greater detail, later, since COPA challenge their honesty.

Dr Wright

131. Dr Wright made 15 witness statements:

    131.1. **Wright1 {E/1/1}** providing his principal evidence in chief.

    131.2. **Wright2 {E/2/1}** addressing RFI requests about the signing sessions.

    131.3. **Wright3 {E/3/1}** giving his version of the mock cross-examination (in response to an Order).

    131.4. **Wright4 {E/4/1}** addressing the remaining RFI requests.

    131.5. **Wright5 {E/20/1}** explaining why the two new hard drives were not previously included in his disclosure.

131.6. **Wright6 {E/21/1}** confirming the facts and statements in Ms Field's first statement (in support of the application to adjourn the trial and to admit the Additional Documents).

131.7. **Wright7 {E/22/1}** addressing the tweets for Mr Ager-Hanssen about the new documents being fake.

131.8. **Wright8 {E/23/1}** relating to his computer environment, which was part of his explanation for signs of inauthenticity in his documents.

131.9. **Wright9 {E/26/1}** responding to Prof Meiklejohn's report (with an appendix attempting to explain some signs of inauthenticity).

131.10. **Wright10 {E/31/1}** providing more assertions about his computing environments.

131.11. **Wright11 {CSW/1/1},** which was supposed to give his final reply evidence. This was an extremely long statement, comprising 1476 paragraphs over 246 pages. It was served on 12 January 2024, along with an application notice by which Shoosmiths sought permission to sign a modified certificate of compliance with PD57AC, which entailed inserting 'To the best of my ability…' in two places relating to compliance with PD57AC and PD32, [18.1] & [18.2] and with the Statement of Best Practice. On the first day of trial, I refused Shoosmiths' application, for reasons in the ruling I gave at the start of the second day of trial. As COPA observed, this application was effectively a concession that PD57AC had not been complied with. COPA then served a lengthy Schedule of Objections on 16 January 2024, to **Wright11** and its Appendices, citing 7 types of objection to large swathes of these materials. As part of my pre-reading I spent many hours reading **Wright11** and the objections, many of which appeared to be well-founded. Fortunately I was relieved of the task of ruling on those objections, being told on the first day of trial that the parties had reached a compromise on **Wright11**, agreeing passages which were to be redacted. In due course, a redacted copy of **Wright11** was put into the trial bundle. Later, Dr Wright wanted an unredacted copy to be available, although I am not at all sure that any of the passages agreed to be redacted were referred to.

131.12. **Wright12 {CSW/7/1}** which further addresses the BDO Drive.

131.13. **Wright13 {E/32/1}**, served after COPA's opening Skeleton Argument had been written, in support of his application to rely on further documents.

131.14. **Wright14 {E/33/1}** providing chain of custody information for the White Paper LaTeX files.

131.15. **Wright15 {E/34/1}** concerning the MYOB Ontier email.

132. At Trial, Dr Wright was called for cross-examination in three separate sessions, being sworn on the first occasion and re-sworn on the second and third occasions:

132.1. The first session occupied Days 2-8 of the Trial (6th-9th & 12th-14th February).

132.2. The second occupied Day 15 (23 February 2024).

132.3. The third was a relatively short session on Day 19 (1 March 2024).

133. During these sessions, we generally took a break after an hour of cross-examination, although on occasion, the period extended by 20-30 minutes or so to the conclusion of the morning or afternoon session. Particularly bearing in mind we were in an extremely hot courtroom for the first week of the trial, Dr Wright showed impressive stamina throughout. His wife was in court throughout to advise on whether he was showing signs of dysregulation. During his cross-examination on Day 15, Dr Wright appeared to me on occasion to be speaking more loudly than previously, but that may have been on account of the adjustment of the amplification system in Court on that day. However, at no point did there seem to be any sign of dysregulation, nor was any warning to that effect given by his wife or legal team. So, in my view, the set of agreed adjustments were adhered to and proved effective.

134. Lord Grabiner KC did intervene numerous times during Dr Wright's cross-examination to warn Mr Hough KC about trespassing on matters which were privileged, interventions which also warned Dr Wright. In my judgment, Mr Hough was well aware when his question *might* encroach on privilege and frequently told Dr Wright that he did not want him to go into privileged matters. These warnings did not seem to deter Dr Wright. On numerous occasions he sought to blame an aspect of a forgery allegation on his previous lawyers. As the Trial progressed, Bird & Bird asserted in correspondence that privilege had been waived by Dr Wright over a number of matters, but in the result, COPA did not require me to decide their allegations of waiver. Nonetheless, Dr Wright's own legal team evidently concluded that privilege had been waived over certain matters and further disclosure and information was provided as a result, which I discuss below.

135. In some of his interventions, Lord Grabiner KC made reference to the fact that Dr Wright was a vulnerable witness. However, I did not get any impression that his ASD prevented Dr Wright from understanding the concept of privilege or that his discussions with his lawyers were privileged, and no point was made in submissions to that effect. In fact, COPA submitted that Dr Wright used privilege as a refuge – referring to something involving his lawyers (at the relevant time) as a way of closing off a particular enquiry. This was, as COPA submitted, an abuse of privilege but one which demonstrated that Dr Wright understood exactly what he was doing.

136. When giving his evidence orally, it seemed to me that Dr Wright was extremely well-prepared. My assessment is that he suffered from no disability in giving his evidence due to his ASD (Dr Wright himself made occasional reference to being an 'Aspie' i.e. a reference to Asperger's syndrome). COPA had a large number of allegations of forgery and inauthenticity to put to him and many of those involved considerable detail. He seemed to be well on top of all the detail. He gave crisp answers when asked whether he saw what appeared on the face of a document ('I do') and, in the vast majority of cases, when it came to the key point, he gave answers which indicated he had already considered the point and prepared for it.

137. Dr Wright proved to be an extremely slippery witness. In many answers he included some slight qualification. He rarely gave a complete answer and this was deliberate – he was giving himself an 'out' for later. On occasion he was extremely pedantic. Initially I was inclined to give him some leeway due to his ASD, but his pedantry was not consistent. He was pedantic when it suited him and not when it didn't.

138. I address most of Dr Wright's evidence in connection with the alleged forgeries in the Appendix. However, in their written Closing, COPA drew my attention to three specific topics (which are not directly related to any of the allegations of forgery) on which they submit that Dr Wright was lying. I address these here, along with two other more general allegations.

The Tyche emails

139. Dr Wright denied the authenticity of emails from him at the email address cwright@tyche.co.uk. His account can be seen from the following exchange **{{Day7/109:9} - {Day7/110:3}}**. From that point, every time he was taken to a Tyche email he denied it was from him}:

> *'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.'*

140. Thus, 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. As COPA submitted, it even includes his characteristic mistake of spelling Dr Back's name as "Black".

141. However, there are a number of apparently authentic documents which evidence that he did work for Tyche:

    141.1. First, there is a Tyche Consulting Contract bearing Dr Wright's signature **{L10/426/1}**. When this was put to him he could only claim that his signature had been forged **{Day8/5:22)} - {Day8/7:7}**, but did not identify who might have done it or why.

    141.2. Second, his employment with the company was recorded in the Implementation Deed of January 2016 **{L11/285/10}** 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 **{Day8/6:15} - {Day8/16:10}**.

    141.3. Third, 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 {see the email at **{L10/385/1}**}.

141.4. Mr Matthews confirmed that Dr Wright had indeed been employed by Tyche Consulting Ltd and that this employment was crucial for the visa **{{Day11/144:19} - {Day11/145:24}**}, and provided independent details about the arrangements as explained in more detail below.

141.5. Fourth, 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) **{L11/329/1**}, although this document was not put to him in cross-examination.

142. In total, Dr Wright disclosed around 20 emails from 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 **{K/2/25}**.

143. In my judgment, the evidence shows that Dr Wright was lying when he said none of the emails sent from cwright@tyche.co.uk were sent by him.

NAB Credit Card.

144. 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 **{H/78/1}**. COPA maintains that the screenshots are forgeries, and I deal with that in section 27 in the Appendix. This point concerns how Dr Wright described the card 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 {**{Day2/30:10} - {Day2/31:11}**}.

145. 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.

146. His evidence is undermined by the contemporaneous documents:

146.1. First, he had disclosed an NAB statement for a "NAB Low Rate Visa" card **{L7/390/1}**, 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.

146.2. 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, even though, as can be seen on the face of the document, payments were also being made.

146.3. Second, Dr Wright was then confronted with another document from his disclosure; a receipt from a garden centre **{L5/70/38}** 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}**.

147. The evidence establishes, in my judgment, that Dr Wright was lying when he said (a) this card was not a credit card and (b) that it had been cancelled in 2005 or that it was not to be used after 2005.

The nCrypt Emails

148. These 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 {see e.g. **{L13/67/1}**, **{L13/78/1}** and **{L13/123/1}**}. 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 as a Primary Reliance Document which he now says he did not send.

149. 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.

150. There are two significant problems with Dr Wright's account:

150.1. First, it is 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.

150.2. Second, his account does not make sense on its own terms. 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.

151. This was put to Dr Wright, and he gave the following incoherent explanation {the full exchange is at **{Day8/23:1} - {Day8/26:25}**:

> *'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.*
> *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.*

152. 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. I agree with COPA that the notion is absurd. Again, I am satisfied that Dr Wright was lying about these nCrypt emails.

The use of Aspose

153. On 23 February 2024, as I mentioned, Dr Wright was re-sworn for a further day of cross-examination in relation to matters which had only just been revealed prior to his first spell in the witness box. Once again, I was left with a clear impression that Dr Wright was not a witness of truth. He lied repeatedly throughout the day. I discuss these further below, but, by way of example, I mention the cross-examination on his use of Aspose to create files in LaTeX. It is clear that on the Aspose files, he sensed that he was trapped and had no answer. It was at that point he reverted to blaming Mr Ager-Hanssen for, it would seem, creating files in LaTeX using Aspose.

The Papa Neema emails

154. In **Wright11, [269-297]**, Dr Wright set out an elaborate story which included him having received emails from Denis Mayaka on 10 and 29 September 2023. Mr Mayaka was a company formation agent who was involved in Dr Wright's acquisition of Tulip Trading Limited as a company incorporated in the Seychelles. Dr Wright claimed that Mr Mayaka had used, not his professional email address, but a Gmail one: papa.neema@gmail.com. Dr Wright said that, on 10 September 2023, "Papa Neema" sent files said to be tied to Dr Wright's companies in 2009 to 2012 **{CSW/25/1}**. These included alleged invoices from Abacus Seychelles and a version of the "Timecoin" paper (which I address in the next section). He also said that "Papa Neema" separately sent photographs of a computer monitor with images of the invoices on them.

155. There are a series of indications that these emails were sent by Dr Wright to himself, as further detailed in **Madden5**, from [87] onwards **{G/9/29}**.

    155.1. 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 +0300). Faced with that inconvenient fact, Dr Wright claimed that Mr Mayaka set his computer clock to London time

because he worked with British clients. I agree with COPA that was an obvious lie: it makes no sense for someone to do that **{Day15/49:23} - {Day15/50:17}**.

155.2. Secondly, there are a series of dubious features to the Timecoin document supposedly sent by Papa Neema, 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.

155.3. Thirdly, there were further suspicious features associated with the Abacus invoices, including the fact that four documents created on different dates across two years (with different templates) had file titles with the same spelling mistake ("Invoive" for "Invoice").

155.4. 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.

156. I am well aware that COPA did not include the Papa Neema emails in their supplemental Schedules of Dr Wright's forgeries, although Mr Sherrell's Twentieth Witness Statement set out in detail COPA's reasons for alleging they were. COPA faced a constantly moving target of forged documents produced by Dr Wright which continued up to the start of trial and, indeed, during it. COPA made their position very clear and Dr Wright was given every opportunity to rebut their allegations. Accordingly, I do not consider that I am disqualified from making findings on these emails and their contents.

157. For all the reasons set out in **Madden5** in his analysis of the Papa Neema emails, I find they were not genuine and were sent by Dr Wright to himself.

The Timecoin paper attached to one of the Papa Neema emails

158. By way of background, 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},** supposedly dating from 2008. In section 24 of the Appendix, I have found that document to be forged by Dr Wright.

159. 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".

160. One feature of Dr Wright's account concerning the Papa Neema emails was that 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 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).

161. This was remarkable for a number of reasons. First, no reason was ever identified as to why Mr Mayaka (a company formation agent) would have had 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 discovery of the Samsung Drive on 15 September 2023 (which, as Mr Madden found, contained a hash-identical document). Dr Wright had no good explanation for that coincidence {**{Day15/57:16}** and following}.

162. In **Wright11 [289]**, 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 (a bank), Centrebet and Hoyts. In a direct contradiction of his evidence in **Wright4**, 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. Mr Jenkins 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. I must return to these points in more detail below when I consider a key aspect of Mr Jenkins' evidence.

163. 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 {**Madden5 [104-126] {G/9/34}** and following}. 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 features (including Tripwire) are then bolted on to tie the document to Dr Wright's areas of expertise {see the cross-examination at **{Day15/63:16} - {Day15/91:8}**}. I agree that it bears all the signs of a forgery prepared in haste to suggest Dr Wright was developing the Bitcoin project in early 2009.

My conclusion on Dr Wright's general credibility

164. It is sometimes said that a good lie contains a kernel of truth. In my judgment, on many and frequent occasions, Dr Wright adhered to this proposition. I sensed there was often something in his answer which was true, but the answer as a whole was a plain lie or not an answer to the question put. There are several consequences from his use of this tactic. First, it would either be impossible to pin down every lie and/or it would take weeks to do so. Second, Dr Wright would simply invent further lies in his attempts to cover up existing lies.

165. I have reminded myself that just because a witness lies on one point, it does not mean that s/he is lying on other points. However, on the basis of all the evidence, I am unable to place any reliance on what Dr Wright has said unless it is self-evidently correct or is corroborated by some other piece of evidence on which I consider I can place reliance.

Mr Stefan Matthews

166. Although Mr Matthews was the last of Dr Wright's fact witnesses to be called, he was the next most significant fact witness after Dr Wright, for two main reasons. First, because he said Dr Wright gave him a copy of a draft Bitcoin White Paper in August 2008. Second, because he was closely involved in the events which occurred from 2014-2016, including the planned sessions to prove that Dr Wright was Satoshi. I discuss both these topics in much greater detail below. Mr Matthews was a cagey witness at times. I can accept much of his evidence with a few notable exceptions which I discuss below.

167. COPA submitted that Mr Matthews gave dishonest evidence that (i) he knew of Dr Wright's work on developing Bitcoin in 2008; (ii) that he received a draft of the Bitcoin White Paper from Dr Wright in August 2008; (iii) that Dr Wright offered him Bitcoin in exchange for money in early 2009; and (iv) that Dr Wright pitched a blockchain-based project to him in early 2009. In addition, COPA submitted that 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. COPA relied on several points.

168. First, in his WhatsApp exchange with Mr Ager-Hanssen on 25 September 2023 **{L20/183/1}**, Mr Matthews 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.*" This is a message which ordinarily would not have come to light. Under cross-examination, he attempted (without success) to deny the plain meaning of these words **{Day11/73:15} - {Day11/79:15}**. He also attempted to explain the message by saying that it was intended to divert Mr Ager-Hanssen, who was threatening to "*destroy*" him **{Day11/79:16} - {Day11/83:23}**. I found this an odd allegation, so I raised the point (at the end of his evidence, see **{Day12/100:1}**) that the balance of power lay with Mr Matthews, who in the event was able to fire Mr Ager-Hanssen and have him injuncted. In my judgment, the plain meaning of Mr Matthews' WhatsApp message is clear from the words he used. This has an impact on other aspects of his evidence which I consider below. Further, I do not accept his evidence that he was just trying to humour or fob off Mr Ager-Hanssen.

169. Second, COPA submit that Mr Matthews' account of receiving the Bitcoin White Paper from Dr Wright was in any event not plausible. They point out it is not supported by any documentary evidence, or evidence from any other witnesses. This account did not emerge until after 2015, when doing so served Mr Matthews' financial interests. Furthermore, 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}**.

170. The second point I raised with Mr Matthews at the conclusion of his evidence is how he dated his receipt of the White Paper to August 2008 and whether he had any anchor points for that date. He responded by saying 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*" **{Day12/97:16} - {Day12/98:11}.** I found this utterly unconvincing.

171. Third, 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 **{L8/340/2}.** In that email, he put Dr Wright forward as a potential partner for a business venture concerned with cryptocurrencies but did not mention his supposed best and singular qualification as the actual creator of the original cryptocurrency. The following exchange {at **{Day11/118/4} - {Day11/118/16}}** highlighted how ridiculous that would have been:

> *'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.'*

172. Overall, I am satisfied that Mr Matthews did not receive a copy of the Bitcoin White Paper in 2008 and his evidence about receiving a copy of it before it was made public was made up. Mr Matthews' WhatsApp message tends to confirm that this evidence was false.

173. 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. As I discuss in greater detail below, in relation to the events of 2015-16, Mr Matthews' evidence was far more consistent than Dr Wright's with the contemporaneous documents. COPA drew my attention to a number of significant differences between Mr Matthews' evidence and Dr Wright's. I agree that 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

174. Mr Robert Jenkins **{E/6/1-9}** made a single witness statement at {E/6/1-9} dated 28 July 2023, in which he set out in 37 paragraphs a fairly detailed account of their relationship over many years from their first meeting in 1998/1999, when Dr Wright worked on security measures for Vodafone in Australia, until around 2010/2011. He says that he discussed concepts of electronic ledgers involving linked blocks of data which in hindsight he relates to the Bitcoin blockchain.

175. His witness statement includes a section dealing with the time he was employed at the Commonwealth Bank of Australia (CBA) from late 2002 until January 2008 and he said:

> *'During the time I was at CBA, which was from October 2022 [sc.2002] until January 2008, Craig and I talked about a whole range of things over that five or six year period: we had a common interest around some stuff that in hindsight related to*

Blockchain and Bitcoin (I first heard the word Blockchain in late 2008, after I left CBA; I don't remember precisely when I first heard the word Bitcoin, but it was later than that).'

176. In the following six paragraphs, it is clear that Mr Jenkins had taken care to mention any aspect of their discussions which might possibly relate to Bitcoin. The next section of his witness statement, which is concerned with his next period of employment at BT, follows the same pattern, in which Mr Jenkins mentioned discussions with Dr Wright of a 'white paper', distributed computing, mining and bitcoin.

177. At the conclusion of his (first) cross-examination, the evidence Mr Jenkins had given was not controversial: 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 {**{Day9/91:24}** and following}.

178. However, Mr Jenkins' re-examination revealed that he had been prepared to answer questions in a certain way, but had not been given 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 was asked: 'Did he show you anything?' He answered, after looking down at notes in front of him, as follows:

'96:19 Did he show you anything?
20 A. I do. I do remember seeing a couple of things, besides
21 what Craig drew on the napkin. At a -- at a subsequent
22 meeting, I was shown a paper. It didn't make mention of
23 Bitcoin but it did make mention of -- of something
24 called Timecoin, and that was something that -- as
25 a White Paper that he -- he showed me at that time.
97: 1 Q. You said a bit later. When was that?
2 A. It would have been in that time window I was saying. It
3 was before I joined Westpac and -- and after those
4 series of lunches where he drew on the -- on the napkin.
5 So, around, again, 2009/2010.'

179. The re-examination continued a few lines further down in the transcript:

'Q. I'm going to show you a document and I want to ask you
17 if you recognise the document. Could you be shown -- or
18 could we look at {CSW/31/1}. That's a Timecoin paper,
19 "A peer-to-peer electronic cash system", with
20 Craig Wright's name at the top of it. Do you recognise
21 that document?
22 A. As far as I can recollect that far back, because this
23 isn't something that was discussed in the -- in
24 the Granath court case, but, yes, it does look certainly

25 similar to the document I saw, yes.'

180. Since that evidence had not featured in Mr Jenkins' statement or in his testimony in the *Granath* proceedings, I permitted further cross-examination. COPA submit that Mr Jenkins' new evidence then unravelled. He admitted that he had referred to a note when giving the evidence I quoted in [178], 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 just 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 {**{Day9/99:16} - {Day9/105:13}**}.

181. Thus, within the space of about a minute, Mr Jenkins contradicted himself about whether the word "Timecoin" was a note written before his evidence. COPA submitted that 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.

182. Before I make any findings about Mr Jenkins and this aspect of his evidence, there are some prior issues I have to address which concern **{ID_006565}** and Dr Wright's evidence about that document. So I return to this issue later.

183. Dr Wright produced in his disclosure a number of "Timecoin" White Papers. One of them, **{ID_000254}**, was one of COPA's pleaded forgeries which I have found, in section 24 of the Appendix, to have been forged by Dr Wright.

184. The document Mr Jenkins was shown in re-examination was **{ID_006565}**, 'TimeDoc 2.pdf'. This was one of three documents attached to **{ID_006564}**, which is one of the Papa Neema emails to which I have referred above. Mr Madden identified **{ID_006565}** as hash identical to a file within the zip file of similar name. As he said, the email had attached to it both the pdf file itself and an encrypted zip of the same pdf. I have already touched on **{ID_006565}** above when considering Dr Wright's credibility but I must consider it in more detail in order to make findings about Mr Jenkins' evidence.

185. As the ID number indicates, it was one of the last documents disclosed by Dr Wright. It was one of the set of documents referred to in **Wright11** which had not previously been disclosed and which were the subject of the application on Day 1 of the Trial for permission to rely upon them.

186. The chain of custody information **{M3/16/3}** shows only that the document was sent by email from Craig Wright to Shoosmiths on 25 January 2024. Shoosmiths' letter dated 9 February 2024 refers to the difficulty in giving further chain of custody information since Dr Wright was in the witness box.

187. In **Madden5**, Mr Madden was unable to undertake a full analysis of this document. He concluded at [126] that the document should be considered as 'unreliable' without further supporting evidence. He also said:

> *'It may be possible to come to a more concluded view if I was provided access to the computing systems used to author and store this document and the emails associated with it.'*

188. The document is dated to 9 April 2009 (i.e. after the publication of the 2008 and 2009 versions of the Bitcoin White Paper) and has several of the metadata property fields populated, whereas the control copy of the Bitcoin White Paper did not. The title is 'TimeChain – Logging System Built on Bitcoin to Extend and Deliver Blacknet'.

189. It has 5 diagrams which appear identical to those in the Bitcoin White Paper. They are embedded as picture items and not as vector diagrams. Mr Madden also found the pictures to be of low resolution and pixelated compared with the equivalents in **{ID_000865}** (a control copy of the Bitcoin White Paper).

190. Although there are differences in the text between **{ID_006565}** and **{ID_000254}** there remains significant similarity. As with **{ID_000254}**, it is clear that there is such a degree of similarity with the text of the Bitcoin White Paper that the only possible conclusion is that {ID_006565} was derived from the Bitcoin White Paper.

191. Indeed, that was Dr Wright's evidence in **Wright11** at **[289]**:

> *'The TimeDoc 2 pdf is a document I created after I had founded Information Defence Pty Ltd ("IDPL") in January 2009. It has similarities to the Bitcoin White Paper because it is an extended version of the time stamping service included in bitcoin that I was using commercially. It deals with my plan to exploit the technology underlying Bitcoin for other purposes. My recollection is that I sent it or a similar document to Qantas Staff Credit Union (now QDOS Bank), David Bridges, Rob Jenkins, Stefan Matthews at Centrebet, Hoyts, and a number of other people. I believe that these individuals would recognise this document. I had not sent the original bitcoin White Paper to either David Bridges or Rob Jenkins. However, I would likely have sent the commercialised version to each of them.' (my emphasis).*

192. One curiosity is that although **{ID_006565}** includes a few references, there is no reference to the Bitcoin White Paper, from which it has clearly been very substantially derived.

193. The bulk of Mr Madden's 'Summary' on **{ID_006565}** reads as follows:

> *'120. Other than the visual observations I make above, I do not comment on or consider the content of the document of as this is outside of my expertise, though I have seen the comments made in the Twentieth Witness Statement of Philip Nathan Sherrell.*
> *121. While I have found no anachronistic metadata characteristics within this document itself in the time available to me, I have made several observations that bring it into contrast with the Bitcoin White Paper control copy {ID_000865}. This is to say that the document has been assembled in a different manner to {ID_000865} and does not appear to have been produced from the OpenOffice document used to create {ID_000865} (and it also does not appear to come from {ID_000254}, a document which I understand is said to be related).*
> *122. The same OpenOffice document could not have been used without undergoing significant changes to the formatting and style of the document as well as its content,*

and the diagrams have been replaced with relatively low-quality static pictures instead of flowchart-style graphic drawings.
123. I also note that the OpenOffice software version 3.0 that was used to author {ID_006565} is still available for download today from Internet resources, and it would have been possible to create a document identical to ID_006565 by downloading and running that software on a computer (or virtual computer) with a backdated clock. The manner in which the email message to which the document was attached has been disclosed is less than ideal and does not allow me a full picture for forensic analysis.
124. The copy of the ZIP file that was created on the Samsung drive has been attributed with timestamps of 31 October 2017, a date I have attributed with significant backdating behaviour on the Samsung drive {G/6/13}.'

194. I regret to say I found Mr Jenkins' evidence about having seen a Timecoin paper deeply unconvincing. If he really had been shown a Timecoin paper at any point in the period 2007-2009, I am sure that Dr Wright would have told his lawyers and Mr Jenkins would have been certain to have mentioned it in his witness statement. Furthermore, I found the way in which this potentially important piece of evidence was elicited in re-examination was also deeply unconvincing. If it was known about in advance (as appears to have been the case), it should have been included in a supplementary witness statement or, at the very least, elicited in examination in chief. Instead, it seems to have been left as a bomb to go off in cross-examination, except the cross-examiner did not trigger the bomb, so it had to be dealt with in re-examination.

195. It is also revealing that the first time Dr Wright made his claim to have shown Mr Jenkins a copy of the "Timecoin" paper was only in **Wright11 at [289] {CSW/1/53**, 12 January 2024}.

196. In the circumstances, I agree that the natural inference to be drawn from this sequence of events is that Mr Jenkins had been primed by Dr Wright to bring up a "Timecoin" White Paper, something he had not mentioned in his witness statement in these proceedings nor in his *Granath* testimony.

197. In these circumstances, I make the following findings: (a) Mr Jenkins was prepared by Dr Wright 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. Furthermore, in view of my finding in section 24 of the Appendix that the Timecoin ODT Whitepaper was forged by Dr Wright and the evidence summarised above, I am compelled to find that **{ID_006565}**, 'TimeDoc 2.pdf' was also forged by Dr Wright. In relation to finding (a) above, I wish to make clear that I do not believe Dr Wright's legal team had anything to do with this, particularly in view of their exemplary conduct of his difficult case.

198. 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.

199. 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 or fed to Mr Jenkins to justify why he had no documents to back up his assertions.

200. Overall, in my judgment 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 remaining witnesses of fact

201. All the remaining witnesses of fact called by Dr Wright gave their opinion that Dr Wright was Satoshi, with varying degrees of support. They divide into three broad categories: family members (Max Lynam and Danielle DeMorgan), people who worked for Dr Wright (Dr Pang and Shoaib Yousuf) and people who encountered Dr Wright in a variety of work environments (Mark Archbold, Dr Jones and David Bridges).

202. Ms Danielle DeMorgan **{E/8/1}** – Ms DeMorgan is Dr Wright's youngest sister. She gave evidence that Dr Wright was interested in Japanese culture and sometimes used nicknames for himself. Her evidence was to the effect that, when she was 16, she and some of her school friends encountered in the local park someone dressed in black as a ninja with a Samurai sword, and this person turned out to be her brother, Craig Wright.

203. 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. Nothing in her evidence gave any credence to Dr Wright's claim to be Satoshi, and she did not support his assertion that he shared a pre-release copy of the Bitcoin White Paper with her. Ms DeMorgan was plainly an honest witness but her evidence was of no probative value.

204. Mr Max Lynam **{E/13/1}** – Mr Max Lynam is Dr Wright's cousin. He gave evidence that he and his father ran some computer code for Dr Wright at their farm in Australia at some time in or after 2009, and that Dr Wright later (in 2013) told them that it had been mining Bitcoin.

205. I should make it clear that I assessed Mr Max Lynam's evidence in conjunction with the CEA evidence from his father, Mr Don Lynam, summarised below.

206. COPA submitted that Max Lynam's evidence gave no support to Dr Wright's claim. They pointed out that the communications he actually had with Dr Wright in 2008 which are in disclosure say nothing about a digital currency project or anything like it **{{Day11/25:14} - {Day11/27:24}}**. Mr Lynam agreed that the only work or projects about which those communications spoke concerned IT security and digital forensics **{Day11/27:24}**. 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 (i.e. IT security work, which is quite different from the Bitcoin system) **{Day11/28:11} - {Day11/33:3}**.

207. In my judgment, the notion that Max Lynam and his father were heavily involved in mining Bitcoin from the very start does not ring true. If Dr Wright, as Satoshi, had involved these relatively close family members in that activity then, in my judgment:

    207.1. First, it is likely that Satoshi would have shared the secret with them yet asked them to maintain the secret that Dr Wright was Satoshi. Yet Mr Max Lynam said that there was no secrecy surrounding the running of this code. Further, prior to 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 **{{Day11/37:19} - {Day11/38:4}}**.

    207.2. Second, and more importantly, Satoshi would have shared at least some of the fruits of the mining with them. There are two aspects to this:

        207.2.1. First, I consider it is inconceivable that Satoshi would not have told them, before they threw away the computing equipment which they used, at least at some point (not necessarily right at the beginning) that they were 'mining' and that, again at some point, they were generating Bitcoin and their Bitcoin were gradually increasing in value.

        207.2.2. Second, in the very unlikely event that Satoshi had not told them that they were 'mining' prior to the disposal of the computing equipment (and the hard drives, on which the resulting Bitcoin were stored) then, in my view, on learning of the disposal of their equipment and their loss of their Bitcoin, Satoshi would have transferred a reasonable number of Bitcoin to them. After all, Satoshi is supposed to possess over a million Bitcoin.

    207.3. In my view, it is inconceivable that Satoshi had them mining for some considerable time but did not transfer any Bitcoin to them for their efforts.

    207.4. In making these findings, I have not lost sight of the fact that Bitcoin in the early days had negligible value. However, Dr Wright placed a 'nominal' value of $50 per Bitcoin in his dealings with the ATO, so the notion that Bitcoin could be ascribed some value would not have been lost on him.

    207.5. I have also not lost sight of the fact that Dr Wright sought to justify never telling the Lynams to save their bitcoin on the basis that it was never about value at the time **{Day6:142:11}**. This is not something which Satoshi would have said: even in February 2009, he clearly envisaged the value of Bitcoin would increase and would be important {see his post at **{L4/489/5}** plus his earlier email to Dustin Trammell on 16 January 2009 at **{L4/335}**}.

208. It is also telling that Mr Lynam had no knowledge of documents Dr Wright later produced which suggested that he and his family had a stake in Bitcoin mined at an early stage {see **{Day11/42:20} - {Day11/45:11}**}.

209. Overall, I formed two related conclusions: first, that Mr Max Lynam's evidence provided no support for Dr Wright's case; and second, that Mr Max Lynam for the most part, tried to tell the truth. One possible exception is the paragraph in his witness statement which I quote at [630]. Due to the fact that Dr Wright's lies have been so extensive, I am unable to reach a conclusion as to whether he did mention the topics mentioned in that paragraph. There are reasons to doubt that he did, but it is unnecessary for me to reach a concluded view.

210. Dr Ignatius Pang **{E/10/1}** – Dr Pang has known Dr Wright since 2007 and he recounted doing some analysis with Dr Wright on social network predatory behaviour. He claimed 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 sometime 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 **{Day9/25:11}; {Day9/28:10}; {Day9/32:5}** and following; **{Day9/37:2}** and following}.

211. COPA submitted that the account of the Lego conversation is so strange and implausible that it cannot be right, and that 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).

212. Dr Pang's account that Dr Wright went around the BDO office asking whether they knew someone with a Japanese name which he now thinks was probably Satoshi Nakamoto, is intriguing for two reasons:

    212.1. First, the timing suggests that Dr Wright had seen the first version of the Bitcoin White Paper soon after its publication.

    212.2. Second, it seems to me to be inconsistent with Dr Wright being Satoshi. The incident seems to me to be far more consistent with Dr Wright finding, reading and being intrigued by the Bitcoin White Paper, and then asking whether anyone had heard of the author.

213. Finally, in closing, Counsel for Dr Wright placed emphasis on the fact that Dr Pang was not challenged on his evidence relating to Dr Wright's improvement to the '*Diffie-Hellman equation*' which he says he was shown when Dr Wright was still at BDO. The submission was that this is 'relevant to Bitcoin'. That is not what Dr Pang said. He said when he saw the paper, he did not know how the revised equation could be applied. Only later in 2014-15, when he worked as casual staff at Hotwire, '*supporting the writing of blockchain related patents and/or white papers',* and came across the paper again, did he understand that *'it is to do with hierarchical key encryption and has very important applications in how to structure ownership of data and how things can be structured hierarchically in data storage, which is very important in any computer security setting, including Bitcoin*.' The high level of generality in his link to Bitcoin is also confirmed by the fact that the Bitcoin system never used ECDH or Diffie-Hellman at all, but ECDSA on secp256k1 (see [315] below).

214. Overall, in my judgment, Dr Pang's evidence provided no support for Dr Wright's claim to be Satoshi. At best, his evidence shows that Dr Wright took an early interest in the Bitcoin White Paper, but no more than that.

215. Mr 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). I agree with COPA that Mr Yousuf gave no useful evidence on 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 **{{Day9/111:1} - {Day9/112:21}}**. He gave no support to Dr Wright's claim to have shared a pre-issue copy of the Bitcoin White Paper with him {**{E/4/21}** at [49i.]}. Even after Dr Wright's claim to be Satoshi became public, Mr Yousuf was not sufficiently interested to discuss it with him **{{Day9/123:7}** and following}.

216. Mr 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 gave evidence that Dr Wright was a capable IT security professional who had a lot of computers at his home and at one point expressed an interest in digital currency. Mr Archbold gave honest evidence, but I agree with COPA's submission that 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 {**{Day10/29:6}** and following}. He did not support Dr Wright's claim {{**E/4/21}, [49n]**} to have shared a pre-release copy of the Bitcoin White Paper with him.

217. Dr Cerian Jones **{E/14/1}** – Dr Jones is a consultant (but not a patent attorney) who has filed patents on behalf of nChain and Dr Wright since February 2016. She spends most of her time working for nChain on their patents. She accepted that she was not a patent attorney but had never objected to being given that title in a series of marketing events she attended on behalf of nChain.

218. She gave evidence about some of Dr Wright's patent applications and claimed to have been convinced that he is Satoshi by a combination of "his academic knowledge, his professional background and [his] previous employment experiences".

219. Her evidence was that Dr Wright could be Satoshi due to him having made three particular inventions recorded in three patents. Even if I assume this evidence might be relevant, she omitted to mention that Dr Wright was not the sole inventor. Indeed, for the first patent, all the internal documents show that the inventive work was done by Dr Savannah. She has personally and professionally associated herself with Dr Wright, nChain and the entire Satoshi story, so it is clear that her evidence was in no way independent. Overall, I agree that Dr Jones' evidence gave no support to Dr Wright's case, as Lord Grabiner KC appeared to accept when objecting that questioning her about the patents which were the subject of her statement was irrelevant to the Identity Issue.

220. Mr 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 described what he perceived as Dr Wright's skill in computer security and also talked 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:

220.1. 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.

220.2. 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.

221. He did not support Dr Wright's claim **{{E/4/21}, [49.p]**} to have shared a pre-release copy of the Bitcoin White Paper with him.

222. Furthermore, as COPA submitted, although disclosure has been given of nearly 100 emails and papers sent by Dr Wright to Mr Bridges ({**ID_006367} - {ID_006463}**), none of them 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, Dr Wright 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}.

Dr Wright's CEA Notice

223. In addition to the written and live evidence of those witnesses, Dr Wright relied on certain statements by way of CEA Notice. The Witness Statement of Mr Jenkin, a partner in Travers Smith LLP, provided further explanation. He set out the reasons why the individuals in question could not or should not be called to give oral evidence.

223.1. The transcript of the deposition of Donald Joseph Lynam in the United States District Court, Southern District of Florida, dated 2 April 2020, in the proceedings *Kleiman v Wright* (Case No. 9:18-cv-80176-BB/BR).

223.2. The transcripts of the deposition of Gavin A. Andresen in the United States District Court, Southern District of Florida, dated 26 February 2020 and 27 February 2020, in the proceedings *Kleiman v Wright* (Case No. 9:18-cv-80176-BB/BR).

223.3. The transcript of the oral evidence provided by Neville Sinclair to the District Court in Oslo, Norway, in *Magnus Granath v Craig Wright* (case number 19-076844TVI) on 16 September 2022.

224. In his witness statement, Mr Jenkin did not identify particular parts of those transcripts which were relied upon and, indeed, the CEA Notice itself makes it clear that the entirety of each transcript was relied upon. Notwithstanding this, very limited extracts in each transcript were highlighted, as I understand matters, as being the principal parts relied upon. Although I read each transcript, it was clear that the highlighted passages were the only parts of any real relevance, and it would have been better if the CEA Notice had been appropriately limited.

225. Mr Don Lynam is Dr Wright's maternal uncle. He served for nearly 30 years in the Royal Australian Air Force, rising to the rank of Wing Commander in the Engineering branch

and received an award for his work in IT in logistics management. He was just verging on age 80 when he gave evidence in deposition for the *Kleiman v Wright* case in Florida.

226. The only passages highlighted in the transcript of the deposition are in his evidence in chief. Indeed, the full transcript of his evidence did not form part of the CEA notice.

227. In Dr Wright's Opening Skeleton Argument, the deposition is described as supplying evidence of Don Lynam's "*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*".

228. Very little of the deposition of Mr Don Lynam is relevant to this Identity Issue which I have to decide. 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.

229. In his evidence in chief in his deposition, he gave some evidence of the familial influences on Dr Wright as he was growing up. Mr Don Lynam gave an account of being close to Dr Wright and regularly discussing his work in the mid-2000s. He spoke of Dr Wright's interests in mathematics, cryptography and internet security, describing him as one of the top three in the world in terms of his cryptography qualifications. Mr Don Lynam described Dr Wright's work for Centrebet as security, but for Lasseter's Casino he said Dr Wright developed what he understood to be the world's first token system enabling global gambling, internet gambling, using all fiat currencies 'so basically doing the same type of thing as Bitcoin'. Mr Don Lynam said he believed the Lasseter's system 'was the precursor of Bitcoin'.

230. 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*". He said '*Craig sent me a copy for my review but it was far too technical for me and also was poorly written'*. He said it was '*way above me technically*'. He didn't think the draft paper was headed Bitcoin but said it was '*clearly to be a digital monetary system'*. He said he had '*no doubt in his mind that that was the precursor because it had the same content as the paper that came out or very similar content*.' He thought it was the natural flow-on from some of the work that Dr Wright been doing over the years, the mathematics and the cryptography and he had been playing about with other digital currency systems which existed earlier than that and the fact that he was working with banks and large accounting systems.

231. In response to a leading question from Dr Wright's lawyer, he 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. When cross-examined by Mr Kleiman's lawyer, Mr Don Lynam said that he could not remember how he had received the paper. He said that he had not attempted to edit it.

232. The contemporaneous material in disclosure paints a different picture. An email in May 2008 provides a family update about Dr Wright's LLM qualification. Another, from December 2008, 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.

233. 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 **{L15/209/2}**, 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*").

234. 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"* **{L15/322/3}.**

235. Following this prompting and the promise of value, Mr Lynam appears gradually to have 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...*") **{L15/322/3}**. According to what he later said in his deposition, he "*went back researching"* for references to Mr Kleiman on the internet {**{E/16/32-33}** at 33 line 21}; he bought books about Satoshi Nakamoto {**{E/16/79}** at line 11}; 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 {**E/16/81}**. He continued researching even up to the week before his deposition **{E/16/75} - {E/16/76}**.

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

237. 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*". As COPA submitted, 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.

238. 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*" and that he had not edited it, stressing that he had actively decided not to edit it **{E/16/61** and the following pages}. In summary, and with the relevant quotations:

238.1. 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..." **{L16/267/22** at internal p85, l.12}.

238.2. 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*" {{**E/16/62}** at line 21 to **{E/16/64}** at line 7}.

238.3. Mr Don Lynam also made clear that he did not have "*any technical input into establishing or operating*" the Bitcoin system **{E/16/64}**. This is starkly in contrast to Dr Wright's contorted story that Mr Don Lynam was "*one of the three people behind Bitcoin*" **{Day6/129:7} - {Day6/132:22}**.

239. 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).

240. 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.

241. I have little doubt that Mr Don Lynam wanted to believe the best of his nephew but also that he had been carefully prepared for his evidence in his *Kleiman* deposition. In all the circumstances, I conclude that his account was made up. Accordingly, the extracts from his *Kleiman* deposition carry no weight at all.

242. The transcript of Mr Gavin Andresen's deposition in the Kleiman case covers some 440 pages (including the indices) with only very few passages highlighted. He considered Satoshi to be in the top 10% of all the programmers he had interacted with (he put himself in the same category) and believed him to be a brilliant programmer. He had looked at the original Bitcoin code (in C++) and gained the impression that a small number of people, possibly one, wrote it because it was dense with few comments – i.e. the code did not include much explanation as to what the code was doing, unlike in a large programming project where it is necessary to co-ordinate among multiple people.

243. Mr Neville Sinclair worked with Dr Wright at BDO from 2006. He was the audit partner in charge of signing off on financial statements. He described Dr Wright as a senior manager in the IT division of BDO and worked with a team in that division to support the general audit area in relation to IT, security and controls. He described Dr Wright's technical skills as extraordinary, particularly in identifying potential threats for clients but in terms of his personal skills, he was very direct which sometimes caused a little bit of friction.

244. Mr Sinclair said Dr Wright was very keen on how clients could better improve their security systems, by better logging of transactions and the holding of data. He recalled something drawn by Dr Wright as 'somewhat similar to what we'd currently look at in terms of the description of the blockchain' but added it wasn't referred to in that context in that sense.

245. Mr Sinclair had further occasional contact with Dr Wright after Dr Wright had left BDO at the end of 2008. One contact seems to have been related to possible support for unspecified systems which Dr Wright was developing. Somewhat later in 2011, Dr Wright told him a bit more about what he was doing with some of our (i.e. BDO) clients, and gave him a circular coin with the Bitcoin symbol on it – that was the first time Dr Wright had mentioned Bitcoin to Mr Sinclair.

246. Ultimately his evidence was that having seen Dr Wright work in IT systems and from a couple of occasions where he was able to 'oversight' what he was doing, Mr Sinclair said there was 'a high probability' that he would be able to do what he was claiming to do with Bitcoin and the blockchain technology. Mr Sinclair also spoke of a conference on 23rd November 2017 on IT security and banking systems. He said the day before an article had been published about Dr Wright being involved with Bitcoin and being the author of that system. He said quite a few of the people there who knew him were in agreement that most likely he would be the likely candidate to have developed the Bitcoin system.

247. COPA sought to call Mr Sinclair for cross-examination but he is out of the jurisdiction and would not agree to be cross-examined. I agree with COPA that his account as recorded in the transcript provides no support to Dr Wright's claim to be Satoshi.

Conclusions on Dr Wright's remaining witnesses of fact

248. Overall, I am able to place very little or no weight on the beliefs expressed by these witnesses (whether individually or collectively) that Dr Wright is Satoshi, principally because none of them had specific enough information to be able to express anything like a persuasive or definitive view. Further, none of them had access to the wealth of detailed information which was presented to me in this Trial. So, although I do not discount their evidence entirely, I must weigh their subjective opinions against the considerable quantity of evidence of objective fact which I heard.

COPA'S EVIDENCE OF FACT

COPA's witnesses of fact who were cross-examined

249. I will deal with COPA's witnesses in the order in which they gave their evidence i.e. these are the witnesses who gave live evidence and were cross-examined. In their closing submissions, Counsel for Dr Wright challenged aspects of the evidence of fact given by Mr Michael Hearn, Mr Zooko Wilcox-O'Hearn, Dr Adam Back and Mr Martti Malmi. I address these challenges below.

250. It will be seen below that COPA called a number of witnesses to address certain claims made by Dr Wright, both in his written statements but also in the course of his cross-examination. Many of these witnesses are third parties and I am grateful to them for their evidence and (for those who were cross-examined), making themselves available. Although a number of these witnesses were not required for cross-examination by Dr Wright's legal team, there remained several where there was an acute conflict between their evidence and that of Dr Wright. Where it is necessary to do so, I have resolved all these conflicts but it is important to point out that I did not resolve each conflict in its own little silo. I could not help but be influenced, to varying degrees, by all the evidence I have heard.

251. Mr Steven Lee is an independent board member of COPA, who gave evidence in person. In cross-examination, Lord Grabiner KC was keen to explore the concept of independence in this context and Mr Lee's other mentions of independence in his witness statement. This went nowhere.

252. Mr Lee was a good witness. He answered all questions clearly and was plainly an entirely honest witness. He was asked questions about the Bitcoin Legal Defence Fund and whether it was funding the legal costs of the Developers in this litigation. Mr Lee said he did not know but said it was likely.

253. Mr Martti Malmi is a computer scientist who corresponded with Satoshi from shortly after the release of Bitcoin in January 2009 until early 2011, during which time he helped set up website content and worked on the Bitcoin Code, as well as the Linux port of the Bitcoin Software. In his first witness statement, Mr Malmi rejected various claims that Dr Wright had made about him and denied 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 exhibited 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.

254. Mr Malmi gave evidence by videolink from Finland. He gave his evidence carefully and precisely. I was entirely satisfied he was telling the truth. His evidence was consistent with the contemporaneous documents. Furthermore, I agree with COPA's submission that the attempts in his cross-examination to suggest that Mr Malmi had had contact with Dr Wright beyond what Mr Malmi had already acknowledged failed miserably. I discuss this in greater detail below.

255. Dr Adam Back is a cryptographer and inventor of "Hashcash", which was cited in the White Paper. He gave 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 Wright1). For instance, Dr Wright said 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. 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.

256. Dr Back gave evidence in person. He gave his evidence in a careful and considered manner. He is plainly highly knowledgeable. The attack on his independence failed, in my view, an issue which again I discuss in greater detail below. Again, I was entirely satisfied he was telling the truth. Accordingly, I feel able to have confidence in his evidence.

257. Mr Mike Hearn also gave his evidence in person. 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. He said his impression was that Dr Wright could not answer his questions and that Mr Matthews shut down the conversation when Dr Wright got into difficulties. In cross-examination, he was the subject of robust challenge by Lord Grabiner KC on three points: first, whether

he requested to meet Dr Wright in 2016, or whether the initiative came from Jon Matonis; second, whether he was aware that the business for which he worked in 2016, R3, was a competitor of nChain; and third, what occurred at the dinner. These challenges were developed in some detail in Dr Wright's closing, and it is more appropriate to address them in chronological context below (see [897] and following, below).

258. Mr Howard Hinnant gave his evidence by videolink from the USA. He is a software developer. Between 2005-2010 he was Chairman of the Library Working Group for the C++ Standards Committee. In his first witness statement, he stated that he was the lead designer and author of various standard features of C++ including the <chrono> time utilities, among others. Bird & Bird asked him whether it would have been possible to use <chrono> or "sleep_for" in C++ code in October 2007. He gave various reasons why he said that would not have been possible including (a) that <chrono> or "sleep_for" were first standardised in C++11, i.e. in 2011; (b) the paper which first proposed both <chrono> or "sleep_for", N2661, was published on 11th June 2008; (c) prior to that date, implementations of <chrono> were limited to his own PC. He also considered various other possibilities, namely that, somehow <chrono> escaped into the wild and was picked up as early as October 2007. He was able to dismiss that possibility by reference to the previous iteration of N2661, namely N2498, on which he was also the lead author. N2498 is dated 19th January 2008 but does not contain any mention of the word 'chrono', and 'sleep_for' is called 'sleep' in this iteration. Mr Hinnant also said that when N2498 was published, <chrono> and 'sleep_for' did not even exist on his computer.

259. After he had explained those matters to COPA's solicitors, they provided him with three documents containing C++ source code disclosed by Dr Wright, each of which had the following metadata: Date Created 8th October 2007, Date Last Modified: 31st October 2007; Date Last Accessed: 15th October 2007

260. In his cross-examination on Day 5, Dr Wright made a number of claims relevant to Mr Hinnant's evidence, so COPA's solicitors provided relevant extracts from the transcript to Mr Hinnant for any further comment. That resulted in Mr Hinnant's second witness statement in which he addressed Dr Wright's further claims and in particular, Dr Wright's claim that he developed his own library using the header file <chrono>, based on an existing library called Project Chrono. Mr Hinnant explained:

> *'Project Chrono is not a time library as std::chrono is. It is a physics simulation library. One would not modify a physics simulation library to come up with a time library. The similarities between Project Chrono and the C++ standard header <chrono> end with the name "chrono".'*

261. Mr Hinnant said that Dr Wright's claims gave rise to no less than three remarkable coincidences:

    261.1. First, Mr Hinnant's evidence was that it was universal practice for all developers of non-standard libraries to put a filename extension on their headers, typically .h. Yet Dr Wright was claiming to have created a file with a name identical to what would be adopted by the C++ standard in the future, and in a style that only the C++ standard uses (extension-less). That, he said, was a striking coincidence that any C++ programmer would find difficult to accept.

261.2. Second, he pointed out that Dr Wright's code uses the phrase "std::chrono::milliseconds". However:

'...Project Chrono does not even use class types to model time units like the standard library does. It typically uses the built-in type double instead. So, Dr Wright claims to have invented the namespace std::chrono and the class type milliseconds, identical in syntax to what would be proposed for the C++ standard in the future. That strikes me as another remarkable coincidence.'

261.3. Third:

'In conjunction with "std::chrono::milliseconds", Dr Wright's code uses the syntax "std::this_thread::sleep_for". This too would not be proposed for the C++ Standard until after the last file modification dates for the code files referred to in my first statement. That strikes me as a third remarkable coincidence.'

262. Mr Hinnant was cross-examined with great care by Mr Orr KC. Mr Orr sought to establish that what Dr Wright had claimed was *technically possible in theory*. However, in any practical environment, Mr Hinnant explained why Dr Wright's claims were, in his succinct summary, '**absurd'**. Mr Hinnant also said Dr Wright's 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, as Mr Hinnant explained. Although Counsel for Dr Wright objected to any reliance being placed on these answers because they represented Mr Hinnant giving expert evidence, both answers were given in response to questions which plainly elicited those responses. I consider I am entitled to rely upon them. Furthermore, I formed the view that those answers were plainly true.

263. In my judgment, Mr Hinnant gave clear and honest evidence. Dr Wright's claims concerning <chrono> were a prime example where he had been caught out in his first account, but then sought to talk his way out by way of a technical explanation which turned out to be without basis. Mr Hinnant's clear evidence showed that Dr Wright was lying.

264. Mr Zooko Wilcox-O'Hearn is a computer scientist in the field of cryptography and cryptocurrency. He wrote early blogposts about Bitcoin and stated that he never received any Bitcoin from Satoshi, as Dr Wright has claimed he did. He also gave his evidence by videolink from the USA.

265. He has been involved in cryptography for many years, including from well before the development of Bitcoin. He worked on DigiCash in the 1990s and described himself as being 'good friends' with some well-known participants in the field including Hal Finney, Nick Szabo, Adam Back and Greg Maxwell, via interactions on Internet Relay Chat ('IRC') channels. He said that later on, he met others involved in Bitcoin after Satoshi, including Gavin Andresen and Peter Todd and 'was active with those folks for years'.

266. He first became aware of Bitcoin when it was announced by Satoshi in 2008. He does not recall any occasion when he had any private discussions with Satoshi. On 26 January 2009, he published a post on his blog entitled 'Decentralized Money' which mentioned

Bitcoin and included a link to bitcoin.org. He said that blog has been called the first blog post about Bitcoin, but he makes it clear that he never actually ran and used Bitcoin then. He recalled he first started using Bitcoin when using a matchmaking service where people traded Bitcoin and that one of his first transactions was with *druidian*.

267. Having stated those recollections to COPA's solicitors, they provided him with a link in the web archive to the relevant records of the matchmaking service, which show his transaction with *druidian* in July 2012 and his earliest transaction in May 2012. On that basis, he said he believed that May 2012 was around or shortly after the time when he first started using Bitcoin.

268. Mr Wilcox-O'Hearn was asked whether Satoshi Nakamoto transferred Bitcoins to him in 2009-2011 and responded (in his witness statement) as follows:

> *'He did not transfer any bitcoin to me at any time. As I have explained above, he could not have done because I didn't use Bitcoin until years later than it was launched.'*

269. Mr Wilcox-O'Hearn was a very engaging and careful witness. In my judgment he was transparently honest, willing to correct himself on reflection. Although Mr Orr KC made a manful effort in his cross-examination to suggest that Mr Wilcox-O'Hearn was mistaken about when he first dealt in Bitcoin and therefore he did receive some Bitcoin from Satoshi Nakamoto, I am entirely satisfied that Mr Wilcox-O'Hearn did not start his dealing in Bitcoin until around May 2012 and that he was not in any position to receive any Bitcoin from Satoshi at any time in the period when Satoshi was actively involved in the running of Bitcoin. 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. When it was put to him that he must have become more actively involved earlier, he replied disarmingly: "*You underestimate my laziness and procrastination*." **{Day14/81:2}**. It is thus clear that Dr Wright's claims (made initially in an interview with GQ in June 2017, and then in the *McCormack* and *Granath* cases) 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. On this issue, I unhesitatingly prefer the evidence of Mr Wilcox-O'Hearn.

COPA's witnesses who were not cross-examined

270. A large number of the witnesses relied upon by COPA and the Developers were not, in the end, required for cross-examination. Furthermore, due to certain allegations made by Dr Wright in the course of his cross-examination which related to certain witnesses, the parties also agreed terms on which their evidence was accepted, thereby avoiding the need to call them to address those allegations.

271. Here I will briefly summarise their evidence, all of which I entirely accept.

    271.1. Mr Joost Andrae **{C/1/1}** – Mr Andrae is a software engineer who contributed to the OpenOffice.org project. He gave 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. {See Madden 1 Appendix PM23}.

271.2. Ms 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 exhibited 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 **{D/490/2}**. As was common ground at the hearing of 12 October 2023, this evidence is admissible. I consider it in relation to Dr Wright's credibility.

271.3. Professor Daniel Bernstein **{C/4/1}** – Professor 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) **{L1/115/1}** 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 Professor 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 which I discuss later).

271.4. Mr Rory Cellan-Jones **{C/5/1}** – Mr Cellan-Jones is a technology journalist who worked as such for the BBC for many years. He was involved in the 2016 signing sessions, which he addressed 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 his bitcoin back.

271.5. In the course of his answers in cross-examination, Dr Wright accused Mr Cellan-Jones and the BBC of being biased and, more importantly, of 'splicing' together various answers on film to create, effectively, a false record of the signing session which Dr Wright undertook with Mr Cellan-Jones. It is understandable that Mr Cellan-Jones would feel aggrieved at these allegations and would want the opportunity to address them. Discussions between the parties led to an agreement that in submissions, Counsel for Dr Wright would not rely upon or repeat any of the allegations made in evidence by Dr Wright against Mr Cellan-Jones.

271.6. Whilst this arrangement was procedurally efficient for this Trial, the effect is capable of being misunderstood. For this reason, I wish to make it clear that I completely reject Dr Wright's spurious allegations about Mr Cellan-Jones and the BBC and I accept the evidence in Mr Cellan-Jones' written statement in its entirety.

271.7. Mr Dustin Trammell **{C/7/1}** – Mr Trammell is an Information Security Research Scientist who corresponded with Satoshi in January 2009. He gave evidence of his correspondence with Satoshi and exhibited it. He denied a claim Dr Wright made in his evidence in the *Granath* proceedings that Dr Wright as Satoshi shared Bitcoin code with him.

271.8. Mr John Hudson **{C/8/1}** – Mr Hudson is the lead designer of the font Nirmala UI and confirmed 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.

271.9. Mr 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 provided evidence of his email communications with Satoshi that had not previously been 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 authenticated and which has been used in the evidence as a control copy. Mr Bohm sadly died just before the Trial commenced.

271.10. Mr 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). This presents as being a set of pre-release development notes on the Bitcoin concept. Mr Ford explained that the notepad was not printed until 22 May 2012. Dr Wright reacted to this evidence in his Chain of Custody schedule by saying that the notes were written in 2011 / 2012. Again, this account has its own difficulties which I discuss further below

271.11. Professor 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 stated 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.

271.12. Professor Richard Gerlach **{C/20.1/1}** – Professor 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 gave evidence that various features of a statistics assignment document in Dr Wright's disclosure are anomalous.

272. Finally, Professor Bjarne Stroustrup, who gave a witness statement in response to certain features of the evidence of Dr Wright. Professor Stroustrup was originally scheduled to be cross-examined, but Dr Wright's team indicated they had decided not to challenge his evidence.

273. Professor Stroustrup is a professor of Computer Science and the designer of the C++ programming language. In his witness statement, Professor Stroustrup explained that he is the designer and original implementer of the C++ programming language and remains involved in the standardisation of C++, having received many international honours for his work.

274. Professor Stroustrup was asked to address a particular issue relating to the libraries <chrono>, <thread> and <random> and when they were first in use in C++. His evidence was that those libraries were part of C++11 (released in 2011) and 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. He said that before C++11, these libraries were called differently: chrono.h, thread.h and random.h. Naturally I accept Professor Stroustrup's evidence in its entirety and I am very grateful to him (and all the third party witnesses) for providing it.

COPA's CEA Notice

275. COPA adduced the following documents under a CEA Notice:

275.1. A letter from Mr Lucas de Groot dated 14 June 2023 explaining that the Calibri Light font was not available until 2012. This was 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.

275.2. A letter from Mr Michael Stathakis and Ms Lee Li dated 10 July 2023 addressing a form of "Quill" notepad. 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 **ID_004013 {L2/159/1}**. Mr Stathakis and Ms Li explain in some detail that this form of Quill notepad was not available until 2012.

275.3. A witness statement from Mr Andreas Furche – Mr Furche has provided a witness statement but was 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 confirmed 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 over the period 2005-2009). His account suggests that a series of statements Dr Wright has made about his work on the development of Bitcoin in various particulars are false.

275.4. Emails in April and May 2022 from Professor Graham Wrightson confirming Mr Furche's account and that he did not know Dr Wright.

275.5. Extracts from the Lynn Wright deposition transcripts from the Kleiman proceedings. 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. I reject this. It is clear from the transcript that at the start of her evidence she gave evidence that she was fit to testify. Furthermore, her testimony in the transcript reads as clear and coherent.

275.6. An extract from the First Witness Statement of Mr John Chesher dated 1 May 2023 which was submitted by Dr Wright in the *Coinbase* proceedings. He has provided bookkeeping and accounting services to Dr Wright and gave evidence on the assets of Wright International Investments Limited. The significance of this extract is that Dr Wright claims to have shared a copy of the Bitcoin White Paper with Mr Chesher before its release, while Mr Chesher says that he did not meet Dr Wright until 2010.

275.7. Emails from Mr Wei Dai from October 2023 confirming, amongst other things, that Mr Dai never provided code to Satoshi, contrary to what Dr Wright claimed. Wei Dai also explains that he has never worked in academia, contrary to Dr

Wright's description of him as an 'academic'. This seems to have been another guess by Dr Wright.

Evidence of Fact from the Developers

276. The Developers served evidence of fact from a single witness – the Fourth Defendant in the BTC Core Claim, Dr Pieter Wuille. He provided two witness statements. He discovered Bitcoin in around December 2010 and started contributing to the project in early 2011, joining the maintainer team for Bitcoin in late April 2011. He left the maintainer team in July 2022 but continues to be an active contributor to the Bitcoin project. Although he undertook his initial contributions to the project in his spare time, he said that since September 2014, contributing to Bitcoin has been part of his job, first for Blockstream and since 2020 for Chaincode Labs.

277. Having summarised his involvement, he went on in his first witness statement to discuss certain concepts related to Bitcoin and the Bitcoin Software. Some of these were used in a short but effective cross-examination conducted by Mr Gunning KC of Dr Wright and I discuss these points later. In the final paragraphs of his first witness statement, Dr Wuille refers to the first time he became aware of Dr Wright which was around the time Dr Wright posted a screenshot in a blog '*that was supposed to be a message signed with one of Satoshi's* keys'. He continued:

> *'I remember reading this blog post when it first came out, and reading articles responding to it which argued that it was not a genuine signature, and instead reused an existing, public signature by Satoshi from the bitcoin blockchain. I remember that I looked at the blog post and myself verified that it took an existing signature by Satoshi and converted it into OpenSSL format rather than the Bitcoin format so it didn't look the same as the original. The most obvious tell is that the signature could not be identical to one that was already used. In short, the signature in the blog post proves nothing; I formed the view that it was a deliberate attempt at making an old signature look like it was a recent one.'*
> *'… I remember that when I reviewed the blog, it convinced me Craig Wright was not Satoshi…'*

278. Dr Wuille's short second witness statement was made in response to certain points made in **Wright11**. Those triggered certain recollections which Dr Wuille followed up by reviewing some contemporaneous records of particular developments in Bitcoin namely the introduction of the 520 byte limit on stack elements in the Bitcoin Source Code and the disabling of certain opcodes. Again, some of this material was used in the cross-examination of Dr Wright.

279. Overall, page for page, Dr Wuille's first witness statement (dated 13 October 2023), as supplemented by his second (26 January 2024), turned out to be the most significant document in this Trial because his ability to detail when certain features of the Bitcoin system were introduced were used to devastating effect in cross-examination of Dr Wright, as I explain below. Each topic was explained in his witness statement clearly, so Dr Wright had more than fair warning of these topics. On some of them, Dr Wright's prior deductions as to what happened turned out to be wrong. On other topics, unusually (bearing in mind that generally Dr Wright appeared very well prepared for cross-examination), Dr Wright was caught out. It does not matter why that was the case, but it

may have been because Dr Wright had to concentrate so hard on keeping so many forgery plates spinning.

280. Counsel for the Developers offered to call Dr Wuille to address any questions I might have for him. Whilst it would, I am sure, have been interesting to discuss some of the technicalities with Dr Wuille, I decided it was not necessary to take up that invitation since none of his evidence was being challenged. Dr Wuille presented very clear and well-explained written evidence. Since, as I have said, none of it was challenged, I accept it in its entirety.

THE EXPERT EVIDENCE

281. I have already referred to the expert evidence on ASD, above. Here I introduce the expert evidence which related directly to the Identity Issue. I will deal with challenges later.

282. As is often said in the Patent field, it is the *reasons* which an expert gives for holding an opinion which matter, not so much the fact s/he has expressed the opinion. In this case, I am very grateful to all the experts who have provided expert evidence. They more than sufficiently educated me so that I was able to make all necessary findings in this Judgment and Appendix.

The expert evidence on cryptocurrency matters

283. The cryptocurrency experts addressed two topics: (a) basic facts of the technology underpinning Bitcoin and other cryptocurrencies; and (b) the signing sessions. COPA's evidence was from Prof Meiklejohn, and Dr Wright's from Mr ZeMing Gao.

284. Most of Mr Gao's report addressed the first topic. Rather than simply addressing the basic facts of the technology, he pursued 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 my Order at the PTR, Dr Wright was not permitted to rely on those parts of Mr Gao's report which deal with his assertion that BSV is the superior implementation of Bitcoin and/or the alleged fidelity of BSV to the suggested intentions of Satoshi. COPA identified these as [65-89], [102-154], [180-197] and [217-225], without demur from Dr Wright's team. In any event, all this argument that BSV is the "true version" of Bitcoin as envisioned in the Bitcoin White Paper seemed to me to have nothing to do with the Identity Issue, which is why I ruled it 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.

285. Following without prejudice discussions, the two experts produced a joint report in which Mr Gao agreed with most aspects of Prof Meiklejohn's evidence. On the topic of the signing sessions, as COPA submitted, they both agreed that the sessions could have been faked and on how that could have been done. The two experts produced short reply reports explaining the rationale for their disagreements (each explained in an annex to their Joint Statement) which are actually of quite limited importance to the issues in the case.

286. In their Written Closing Submissions, Counsel for Dr Wright and Counsel for COPA levelled various criticisms at the opposing expert. Those levelled at Professor Meiklejohn were directly related to her evidence regarding the signing sessions. These are best addressed in the context of my assessment of the signing sessions, in a later section of this Judgment. Those levelled at Mr Gao were more general and I can deal with those here.

287. I should say, however, that most of the evidence given by Professor Meiklejohn and Mr Gao was uncontroversial. In particular I am grateful to them for conducting a productive joint meeting and producing their useful Joint Statement (which also identified where they differed).

Mr ZeMing Gao

288. COPA submitted that Mr Gao's articles and posts demonstrate an extraordinary lack of independence and objectivity, citing the following examples. In his recent self-published book, he treats Dr Wright as a messianic figure, misunderstood by the world **{L20/121/67}**:

> *"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?"*

289. 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 **{Day18/67:10}**:

> *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.*

290. Mr Gao also accepted that he had staked his personal reputation on the case **{Day18/74:16}**:

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

291. His lack of independence extended to a personal hostility to COPA, claiming that its approach in these proceedings is to trick the court {**{Day18/66:10}** and blog at **{L19/264/1}**}, 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 **{Day18/75:20}**.

292. I agree that certain aspects of Mr Gao's report lacked independence and objectivity and, in view of his publicly stated view of Dr Wright, I would be very cautious about relying

on any of his evidence which conflicted with that given by Professor Meiklejohn. However, on the important matters – the signing sessions and the technical aspects of cryptographic proof, he did not dispute Professor Meiklejohn's evidence.

293. However, COPA submitted that one feature of his evidence demonstrated his lack of independence. This was where he attempted 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. So I give no weight at all to Mr Gao's efforts to argue for a particular interpretation of the post.

294. Notwithstanding the trenchant attack on Mr Gao's independence, I am not sure his lack of independence really affected anything I have to decide. As COPA submitted, during his cross-examination Mr Gao accepted the following points (which were all the points which COPA needed):

294.1. 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 {Day18/5:17}. 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.

294.2. 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 **{Day18/7:13} - {Day18/9:24}**.

294.3. 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 **{Day18/11:3} - {Day18/12:1}**.

294.4. 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 – see the whole section at **{Day18/17:3} - {Day18/33:1}** – regarding Mr Gao's agreement with the technical steps set out in Ms Meiklejohn's evidence about how the signing sessions could be subverted.

294.5. 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 doing so did not confer any benefit in terms of security or preventing subversion **{Day18/38:6} - {Day18/41:8}**.

294.6. The Sartre blog was "*clearly not a genuine proof*" of possession of any private key **{Day18/45:4}**.

The expert evidence on forensic document analysis

295. Mr Patrick Madden was the principal expert witness called by COPA on matters of forensic document analysis.

296. Mr Madden made six expert reports for this Trial:

    296.1. **Madden1** was a very substantial report (amounting with Appendices to around 970 pages) served on 1 September 2023. It addressed Dr Wright's initial list of 107 Reliance Documents.

    296.2. **Madden2** (17 November 2023) was supposed to be his report in reply to Dr Placks' report of 23 October 2023 (which focussed on the 48 Reliance Documents analysed in **Madden1**, and certain extra MYOB files, but not other documents analysed in **Madden1**). As Mr Madden says, he was provided with a significant amount of new documents when he was preparing it and he analysed these.

    296.3. **Madden3** (7 December 2023) contained his preliminary analysis of certain aspects of the 97 Additional Documents, the BDO Image and the question of whether the Bitcoin White Paper was created using LaTeX or not. This was done for the purposes of the PTR. He detected that the BDO Image had been manipulated, which included the use of clock manipulation and metadata editing. He observed that the vast majority of the 97 documents were in formats with little or no metadata for forensic analysis, and made the point very clearly that any proper analysis would require access to a forensic image of the drive from which the BDO Image was taken. Of the minority of files which provided information which could be analysed forensically, he found that several bore strong indications of metadata tampering and backdating.

    296.4. **Madden4** (18 January 2024) contained a much fuller analysis of the 97 Documents and the BDO Drive.

    296.5. **Madden5** (18 February 2024, i.e. served in the middle of the Trial) addressed the new documents which I permitted Dr Wright to adduce at the start of the Trial, as well as some of the opinion evidence in Wright 11.

    296.6. **Madden6** (28 February 2024, served towards the end of the evidence in the Trial) addressed the MYOB Ontier email.

297. Mr Madden's evidence underpins almost all of COPA's allegations of forgery. In their Closing Submissions, Counsel for Dr Wright attacked Mr Madden's evidence, his qualifications and his independence. These were developed in Lord Grabiner KC's oral closing and led to his submission, (which he accepted was a fairly drastic conclusion) that the safest course for me to take would be to disregard Mr Madden's evidence '*because of the serious doubts about his independence'*.

298. This was a bold submission to make in view of the fact that Dr Wright's experts (Dr Placks & Mr Lynch) had agreed with most of Mr Madden's findings in his first to fourth reports, but it was at least consistent with the position taken in cross-examination by Dr Wright where he dismissed all the expert evidence on the basis that none of the experts were properly qualified, the sub-text being that only Dr Wright was.

299. I deal with all the attacks on Mr Madden and his evidence below.

300. The principal expert relied on by Dr Wright was Dr Simon Placks, at least until Dr Wright decided to dispense with his evidence:

    300.1. His first report (served on 23 October 2023) was limited to responding to Mr Madden's analysis of the 48 Reliance Documents in **Madden1**.

    300.2. Following without prejudice discussions, he and Mr Madden agreed a very helpful Joint Statement (served 8 December 2023).

    300.3. On 18 January 2024, Dr Placks served his Second Report.

    300.4. On 22 January 2024, he and Mr Madden agreed their Second Joint Statement.

301. Mr Spencer Lynch was brought in to address the Additional Documents, the Samsung Drive and the BDO Image. He served his report on 18 January 2024 and agreed a Joint Statement with Mr Madden which was served on 22 January 2024.

The experts on LaTeX

302. COPA's expert on LaTeX was Mr Arthur Rosendahl, and Dr Wright's expert was Mr Lynch.

303. In their Joint Statement (served 22 January 2024), they agreed that:

    303.1. The White Paper was not written in LaTeX but in OpenOffice 2.4 (a finding consistent with the metadata of the public Bitcoin White Paper versions).

    303.2. 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.

    303.3. Reverse engineering the Bitcoin White Paper into LaTeX source code to make something superficially similar is not too difficult.

    303.4. 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.

304. After their Joint Statement, Mr Rosendahl served his second report (on 12 February 2024) to address two sets of metadata information and their associated files, which related to the project editing history of the LaTeX files he had analysed in his first report.

305. As I have related, Dr Wright did not rely on Mr Lynch's evidence. Mr Rosendahl came to London to be cross-examined in person. He is obviously extremely knowledgeable about LaTeX and he gave his evidence carefully, precisely and with obvious honesty. He was an ideal expert witness.

306. Although Dr Wright jettisoned Dr Placks and Mr Lynch as witnesses, I am grateful to them for their work. I should add I have no reason to conclude that they acted other than entirely in accordance with their duties as experts to be objective and independent. Both made and agreed findings adverse to Dr Wright and (although it does not matter for any

of my conclusions) it is likely that their objective and independent approaches were the very reason why Dr Wright jettisoned their evidence.

TECHNICAL BACKGROUND

307. These Bitcoin cases were originally docketed to me due to a concern that they might involve issues of some technical complexity. It turned out that the issues relating to Bitcoin technology are not particularly complex, and in this section I set out an overview of cryptocurrency technology by way of relevant technical background. In addition, some of the evidence relied upon to indicate forgery (or not) raised some technical issues, but those points are best discussed in the context of the forgery allegations.

308. This section is based on Professor Meiklejohn's account of the technology, which was largely agreed by Dr Wright's expert, Mr ZeMing Gao.

309. Bitcoin was the first cryptocurrency, originating in 2009. Bitcoin is known as a cryptocurrency because it is a cryptographic system, in that it relies on principles of cryptography and uses cryptographic algorithms to form and verify transactions and blocks. The two cryptographic primitives that Bitcoin relies on are hash functions and digital signatures.

310. It is a peer-to-peer system, meaning users can transfer payments between themselves without an intermediary or central authority. 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.

Hash Functions

311. A cryptographic hash function is a function, which can be denoted as H, that has the following properties:

    311.1. It takes in inputs of arbitrary size (meaning that they can be nearly any size and the size does not matter in practice).

    311.2. It produces an output of some fixed size.

    311.3. It is efficiently computable, meaning given any input it is fast to compute the output.

    311.4. It is pre-image resistant. This means that given a hash h it is hard to find an input x such that $H(x) = h$.

    311.5. It is collision resistant. This means that it is hard to find two different inputs x and y such that $H(x) = H(y)$.

312. The most used hash function today is SHA256, and this is what Bitcoin uses. SHA256 hashes are usually encoded and expressed as a string containing 64 alphanumeric characters, such as the string

2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824 (the hex encoding of the SHA256 hash of "hello").

313. The Bitcoin White Paper defines a coin as "a chain of digital signatures". An owner transfers a coin by "digitally signing" a "hash" of the previous transaction involving the coin and the public key of the next owner. Because the hash used in a transaction includes both the previous transaction involving the coin and the public key of the next owner, the hash embeds the history of expenditure of that coin.

Digital Signatures

314. 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. A digital signature acts to verify the signing of a given message and involves three algorithms: KeyGen, Sign and Verify. Their interaction was illustrated by Professor Meiklejohn in her Figure 1:

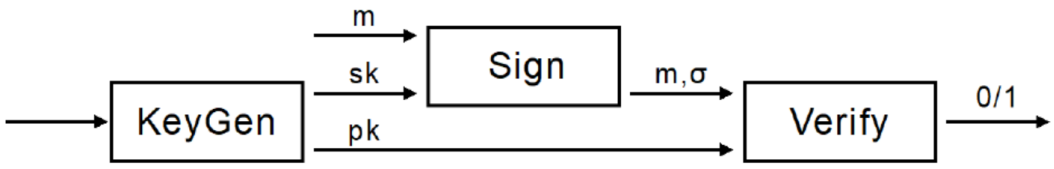


Figure 1. The inputs and outputs of the algorithms KeyGen, Sign, and Verify that make up a digital signature scheme. In terms of notation, m is the message being signed, sk is the secret key, pk is the public key, and σ is the signature.

314.1. KeyGen is a randomised algorithm that produces two keys: a private key (sk) and a public key (pk). Each time KeyGen is run, it produces a new keypair. These keys have the property that it is hard to compute the private key given only the public key.

314.2. Sign is a randomised algorithm that allows the holder of the private key to produce a signature (σ) on some message (m).

314.3. Verify is a deterministic algorithm which allows anyone in possession of the public key to verify that the signer produced a valid signature on a given message. It outputs 0 if the signature does not verify and 1 if it does.

315. There are several standardised digital signature schemes, with the one being used in Bitcoin known as ECDSA (Elliptic Curve Digital Signature Algorithm). The curve used in Bitcoin is secp256k1, and ECDSA signatures are usually encoded and expressed as 64 alphanumeric characters.

316. So, digital signature is a process designed to provide confidence that an entity has signed a given message. A randomised algorithm (Sign) allows the holder of a private key (one of the outputs of KeyGen) to produce a signature (σ) on a message (m). The recipient of a digital signature uses a deterministic verification algorithm (Verify) to check whether

the signature conforms to the public key of the sender. The digital signature of a transaction involving bitcoins enables the recipient (R) to be satisfied that the sender was entitled to transfer the relevant sum.

317. However, if the transaction process ended at that point, the '*double-spending problem'* would remain and the solution to this problem in the Bitcoin White Paper was the use of a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions using a '*proof-of-work'* system.

318. Section 4 of the Bitcoin White Paper is headed 'Proof-of-Work' and it explained:

> *'To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.*
> *For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. …'*

319. However, when it came to the Bitcoin Source Code, Satoshi implemented an improved proof-of-work function which departed from the system described in the Bitcoin White Paper, which contemplated that the target value would be set with leading zeros – as in Dr Adam Back's 'Hashcash' paper. Instead, the code used a numerical comparison (whether the hash of a Block Header is equal to or below a set target number). It is true that being equal to or below a long target number implies there will be a number of leading zeros in the target number, whether in binary or hex or any other base. However, the improvement meant that the target number could be set precisely, which in turn allowed the difficulty to be very precisely adjusted. This improvement is relevant to an issue raised in the cross-examination of Dr Back which I address later.

The 'control' copies of the Bitcoin White Paper

320. Having cited an extract from the Bitcoin White Paper, I should mention that, perhaps not surprisingly, there were several 'versions' of it in disclosure. Mr Madden addressed this issue at an early stage. His analysis shows there were 68 documents in disclosure which were either versions or relations of the Bitcoin White Paper, but 24 unique documents. After significant scrutiny and verification via third party sources, he identified **{ID_000226}** and **{ID_000865}** as suitable 'control' copies of versions of the Bitcoin White Paper {see **PM3 {H/20/14}**}. **{ID_000226}** has a creation date of 3 October 2008. **{ID_000865}** bears a creation date of 24 March 2009 and is hash identical to a file 'Bitcoin.pdf' from a web archive capture dating to 28 November 2009 from the sourceforge.net project.

Transacting in Bitcoin

321. 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. 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).

322. 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. 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.

323. In Bitcoin, a transaction can have multiple senders and recipients. Senders and recipients are identified using addresses, and the value being sent or received by each party is identified in bitcoins. Bitcoins are divisible, and can be divided to the eighth decimal place; i.e., the smallest amount it is possible to send is 1×10^{-8} bitcoin (0.00000001).

324. A transaction contains, in its simplest form, an input corresponding to the sender and one output corresponding to the recipient. The transaction output (TXO) 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. 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.

325. 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. To prevent double spending, Bitcoin tracks which transaction outputs are unspent and allows only those unspent outputs to spend the coins they receive. Sometime in about 2011 or 2012, the term UTXO was introduced to refer to an unspent transaction output.

326. Moving beyond the simple example with one input and one output, transactions with multiple inputs function in the same way: each transaction input needs to specify its own distinct UTXO and valid signature on the transaction data. Transactions with multiple inputs do not necessarily have multiple senders, as they could just represent one sender spending the contents of multiple UTXOs associated with the same address.

327. Similarly, transactions can have multiple transaction outputs, where again there can be multiple distinct addresses (representing different recipients) or not. This latter type of transaction is needed to divide bitcoins, as again any bitcoins received in a transaction must be spent all at once. For example, if a user has 10 BTC associated with a UTXO and wants to send two bitcoins to another user, they can form a transaction with one input representing their 10 BTC UTXO (and a valid associated signature) and two outputs: one containing the address of the other user and receiving 2 BTC, and the other containing an address they control and receiving 8 BTC. In this way, a user can make change, just as happens when spending physical cash.

Transaction Ordering

328. 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. This is the role of the Bitcoin blockchain, which acts as a ledger of all valid transactions propagated through the network.

329. 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. 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.

330. The initial block reward was 50 bitcoin, but that halves with every 210,000 blocks. At the time of the Trial it was 6.25 bitcoin. It is presently 3.125 bitcoin. The total number of bitcoin capable of being generated as rewards is capped at 21 million bitcoins in total. 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. The difficulty level itself changes according to the expected time to produce blocks divided by the actual time, meaning that difficulty increases or decreases depending on the collective computation power.

Blockchain Forks

331. 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. A backwards-incompatible change is known as a hard fork, which creates two different blockchains diverging at a single block. The most popular cryptocurrency based on the White Paper and Genesis Block is Bitcoin (BTC). Further hard forks have created the cryptocurrencies Bitcoin Cash (BCH), and Bitcoin Satoshi Vision (BSV).

Storage and Use of Bitcoin

332. 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. 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. 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).

333. 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 being known as Shamir Secret Sharing. 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.

Security of Digital Signatures

334. 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. The message must be a new one, since otherwise the recipient could simply copy a signed message and later hold it out as proof of ownership of the underlying private key (a process known as a "replay attack"). It is for this reason that a user must be asked to sign a new message. This explanation is significant for the topic of the Sartre message.

335. 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. Trust in the software that is being used is therefore important. In a section of her report agreed by Mr Gao, Prof Meiklejohn set out several requirements which must be fulfilled to establish possession of a private key:

    335.1. Unique message – The message to be signed must not have been signed before for that public key.

    335.2. 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.

    335.3. 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.

    335.4. 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.

    335.5. 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).

Public keys Associated with Satoshi

336. 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. 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.

COPA's ALLEGATIONS OF FORGERY

337. I have addressed the detail of COPA's allegations of forgery in the Appendix. I have also addressed certain other documents (e.g. the Papa Neema emails and their enclosures) in the body of this Judgment.

338. As I have related above, at various stages of my management of this case, I had to limit the number of forgery allegations which COPA was permitted to pursue, to keep the case within manageable proportions and on track. This resulted in all or the vast majority of the documents disclosed or relied upon by Dr Wright falling into one of the following categories:

    338.1. First, documents in respect of which COPA's allegation of forgery was permitted to be pursued at trial – as just mentioned, I have addressed these documents in the Appendix, and certain other documents in the body of this Judgment.

    338.2. Second, documents pleaded by COPA to be forgeries at an earlier stage, before I placed a further limit on the allegations which COPA could pursue, but which could not be pursued at trial.

    338.3. Third, documents falling outside the first two categories which were examined in Madden1 and which he found to be inauthentic.

    338.4. Fourth, documents whose authenticity was not challenged by COPA. Most, if not all of these documents are relied on by COPA as establishing the relevant sequence of events and are referred to, explicitly or implicitly, in this Judgment.

339. Thus, the documents I deal with in the Appendix are (i) the original forgeries alleged in the Particulars of Claim (ii) the 'top 20' from the first set of forgery allegations, plus (iii) a further 20 selected from the 'Additional Documents'.

340. I should briefly mention some of the consequences of my case management which gave rise to the documents in the second category. The point is that the choices made by COPA when deciding on their original 50 additional allegations of forgery were disrupted. I mention two main effects of this:

    340.1. First, it is apparent that allegations of forgery were made against a number of related documents which purported to be versions or drafts of the Bitcoin White Paper, including three documents labelled 'Backdated Bitcoin White Paper' (1), (2) & (3), **{ID_000536}, {ID_000537}** and **{ID_000538}**, and three coffee-stained copies or images **{ID_003330}, {ID_004011}** and **{ID_004010}**. Three of those documents had to be excised from the list of forgeries that COPA could pursue at trial, even though there was a degree of cross-reference between the reasons for the allegations of forgery. I have taken account of this in section 30 of the Appendix, as this is the only way to make sense of the allegations made against **{ID_004011}**. In doing so I was satisfied that Dr Wright had every opportunity to make his case in response.

    340.2. Second, it is apparent that COPA was thereby prevented from pursuing a number of allegations of forgery which related to the establishment of the Tulip Trust and Dr Wright's acquisition of Tulip Trading Limited, specifically in relation to

{ID_001421}, {ID_001919}, {ID_001925} and **{ID_001930}**. I have little doubt that COPA were sanguine about those allegations, since they were likely to re-emerge in the claim brought by Tulip Trading Limited against the Developers. (As a postscript, whilst preparing this Judgment I have learned that that claim has recently been discontinued).

340.3. A third point to mention is that some of these documents were the subject of cross-examination of Dr Wright in any event.

341. I was addressed by the Developers on the status of a number of documents relating to the establishment and acquisition of Tulip Trading Limited, but I was not otherwise addressed on the documents in the second and third categories. As far as I am aware, no such document was relied upon by Dr Wright in his Closing Submissions. However, due to my confidence in the reliability of the analysis carried out by Mr Madden (most of which was agreed by Dr Placks or Mr Lynch in their respective Joint Statements) and in so far as is necessary I make a general finding that none of the documents in the second and third categories are authentic.

General points made by Dr Wright in response to the allegations of forgery

342. For the most part, Dr Wright's positive case (as set out in sections II-IV of his Written Closing) did not pay any attention to COPA's numerous forgery allegations, no doubt because his position is that they were unfounded. For that reason, in their Written Closing, Counsel for Dr Wright turned to COPA's forgery allegations in section V and they raised a series of important general points which I address here. I emphasise that I have taken these points into consideration when making my findings in the Appendix.

343. First, I was reminded that COPA's forgery allegations are not a freestanding part of COPA's claim and they are ultimately sub-issues to the broader Identity Issue. I agree with that submission. Counsel for Dr Wright held out the beguiling prospect that, '*if the Court considers itself able to determine the Identity Issue without having regard to Dr Wright's Reliance Documents, it will not need to trouble itself with the complex and lengthy detail of COPA's forgery allegations*.'

344. In my judgment, it would have been a denial of my responsibility as the Judge if I were to decline to decide the forgery allegations. Anticipating that, Counsel for Dr Wright provided me with their responses to all the forgery allegations, in three parts. The original forgery allegations are dealt with in their Appendix 1 to their Closing; the Additional Forgery allegations are addressed in section V.B. at [220]-[222] and the Ontier Email allegation in section V.C. at [223]-[234]. In what follows I address the submissions in these three sections, which must be combined with the detailed submissions from COPA and the Developers.

A. The forgery allegations concerned with Dr Wright's original disclosure.

345. Before descending into the detail, Counsel for Dr Wright submitted I should be cautious about making any forgery findings against Dr Wright, for the following reasons:

345.1. First, because forgery allegations are of the utmost seriousness and would, if established, do great damage to Dr Wright's reputation and future endeavours. In this regard, I was reminded of the principles which I set out in paragraph 113

above. This point is undoubtedly true, but if forgery is established the person responsible must live with the consequences of their actions.

345.2. Second, because COPA's evidence, it was submitted, was neither satisfactory nor cogent. For the reasons explained in this Judgment and in the Appendix, I reject this. COPA's evidence was cogent and compelling.

345.3. 'The **third** reason is that, due to how late in the proceedings they were raised and the unfortunate sequencing of the relevant factual and expert evidence, it has not been possible for the forgery allegations to be explored and responded to in a suitable way.'

346. This third reason was developed in the following way. First, I was reminded of the procedural history of the development of the forgery allegations following the service of **Madden1**. I have been acutely aware of this procedural history throughout my case management of this litigation down to and including this Trial. I have summarised it above. Second, attention was drawn to Dr Wright's reply evidence in **Wright9, 10 & 11** and in particular to his evidence that '*a number of the anomalies identified by Mr Madden and relied on by COPA as evidence of forgery were the innocent result of his complex computer environment and collaborative working practices*.' Then, this submission was made:

> *'Ideally, this evidence should have formed the factual background to Mr Madden's analysis from the outset. Instead, this case has involved the reversal of the orthodox sequencing of factual and expert evidence, where the former comes first and forms the factual basis for the latter. As a result, the very lengthy detail of Dr Wright's complex computer environment has received only cursory treatment by Mr Madden, across just over 2 pages of his fourth report.'*

347. That last sentence is a travesty of the true position, as Counsel for COPA demonstrated when responding to it. In summary:

347.1. It is true that Dr Wright devoted many paragraphs when describing his '*complex computer environment'* (particularly in **Wright8** and **10**), but in reality there were relatively few technical points which emerged which were capable of affecting the allegations of forgery.

347.2. I am entirely satisfied that Mr Madden considered Dr Wright's explanations carefully. In **Madden4**, it was apparent that Mr Madden had reviewed **Wright9, 10 & 12**, and had been asked specifically whether they led him to change his opinions in that Report or in his previous reports. He stated in terms '*They do not*'. In that review process, I am certain that Mr Madden adhered to his duties as an expert, in particular to be ready to change an opinion on new information coming to his or her attention.

347.3. One of the reasons why Mr Madden was able to address these points relatively succinctly in **Madden4** was because he had already taken account of any that mattered in his first report. To cite two examples, in Appendix 24 to his first report, Mr Madden acknowledged the possibility of overlapping edit times due to multiple computers being operated simultaneously, but made it clear that he did not draw any conclusions on individual documents on the basis of edit time

observations alone. They are not irrelevant but part of the context. In the same Appendix, Mr Madden took account of the possibility of multiple virtual machines being in operation simultaneously – long before Dr Wright even raised the point.

347.4. In any event, Mr Madden's analysis and COPA's reasons for alleging forgery identified, in each case, numerous indicators which, when combined, gave rise to a compelling case which Dr Wright was unable to answer. Further, when considered against all the circumstances of this case, the compelling case on each allegation of forgery became unanswerable.

348. Furthermore, the complaint about reversing the orthodox sequencing of factual and expert evidence has very little substance, bearing in mind (a) this was done at the explicit request of Dr Wright's then Counsel and (b) Dr Wright's late and very late disclosure of documents said to be critical to his case. In any event, I am entirely satisfied that all matters relating to Dr Wright's '*complex computer environment and collaborative working practices*' were fully considered by the experts and fully explored in evidence. It should also be noted that (a) Dr Wright's own experts did not support his position and (b) the '*innocent explanation*' came from Dr Wright himself. When considering the allegations of forgery, I have taken into account some of Dr Wright's points regarding persistence (as the experts did) and also differences between Windows and Unix systems as regards certain aspects of metadata. It is, however, clear that the experts did not rely on metadata anomalies alone. Furthermore, as explained in the Appendix, for each document alleged to have been forged, there were numerous pieces of supportive evidence, which are only reinforced by the overall scale of Dr Wright's forgery. In short, those matters do not provide an innocent explanation for all or even some of the alleged forgeries.

No time capsule documents in Dr Wright's original disclosure

349. The next point taken is that, particularly in relation to the allegations concerning Dr Wright's original disclosure, Dr Wright never suggested that his original Primary Reliance Documents were not accessed or edited by anyone since the publication of the Bitcoin White Paper, such that they could be treated as a 'time capsule'. It is further contended that '*Indeed, the opposite was clear from Dr* Wright's *own Chain of Custody of Reliance Documents schedule*' along with a footnote: '*13 October 2023 {K/11/1}. Although the custody details provided by Dr Wright in this document were provided after service of Madden 1, COPA is not understood to have challenged them and they are consistent with Dr Wright's original 11 May 2023 Chain of Custody schedule at {M/1/778}, which also explained that the documents had been stored on third party devices.'* It is also said that Dr Wright re-emphasised this point during his oral evidence at **{Day 3/16/5} to {Day 3/16/21} and {Day 3/53/4}**. On this basis, the submission is made that '*evidence that his documents were accessed or even edited after the publication of the Bitcoin White Paper should not,* ***by itself****, lead the Court to conclude that they have been deliberately forged by Dr Wright*.' (emphasis added).

350. It is true that Dr Wright did emphasise this point in his oral evidence. However, by that point, Dr Wright was looking for ways to explain away the anomalies identified by the experts as indicative of forgery. Indeed, this point involves a certain amount of re-writing of history. I have reviewed his original Chain of Custody Schedule {**M/1/778-799**, letter of 11 May 2023 from Ontier} and it is true that Dr Wright repeatedly says that he was

not the owner of a particular hard drive or laptop. Instead, (most frequently) Lynn Wright or one of the companies which he owned (DeMorgan) is identified as the owner. The vast majority of the documents are identified as '*Drafted by Dr Wright*' or '*Drafted by Dr Wright, typed by Lynn Wright'*. If these were 'third party devices', they were third parties very closely associated with Dr Wright, and he is identified as the author and custodian for most of the documents. Furthermore, at that stage I understand that requests for intermediate custodian information were rejected as disproportionate.

351. The Chain of Custody information related to documents which Dr Wright had identified as his Primary Reliance Documents {**K/5**, Ontier letter of 4 April 2023} i.e. the documents on which he primarily relied to substantiate his claim to be Satoshi. Against that backdrop, it is in my view clear that, in the original Chain of Custody information, Dr Wright was representing each of these documents to be genuine and authentic, a representation also made by way of his production of these documents on disclosure, and his signed Disclosure Certificate. No qualification was hinted at, either on disclosure or in the Chain of Custody information.

352. It might be said that, at that stage, Dr Wright had no reason to investigate whether any changes had been made to his documents dating from 2007/2008/2009, especially since many of the changes relied upon by COPA and their experts as indicating forgery lay in metadata, changes which one would not see if simply opening a document to review its content (e.g. to confirm it was a draft of the Bitcoin White Paper).

353. Almost all of his Primary Reliance Documents were the subject of COPA's List of Challenged Documents {**K/8**, 30 May 2023}, along with almost all of the documents he produced on disclosure. Many documents were alleged to have been altered. For others, COPA clearly reserved their position on the basis that '*Context unknown to the Claimant, pending chain of custody and provision of further explanation*.'

354. From that point, at the very least, Dr Wright must have been well aware that the authenticity of a large number of his documents, including nearly all of his Primary Reliance Documents, was challenged.

355. The second set of Chain of Custody information {Schedule at **K/11**, 13 October 2023} was long and confusing. Much fuller information was provided. Overall this document represented a significant change in tack. Now it was suggested that numerous unnamed staff members might have altered documents. With the benefit of hindsight, it can be seen that Dr Wright laid the foundations for a number of his answers to the forgery allegations which were introduced later. These include: (i) identifying others as the owner of or responsible for particular data sources, including Lynn Wright, Ramona Ang, DeMorgan, Hotwire etc. and nChain; (ii) documents said to be drafted in Open Office and LaTeX, (iii) his inability to comment on the authenticity of a document because e.g. 'many parties had access to it or copied it from the shared servers from 2002 onwards' and 'upwards of 70 staff members from the various companies would have had access to this document on the respective companies' 'shared server'.

356. Overall, the Chain of Custody Schedule is internally inconsistent and unreliable, as demonstrated by **Madden2** and Appendices **PM43** and **PM44**. It also adopts a position which is at odds with previous chain of custody information (which simply presented Dr Wright as author and custodian).

357. Overall, the possibility of documents being accessed by other staff members cannot, in my judgment, account for all the indicia of forgery identified by the experts and which are set out in the various sections in the Appendix. However, this point has been taken into account in my assessments in the Appendix, to the extent appropriate.

358. More generally, the service of **Madden1** can be seen as a 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 gave rise to so many of Dr Wright's changes in story. In addition to the second set of Chain of Custody information, this also led to (a) 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 **Wright9** (Appendix A) and **Wright10**, which suggested that features of those systems could account for apparent signs of document alteration and tampering.

Alleged problems with Mr Madden's reliability as an expert witness

359. Counsel for Dr Wright submitted there were two main problems with Mr Madden's reliability as an expert witness which they suggested may have been the cause of three fundamental flaws in his analysis.

360. The first main suggested problem was that, although acknowledging that Mr Madden has worked as a computer forensic examiner for some years, it is suggested that he is not suitably qualified, on the basis it was alleged he had only a single formal relevant qualification (as an EnCase Certified Examiner) and no specific formal qualifications relevant to Citrix networks, VMware virtual machines or SANs, all of which are said to be particularly relevant.

361. I reject this suggestion. I very much doubt that formal qualifications are an adequate substitute for years of practical experience in forensic analysis, which Mr Madden undoubtedly has. So I was entirely satisfied that Mr Madden was suitably qualified to make the findings which he did in his various reports. As I said above, I formed the view he was a precise and careful witness and one who did not stray outside his area of expertise. Above all, this submission fails to recognise that most of Mr Madden's findings were agreed to by the experts instructed on behalf of Dr Wright. As for Dr Wright's contention that none of the experts were properly qualified (and only he was), it is notable that neither he in his evidence nor his Counsel in any submission provided any concrete example to substantiate this.

362. The second main problem was said to be more important: it was that Mr Madden's independence was undermined due to the way in which his expert reports were prepared. On this point, I have already set out, in paragraph 121 above, the applicable legal principles.

363. Lord Grabiner KC pointed to Mr Madden's explanation of the process (e.g. **Madden1** at [33]) but submitted that under cross-examination, a rather different picture emerged. He drew attention to the following points:

    363.1. That there had been at least 6-8 meetings between him and Bird & Bird.

363.2. That the drafting assistance appeared to have been extensive: see **{Day 16.121/5-22}**.

363.3. That he had not adopted the same approach when preparing his expert evidence in other matters.

363.4. That he failed to provide any coherent explanation as to why such an approach was necessary in the present case or why he could not have engaged a suitably qualified and independent assistant.

364. As I think Dr Wright's submissions on these points acknowledged, their validity is closely entwined with the alleged three fundamental flaws in his analysis. Before I address these alleged fundamental flaws, I should say something about the allegation that there was something inappropriate in the way Mr Madden's reports were prepared.

365. Based on my experience in Patent cases (conducting and trying them) and in view of the scale of the work required of Mr Madden (particular in preparing his enormous first report), I saw nothing at all wrong in the way his reports were prepared. Experts in Patent cases often work closely with solicitors, who guide and assist the expert, based on a recognition that, without such guidance and assistance, a suitable report would either not get written or would take an inordinate amount of effort and time. In particular, having a solicitor prepare a first draft of a section is not considered objectionable provided, of course, (a) it is based on matters already expressed by the expert (usually in a meeting) and (b) the expert reviews the wording carefully and makes any changes necessary so that it properly represents his considered evidence and opinion in the text adopted in the report which is served. Depending on the complexity of the technology and the issues, the preparation of a long expert report (albeit not as long as **Madden1**) may well involve more meetings than Mr Madden was involved in.

366. Having made those observations, I reserve my conclusion until after I have considered the three fundamental flaws alleged by Counsel for Dr Wright. These were explained as follows, and I identify them as the 'unjustified haste', the 'content' and the 'gap' allegations:

366.1. First, that on multiple occasions, Mr Madden had concluded with unjustified haste that a document has been dishonestly tampered with or altered, when other explanations were equally plausible from a technical perspective. It was submitted that this was clearly illustrated when he was cross-examined in relation to the following documents in COPA's list of 20 core forgeries: (a) **{ID_004013}** Handwritten BDO minutes **{L2/159}**; (b) **{ID_004019}** JSTOR Article – Tominaga Nakamoto **{L2/245}**; and (c) **{ID_000073}** Statistics assessment homework. The relevant details were said to be set out in Appendix 1.

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

366.3. Third, and most importantly, Mr Madden seems to have been unwilling to grapple properly with Dr Wright's complex IT environment, or with how that environment might have caused some of the digital anomalies on which he relied to reach his conclusions. In this respect, Mr Madden's analysis lacked rigour and was unconvincing.

367. On the first point 'unjustified haste', I will deal first with the three specific examples cited and then make some more general observations.

368. In relation to the BDO Minutes **{ID_004013}**, his 10-page analysis of the document is in PM5 **{H/31/1-10}**. From that analysis it is clear that Mr Madden reached his finding of manipulation in relation to this supposedly 2007 handwritten document after:

368.1. Receiving evidence from the manufacturer of the pad that the proof (in MS1 to the confirmation of Michael Stathakis & Lee Li dated 10 July 2023) from which the pad was created had first been created in 2009 and first shipped in 2012;

368.2. Putting to one side exhibit MS2 as dated from 2014.

368.3. Carefully inspecting the PDF file of the proof and checking its metadata in order to satisfy himself that the proof is an authentic document dating from 9 November 2009; and

368.4. He had carried out a painstaking examination of the proof against the document.

369. There are two further points to note:

369.1. First, Mr Madden clearly stated in paragraph 25 of Appendix PM5 various points on which he had not been able to form an opinion.

369.2. Second, Dr Placks agreed that the BDO Minutes had been manipulated **{Q/2/9}.** Mr Madden and Dr Placks agreed that their opinion about the authenticity of the document depended on whether Exhibit MS1 was the first ever proof of the notepad. Both experts agreed that there was no reason to doubt the authenticity of exhibit MS1.

370. The second example is the JSTOR article **{ID_004019},** analysed with **{ID_003830}**, in Appendix PM6, **{H/40/1-31}**}. Mr Madden only made his finding of manipulation after:

370.1. First, he had found visible signs of document alteration: misalignment of the key date figures which dated it to 2008.

370.2. Second, he had found an authentic version online which dated to 2015, which was otherwise identical and in which the figures aligned perfectly.

370.3. Third, he had exhaustively reviewed over 180 JSTOR documents, spot testing a sample (around 10%) of those for authenticity, and established that the footers used at different times had a consistent pattern and showed that the footer shown in **{ID_004019}** did not date from 2008.

371. A review of PM6 shows a painstaking analysis, all very clearly explained in minute detail.

372. In their Second Joint Statement, Dr Placks agreed that **{ID_004019}** was unreliable but did not go as far as to agree it was manipulated because (it seems) he thought the footer style in use in 2008 should be verified with JSTOR.

373. The third example is Dr Wright's MSTAT assignment **{ID_000073}**, which Mr Madden analysed in his Appendix PM38 {**H/145/1-17**}. As I found in section 6 of the Appendix, I found Mr Madden's analysis of this document entirely convincing. Furthermore I found no indication that it was done hastily or without due care.

374. On top of my consideration of these three examples, I add my consideration of the entirety of Mr Madden's work, explained in his six reports. I acknowledge that Mr Madden was put under time pressure to prepare his later reports, his Sixth Report in particular, and I noticed a slight unease on his part giving evidence about the MYOB Ontier Email allegations because there were indications he did not feel entirely on top of all the detail. Having said that, I concluded that his unease was not a reflection that his evidence was flawed in any respect, but a reflection of the care he wishes to take when presenting his analysis and when answering questions about it in the witness box.

375. Overall, I find the accusation levelled against Mr Madden that he reached conclusions with 'unjustified haste' to be absurd. I reject the first point.

376. The second point, regarding 'content', is, in my view, misplaced. Mr Madden did not need to be an expert in '*any of the multiple academic fields covered by Dr Wright's disclosed documents*'. As a forensic document expert, he was and is entitled to rely on passages of identical text and/or evidence of text edited away from the apparent original. I saw nothing inappropriate in his analysis of text/content.

377. The third 'gap' point was developed further and requires further discussion:

    377.1. First, it was suggested that 'this gap' in COPA's evidence '*may be the inevitable result of the unorthodox sequence and timing of the expert and factual evidence in this case'*.

    377.2. Second, that whatever the reason for 'this gap', '*the fact remains that none of the documents considered by Mr Madden was analysed on the machines or within the environments from which it was collected and no exercise was undertaken by Mr Madden to recreate the relevant IT environment (or parts of it*)'.

    377.3. Third, it was said that this matters because, as Mr Madden himself accepted, where the authenticity of documents is in question, it is prudent to analyse not just the documents themselves, but the environments in which they were authored and thereafter stored, as this can throw important light on their forensic analysis {fn: **{Day 16/11:15} to {Day 16/11:23**}}.

    377.4. Fourth, that this would have assisted, in particular, in the interpretation of timestamps, which Mr Madden agreed is inherently prone to difficulties that are well recognised by digital forensic professionals, such that relying on them to prove that a particular event occurred is not a sound approach. {fn: **{Day 16/12:11} to {Day 16/13:8}**. See, for example, Chow et al, *The Rules of Time on the NTFS File System,* at **{X/50}**, in which the authors explain that "*Temporal analysis on individual digital file[s] has been adopted since the evolvement of*

computer forensics. However, it is not evidentially secure to rely on the timestamps of a particular file to prove a particular event occurred at the corresponding MAC times" (p1, LH column), and (at p1, RH column) that "*since file timestamps can be altered inherently by batch operations such as automated tools scanning, previewing activities, etc, it is difficult to determine whether a particular file was accessed or opened explicitly by the user*."

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

377.5.1. A Creation Date may indicate that a document has been copied, or even "unzipped" from a zip file {accepted by Mr Madden at **{Day16/51:2**}.

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

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

377.6. Sixth, that the importance of analysing the authenticity of documents in the context of the environments in which they were created and stored must, as a matter of common sense and logic, be *a fortiori* where the relevant environment is a complex one, far removed from that of a standard home user or single machine.

378. The first and second submissions presuppose that there was a relevant 'gap' in COPA's evidence. For the reasons explained in this Judgment, I do not believe there was.

379. The second submission arises out of a point put to Mr Madden at the very start of his cross-examination to the effect 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). There are three main points to make in response:

379.1. First, of course this point was true but the attack was highly 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 **{M/1/805}** at para. 11.6 **{M/1/810}**. This was refused in Travers Smith's letter of 12 July 2023 **{M/1/951}** at paras. 23ff **{M/1/956}**, and that position was maintained thereafter, notwithstanding further mentions of this point in Mr Madden's reports. The fact remains that it was Dr Wright who could have supplied forensic images but he chose not to do so. It is also relevant to note that when Dr Wright was forced (by my PTR Order) to provide more data (in relation to the LaTeX files), they provided very strong support for the allegations already made. Accordingly, 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.

379.2. Second, in any event, the point was misplaced 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 the material he had. It seems likely

that access to the computing environments would only have helped him make further findings of anomalies (as his work on the BDO Drive showed).

379.3. Third, in the absence of Dr Wright supplying forensic images, it seems to me to be very clear that, as a practical matter, it would have been impossible for Mr Madden to have recreated Dr Wright's relevant IT environment. Furthermore, I am certain that any attempt to do so would have been a fool's errand – Dr Wright would always have been able to point out and would have pointed out some respect in which he asserted (whether truthfully or not) the attempt was deficient.

380. However, all these points beg the question as to whether the complexity of Dr Wright's IT environment is capable of explaining *all* of the apparent anomalies of any or all of the documents considered either in the body of this Judgment or in the Appendix.

381. To address this question, I must first set out the most important complexities relied upon. Although there is much more detail set out in Dr Wright's witness statements, the key elements were conveniently summarised in his Written Closing as follows (and I quote):

381.1. **'Rocks Clusters:** Dr Wright stated that he has been running Rocks Linux (an open-source distribution designed for building high-performance computing clusters) as a base system since 2002/2003. Dr Wright explained that "*A cluster is a group of linked computers that work together closely, making them appear as a single system. Rocks Linux is a specialized Linux distribution for building and managing high-performance clusters. A key feature of Rocks Linux is its ability to aggregate the resources of multiple physical servers into a unified, virtualised environment*." {Wright 10, paras 11 & 12 {E/31/4}.

381.2. **Virtual Machines:** The above cluster system was used to host a series of virtualised machines, essentially separate computers running within a single physical machine, each with its own operating system and applications. {*ibid.* paras 13-14}. As part of this, Dr Wright used VMware and Xen hypervisor, the latter being "*a process that manages the creation and operation of a virtual machine*" {Wright 10, para 18 {E/31/5}; Meiklejohn 1 para 120(d) {G/2/50}; Wright 9, App A para 2.2(4) {E/26/35}}.

381.3. **Citrix**: In addition to using virtual machines, Dr Wright stated that he accessed servers remotely using Citrix {See e.g. Wright 9, App A para 2.2(4) {E/26/35}; Wright 8 para 3 {E/23/3}}. Citrix is software that enables users to work from remote locations using computer virtualisation {Wright 9, App A para 2.2(4) {E/26/35}}. Dr Wright also explains that he used Storage Area Network systems alongside Citrix, and that these "*offer high performance and flexibility in handling large volumes of data, which is accessible to various users across the network*" {Wright 10, paras 84, 86}.

381.4. **Access Times**: Dr Wright explained that in his SAN and Citrix virtual environments, access times on files were often not updated as a deliberate performance optimisation strategy {*ibid,* para 142}.

381.5. **Symbolic Links**: Dr Wright stated that he made use of symbolic links, which act as a window or portal to a folder somewhere else on an IT system. Dr Wright said that he used symbolic linking to connect areas in his Windows systems to areas

in his Linux systems, to enable him to manage and access his files across those systems {*ibid,* paras 35, 37, 38}.

381.6. **Group Policies:** Dr Wright explained that organisations in which he worked enforced various group policies throughout their IT systems, and in particular that nChain applied a policy that enforced the use of a standard 'normal' Microsoft Word template and specified applications that were to be deployed throughout the network {Wright 9, App A paras 2.17-2.20 {E/26/43}; and Wright 9, App A para 2.37-2.38 {E/26/47-48}}. Such applications included both Grammarly and Math Type {Wright 9, App A para 2.38 {E/26/48} and 2.57, last sentence {E/26/53}}. Dr Wright added that the relevant group policy was implemented by using the Group Policy Management Console on windows systems {Wright 9, App A paras 2.19-2.20 {E/26/43}}.

381.7. **Collaborative Working**: Finally, Dr Wright explained in his witness statements, and in oral evidence, that staff in the organisations with which he has been involved worked collaboratively and shared documents, and that hundreds of those staff members had accessed and used his documents over many years {See e.g. Wright 9, para 2.55 {E/26/52}; Wright 4, para 6(c)(iii) {E/4/5}. See also {Day 2/136/4}; {Day 2/140/4}; {Day 3/19/11}; {Day 4/35/11}; and {Day 4/43/1}}.'

382. Counsel for Dr Wright stressed that there was no challenge to his evidence on these points and that Mr Madden accepted they were technically plausible arrangements. This was said to be important '*because, as Mr Madden also accepted,* many *of the alleged indicia of forgery that he and COPA have relied on in this case could just as readily have been caused by that environment, or those working practices (or a combination of both).*' (my emphasis – 'many' is an exaggeration, 'one or two' is nearer the mark).

383. Furthermore, Counsel for Dr Wright stressed that Mr Madden had accepted the following technical propositions. Here I quote the submissions made, with the footnote references inserted:

383.1. 'It is possible for an organisation to engineer the Normal.dotm template "*to contain…pretty much anything you want*" {Day 16/31/25}, including matters such as the use of **specific fonts** and the automatic running of certain functionalities or add-ins, such as **MathType** {Day 16/31/24} and **Grammarly** {Day 16/40/17} software. Mr Madden also agreed that that it is possible for a system to be configured in such a way that default styles and customisations in the Normal.dotm template are automatically applied to all Microsoft Word documents opened by a user, including pre-existing documents, and for such changes to be retained by both new and existing documents once they are saved (whether actively or automatically) {Day 16/35/7} to {Day 16/37/12}.

383.2. What may appear to be an **anomalously long edit time** recorded in a MS Word document's metadata can have been caused by that document having been accessed by a user on a remote server during a Citrix session, and the relevant Citrix session then being disconnected without the Word document being closed {Day 16/25/21} to {Day 16/31/14}.

383.3. If Dr Wright's working practices involved creating and working on multiple files across multiple computers that accessed remote storage devices, that could explain different documents having **overlapping edit times** {Day 16/48/3} to {Day 16/49/2}.

383.4. Where a file is created by copying an existing file, including by using the Windows command XCopy, this will typically cause the **Created timestamp recorded in the metadata of the new file to post-date its Last Modified timestamp** {Day 16/45/16}. Although this would also typically cause the Last Accessed timestamp of the destination file to be updated alongside the Created timestamp, many program, file system and operating system settings can affect whether the former timestamp will in fact be updated in that way, and indeed it is possible for a system to be configured so as to **disable updates to the Last Accessed timestamp {**Day 16/45/16} to {Day 16/46/10}. Mr Madden suggested in oral evidence that this would not affect the destination file, but oddly he had not tested this for the purposes of these proceedings, even though COPA knew that the behaviour of the Last Accessed timestamp following a file copy was in issue {Day 16/46/14} to {Day 16/47/13}.

383.5. Where **multiple symbolic links are created to a single file**, it is possible for **complications to arise** as a result of changes made to the file across a network Wright 10 para 42 {E/31/8-9} and {Day 16/21/16}.'

384. In relation to these points:

384.1. The critical element of the first point is that the file once opened must be saved (either manually or automatically). If the Word document is merely accessed and not saved afresh, this point has no application.

384.2. I acknowledge that persistence in Citrix systems is a possible explanation for what appear to be very long edit times.

384.3. In relation to the third point, *if* that is really how Dr Wright worked, then it might explain overlapping edit times alone.

384.4. I have taken into account these possible effects of the use of XCOPY.

385. In Closing, Counsel for the Developers highlighted an example which involved Dr Wright's allegation that Citrix persistence and his use of XCOPY accounted for (some of) the anomalies relied upon as indicating forgery. The document in question was **{ID_000258}**, Economic Security.doc which I have addressed in section 31 of the Appendix.

386. The detailed analysis in Mr Madden's Appendix PM29 shows that Mr Madden analysed both external OS/file property metadata and the internal metadata. As he pointed out, the total time difference between the indicated Created Date and the Last Modified Date (both in 2008) was 2,594 minutes or 1 day, 19 hours 14 minutes. The MS Word total Edit Time was much longer, recorded as 83,165 minutes or 57 days 18 hours 5 minutes.

387. As Counsel pointed out:

387.1. The use of XCOPY would only affect the external metadata, as the experts agreed (see e.g. **Placks2, [8.05] {I/6/13}**).

387.2. Persistence in a Citrix environment might explain a long time period between the Created and Last Saved Dates but was unlikely to explain the inconsistency between those dates and the edit time.

388. To establish that persistence was not a valid excuse, Counsel turned to another example document: **{ID_004516}**, which was in COPA's original list of additional 50 forgery allegations but which could not be pursued due to my PTR Order. It had been fully analysed by Mr Madden. Its internal metadata showed a difference between Created and Last Saved Dates of 1 day 17 hours, back in November 2002, but it had a recorded edit time encoded in the document. Mr Madden and Dr Placks were able to explain this. If the encoded edit time is treated as a positive number, it is 4,287,839,314 minutes i.e. an impossible edit time of over 8,000 years **{H62.1}**, whereas if it is treated as a negative number it decodes to -7,127,982 minutes or 13 years, 7 months and 4 days, albeit expressed in the negative indicating an unusual negative time shift **{H/62/21}**. Dr Placks agreed the 'two's complement conversion' of the edit time **{I/6/33}.** He also agreed the presence of the Grammarly timestamp from 02.06.2016 identified by Mr Madden in **PM9, [79]** which was 7,127,922 minutes after the Last Modified Timestamp, an approximately 60-minute difference, which could be accounted for by the time which Dr Wright spent making his edits. Both experts agreed the Last Modified timestamp had been manipulated.

389. In practical terms, these data can be explained by the fact that the document was created with the computer clock set to 11 November 2002 and saved and closed. It is then opened with the clock set to 2 June 2016 and edits are made using Grammarly, but the user then realises the wrong clock date is in use, so re-sets the clock back to 11 November 2002. That process is responsible for creating the long negative edit time.

390. To conclude the points on **{ID_000258}**, the experts agreed the document had been manipulated in their first Joint Statement **{Q/2/6}** and maintained that view in their second Joint Statement **{Q/4/6}** on the basis that nothing said by Dr Wright had caused them to change their minds. As I point out in section 31 of the Appendix, there were other clear indicia of forgery, as there were for all the other documents in the Appendix.

391. Reverting to the submissions made by Counsel for Dr Wright, the ultimate end point of them was the submission that I should not conclude that a document has been forged simply on the basis that it contains timestamps, fonts and/or versions of software that post-date the date on the face of the document.

392. I have not done so.

393. Furthermore, if there had been just one or two allegedly forged documents in respect of which these were the only indicia, this case might look very different. However, these are not the only indicia, and furthermore, there are a large number of allegations of forgery. It seems to me that once my findings of forgery attain a critical mass (as I find they have done), those findings provide support for other allegations where there may be fewer indicia. The converse is also true: if I had found a number of Dr Wright's documents did genuinely date from 2007/2008, his points about his computer environment might well have carried much greater weight. However, if I have found that

Dr Wright has clearly forged a large number of documents which are said to pre-date the release of the Bitcoin White Paper in order to support his claim to be Satoshi, why should I be slow to find forgery in relation to other documents which have the same aim and which also share indicia of forgery? As I have said, the evaluation of all these allegations is an iterative process.

394. On these points, it may be noted that my answer to Dr Wright's own submission (in paragraph 391 above) provides a negative answer to the question I posed at paragraph 380 above.

395. I can now return to the challenge made to Mr Madden's reliability as an expert witness. This challenge was a bold submission in view of the following:

    395.1. Only a tiny proportion of Mr Madden's very detailed analysis was challenged in cross-examination. Indeed his cross-examination was considerably shorter than the time estimate provided. I have addressed the more general points taken by Dr Wright (above, in the following sections and in the Appendix) and none of them deflect any of the allegations of forgery.

    395.2. All or very nearly all of Mr Madden's conclusions were agreed by Dr Placks and Mr Lynch. In other words, there was effectively no expert evidence to contradict Mr Madden's conclusions.

    395.3. The only contrary evidence came from Dr Wright and his points have been considered in the Appendix. Dr Wright was unable to deflect any of the allegations of forgery. Furthermore, far from Mr Madden being an unreliable witness, Dr Wright established himself very firmly as a completely unreliable witness.

396. In conclusion, I reject any suggestion that Mr Madden was an unreliable witness. In my view, he plainly adhered to his duties as an expert witness and I have full confidence in the evidence he gave. Furthermore (and reverting to the point I discussed in [365] above), due to their extensive experience in Patent litigation, I acquit Bird & Bird of any charge that Mr Madden's reports were prepared in an inappropriate manner. So too, Mr Madden. I am very grateful to him for all the work he did in this litigation.

Common features of Dr Wright's explanations for the forged documents

397. I can now return to make some general points about the various explanations put forward by Dr Wright. In general terms, his explanations given for inauthentic or forged documents in his original disclosure largely rested on computing environment(s). By contrast, as can be seen from the Appendix, for most of the allegations of forgery relating to the Additional Documents, the explanation was that he was hacked by various third parties. In this section I concentrate on the explanations for documents in his original disclosure.

398. A notable feature of Dr Wright's explanations in response to the allegations of forgery or inauthenticity was that his explanations were only produced after he had been found out. Given Dr Wright's avowed expertise in forensic document examination and IT more generally, it is surprising that he repeatedly produced key Reliance Documents for a

series of important legal cases without noticing serious anomalies in them. Examples of his professed expertise were as follows:

> *"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 *transcript for 14 September 2022, internal p71* **{O2/11/19}**.)
> *"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." (**Wright10,** [6]* **{E/31/2}**)

399. Despite this supposedly unparalleled expertise, his case must be that either (a) he failed to notice any of the myriad problems with his documents pointed out in **Madden1**, or (b) he noticed some, but chose not to mention them.

400. 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 numbered sections in the Appendix, but the main responses can be classified as follows:

    400.1. <u>False technical excuses / technobabble</u> – 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 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 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.

    400.2. Mr Madden gave clear evidence disputing Dr Wright's points, both in **Madden4**, **[155-162] {G/6/51}-{G/6/55}**, and in his oral evidence {see, in particular **{Day16/35:19} - {Day16/38:11}**; **{Day16/125:7} - {Day16/125:18}}**. Dr Placks and Mr Lynch agreed with Mr Madden on these issues in their respective joint reports {**{Q/4/6} at [8]**; **{Q/6/3} at [9]}.** 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 these matters. Dr Wright's answers betrayed a consistent effort to "*blind with (computer) science*". Many of his answers were extremely fragmented and scattered references to computer systems seemingly at random.

    400.3. <u>Deliberate forgery by others</u> – There is a long list of those whom Dr Wright blamed for his disclosed documents bearing signs of forgery. In a number of instances 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 numbered sections below, these theories were uniformly unsupported by any evidence. Many were also implausible and failed to account for the document appearing to 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.

400.4. Accidental alteration by others – A common refrain of Dr Wright's evidence (both in **Wright9**, **Wright10** and **Wright12**, and in cross-examination) 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 explained 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, 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. This was a remarkable retreat from his original position that he could prove his claim to be Satoshi by authentic evidence of precursor work, but 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, by of examples, from 15 years previously.

400.5. In a similar vein were his claims 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 {see **Lynch1 at [123-128] {I/5/37}**; Joint Statement Madden/Lynch at **[9] {Q/6/3}},** and Dr Placks {see Joint Statement Madden/Placks at **[8] {Q/4/6}**}, as well as by Mr Madden {see **Madden4** at **[155-162] {G/6/51}**}.

400.6. 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 sections 6, 20 & 24 of the Appendix for **{ID_000073}**, **{ID_000536}** and {**ID_000254}**

401. Despite the length of the statements and the elaborate account of Dr Wright's past IT systems, I agree this was speculation on effects which *might* occur, without any supporting technical evidence. In general terms, the experts for both parties disputed that these effects would occur as suggested. If and insofar as Dr Wright wished to establish that features of his IT systems in fact accounted for particular signs of alteration, his Counsel would have needed to have put specific points to Mr Madden (although it is difficult to see this being done with any foundation, given the joint expert evidence). However, even if I assume Dr Wright did work in the way he asserted, I remain of the view that the features of his systems cannot account for all of the many and diverse signs of forgery I discuss in the Appendix. In addition, there are other non-technical indications of forgery which cannot be explained away by reference to Dr Wright's IT set-up.

402. The related issue with Dr Wright blaming his system architecture now is that he never mentioned this topic before service of **Madden1**. This is surprising in view of his vaunted expertise. One would have expected him to say, when serving his list of Primary 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*" {RFI Response 66 at **{A/13/23},** 11 September 2023}.

403. That response was given *after* service of Madden1 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 **Madden1**. If Dr Wright really did have the expertise in digital forensics which he claims, then even an initial read of **Madden1** 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 findings which Dr Wright now seeks to attribute to his operating systems, and others besides.

404. There is, of course, a very stark contrast between his claim that the operating systems were irrelevant and what became a central theme in his attempts to deflect the allegations of forgery made in October 2023 (and as addressed in Appendix B to **Wright11**). COPA submitted that, 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), and I have no reason to doubt that submission.

405. COPA had further objections to Dr Wright's attempts to attribute signs of document manipulation to the unusual effects of his operating systems.

    405.1. First, that Dr Wright never adduced any independent expert evidence, or clear documentary evidence, to support his assertions about the effects of his systems. Despite having **Madden1** since 1 September 2023, Dr Wright 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 **Wright11** (as well as 13 other statements since October 2023) had the time to identify experts.

405.2. Second, COPA submitted there was 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 {a Slack post he made attaching his forged 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}}** and Dragon Dictate Legal {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": **Wright11** at **[278] {CSW/1/51}**. But even that was wrong: **{P1/20/13}** and **{G/9/48}}**. 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.

405.3. Third, COPA pointed out that Dr Wright's accounts often also involved computing environments being used in very unusual ways. For instance, he sought to account for very long edit times by saying that he would leave Citrix sessions open for extraordinarily long periods, sometimes of more than a year in length. In any event, Mr Madden never used this as a freestanding reason for finding a document inauthentic {see **Madden1**, Appendix **PM24**, **[35] {H/116/12}**; **Madden2**, **[47b] {G/3/19}**}. Dr Wright 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).

406. In view of the general unreliability of Dr Wright as a witness, plus the fact that he had no independent expert evidence to support his assertions about the effects of the relevant computer environments, I agree that they carry very little weight. Furthermore, to the extent that any of his assertions had some validity, I am satisfied Mr Madden took account of them.

B. The Forgery Allegations in relation to the Additional Documents.

407. COPA's Additional Forgery Allegations were made following the disclosure of, and my permission to Dr Wright to rely on, the Additional Documents. In relation to the LaTeX files, Dr Wright's submissions were set out in section IV of his Written Closing. I consider those submissions below. In relation to the remainder (i.e. the BDO drive image and the 17 other documents in the Samsung drive alleged to be forgeries), Counsel for Dr Wright relied on the submissions made in relation to his original disclosure, and indeed, I took that into account when considering those submissions, above.

408. However, it is relevant to note that the BDO Drive image was relied upon as a time capsule dating from 31 October 2007.

409. Nevertheless, Counsel for Dr Wright relied on some additional points. First, the alleged hack by Mr Ager-Hanssen prior to his dismissal from nChain, which I discuss below. Second, they pointed out that Dr Wright took issue with the evidence of Mr Hinnant and Professor Stroustrup relating to **{ID_004712}** and **{ID_004713}**. I have considered these submissions in the Appendix, see section 33.

410. So far as the alleged hack by Mr Ager-Hanssen is concerned, Counsel for Dr Wright submitted the evidence was as follows, and I quote (although the underlining is my added emphasis):

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

    410.2. On 1 December 2023, Dr Wright set out his account of his discovery of the Samsung Drive. At paragraph 22, he explained that after finding the drive at his home on 15 September 2023, he plugged it into his laptop to ensure that it was working{E/20/7}.

    410.3. On 11 December 2023, Dr Wright explained in **Wright 7** that tweets and photographs subsequently posted by Mr Ager-Hanssen on 5 October 2023 revealed that the latter had obtained access to the BDO Drive, because those photographs revealed the contents of the BDO drive being displayed on a laptop that was not his {Wright 7, paras 12-14 {E/22/6-7}.

    410.4. In **Wright 14**, Dr Wright stated his belief that Mr Ager-Hanssen had access to his company laptops and files from around May 2023 {E/33/5}.

    410.5. When the Additional Forgery Allegations were put to him in cross-examination, Dr Wright repeatedly denied them and maintained that they must have been caused by whomever had obtained unauthorised access to his systems in 2023 {Day 5/23} to {Day 5/121}. He confirmed orally, when asked, that he had left the Samsung Drive connected to his laptop for some time after checking that it worked, and that he did not recall having logged out of it before stepping away from it {Day 5/36}. Notably, COPA has not challenged Dr Wright's account of his systems having been hacked.

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

> Samsung Drive when it was connected to Dr Wright's computer, and in turn to the BDO Drive {Day 16/84/17} to {Day 16/88/5}.'

Mr Christen Ager-Hanssen

411. I introduced Mr Ager-Hanssen earlier (see [63]-[67] above).

412. Although Dr Wright asserted in certain answers in cross-examination that there was a conspiracy against him involving COPA and Mr Ager-Hanssen, COPA emphasised in their Closing Submissions that they have had nothing to do with Mr Ager-Hanssen and merely relied on material publicly available due to his disclosures. For all the reasons set out in this Judgment (see the next section in particular), I am satisfied this alleged conspiracy was another lie from Dr Wright in his attempts to deflect responsibility from his own forgeries.

413. I should add, for the avoidance of any doubt, that I have not relied or placed any weight on the reported conclusions of either Mr Ager-Hanssen or Mr Ayre. I have reached my own conclusions based only on the evidence and submissions I received during the Trial, albeit, as indicated above, I have also had regard to events which occurred during my case management pre-Trial.

Dr Wright's various allegations that forged documents were planted

414. At this point it is appropriate to draw together the various allegations which Dr Wright made that various forged documents were planted by Mr Ager-Hanssen or some other 'Bad Actor'. As I understand Dr Wright's assertions, he makes them on the basis that the documents in questions are forgeries, because if they were not, he would continue to rely on them as supporting his claim to be Satoshi. So the issue is whether the person responsible for the forgeries in question was Dr Wright or some third party or parties, with, presumably, a grudge against him.

415. I address the allegations of planting by others in sections 1, 2, 13, 17, 35 and 40 in the Appendix, but undoubtedly the allegation has the greatest scope in section 2 concerning BDOPC.raw. In his oral closing submissions, Counsel for COPA addressed this principal allegation, submitting it was both absurd and incredible. He made the following six points:

415.1. First, he drew attention to an inconsistency in Dr Wright's evidence:

415.1.1. In **Wright5 [22], [28]-[30]** {served 1 December 2023}, his evidence was to the effect that he had simply connected the 2 hard drives to his laptop to check they still worked, but did not access the BDO Drive on the Samsung drive or any files on either hard drive. He mentioned one qualification, in **[29]** that Stroz Friedberg, on examining the BDO Drive, had identified '(i) metadata suggesting that the recycle bin on the Samsung Drive (which sits on the Samsung Drive outside the BDO Drive, which has its own recycle bin) was emptied in September 2023, (ii) the ordering of files added to the recycle bin and (iii) transactional log files within the BDO Drive with a created, modified and access date of 17 September 2023'. In **[30]**, he explained these points by the software systems and processes that he habitually uses which, he said, may have

caused the recycle bin on the Samsung Drive to have been automatically emptied when it was connected. He also said it was possible that one of these systems or processes might have opened the BDO Drive automatically, when he checked that the Samsung Drive was working. The import of all of this was to provide reassurance that no material change had occurred to the BDO Drive.

415.1.2. Counsel contrasted that account with what Dr Wright said in cross-examination to the effect that, for some inexplicable reason, he had left the BDO Drive connected to his laptop for the days which followed, providing the opportunity for some 'Bad Actor' to plant the forged documents on the BDO Drive when hacking into his computer.

415.1.3. There are a number of reasons why his latter account is implausible. First, it must have been clear to Dr Wright that the provenance and chain of custody in relation to this BDO Drive would be closely scrutinised. This is confirmed by his careful evidence set out in **Wright5**. Second, leaving the BDO Drive connected would have been a breach of basic security principles, well-known to a professed IT security expert such as Dr Wright. Third, it is inconsistent with his evidence in **Wright5**.

415.2. Second, Dr Wright's account presupposes that the 'Bad Actor' (whether Mr Ager-Hanssen or one of his associates) was able to identify and taint the 71 critical new reliance documents. The alternative explanation, that the Bad Actor created those 71 documents themselves and planted them, is highly implausible because Dr Wright would not have recognised them as his, and would not have relied upon them.

415.3. So the Bad Actor had to work out which were the new documents which Dr Wright himself would identify as his new critical reliance documents which, we are told, was done on the basis of a set of bespoke search terms and then careful review of the content. So on this hypothesis, the Bad Actor must have found those documents, identified those that might actually support Dr Wright's claim to be Satoshi, and then set to work on them, carrying out a very elaborate set of editing actions to give the impression that those particular documents had been added in mid-September 2023. They would have been working on a drive which contained a huge number of documents, with no guide to help them, because Dr Wright's account is that between 15 and 20 September 2023, he hadn't gone into the BDO Drive, let alone examine its contents or tell Mr Ager-Hanssen all about the critical reliance documents.

415.4. As Counsel for COPA submitted, the Bad Actor's success would have been quite remarkable, because, on this hypothesis, he/they managed to identify every single new reliance document which was later identified and relied upon by Dr Wright as supporting his claim to be Satoshi.

415.5. Third, on top of the ingenuity described so far, the Bad Actor had to insert content which was anachronistic to 2007/8, and then edit out that content. They had to seed the BDO Drive with the edited versions. They then had to delete the drive which contained the anachronistic versions, InfoDef09.raw. All that had to have been done in just a few days, but in the hope that Mr Madden would, in due

course, (i) be given access to the BDO Drive (something which Dr Wright made efforts to resist) and (ii) be able to recover from the deleted InfoDef09.raw the prior versions of the documents. If Mr Madden had not been able to do those two things, all this work would have been for nothing.

415.6. Fourth, the Bad Actor had to have had some documents ready for planting – at least King.rtf and King2.rtf – by 12 September 2023, three days before Dr Wright says he found the Samsung drive in a drawer.

415.7. Fifth, the hypothesis assumes that the Bad Actor must have been extremely fortunate: not only did Dr Wright proceed to nominate the documents they had tainted as his new critical reliance documents, but he failed to notice that any of them had been edited. Instead, he studied the documents and provided the instructions to Shoosmiths to create a detailed schedule of the 97 new documents, **{P/10/1-7}** annexed to **Field1**.

415.8. Sixth, as Counsel for COPA pointed out, there is no evidence of this alleged hack. Indeed, the principal point said to evidence a hack (see the submission at 410.1 above) is factually incorrect. The images published by Mr Ager-Hanssen were not screenshots, they were photographs of a monitor. Although they are described as screenshots in **Wright3 [18]**, the exhibit CSW4 clearly contains photographs of what is shown on the screen of a Lenovo laptop **{E/3/29-33}**. The photograph on p33 shows 3 windows: on top is a Google search for 'quill 01916 before 2010' (the text is somewhat difficult to make out); underneath that is a Windows directory window, and the foot of the window shows 'Assignment-2.doc' selected; underneath that is a window with some file open from the BDO Drive but with browsing history displayed – again most of the text is unclear but one can see, at the end, 'the timestamp proves that the data must' (a phrase in section 3 of the Bitcoin White Paper). On p32, the photograph shows the whole of the Lenovo laptop screen, with the top window being a file search of the term 'bitcoin' on the BDO Drive and the second window being the same Google search as p33. On p31, the top window is from an internet browser which has navigated to a page concerning the 'Quill A4 Planner Pads Meeting Minutes 50lf'.

415.9. Counsel for COPA pointed out that these photographs show that Mr Ager-Hanssen was able to take photographs of a screen showing the BDO Drive being accessed and, in some cases, Dr Wright's browsing history in mid to late September i.e. before Mr Ager-Hanssen turned against Dr Wright and was sacked from nChain. He suggested these photographs were taken at a time when Dr Wright wanted to give Mr Ager-Hanssen access to material to secure his continued support. He pointed out that Dr Wright sent Mr Ager-Hanssen a photograph of a document on screen (subsequently disclosed as a LaTeX file but not the pdf version shown on screen), apparently on 5 September, accompanying messages saying 'the encrypted drive' ; 'has everything'; '4 million pages' etc. **{P/18/11}**. The point being that, at this point, Dr Wright was actively collaborating with Mr Ager-Hanssen.

415.10. The distinction between a screenshot and a photograph of a screen may appear slight but it is of some significance. The ability to take a screenshot is more consistent with control over the computer itself, whereas the ability to take a photograph of what is shown on the screen is less consistent with control. Further,

the sending of a photograph of a screen by Mr Ager-Hanssen is inconsistent with a hack.

416. The only other point I need address from Dr Wright's submissions quoted at paragraph 410 above is the submission that COPA did not challenge Dr Wright's account of being hacked. Counsel for COPA responded by submitting this was a bad point. I agree. As Counsel submitted, COPA did not have a positive basis to say what Mr Ager-Hanssen did or did not do, but what was put to Dr Wright repeatedly was that he was responsible for the editing and falsifying of the BDO materials.

417. The final point to make is that the notion that some Bad Actor was responsible for the forgeries of documents on the BDO Drive does not sit well with the clear positive evidence (which I address in the next section) that during September 2023, Dr Wright himself was creating the LaTeX documents. Indeed, in his answers on Day 5 when being cross-examined about two particular LaTeX files – LPA.tex and LP1.tex – Dr Wright asserted that these documents were planted by Mr Ager-Hanssen or someone associated with him **{Day5/86:14}**. I have addressed that assertion in the context of the detailed evidence on those two documents in section 17 of the Appendix. That detailed evidence demonstrated, as I found in section 17, that these two documents were forgeries, and I am entirely satisfied they were forged by Dr Wright himself.

418. Overall, the notion that a Bad Actor was responsible for the forgeries on the BDO Drive is literally *in*credible. It would depend on multiple bizarre coincidences, the combination of which is completely implausible.

C. The Ontier Email Forgery Allegation

419. I have addressed the points made by Counsel for Dr Wright in section 40 in the Appendix.

D. The LaTeX documents

An outline of Dr Wright's position in closing

420. I have already discussed how Dr Wright portrayed the critical importance of the LaTeX documents (and the other Additional Documents) in his evidence for the PTR (see [79] above). COPA's evidence for the PTR suggested that Dr Wright's case on these documents faced some difficulties which I concluded it was not appropriate to decide on that occasion. It is fair to say that the case on these documents has been going downhill ever since Field1 and Wright6 were served.

421. In marked contrast to the case put at the PTR about the critical importance of these documents, in closing Counsel for Dr Wright submitted they have proved to be far less important, for three reasons:

    421.1. First, it was said that Mr Rosendahl accepted that the Bitcoin White Paper could in principle have been produced using LaTeX, albeit using non-standard versions of the software available at the time, but that he also explained that the Bitcoin White Paper had features indicating it was produced using OpenOffice software. It was further said that '*Dr Wright's evidence is that he used both OpenOffice and LaTeX to produce the Bitcoin White Paper, which is consistent with Mr Rosendahl's findings. Accordingly, the evidence on how the Bitcoin White Paper*

*was produced is **consistent** with Dr Wright being Satoshi Nakamoto, but it does not of course establish that he **is** Satoshi Nakamoto*.'

421.2. Second, it was said that '*the relevance of the White Paper LaTeX Files to the Identity Issue depended on Dr Wright establishing two propositions: first, that the White Paper LaTeX Files can be compiled into the Bitcoin White Paper; and second, that it is practically impossible to reverse engineer the White Paper LaTeX Files from the publicly available Bitcoin White Paper. If **both** propositions were established, then it would not matter that the White Paper LaTeX Files do not (expressly on Dr Wright's case) date from before the release of the Bitcoin White Paper. In the event, however, Dr Wright accepts he has not established the first proposition (not least because it has not been possible to recreate the LaTeX environment that Dr Wright says he used to produce the Bitcoin White Paper). In these circumstances, the White Paper LaTeX Files are not probative of the Identity Issue based on the evidence available to the Court*.'

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

422. Accordingly, by the time of the written closings, Dr Wright's case on the LaTeX documents had retreated to this:

422.1. First, it is now submitted that Dr Wright does not need to prove a positive case that the Bitcoin White Paper was created using LaTeX to succeed on the Identity Issue, although it is acknowledged that he does need to resist a negative finding that LaTeX was **not used**, even in conjunction with OpenOffice in the manner asserted by Dr Wright.

422.2. Second, in order to resist such a negative finding, Dr Wright's case now hangs on the proposition that Mr Rosendahl gave undisputed evidence that the Bitcoin White Paper *could* have been produced using LaTeX.

422.3. Third, Counsel for Dr Wright submitted that the Court cannot safely reach the conclusion that LaTeX was not used in the creation of the Bitcoin White Paper.

423. On that third point, I disagree. In my judgment, the evidence is overwhelming that LaTeX was not used to create the Bitcoin White Paper. In particular, I reach the clear conclusion that the LaTeX files were a recent invention, created by Dr Wright in September 2023 as a key part of his response to **Madden1**. The detail which established that conclusion is set out in this section.

424. The Closing Submissions made by Counsel for Dr Wright on this point divide into two broad parts. The first part is a convoluted explanation which seeks to contend that, from the wreckage of what remains from the high point of the evidence in **Field1** and **Wright6**, Dr Wright still has a point. It is not necessary to set out all of this convoluted explanation. It is adequately summarised in the proposition at sub-paragraph 422.1 above. The second part seeks to persuade me of the very fine point which remains which is that because Mr Rosendahl gave evidence that the Bitcoin White Paper *could* have been produced using LaTeX, I cannot safely reach the conclusion that LaTeX was not used in the creation of the Bitcoin White Paper.

425. As will be seen, a relatively succinct answer can be given to this point. However, it would be remiss of me to leave out of account the whole LaTeX story, because the story provides a prime example of what became a familiar sequence: (a) Dr Wright produces documents in respect of which it is suggested, either implicitly or explicitly (and as regards the LaTeX files, with *certainty*), that they prove he is Satoshi; (b) analysis of the documents suggests they cannot pre-date the Bitcoin White Paper; whereupon (c) Dr Wright maintains they are genuine but his story changes; and (d) when seeking to maintain his position under cross-examination, the story changes further and can only be supported by yet further lies from Dr Wright.

E. The development of the case based on the LaTeX files

426. This section is largely based on a section from the Written Closing Submissions from Counsel for the Developers, after I had checked the numerous references provided. It involves considerable detail, but in broad terms, the development proceeds through the following stages:

    426.1. First, the '*before*' stage: it is important to note that, despite Dr Wright having numerous opportunities to mention that he had created the Bitcoin White Paper using LaTeX, but, more importantly, the notion that he had a LaTeX file which produced an 'exact replica' of the Bitcoin White Paper, such that mere possession of the file proved he was Satoshi, no mention of LaTeX was made in these proceedings until October 2023, or in any of the previous sets of litigation involving his claim to be Satoshi.

    426.2. Second, the '*tease*', namely what was said the LaTeX files established in Dr Wright's evidence for the PTR, followed by the '*reveal*', the provision of a compilation of his version of the Bitcoin White Paper (from LaTeX) on 13 December 2023.

    426.3. Third, the *'(partly failed) cover up'*, in which the contrast is drawn between the fragmentary information made available concerning Dr Wright's Overleaf account and Dr Wright's efforts to resist the provision of metadata.

    426.4. Fourth, what Counsel for the Developers submitted was inescapable evidence of forgery of the LaTeX files by Dr Wright.

The 'before'

427. As Counsel for the Developers submitted, despite the fact that Dr Wright had either given evidence or an account of his authorship of the Bitcoin White Paper no less than four

times, he did not mention LaTeX at all until after the service of **Madden1** on 1 September 2023.

428. The four (or more) previous occasions on which one might have expected Dr Wright to have mentioned that he drafted the Bitcoin White Paper using LaTeX, yet no mention of LaTeX was made, are:

428.1. when he was deposed, examined-in-chief and cross-examined in the *Kleiman* proceedings, notwithstanding that he gave evidence about his supposed authorship of the Bitcoin White Paper;

428.2. in his lengthy Amended Reply in the libel proceedings brought by Dr Wright against Mr McCormack, which directly addressed the question of whether he wrote the Bitcoin White Paper. On this point, reference was made to (i) Dr Wright's Amended Reply in those proceedings at paragraphs 13 et seq **{L16/342/14}** and (ii) that Ontier, who represented Dr Wright in the claim, have subsequently confirmed that Dr Wright did not tell them about the so-called White Paper LaTeX Files: **{AB-A/5/10}**.

428.3. in his lengthy evidence given in *Granath* in Norway on 14 September 2022, which included evidence about the way in which he had supposedly composed the Bitcoin White Paper from handwritten form to the printed page: see **{O2/11/9}** (internal transcript pages 29-31); or

428.4. in his first witness statement in these proceedings, dated 28 July 2023, notwithstanding that his statement included a 2½ page section **{Wright1 [86-99] {E/1/17}}** headed "*Writing and sharing the White Paper*" and purporting to describe the drafting process.

429. As far as I am aware, the first mention of LaTeX came in Dr Wright's second Chain of Custody schedule, served on 13 October 2023, followed by a brief mention in **Wright4**, served 23 October 2023, where, at **[6.c] {E/4/5}**, he said that the development of the Bitcoin White Paper involved a "*complex workflow utilising various software platforms, including LaTeX, OpenOffice and Microsoft Word*". No further detail was provided at that point.

430. These first mentions of LaTeX came after **Madden1**, in which Mr Madden had set out detailed evidence of Dr Wright's manipulation of the metadata of many of the electronic documents on which he primarily relied in support of his claim to be Satoshi Nakamoto.

431. In his Eighteenth Witness Statement for the PTR, Mr Sherrell of Bird & Bird exhibited a Tweet on 30 September 2023 from Mr Ager-Hanssen in which he set out a screenshot from a report (which he tagged as #faketoshi) which indicated that:

431.1. Under a heading 'Incriminating content of browsing history' the report referred to 'The contents of the browsing history file show that Dr Wright has researched topics relating to backdating files and manipulating metadata' followed by 'Here are some examples'.

431.2. The first example given is under the next heading 'LaTeX software'. The screenshot included in the report indicates Dr Wright had accessed an online

Q&A on TEX asking '*Was anything in Satoshi Nakamoto's original Bitcoin paper compiled in LaTeX*?'

431.3. Underneath that screenshot, the report continues with this question: '*The obvious question is: if Dr Wright is Satoshi Nakamoto, why would he ask what software he had used when he wrote the White Paper?*'.

432. As Counsel for the Developers observed, at best this would have been a bizarre question for Satoshi to have asked. Counsel also drew attention to the feature of PDF documents compiled from LaTeX code that the PDF file's internal metadata properties may be defined by the document author. He suggested that would have appeared attractive to a person who wanted to avoid the metadata pitfalls exposed by **Madden1**.

The 'tease'

433. On 27 November 2023, Shoosmiths wrote to COPA and the Developers (a) to reveal the existence of the White Paper LaTeX Files, said for the first time to be stored on Overleaf, (b) to seek to impose stringent limitations on their disclosure and (c) asking to adjourn the trial **{AB/2/2}**.

434. Neither COPA nor the Developers were prepared to accede to the proposals made by Dr Wright and so, on 1 December 2023, an application was made by Dr Wright for permission to rely on the so-called White Paper LaTeX Files (and other documents), for an adjournment of the trial and for revised directions to that adjourned trial. I heard and determined that application at the PTR.

435. **Field1** and **Wright6** repeated and amplified claims Shoosmiths had made (on instructions) in their 27 November 2023 letter. It was said that (and note that all references to **Field1** were confirmed in **Wright6** at **[4]**):

435.1. Prior non-disclosure: documents on Dr Wright's Overleaf account had not previously been reviewed for disclosure by Ontier because they were considered to fall outside the date ranges for searches specified in the DRD {**Field1 [19.2.3-19.2.4] {E/24/7**} & Shoosmiths' letter at [15]} and the LaTeX code on Overleaf did not "*have a metadata date*". That evidence was confirmed at {**Wright6 [4] {E/21/3}**}.

435.2. Relevant Overleaf folder: the only relevant or potentially relevant material hosted on the **Overleaf account was in a folder entitled 'Bitcoin', Field1** [19.2.5] {E/24/8} (The other material was said to relate to Dr Wright's academic and personal interests post-dating 2020). That evidence was confirmed at **Wright6 [4] {E/21/3}**.

435.3. Exact replica: the White Paper LaTeX Files compiled into an "*exact replica*" of the Bitcoin White Paper, **Field1 [48],{E/24/16}**. The words "*materially identical*" were used at **Field1 [19.2.6] {E/24/8}**. At **Field 1 [30] {E/24/10**} it was indicated that the code for the images matched "*the exact parameters of the images in the White Paper*". That evidence was confirmed at **Wright6 [4] {E/21/3}.**

435.4. Unique position: at **Field1 [27] {E/24/10}** it was said that the LaTeX code uniquely coded for the Bitcoin White Paper and a claim for swingeing

confidentiality restrictions was made based on their unique nature (**Field1 [48] {E/24/16}**, confirmed at **Wright6 [4] {E/21/3}**).

435.5. Digital watermark: it was suggested (at **Field1 [29] {E/24/10}/Wright6 [4] {E/21/3}**) that the White Paper LaTeX Files used "non-standard formatting (for example, coding for differences in the size of spaces between words) in effect as a form of digital watermark".

The 'reveal'

436. Dr Wright first provided a compilation of his version of the White Paper on 13 December 2023, a little over 24 hours before the PTR. It was self-evident from the content of the compilation {at **{L20/248.2}**}, when it came, that it was not "*materially identical*" to the Bitcoin White Paper, let alone an "*exact replica*".

437. Shoosmiths sought to explain the dissimilarity on two footings, which they confirmed would be explained by Dr Wright in his reply witness evidence (see **{AB/2/68} at [5]**), namely:

437.1. The compiled output would "*vary according to the parameters and process used for compilation" and it was "necessary to use the compilation process in fact used by Dr Wright when he published the Bitcoin White Paper as Satoshi Nakamot*o" (see **{AB/2/67} at [2]**).

437.2. Dr Wright had "*since the Bitcoin White Paper was published made a number of minor corrections to the White Paper LaTeX Files to address typographical errors in the published form of the Bitcoin White Paper (for example, replacing quotation marks to open a quotation in the form (") with double backticks in the form (") ...*" (see **{AB/2/67} at [3.1]**).

438. The PTR took place on 15 December 2023. At the PTR Dr Wright presented the White Paper LaTeX files as containing a form of digital watermark that rendered them potentially determinative of the identity issue (see Dr Wright's skeleton **[57-57(1)] {R/2/19}**), as impossible to reverse engineer (see Dr Wright's skeleton **[57(2)] {R/2/20}**) and as uniquely coding for the published form of the Bitcoin White Paper (Dr Wright's skeleton **[57(3)] {R/2/20}**).

439. In my Order from the PTR, I ordered Dr Wright:

439.1. In [3], to produce the advice from Ontier upon which had he relied, since I had ruled that privilege had been waived.

439.2. In [5], to provide COPA and the Developers inspection of the so-called White Paper LaTeX files in native form on standard Patents Court confidentiality terms.

439.3. In [7], to request Overleaf to give access to metadata and current and historic information regarding document activity, revision and edit history and account creation information.

440. On 18 December 2023 Shoosmiths wrote to COPA confirming that Ontier had informed them that, so far as it was aware:

"a. At no stage during the course of its retainer with Dr Wright (across all litigation matters) did Dr Wright inform Ontier that (i) he had an Overleaf account; (ii) this account may contain documents or be capable of generating documents which may be relevant to the issues in dispute; and/or (iii) the Overleaf account hosted LaTeX code or files which would produce a copy of the Bitcoin White Paper;
b. Ontier has never seen and/or received copies of any documents or material from Overleaf (whether LaTeX code or otherwise)"

441. As Counsel for the Developers submitted, Dr Wright's account, as to why the White Paper LaTeX Files had not been disclosed previously, fell apart. Dr Wright hinted that Ontier might have some motivation for lying about his LaTeX files, but the truth is more simple. As explained below, it is highly likely that Dr Wright's Overleaf account did not exist during the period of Ontier's instruction.

442. After the PTR, Shoosmiths produced the so-called White Paper Latex Files on 20 December 2023, by way of a zip folder entitled 'Bitcoin (3).zip' **{AB/2/31}**. The 'Bitcoin' folder that was disclosed had been received by Shoosmiths on 24 November 2023 {**Shoosmiths' letter, 10 January 2024**}. It was the same folder that had been used to produce the compilation that had been disclosed on 13 December 2023 {**Shoosmiths' letters of 29 December 2023 at [2] & 4 January 2024 at [2]**}. The main document path that had been used to create the compilation was a file in the TC subfolder and called main.tex.

443. Counsel for the Developers submitted that Dr Wright provided only very limited information concerning his Overleaf account(s), and then only reluctantly. I agree that he appears to have believed that the Overleaf platform recorded little or no metadata or document editing history (see **{Day15/148:4-9}**). I also agree that, in the period between the disclosure of the so-called White Paper LaTeX Files and Dr Wright's cross-examination about them on 23 February 2023, he appears to have made efforts to prevent the production of that information to the Developers and COPA.

444. However, acting entirely properly, Shoosmiths had to disclose certain matters on 16 February 2023, mid-way through the trial. Even after that disclosure, it remains the case that we only have a partial view of Dr Wright's activity in relation to the LaTeX files. The data we have relate to a 7-day period between 17 November 2023 (the date of creation of a folder entitled "Maths (OLD)") and 24 November 2023 (the date of export of the White Paper LaTeX Files from the 'Bitcoin' folder). Counsel for the Developers submitted that even those limited data comprehensively destroy any credibility that the so-called White Paper LaTeX Files might otherwise have had.

445. This submission is based on the history of Dr Wright's Overleaf account, pieced together as best as one can in light of the fragmentary information Dr Wright provided. That is then contrasted with Dr Wright's efforts to avoid the truth of the account coming out.

i. Dr Wright's Overleaf account

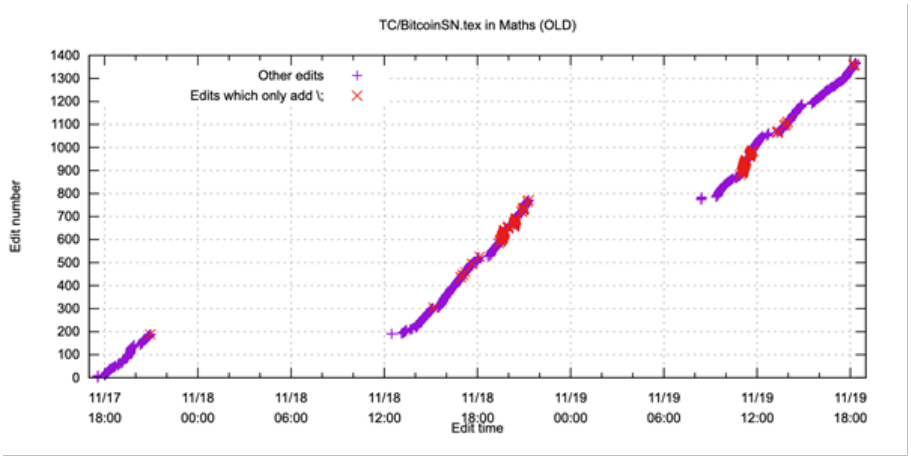
446. Dr Wright professes to have held multiple Overleaf accounts associated with multiple (21) universities since 2020 {See Dr Wright's 'cookbook' at **{M/2/776}** at section 7 (second para) and Shoosmiths' letter of 4 January 2024 at [3] **{M/2/802}.** However, his relevant account for present purposes is that associated with his craig@rcjbr.org address {Shoosmiths' letter to Overleaf of 10 January 2024 at **{M1/2/39}**}.

447. Although Shoosmiths stated that Dr Wright's Overleaf account was created in June/July 2023, the account number incorporates a Unix timestamp in hex {64d1faf7} that can easily be converted to a precise date and time of 8 August 2023 at 8:21am. That probably explains why Ontier had never heard of it: they had been replaced by Travers Smith on 12 June 2023 **{M/1/881}**, two months before Dr Wright created the account.

448. It seems (from a letter dated 27 February 2024 – after Dr Wright's cross-examination) that on 5 October 2023 (three days after Shoosmiths' instruction) a former fee earner of Shoosmiths received some form of demonstration from Dr Wright relating to LaTeX. The demonstration was so inconsequential that the current fee earners do not recall it. Shoosmiths have not subsequently received any documents relating to that demonstration **{M/3/48}**. Dr Wright performed a further demonstration for Shoosmiths in relation to his Overleaf account on 17 November 2023 between approximately 12.00-12.30 and 14:00-14.30 {Shoosmiths' letter of 16 February 2024 **{M/3/15} at [8.a]**}.

449. That same day, i.e. 17 November 2023, at 16:26 (after the demonstration to Shoosmiths) Dr Wright created a folder titled "Maths (OLD)" and copied the White Paper LaTeX Files into it {Shoosmiths' letter of 20 February 2024 **{M1/2/210}**. No earlier folders have been disclosed. The main document used by Dr Wright was titled BitcoinSN.tex. He created that file at 17:29 on 17 November 2023 **{L21/16.1/92}** and copied into it the content of a file entitled TC8.tex that he had imported into the Maths (OLD) folder when that folder was set up **{L21/17.1/2}**. He appears to have then given another demonstration to Shoosmiths between 17:00 and 17:30 {Shoosmiths' letter of 16 February 2024 **{M/3/15} at [8.a]**}.

450. Thereafter, Dr Wright made a series of changes to the BitcoinSN.tex file over the course of the next 22 hours, spread over three periods between 17 and 19 November 2023, as set out below and at **{M1/2/157}**.



451. On 19 November 2023 at 18:23 Dr Wright created a new project, 'Bitcoin'. Around one minute later he copied the content of the final version of the BitcoinSN.tex file from the Maths (OLD) folder into the main.tex file of the 'Bitcoin' project, i.e. the main document path of the so-called White Paper LaTeX Files **{L21/14.1/44}**.

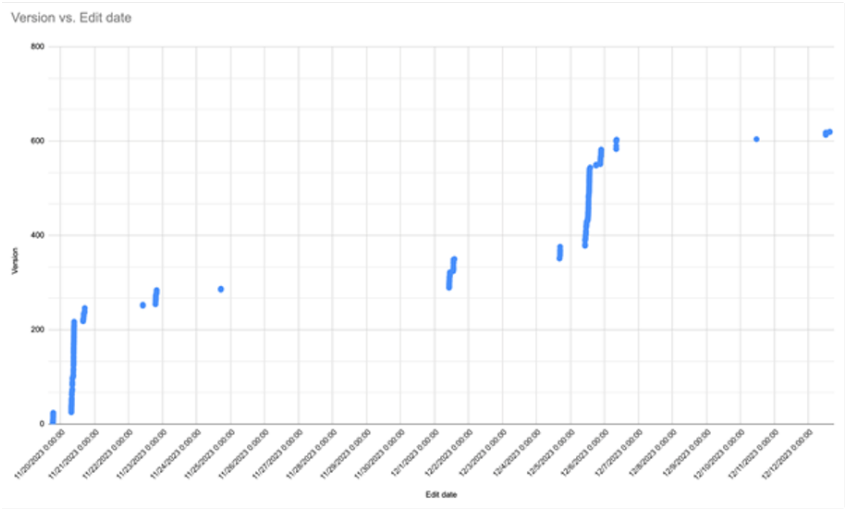
452. Dr Wright spent several hours making changes to the main.tex file in the morning of 20 November 2023. He then held further demonstrations with Shoosmiths between 15:00-

15:30 and 16:30-17:00 {Shoosmiths' letter of 16 February 2024 **{M/3/15} at [8.b-8.c]**}. Only four inconsequential changes were made during those demonstrations; and then only in the latter session i.e. no changes are shown between 15:00-15:30 at **{L21/14.1/238}-{L21/14.1/239}**; four changes were made between 16:30-17-00 at **{L21/14.1/244}-{L21/14.1/245}**.

453. Dr Wright sent downloads from Overleaf to Shoosmiths (including various compilations) on 20 November 2023 at 15:54, 16:22 and 16:57. Those downloads and the associated compilations were not produced to COPA and the Developers until 16 February 2024 (after the conclusion of Dr Wright's first cross-examination) {Shoosmiths' letter of 16 February 2024 **{M/3/15}**}. The covering emails **{{L20/252.86}, {L20/252.87}** and **{L20/252.88}**} made no reference to Dr Wright having made any changes, or to him planning to do so.

454. Dr Wright continued to make changes to the main.tex file between 20 November and 24 November 2023. He then downloaded and sent the 'Bitcoin' folder to Shoosmiths at 17:20. The covering email again made no reference to any changes that Dr Wright might have made – and described main.tex as "*the one Ppl know*"**{L20/252.89}**.

455. Dr Wright then went on to make yet further changes to the main.tex file. His activity on main.tex is illustrated below and at **{M1/2/103}**.



ii. The efforts made to resist providing metadata

456. The preceding account of Dr Wright's activity on his Overleaf account has only emerged as a result of documents and information provided by Shoosmiths during the trial.

457. Dr Wright had numerous opportunities to tell the truth – that the so-called Bitcoin White Paper LaTeX Files were the product of days of work done on Overleaf in November 2023 and not the processes described in his first and fourth witness statements but he failed to take them:

457.1. He said nothing to that effect when asking for an adjournment of the trial at the PTR.

457.2. Nor did he provide any such description when, on 20 December 2023, he served Wright8, a 24-page statement in which he purported to provide details of his LaTeX environment. **{E/23}.**

457.3. Nor did he provide that description on 12 January 2024, when he served his reply evidence, **Wright11**. Shoosmiths' letter of 13 December 2023 stated that this statement would give Dr Wright's account of "*the corrections he has made to the White Paper LaTeX files since the first publication of the Bitcoin White Paper, to the best of his recollection given the passage of time*". His witness statement gave no such account. In truth, there had been no "corrections" to the files, and the passage of time (less than two months) was unlikely to have clouded Dr Wright's recollection.

457.4. Nor did he provide any such description in **Wright14**, served on 30 January 2024 and produced in response my Order that Dr Wright identify the chain of custody in relation to the so-called White Paper LaTeX Files **{E/33}**.

458. As an aside, Dr Wright did make reference to how the files had been stored on the QNAP server in **Wright14**. At one point it seemed that Dr Wright might place some emphasis on this server as a repository of relevant information. In **Wright14 at {E/33/4}** Dr Wright explained how Alix Partners came to copy the QNAP server and took it away. Dr Wright suggests that he copied the White Paper LaTeX Files onto an external drive from the QNAP server at that time. I agree that suggestion cannot be true. AlixPartners have confirmed that they collected the QNAP server on 4-5 February 2019: see Shoosmiths' letter of 29 January 2024 at **{M1/2/138}**. AlixPartners inspected the QNAP server onsite, detected it was encrypted and took it away **{M1/2/139}**. They did not seek to image the QNAP server because it was encrypted, as Dr Wright has confirmed **{M1/2/140}**. Given that the QNAP server was "*not accessible to them without valid credentials and keys*" and "*inaccessible whether by AlixPartners, [Dr Wright] or a third party*" **{M1/2/140}**, Dr Wright cannot have accessed it to remove the White Paper LaTeX Files. In Tulip Trading, Dr Wright has suggested that the QNAP server is not even owned by him, but is instead owned by nChain **{S1/1.36/2} at [5]** and so the QNAP server faded from attention in the present proceedings.

459. Dr Wright dragged his feet in providing any useful metadata in compliance with my Order made at the PTR:

459.1. By January 2024 no metadata had been provided – and Dr Wright had not even provided Shoosmiths with the login credentials to his Overleaf account {Shoosmiths' letter of 8 January 2024 **{AB/2/189} at [1]**}.

459.2. Accordingly, COPA wrote to Overleaf directly on 3 January 2024. Overleaf responded to say that they had provided information to Shoosmiths, and separately wrote to Shoosmiths directing them to the Project History feature on Dr Wright's Overleaf account.

459.3. On 8 January 2024, Shoosmiths provided 17 files said to have been provided by Dr Wright to demonstrate Overleaf's "Other logs and files" feature. None of those files was at all informative as to Dr Wright's activity on the account.

459.4. The Developers wrote to Overleaf on 10 January 2024 requesting that they produce the relevant files. That same day, Shoosmiths wrote to advise that Overleaf had emailed to Dr Wright "*an export of the project history*" for his account. In the event, Overleaf declined to provide information to the Developers.

459.5. Faced with the imminent start of trial, the Developers made an application for Dr Wright to be ordered to consent to Overleaf providing the data from his account on 16 January 2024. That application prompted Shoosmiths to confirm that they would be "*in a position to provide the materials requested*" on 22 January 2024.

460. On 22 January 2024, Shoosmiths finally produced four zip files, including one containing a redacted version of the data that had been supplied by Overleaf. Even now it is not clear who had decided on the relevant redactions or why. The files included:

460.1. A file entitled REDACTED_project.json, which related to the Maths (OLD) folder, the existence of which had not previously been revealed. The file showed that Dr Wright had carried material from the Maths (OLD) project into the (disclosed) main.tex file of the Bitcoin project.

460.2. A spreadsheet entitled "chunks" that had been prepared for the Bitcoin project. This file recorded the changes made to the main.tex file in the 'Bitcoin' folder set out at paragraph 455 above.

461. On 1 February 2024, after being pressed further in correspondence, Shoosmiths wrote to Macfarlanes about the Maths (OLD) project. They confirmed that Dr Wright had put the REDACTED_project.json file associated with the Maths (OLD) project into the Bitcoin folder that had been disclosed to COPA and the Developers "*inadvertently*". As Counsel submitted, put another way, Dr Wright had never intended to reveal the existence of the Maths (OLD) project to the Developers.

462. However, the materials disclosed from the Maths (OLD) project were a revelation. They showed for the first time details of Dr Wright's repeated tinkering with the White Paper LaTeX files between 17 and 19 November. Nevertheless, the Maths (OLD) files were defective in two respects:

462.1. First, Dr Wright was continuing to assert privilege over some of the files: including the ZZZ and Test subfolder into which Dr Wright had first placed the BitcoinSN.tex file {see **{M1/2/153} at [2.d]}**;

462.2. Second, the changes to the White Paper LaTeX files were shown in a Maths (OLD)_chunks spreadsheet rather than in their native chunks.json format. As a result (although it was possible to track most of the changes on a row-by-row basis from the spreadsheet) it was impossible to rebuild and compile the changes sequentially from the available data.

463. On Day 5 of the trial, Mr Hough KC turned to the topic of the White Paper LaTeX Files in his first cross-examination of Dr Wright. In particular, he took Dr Wright to the chart set out at paragraph 455 above and suggested that Dr Wright was responsible for the edits shown in that document. Dr Wright admitted that he was, but then said that he had made all of the changes during demonstrations to Shoosmiths:

"153: 5 Q. You were responsible for those edits, weren't you,
6 Dr Wright?
7 A. I was.
8 Q. So the file was being edited right up to the day before
9 the LaTeX files were received by Stroz Friedberg?
10 A. Yes. I demonstrated to Shoosmiths, making a small
11 change, adding a full stop, adding a percentage. And
12 where you say there are extensive edits, that's actually
13 not true. Adding a full stop, removing that full stop,
14 is actually two edits. So, when I add a space, that's
15 an edit. If I go percent, comma, slash, etc, that's
16 three edits. So, at one stage, I typed in Matt's, one
17 of my solicitor's, name. That was probably 10 edits.
18 I then undid it and put the original name back. So
19 I was demonstrating how using that, you could change
20 the date and produce a new version, etc.
21 Q. Dr Wright, first of all, this was a document which you
22 were going to present as being a perfect digital
23 watermark of the Bitcoin White Paper. Didn't it occur
24 to you, as an IT security expert, that you shouldn't be
25 mucking with it extensively over the period of time
154: 1 before you produced it?
2 A. I downloaded a copy of the file and gave it to
3 Shoosmiths before I did any of this. So, the first
4 thing is, I downloaded the ZIP from Overleaf, sent it to
5 the solicitors. We did that right at the beginning of
6 this process. And as such, once I've given them a copy,
7 I'm saying that I can't change the copy they have,
8 therefore my making changes and undoing those changes is
9 not a material change.
10 Q. Do you say that all of those edits were done in
11 the presence of Shoosmiths?
12 A. They were on videos, on calls, I sent them some emails
13 while they weren't on there, I sent, like --
14 Q. You say that all these edits were done in their
15 presence?
16 A. Not in their presence. I emailed them. They weren't
17 there. And do you consider on a video call presence?"

464. Although Dr Wright's Counsel then observed that issues of privilege were being traversed, Dr Wright's answers put Shoosmiths in an impossible position. I agree that it plainly was not true that Dr Wright had made the changes in demonstrations to Shoosmiths. Indeed, as noted at paragraphs 453 to 454 above, he had not even mentioned any changes in his emails to Shoosmiths enclosing the Bitcoin folder.

465. In these circumstances, there had to be a waiver of privilege in relation to the Maths (OLD) and Bitcoin folders – and that occurred on Friday, 16 February 2024. For the first time, unredacted chunks.json files were produced by Dr Wright. That enabled the Developers to set about compiling each of the revisions that Dr Wright had made to the White Paper LaTeX Files between 17 November 2023 and 24 November 2023. The

Developers presented that work to Shoosmiths on Monday 19 February 2024, together with the code that they had developed to compile the documents from the chunks.json files.

iii Summary

466. Before turning to the evidence which emerged from production of the metadata underlying the White Paper LaTeX Files, I mention four points which arise from the sequence of events set out above.

467. First, Dr Wright deleted the previous folders on Overleaf from which he derived the Bitcoin folder. In Shoosmiths' letter dated 20 February 2024, they said:

> *"Dr Wright tells us that he cannot remember what those previous project folders were called or whether he copied them directly within Overleaf or copied them from local copies he had previously downloaded from Overleaf. In any event, Dr Wright says that he deleted the previous projects folders after copying their contents into Maths (OLD). As a result, Dr Wright says he no longer has the project folder used for the Overleaf demonstration to this firm earlier on 17 November 2023."*

468. I agree that there can have been no good reason for Dr Wright to have deleted those folders. From his own writings, Dr Wright is well aware of the adverse consequences attendant on the destruction of documents in this way: **{L1/470/8}-{L1/470/9}** and **{Day15/114-117}.**

469. Dr Wright was challenged on the deletion of the previous files in this passage of cross-examination:

> *"151:17 Q. So earlier, on 17 November, you had the so-called White*
> *18 Paper LaTeX files in a different folder to Maths (OLD)*
> *19 or the Bitcoin folder, right?*
> *20 A. I copied it into my R drive and then uploaded into*
> *21 multiple places for the demonstrations.*
> *22 Q. And you have failed to produce the folder that held*
> *23 those earlier files, haven't you?*
> *24 A. Because I copied back and forwards between the others.*
> *25 Q. You deleted it?*
> *152: 1 A. No, I did not. I moved it.*
> *2 Q. Can we go to {M1/2/210}.*
> *3 This a letter from Shoosmiths, dated*
> *4 20 February 2024, so very recently, and we can see in*
> *5 paragraph 2.1:*
> *6 "As you note in Your Letter, the Maths (OLD) project*
> *7 was created on 17 November 2023 at 16:26 [pm] ..."*
> *8 As I just put to you:*
> *9 "Dr Wright instructs us that this project was*
> *10 created by merging and/or copying files into Maths (OLD)*
> *11 from previous Overleaf project folders. Dr Wright tells*
> *12 us that he cannot remember what those previous project*
> *13 folders were called or whether he copied them directly*
> *14 within Overleaf or copied them from local copies he had*

15 previously downloaded from Overleaf. In any event,
16 Dr Wright says that he deleted the previous projects
17 folders after copying their contents ..."
18 Why have you lied to me about that basic point,
19 Dr Wright?
20 A. I didn't. If you're talking about the previous things,
21 then, yes, I've deleted them multiple times. Overleaf
22 goes back quite a while, including multiple accounts.
23 And have I kept them? No. I've copied between
24 different Overleaf folders.
25 Q. I said specifically to you that you had deleted those
153: 1 previous folders, and you said, "No, I did not, I moved
2 it", is what you said.
3 A. When you're moving, it actually changes the folder
4 structure. So, we're talking about different things.
5 I'm talking about the earlier stuff that I had in
6 Overleaf here; you're talking about what I did on
7 the 17th. So, they're different things.
8 Q. Dr Wright, you deleted relevant and disclosable material
9 just a couple of weeks before your application for an
10 adjournment, didn't you?
11 A. No. I didn't want an adjournment, for a start. But
12 what I did was copy and paste these into different areas
13 for demonstrations. The files in total were kept.
14 Q. You must have known, Dr Wright, that that was improper?
15 A. No, at that stage, everyone was telling me that there
16 was no purpose of these and we wouldn't get them in.
17 That's why I did the demonstrations. I did
18 the demonstrations to show how little teeny weeny
19 changes and how important it was, so I structured
20 a whole lot of demonstrations to show just how critical
21 these little tiny tweaks were and that you couldn't
22 guess them."

470. I agree with the Developers that in that passage of evidence, Dr Wright was doing his best to avoid the point and, in essence, not telling the truth.

471. The result of this deletion of data is that the Court has no information as to what Dr Wright did with the so-called White Paper LaTeX Files at any time before 17 November 2023.

472. Second, the Maths (OLD) folder itself was obviously relevant. However, Dr Wright had actively sought to hide it, saying that all folders other than the 'Bitcoin' folder related only to his personal and academic interests. Confronted with this point on Day 15, Dr Wright seemed to regret disclosing the Maths (OLD) folder at all and to pray in aid his deleted folders, before contending that he was demonstrating Overleaf to his solicitors (a point to which it is necessary to return later):

"149:15 Q. Can we go to page 8, please, at 19.2.5, which I know you
16 glanced at earlier {E/24/8}. We can see that, in
17 the second sentence:

18 "Dr Wright instructs me that the only relevant or
19 potentially relevant material hosted on his Overleaf
20 account is the material in a folder entitled 'Bitcoin'
21 did ... and that the other material hosted on
22 Dr Wright's Overleaf account relates to academic and
23 personal interests post-dating 2020 that are not
24 relevant to these proceedings."
25 Right? That's what you told her?
150: 1 A. Yes.
2 Q. And that wasn't true, was it?
3 A. No, I believe it's true. We've disclosed other
4 material, including stuff to do with CookBook, etc, but
5 my university stuff, the work on Teranode, etc, I don't
6 believe is relevant.
7 Q. The Maths (OLD) folder contained -- didn't only contain
8 material relating to your academic and personal
9 interests, did it?
10 A. Only because I copied into the wrong folder.
11 Q. It contained material that was directly relevant to your
12 creation of the White Paper LaTeX files, right?
13 A. No, it didn't. It had where I loaded, on the 17th,
14 files from a different directory so that I could
15 demonstrate the changes. That is directly loaded on
16 the 17th. As you already know, I had meetings with my
17 solicitors demonstrating Overleaf and those files, so
18 they had to exist before the 17th. They were there at
19 my house."

473. Dr Wright was challenged on his inadvertent disclosure of the Maths (OLD) project:

"190: 5 Q. Now, we know that it was inserted inadvertently by you
6 because we see that at {M1/2/153}. This is a letter
7 from Shoosmiths of 1 February 2024. 2(c):
8 "We understand from our client that the content of
9 the 'Maths (OLD)' project was inadvertently put into
10 this folder by our client."
11 Do you see that?
12 A. That's not what it's saying. It was a copy of the --
13 the thing. If you're saying a redaction, that's
14 a different thing. So I'm --
15 Q. The only Maths (OLD) project-related file that we
16 received, when you produced materials to us on
17 22 January, was that json file that I've just taken you
18 to?
19 A. I've no idea. I didn't actually open the file. KLD
20 came out, I clicked the link, we downloaded it, I gave
21 it to them. That's all I know.
22 Q. "We understand from our client that the content of
23 the 'Maths (OLD)' project was inadvertently put into
24 this folder by our client."

25 Right? It was you?
191: 1 A. No, that's not the downloaded file. The Maths (OLD)
2 file, what we're talking about, is Overleaf.
3 I inadvertently copied the Bitcoin stuff into
4 the Maths (OLD). That's what that there is describing.
5 Q. It's talking about the opposite. It's about content of
6 the Maths (OLD) project inadvertently being put into
7 something, right?
8 A. No, not at all. The download was done by either Stroz
9 or KLD at my house when we clicked on the file, and they
10 captured it.
11 Q. Now, if we --
12 A. I had no interaction with that process.
13 Q. If we hadn't immediately spotted the existence of
14 the project json file in relation to the Maths (OLD)
15 project in your Bitcoin folder, we would never have
16 known of all of the changes that you had made to
17 the White Paper LaTeX files, would we?
18 A. As I said, they were all part of the demonstration
19 process, so all that happened was I clicked the download
20 and all that comes across.
21 Q. So when saying that you had inserted it inadvertently,
22 what that actually means is that you had intended to
23 suppress that file from disclosure to us, right?
24 A. Not at all."

474. As Counsel for the Developers submitted, these were evasive answers but they do not detract from the points that (a) I had ordered these data to be disclosed; (b) either Dr Wright did not make any attempt to find out from Overleaf whether these data existed or, (c) he knew these data existed and did not mean to disclose them.

475. Third, these data show that Dr Wright's four witness statements presented a profoundly misleading picture that all he had done was make "*minor corrections to address typographical errors in the published form of the Bitcoin White Paper*".

476. Fourth, Dr Wright had lied about the reason why the White Paper LaTeX Files had not been included in his disclosure. He had not (indeed could not have) received the advice that he alleges from Ontier. Moreover, Dr Wright sought to abuse legal professional privilege as a way of avoiding disclosure of damaging information. Thus, Dr Wright's BitcoinSN.tex file was first created by Dr Wright in a subfolder of Maths (OLD) entitled "ZZZ Notes" **{L21/16.1/92}**. It was then moved to a subfolder entitled "Test" **{L21/16.1/101}**, before being moved to the "TC" subfolder **{L21/16.1/102}**. Dr Wright subsequently claimed privilege over the content of the ZZZ Notes and Test folders. As a result the origin and initial content of BitcoinSN.tex was concealed from COPA and the Developers until 16 February 2024 (midway through the trial), when Shoosmiths recognised that a waiver/withdrawal of the alleged privilege was essential**{M/3/15}.**

477. In the circumstances (which include all the evidence about the LaTeX files), I agree with the Developers that the only reasonable inference is that Dr Wright lied about these matters (and sought to abuse legal professional privilege) to conceal the fact that the White Paper LaTeX Files were a recent creation.

F. The evidence of forgery of the LaTeX Bitcoin White Paper

478. Under this heading, it is necessary (a) to discuss the animations prepared by the Developers from the chunks.json data, (b) to address Dr Wright's evidence about the metadata entry in the files, (c) to describe the nature of his revisions to the text formatting, (d) to discuss his use of Aspose in creating the images and (e) to discuss his evidence about the use of Apose.

a. The animations

479. Apparently unbeknownst to Dr Wright, the alterations he made to the White Paper LaTeX Files between 17:29 on 17 November 2023 and 17:07 on 24 November 2023 were recorded by Overleaf and are now available in the chunks.json files. From those data, the Developers created the two animations at **{L21/12}** and **{L21/13}**. The former is set against a blank background, the latter against the control version of the March 2009 Bitcoin White Paper.

480. I agree that the animations produced by the Developers illustrating the output of those alterations show the process by which Dr Wright forged the White Paper LaTeX Files in real time. They are the digital equivalent of a video capturing Dr Wright in the act of forgery.

481. The following information emerges from the animations themselves:

481.1. The first frame of the animation (which is derived from the first version of the BitcoinSN.tex file, which was in turn drawn from TC8.tex: see paragraph 449 above) shows that Dr Wright had managed to produce a reasonable approximation of the first page of the Bitcoin White Paper. Even that first page was far from perfect, and it was certainly not an "exact replica". However, it may have been sufficiently similar for Dr Wright to try to persuade Shoosmiths that the document was of some probative value. I agree the rest of the document was a mess.

481.2. Over the course of the next few hours, Dr Wright focussed his attention on making adjustments to the text of the first page of the White Paper LaTeX Files. He then proceeded to make adjustments to the remaining pages in a broadly sequential order.

481.3. The process was extremely hit-and-miss. For example, at about 14:21 on 18 November 2023, Dr Wright made a change to the formatting of the headings by introducing a "stretchtitle" command which caused them to jump to unnatural sizes {see row 535 at **{L21/5}**}. But more generally the blank-background version of the animation shows the stretching and shrinking of spaces between words and knock-on effects for line-breaks, page breaks and so on.

481.4. Dr Wright also had to play with the placement of the images in the Bitcoin White Paper. Initially, the images in BitcoinSN.tex were mostly comprised of png images (though Image1 was based on the importation of the Image1.tex file from an Images subfolder). Dr Wright gradually replaced those image files with pdf images that he had created from those image.tex files, that he effectively had to drag into place {In **{L21/5}**, the replacement of the image.tex files can be seen for Image1 at Row 498, for Image2 at Row 703, for Image3 at Row824, for

Image4 at Row 1075, for Image5 at Row 1073, for Image6 at Row 1066 and for Image7 at Row 1064}. The effective dragging and dropping of image 1 can be seen in the blank-background version of the animation from Rows 625 to 679 (each frame in the animation can be advanced individually by using the right-arrow key on a keyboard).

482. In short, the process was not one in which "*minor corrections*" were being made to put right known "*typographical errors*" in the Bitcoin White Paper (as had been stated twice by Shoosmiths on instructions from Dr Wright {Shoosmiths' letter dated 13 December 2023 at [3.1] **{AB-A/2/67}** and Shoosmiths' letter dated 29 December 2023 at [3] {**AB-A/2/141**}}).

483. Instead what the animations illustrate is that Dr Wright was trying to get his White Paper LaTeX files to fit the formatting of the Bitcoin White Paper. He was literally reverse-engineering the White Paper LaTeX Files from the Bitcoin White Paper. That was the very process that on 1 December 2023 he had sworn (in support of his application of that date) was "*practically infeasible*".

484. Perhaps appreciating the impossibility of the "*minor corrections*" explanation formerly provided, when the unredacted chunks.json files were produced to COPA and the Developers on 16 February 2024, Dr Wright instructed Shoosmiths that {Shoosmiths' letter dated 16 February 2024 at [14] **{M/3/16}**}:

> *"Dr Wright did edit the code in the intervening years for personal experimentation and to make corrections and improvements, and for the purposes of the demonstrations referred to above, and that Dr Wright then sought to undo the changes to the LaTeX code he had made since publication of the Bitcoin White Paper in order to put the code into the form that would compile the Bitcoin White Paper".*

485. That explanation is untenable in light of the changes recorded in the chunks.json and visible in the animations. It is absurd to suggest that the process of continual, iterative change and adjustment demonstrated through the animations represents the "*undoing*" of changes made previously. Still less is it tenable that the changes were made during demonstrations.

486. Dr Wright emphasised the "*I was giving demonstrations*" explanation in his oral evidence, as for example in the following passages on Day 15:

> *"125: 9 Q. We're going to come to the changes in a minute and we're*
> *10 going to come to the demonstrations in a minute, but the*
> *11 changes that you made to the BitcoinSN.tex file of*
> *12 the Maths (OLD) project and then to the main tex file of*
> *13 the Bitcoin project included changes which were designed*
> *14 to make the text of your LaTeX file more closely*
> *15 resemble the formatting of the Bitcoin White Paper;*
> *16 correct?*
> *17 A. No, not at all. The demonstrations were to show how*
> *18 the differences were. I'd actually already told my*
> *19 solicitors about it going back to October.*
> *20 Q. We can see, and we're going to go through some of this*
> *21 but hopefully fairly briskly, that you were adjusting*

22 the size of the spaceskip commands; do you agree?
23 A. Yes. Like I was saying, you demonstrate how the thing
24 works and I put them in and out.
25 Q. And then you were adding and moving "/:"s, right?
126: 1 A. Yes.
2 Q. And that was to try to enable you to try to replicate
3 the line breaks and the spaces between words in
4 the Bitcoin White Paper, wasn't it?
5 A. Not at all. It was actually putting things back to
6 demonstrate what it is without it and how these things
7 work."

"127: 5 Now, what that animation shows is that you were
6 moving and adjusting text, right?
7 A. Yes, that was part of capturing and what I was
8 demonstrating. The original was demonstrated to my
9 solicitors at my home before any of this happened.
10 Q. And we can see that, generally, the changes started on
11 page 1 and continued down the document, right?
12 A. Oh, as I made each of the change, it's not the whole
13 document changes. To demonstrate what the different
14 commands do, I had to actually put them in."

"132:11 Q. Were you very familiar with LaTeX before you were doing
12 this?
13 A. I know LaTeX. I don't -- I'm not an academic, I don't
14 teach it, so I don't know all the terminology.
15 Q. Because there seemed to be a lot of faffing around with
16 LaTeX in your adjustments, which looked like somebody
17 learning how to do it on the go?
18 A. No, it's demonstrating the differences. Like I said, if
19 you make one small change in any of those values, it
20 significantly changes everything in the line and
21 the only way to demonstrate that is to show it."

487. I agree that Dr Wright's "*demonstrations*" excuse is demonstrably false. The period of the demonstrations to Shoosmiths is illustrated in the animations by changing the background colour to red. It occupies just 4 frames of the animations. Dr Wright was not otherwise demonstrating anything to anybody. He was trying to work out what adjustments he might make to the LaTeX code to get his text and images to fit the layout of the Bitcoin White Paper.

488. With that in mind it is useful to turn to Dr Wright's evidence about the text, images and other commands in the LaTeX code.

b. Metadata command

489. On a number of occasions, when confronted with evidence of anachronistic metadata, Dr Wright sought to explain the anomaly by reference to his use of a metadata command in LaTeX. For present purposes, these points are only concerned with the relevant command used in the White Paper LaTeX Files.

490. Dr Wright provided evidence about that at **Wright11 [358-367] {CSW/1/68}**. In particular at **Wright11 [365] {CSW/1/69}** he suggested that he has used the following LaTeX command: pdfcreationdate={D:20090324103315-07:00}.

491. Counsel for the Developers suggested there were three problems with that evidence.

492. First, that command would not have produced the Created date that appears in the Bitcoin White Paper pdf. The CreateDate in the relevant version of the Bitcoin White Paper is 2009-03-24T11:33:15-06:00 **{G/7/17}**. Dr Wright had identified the wrong time zone in his supposed LaTeX code. As the Developers noted, Dr Wright may have been in a muddle arising from the fact that the October version of the Bitcoin White Paper used a -7 hours time zone: PM3 [22] **{H/20/8}**. When presented with that error on Day 15, I agree that Dr Wright dissembled, including in response to questions from me:

"167:18 Q. What is the point of putting in a witness statement
19 a description of a PDF creation date command if it
20 wasn't a PDF creation date command that Satoshi made?
21 What's the point of mentioning it?
22 A. One, I am Satoshi. Two, the command that I put in there
23 is going to change over time as I'm working on
24 the files.
25 Q. So if you're Satoshi, was that the PDF creation date
168: 1 that you put into the Bitcoin White Paper or not?
2 A. The original White Paper has changed many times and
3 there are multiples.
4 Q. Right.
5 A. So your problem is that you keep saying, "The paper".
6 One, there are multiple versions of the paper, and there
7 are multiple versions of what I've done.
8 Q. No, the problem isn't mine, it's yours.
9 A. No, it's not mine.
10 Q. And the reason the problem is yours is because
11 the relevant version of the Bitcoin White Paper that
12 you're talking about here had a minus six hours time
13 zone.
14 A. No, it had a minus six because of changes in location.
15 Q. We can see it at {H/20/11}.
16 A. Minus seven goes to minus six when you add summer time.
17 Q. Dr Wright, we can see here that the creation date was
18 20090324113315 minus 6, right?
19 A. Minus 7, in the statement, when you add summer time
20 becomes minus 6, plus one hour, so minus 7 plus one is
21 minus 6.
22 Q. Dr Wright, I perfectly well understand that if you were
23 trying to state the relevant time at a minus seven-hour
24 time zone that you would have put 103315, but actually,
25 Satoshi didn't use a minus 7-hour time zone for this
169: 1 version of the White Paper, did he?
2 A. No, you're incorrect once again. Time zones. If you
3 compile it and you change, like, that not to be that

4 part of the year, it will be different.
5 Q. Dr Wright, the whole point of this section of your
6 witness statement is for you to describe the -- is to
7 describe what you were saying was the way in which you
8 could configure the metadata properties, right?
9 A. Yes.
10 Q. But you put in duff metadata properties in your 11th
11 witness statement, didn't you?
12 A. Again, time zones. I know you seem not to understand it
13 on purpose, but when you have a plus one on a time zone,
14 it changes. So time zone plus one means negative 7 plus
15 one, which comes out on the final document as
16 negative 6.
17 Q. If you're manually configuring the Bitcoin White Paper
18 to identify -- and you're doing it in LaTeX, which
19 Satoshi did not do, if that's what he had done, he would
20 have had to put minus 6 to get the output that we're
21 seeing here as the creation --
22 A. No, if you did it on minus 6, because of plus 1, you'll
23 actually get negative 5. So again, it's like London
24 time. We keep adding an hour, subtracting an hour,
25 making people change clocks --
170: 1 MR JUSTICE MELLOR: Hang on, Dr Wright. As I understand
2 your evidence, in LaTeX, it's nothing to do with any
3 clock, you put in these numbers.
4 A. Ah, but the system will still use the timestamp
5 information. So you put in those numbers --
6 MR JUSTICE MELLOR: How? Which bit of this creation date
7 field does the system change then?
8 A. You still have to put in the time zone information if
9 you want it not to change naturally on the system clock,
10 my Lord. So the system clock, when it compiles, will
11 recognise if it's a plus one and add that and modify it.
12 So, when you do this, unless you do something like
13 specify GMT, or Eastern Standard Time specifically, then
14 it's going to take the natural sort of changes and
15 drifts.
16 MR JUSTICE MELLOR: Mm. I think I've previously asked you
17 about whether there was a default or whether you had to
18 put all this in manually.
19 A. If --
20 MR JUSTICE MELLOR: And I recall you answered it's manual.
21 A. Yes, but what I'm saying here is the difference between
22 the negative 7 and the time zone information, my Lord.
23 They're actually two different settings.
24 MR JUSTICE MELLOR: Yes, I mean, I'm afraid, Dr Wright,
25 I simply don't understand that answer. So if you want
171: 1 me to understand it, you're going to have to explain
2 precisely how this works.
3 A. Yes, my Lord.

4 All right, so what happens is you set a default, and
5 if you put negative 7 and the --
6 MR JUSTICE MELLOR: Where do you set the default in LaTeX?
7 A. In a command.
8 MR JUSTICE MELLOR: In this command?
9 A. Yes.
10 MR JUSTICE MELLOR: But I thought you said earlier it's just
11 what you type in?
12 A. The negative 7, though, is different to the time.
13 The time is what you type in. Now, you also either set
14 explicitly whether you have time zones changing for
15 summer time, etc, or not. If you don't, then it goes to
16 your clock time, as you're doing it.
17 MR JUSTICE MELLOR: Okay, but I don't understand why you
18 would be worrying about summer time, plus 1, minus 1,
19 etc.
20 A. That's why it comes out, if you put 7 in --
21 MR JUSTICE MELLOR: No, no, no, why wouldn't -- okay, we'll
22 assume Satoshi is putting in the creation date.
23 A. Yes.
24 MR JUSTICE MELLOR: Why would he worry about whether it was
25 summer time or not?
172: 1 A. No, it's a time zone negative 7. At the time, I was
2 doing a lot of work with American and Caribbean
3 companies, so my default when I printed things was
4 negative 7. The reason for that is, in Antigua, various
5 other islands, a lot of gaming happens. So when I was
6 doing, you know, documents, etc, I used standards for
7 either South American or Caribbean time. Now, that
8 comes with certain plus 1 minus or plus 10 type
9 adjustments. Now --
10 MR JUSTICE MELLOR: Adjustments from when?
11 A. I'm not exactly sure when summer time does or doesn't
12 start.
13 MR JUSTICE MELLOR: No, no, no, but if you're talking about
14 Antigua and Caribbean saying plus 1/minus 1, that's
15 adjusting relative to which time zone?
16 A. To the negative 7. So it will take negative 7 and add
17 one. So when it compiles, it becomes negative 6. So,
18 the document here says that date, but then it becomes
19 negative 6 in the PDF, because the PDF will display plus
20 summer time, etc.
21 MR GUNNING: Dr Wright, the last time I looked, the time
22 zone difference in the Caribbean was minus 5 hours,
23 but ...
24 A. As I said, also Belize, other places. I did
25 South American and the others.
173: 1 Q. You had a sort of travelling time zone then, did you?
2 A. I did. I had dealings with a variety of
3 Central American and Caribbean areas. I still do."

493. The second problem with Dr Wright's evidence was that the supposed pdfcreationdate command to which he referred was not present in the White Paper LaTeX Files at all at the time of the Maths (OLD) project. It was introduced into the main.tex file in the Bitcoin project in two stages. On 22 November 2023 at 18:58 he entered a pdfcreationdate of 20241122010000: see row 746 of **{L21/4}**. He then changed the date to 22 November 2006: see row 755 of **{L21/4}** (where the characters "06" were added at character 5525). Finally, he replaced the then resulting characters "61122010000" with the characters "90324173315": see row 769 of **{L21/4}**. As a result, when the White Paper LaTeX Files were produced to the Developers on 20 December 2023, they showed a pdfcreationdate of "20090324173315": see **{L21/9.1/4}**.

494. The third problem with Dr Wright's evidence was that the command to which he referred had been entered by him, but only 1 December 2023, as part of the adjustments that he continued to make to the White Paper LaTeX files. The change was made in two rows. First he entered 20090324173315: see row 953 of **{L21/4}**. He then added the –06:00 time zone at row 955 of **{L21/4}**. When confronted with these changes, Dr Wright denied them:

> *"173:19 Q. .....*
> *20 And we know how you came to put this command into*
> *21 the White Paper LaTeX files; it was something that you*
> *22 did not do until 1 December 2023.*
> *23 A. No, that's incorrect. I'd already demonstrated files*
> *24 set in the future, set in the past, and I've done that*
> *25 multiple times.*
> *174: 1 Q. It's a matter of record. There is no PDF creation date*
> *2 command in the Maths (OLD) project, right?*
> *3 A. I've no idea.*
> *4 Q. It's the PDF creation date that's entered in the Bitcoin*
> *5 project up to 24 November is not the -- doesn't include*
> *6 the time and time zone that you've provided there.*
> *7 A. The one that I demonstrated when they were over at my*
> *8 house in October had all this, and when I demonstrated,*
> *9 I demonstrated how that worked.*
> *10 Q. And we can see where it comes in by looking at*
> *11 the chunks file and this command goes in on 1 December,*
> *12 right?*
> *13 A. No, you can see the demonstrations I did after they'd*
> *14 already come out to my house.*
> *15 Q. Dr Wright, we can take that up in closing, but you're*
> *16 lying.*
> *17 A. No, I'm not."*

495. The conclusion is inescapable in my judgment. Dr Wright was lying.

c. Text formatting

496. In his witness evidence Dr Wright had contended that the formatting of the spaces between words in the White Paper LaTeX Files was a form of digital watermark. He implied during his evidence on Day 5 that this was a form of steganography intended to mark him out as the author. If that had been so, it was a surprising oversight for Dr Wright

to have omitted to mention the White Paper LaTeX Files in his evidence in *Kleiman*, *McCormack*, *Granath* or prior to October 2023 in this litigation.

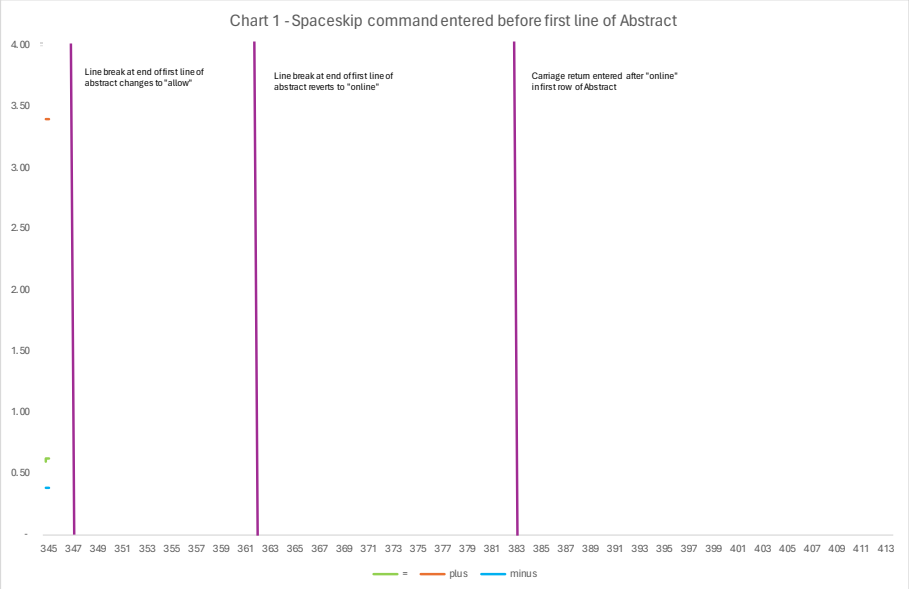
497. Counsel for the Developers suggested that Dr Wright probably happened upon the idea of saying that his attempts to adjust the spacing between words in his White Paper LaTeX files was a digital watermark in the evening of 17 November 2023 after making all of his formatting changes and that he was probably inspired to promote that theory by the fact that his repeated entry of \; and spaceskip commands would otherwise be an obvious sign of forgery. At that point he chose to post mysterious references to watermarking on his Slack channel **{M1/2/156}**. The times are in EST. Dr Wright suggested that someone else posted this on his behalf, but could not name the culprit: **{Day15/122-123}**, and then when he had completed his work on the Maths (OLD) project he inserted two comments into BitcoinSN.tex referring to watermarking and steganography {see **{L21/16.1/696}** and **{L21/16.1/698}**.

498. In reality, Dr Wright's changes to the spaces between words were attempts by him to replicate the spacing of the Bitcoin White Paper, which (as explained below) was a consequence of the justification of the text in OpenOffice 2.4.

499. An example of Dr Wright's attempt to fiddle with the formatting was explored in cross-examination, it concerned his use of the spaceskip command ahead of the initial line of text in the abstract of the Bitcoin White Paper. That command was introduced by Dr Wright in Row 345 of Maths (OLD)_chunks **{L21/5}** and can be seen at **{L21/29.1/4}**: see the command "*spaceskip=0.3em plus 3.4em minus 0.10em*".

500. Mr Rosendahl explained that spaceskip is a somewhat arcane LaTeX command **{Day5/139-140}**. Dr Wright did not seem entirely clear what the figures in its syntax meant **{Day15/131-133}**. However, he confirmed that the first number represented the base spacing, the second number reflected the amount by which the base spacing could be stretched and the third number represented the amount by which it could be reduced {Day15/133:8-25}.

501. Having inserted the spaceskip command described above, Dr Wright spent a little over half an hour on 17 November 2023 adjusting its parameters to try to get the spacing of the first line of the abstract to fit. During the course of those changes, he changed the position of the line-break in the text at the end of the first line (as shown by the first purple bar below). The changes (which resulted in the command reading "*spaceskip=0.30em plus 2.0em minus 0.16em*") can be shown as follows **{X/61}**:



502. Dr Wright initially resisted looking at these changes on the footing that there were prior commands that needed to be considered with those changes, namely "*\vspace{5.40mm}*" and "*\begin{adjustwidth}{13.48mm}{14.81mm}*" {see Day15/136:3-14}. It is not clear why Dr Wright saw fit to mention those commands save for the purposes of distraction. Those commands did not change at all during the course of the changes to the spaceskip command shown above (as can be seen if one examines page 4 of each of the compilations at **{L21/29.1/4}** to **{L21/90.1/4}**). The former command had set the vertical space above the abstract. The second had set the width of the abstract.

503. Dr Wright then sought to suggest that the entire process of adjustment illustrated by the above was a demonstration:

> *"136:18 If we look at the spaceskip command here, we can see*
> *19 you start off having it at 0.3em, right?*
> *20 A. Like I said, I did a demonstration where I was going*
> *21 through each of these settings to show how much it*
> *22 changes.*
> *23 Q. And you then increased it to 0.6em, right?*
> *24 A. I did.*
> *25 Q. And you then reduced it to 0.2em in a bit below that?*
> *137: 1 A. Yes, the best way of demonstrating how it works is to*
> *2 make a large change.*
> *3 Q. Yes, but none of this is being done on one of your*
> *4 demonstrations to Shoosmiths?*
> *5 A. This was actually part of what I was documenting at the*
> *6 time.*
> *7 Q. How were you documenting it?*
> *8 A. I had files.*
> *9 Q. What files?*

10 A. I had screenshots, etc, for some of the --
11 Q. Sorry, you were taking screenshots every time you made
12 a change to your Overleaf files?
13 A. Some of these, yes. Not every single time, but when
14 I was making differences. I also had other
15 conversations even before this. Shoosmiths were at my
16 house --
17 Q. I'm not interested in your discussions with Shoosmiths.
18 What I'm going to explore is how spaceskip changes and
19 we've seen how the first parameter changed, right?
20 A. Mm-hm.
21 Q. The second parameter was the max stretch that LaTeX
22 would permit to that base spacing, right?
23 A. Yes.
24 Q. And it started at 3.4?
25 A. Mm-hm.
138: 1 Q. And we can see you then reduced that in a number of
2 stages, right?
3 A. Yes, to demonstrate --
4 Q. A minor tweak upwards we can see at around 370 or 371?
5 A. It's a bit more than that. You'll notice that there are
6 three values. So it was demonstrating, like a three
7 body problem, just how difficult it is to actually find
8 something that matches. But you can't just, like you're
9 suggesting, go, "Oh, I'm going to guess a value" and
10 it's going to match --
11 Q. The third --
12 A. -- because if you do that it's going to be way, way out.
13 Q. The third parameter was the shrinkage parameter, right?
14 A. Mm-hm.
15 Q. And that's depicted in blue and it starts at 0.1, yes?
16 A. I'm not sure where it starts, but ...
17 Q. Well, it's -- take it from me, it's at 0.1.
18 A. Yeah.
19 Q. You then increased it to 0.3?
20 A. Mm-hm. Yeah.
21 Q. Before reducing it?
22 A. Yes.
23 Q. And then increasing it, before finalising it at 0.16?
24 A. Mm-hm.
25 Q. Now, so you had in fact at one point set the shrinkage
139: 1 to a level that was lower than the base spacing?
2 A. Yes.
3 Q. Which doesn't make any sense, does it?
4 A. That's the whole point. By doing this, I'm
5 demonstrating just how sort of many changes can occur
6 from a simple little tweak.
7 Q. You're not showing it to anybody, Dr Wright. We know
8 the times when you're showing it to Shoosmiths. This
9 can only be something that you're doing for yourself?

10 A. No, actually, it's not, because I also created documents
11 and I also documented the changes I was doing in what
12 they wanted.
13 Q. We're going to come to the documents that were produced,
14 but standing back from this, we don't see that you were
15 making adjustments to reintroduce known parameters from
16 the Bitcoin White Paper, do we? That's not what you're
17 doing?
18 A. No, I'm actually adjusting it to show how different it
19 can be.
20 Q. What you're doing is tweaking parameters to try to get
21 them to fit the layout of the Bitcoin White Paper,
22 aren't you?
23 A. No, actually, you wouldn't do that. And what
24 you're actually -- you're saying --
25 Q. It's not a question of what I would do --
140: 1 A. Well --
2 Q. -- that's what you did.
3 A. No, I demonstrated how these changes worked. Now, what
4 you're saying in the thing you said, it would be
5 ridiculous, and yes, I noted so how ridiculous some of
6 these things could end up and how different. You notice
7 some of them, the whole structure changes just by
8 a small change."

504. Counsel suggested that three points emerge from this:

504.1. First, it is clear that the changes were being made at times when no demonstration was being carried out. The changes that he made resulted in the final spaceskip coding in the relevant part of his so-called White Paper LaTeX Files which reads "*spaceskip=0.30em plus 2.0em minus 0.16em*": **{L21/9.1/7}**. I agree that Dr Wright's attempts to suggest this was all part of demonstrations was absurd.

504.2. Second, the changes were plainly indicative of a process of iterative adjustment seeking to achieve a particular result. The iterative nature of that process contradicts the further assertion (by Shoosmiths on instruction from Dr Wright) that this was merely a process of seeking "*to undo the changes to the LaTeX code he had made since publication of the Bitcoin White Paper*". I agree.

504.3. Third, this was plainly not a steganographic process either. Dr Wright did not even contend that some message was encoded in the document. If Dr Wright's White Paper LaTeX Files bear any watermark, as Counsel submitted, it is simply the smudge of Dr Wright seeking incompetently to reverse-engineer the Bitcoin White Paper.

d. The images

505. The Bitcoin folder disclosed by Dr Wright contains a subfolder entitled "Images" which contains the seven images from the Bitcoin White Paper in two formats. They were stored as .tex files in which specific drawing commands were entered in LaTeX code: see e.g. **{L21/22.2}**. In addition, they were provided as PDF files. As described at paragraph

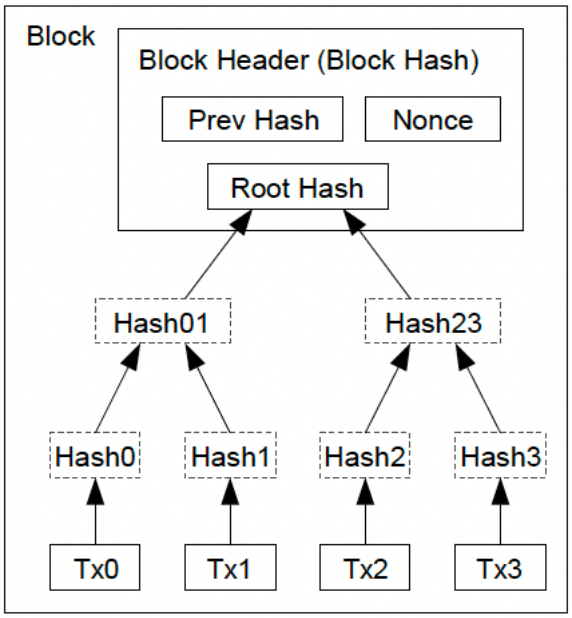
481.4 above, Dr Wright ultimately used the PDF files in his production of the White Paper LaTeX Files.

506. Dr Wright placed specific and elaborate emphasis on the images in his White Paper LaTeX Files as a particularly strong indicator of the probative significance of those files. It is necessary first to draw attention to that evidence, before exploring the evidence that they were produced by Dr Wright using an online PDF-LaTeX conversion tool called Aspose.

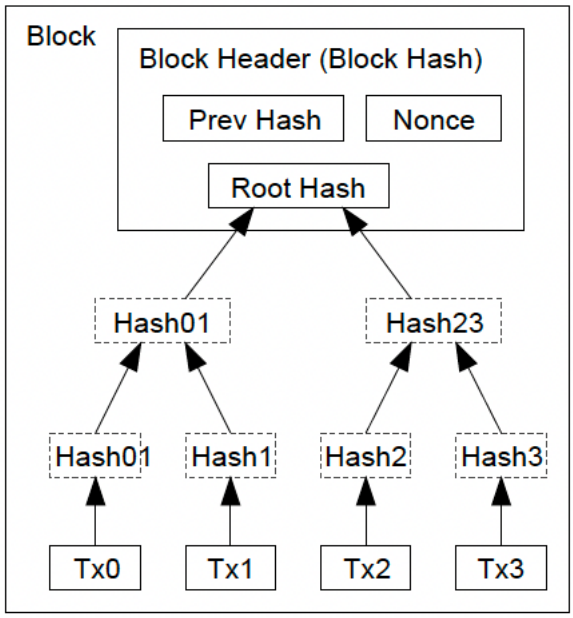
507. The first point, however, is a clumsy error which Dr Wright made in the production of Image 4 in his White Paper LaTeX Files.

i. Image 4

508. The erroneous version of Image 4 in Dr Wright's White Paper LaTeX Files can be compared with the real Bitcoin White Paper as follows:



Left part of Image 4 from Bitcoin White Paper



Left part of Image 4 from the White Paper LaTeX Files

509. The comparison reveals two parts to Dr Wright's error:

509.1. First, he had referred to the hash of Tx0 in the Merkle Tree as Hash01, when Hash01 was shown in the Bitcoin White Paper to be the combined hash of Hash0 and Hash1. This error probably arose when Dr Wright was adjusting his Aspose output in the manner described below.

509.2. Second, and as a consequence of the first error, the related text overflowed its bounding box.

510. Dr Wright spotted the latter error, but not the former. When the error in the content of the Merkle tree was drawn to his attention, Dr Wright's evidence went through a characteristically illogical arc: concession {177:2-6, 11-20, 24-178:2}, confusion {177:7-10}, denial {177:21-23}, dissembling {178:3-179:8} and irrelevant/technobabble {179:8-18}:

177: 2 Q. And do you see that, in the second row up, above "Tx0",
3 the text "Hash01" overflows the bounding box, right?
4 A. I do.
5 Q. And that's obviously an error, isn't it?
6 A. Yes, in this version.
7 Q. Any other comments on that?
8 A. Not off the top of my head, no.
9 Q. Isn't there something rather strikingly obvious?
10 A. I don't memorise every part of my diagram, no.
11 Q. Okay, well, let's go back to the Bitcoin White Paper.
12 It's at {L5/26/1}. Let's go to page 4 of that
13 {L5/26/4}. Perhaps we could put that up alongside --
14 yeah, sorry. So, do you see, if we look at those two
15 things, in the original Bitcoin White Paper, which is on
16 the left, the error isn't one of overflowing
17 the bounding box, the mistake is that in your image,
18 you've identified the hash of transaction 0 as "Hash01",
19 right?
20 A. Yes. There's a typo in it, yes.
21 Q. And that is an error in your LaTeX code, right?
22 A. No, it's not an error in the LaTeX code, it's an error
23 in the diagram that's been introduced at some point.
24 Q. It's an error in your code. If we go to {L21/11.2/7}.
25 This is the code for image 4. Do you see, about ten
178: 1 lines down from the top, it says, "put(154.8, -548.3)"?
2 A. Yes, and I've typed in "Hash01" instead of "Hash0".
3 Q. Right. Because it doesn't make any sense to describe
4 the hash of transaction 0 as Hash01, does it?
5 A. It does in certain other versions of the document.
6 Q. No, no, no.
7 A. Well, yes, it does in other versions. This isn't
8 the only time I've used that.
9 Q. As a hash of transaction 0?
10 A. As I said, this diagram has been used in multiple
11 things, so where it says "Hash01", others were 00011,
12 etc.
13 Q. Oh dear.
14 Shall we go back to {L5/26/4}. You understand how
15 Merkle trees work, right?
16 A. Of course I do.
17 Q. Right.
18 So the way that they work is that you take a hash of
19 each of the transactions at the bottom, right?
20 A. Mm-hm.

21 Q. And a hash of transaction 0 is going to be hash 0,
22 right?
23 A. That's one way of naming. In a binary tree structure,
24 you could also do other structures and names. Now, in
25 my diagram, I've noticed I've put "Hash01" there and
179: 1 I've got an error in one of the versions, yes.
2 Q. Because it doesn't make any sense to refer to the hash
3 of transaction 0 as hash 0[1], because hash 01 is the hash
4 of both hash 0 and hash 1, right?
5 A. No, not necessarily. If you have Tx01 and you have
6 other naming, then it's going to be different. So
7 there's an error in my diagram because I've used it in
8 multiple things. So I know you want to sort of try and
9 make out that I don't know anything about this stuff,
10 despite the fact that we have -- BSV are now doing
11 1.1 million transactions a second on a public testnet,
12 which is about a million times what you guys can do, but
13 -- and actually faster than Oracle.
14 MR JUSTICE MELLOR: We're talking about the original
15 White Paper.
16 A. This is part of the original White Paper, my Lord.
17 I said it scaled undoubtedly. That's what I worked on
18 doing and that's what these guys want to stop.

511. That last 'Teranode' part of his answer is but one example of (a) how far Dr Wright strayed from the question and (b) his propensity to resort to technobabble by way of avoidance. In making that latter point, I am not disputing his assertion about his Teranode system, it is the fact that he resorted to it when it had nothing whatever to do with the question.

512. Although, in one sense, the error in Image 4 of Dr Wright's White Paper LaTeX Files is relatively inconsequential, the fact remains that Dr Wright's response to it evidenced his detachment from the real content of the Bitcoin White Paper. It also set the scene for his evidence about the images in the White Paper LaTeX Files.

ii. Dr Wright's written evidence about the images

513. The first occasion on which Dr Wright sought to place specific emphasis on the image files was in the evidence in support of the application for an adjournment, in which it was said that "*it would be particularly difficult to reverse engineer the LaTeX code for the images in the Bitcoin White Paper because such code would produce images that did not match the exact parameters of the images in the White Paper (for example, as to the precise location and angle of lines and arrows).*" {**Field1 [30] {E/24/10},** confirmed at **Wright6 [4] {E/21/3}.** That point was emphasised at paragraph 57(2) of Dr Wright's Skeleton Argument for the PTR **{R/2/20}**}.

514. Dr Wright expanded on that theme in **Wright11**. In a lengthy section of that statement at **Wright11 [329-346] {CSW/1/61}** he purported to provide a detailed account of the technical artistry on display in his LaTeX image files. For example:

"*It's important to note that the original source LaTeX code for the Bitcoin White Paper, including any images created with TikZ or similar tools, is not publicly available on the internet. This means that the precise methods and code used to create the document and its elements have not been shared publicly, nor have they been reverse-engineered. This lack of public availability underscores the unique creation process of the Bitcoin White Paper, where the specific LaTeX coding and formatting techniques used remain exclusive to the original document.*" (**Wright11 [330] {CSW/1/62}**).

"*The creation process of Figure 1 in the Bitcoin White Paper using LaTeX demonstrates a sophisticated use of the tool, blending text and graphical elements in a way that enhances the document's functionality and accessibility …*" (**Wright11 [334] {CSW/1/62}**).

"*In the Figure above of the Bitcoin White Paper, the illustration is a result of lines of code compiled from a LaTeX file. This method of image creation, where every line is meticulously drawn using code, exemplifies a technique often favoured by developers and computer scientists rather than graphic artists.*" (**Wright11 [335] {CSW/1/63}**).

"*This approach, rooted in programming, involves defining each element of the image through code - every line, curve, and text element is explicitly described in the LaTeX file. This method is particularly appealing to those with a background in computer science or development, as it allows for precise control over the image's composition. Each aspect of the image can be fine-tuned by adjusting the code, offering a high degree of customisation and accuracy.*" (**Wright11 [336] {CSW/1/63}**).

"*Such a technique contrasts with more traditional graphic design approaches, where images are created using visual tools and software geared towards graphic artists. These tools often involve direct manipulation of visual elements using a graphical user interface, which is more intuitive for visual design but may lack the precision and programmability of a code-based approach.*" (**Wright11 [337] {CSW/1/63}**).

"*The use of LaTeX to create images, as seen in Figure 2 of the Bitcoin White Paper, underscores the flexibility and power of the LaTeX system in handling not just text and formulae but also complex graphical representations. This code-based method of image creation aligns well with the ethos of fields like computer science and development, where control, precision, and the ability to programmatically define elements are highly valued.*" (**Wright11 [338] {CSW/1/64}**).

"*The code provided for Figure 2 in the Bitcoin White Paper demonstrates the complex nature of image development using LaTeX, particularly for those with a background in computer science and development rather than graphic design. This complexity is evident in the detailed and precise specification of every element within the image, using TikZ (a LaTeX package for creating graphics programmatically).*" (**Wright11 [339] {CSW/1/64}**).

"*In this specific example, the TikZ package is used to draw and position elements such as text and shapes within the document. The code meticulously defines each aspect of the image, from the rotation and placement of text to the dimensions and positions of shapes. This method requires a deep understanding of LaTeX syntax and*

the TikZ package, as well as a clear vision of how the code translates into the visual elements of the image." (**Wright11 [340] {CSW/1/64}**).

"*Possessing the ability to hold, create, and rebuild a document as intricate as the Bitcoin White Paper, especially with the use of complex LaTeX code as demonstrated, strongly indicates a direct involvement in its original creation. This level of proficiency and understanding goes beyond mere familiarity with LaTeX or TikZ; it implies an intimate knowledge of the White Paper's specific requirements and a deep understanding of its underlying structure. Such expertise is not commonly found and suggests a connection to the identity of Satoshi Nakamoto. I hold these documents and can recreate them as I created them when I wrote the Bitcoin White Paper.*" (**Wright11 [342] {CSW/1/65}**).

515. The Developers strongly suspected that these ornate passages of Dr Wright's statement were made up by ChatGPT. The Developers pressed for Dr Wright's ChatGPT records to be preserved and produced **{M1/2/133}**. He appears to have held two accounts, one of which he supposedly does not have access to and the other of which holds 22 million lines of text {Shoosmiths' letter at **{M1/2/149}**}. The Developers proposed code to enable Stroz Friedberg to check that text for content from Dr Wright's witness statement {Macfarlanes' letter at **{M1/1/151}**}. Shoosmiths responded to suggest that they "*understood*" that those checks had not resulted in any findings suggesting the use of ChatGPT {Shoosmiths' letter at **{M1/2/161}**}, but declined to respond to a request for clarification of what that meant (in particular, whether there had been any hits) {Macfarlanes' letter at **{M1/1/16**2}}. Thus, contrary to the evidence of Dr Wright **{Day15/85:12-17}**, he did not provide his ChatGPT data to COPA or the Developers.

516. In any event, Dr Wright's evidence as to his LaTeX images continues in similarly florid prose at **Wright11** Appendix B:

"*When considering the compilation of a LaTeX document into a PDF, it's crucial to understand that this process is inherently one-directional, a characteristic that is rooted in the very nature of how LaTeX interprets and renders its markup language into a document format designed for consumption, such as PDF. In technical terms, the compilation involves parsing the LaTeX source code, which includes all manner of textual content, commands for formatting, and instructions for the inclusion of additional elements, and then rendering this into a fixed layout format that PDF readers can display.*" (**Wright11 AxB [7.10] {CSW/2/27}**).

"*During this compilation, the nuanced and specific instructions contained within the LaTeX source are executed to produce a visually and structurally formatted document. This process involves a considerable amount of calculation and rendering, especially for complex document elements such as vector-based objects, which, in the case of the Bitcoin White Paper, are not separate image files but are instead generated by the LaTeX engine directly within the document as vector arrays. Once these elements are rendered into the PDF, they exist as fixed graphical entities without the underlying LaTeX instructions that generated them.*" (**Wright11 AxB [7.11] {CSW/2/27}**).

"*The transformation from LaTeX to PDF is much like translating a detailed concept into a finished artwork; the final piece does not inherently contain within it the instructions for its creation. Consequently, attempting to reverse this process (reverting a PDF to its original LaTeX source) is akin to an art analyst trying to*

deduce the precise movements and techniques used by an artist solely from the finished painting. While certain broad strokes may be inferable, the exact method and sequence of creation are lost once the artwork is complete." (**Wright11 AxB [7.12] {CSW/2/27}**).

iii. Aspose

517. Aspose is an online tool that converts PDF files to LaTeX. It encodes images using TikZ {**Rosendahl1 [196] {G/7/60}**}. On an initial review of the .tex format images in the White Paper LaTeX Files, Mr Rosendahl suspected that they might have been generated from an extant PDF document using Aspose {**Rosendahl1 [201] {G/7/61}**}, rather than in the manner described by Dr Wright. Mr Rosendahl was not able to confirm that point conclusively at the time of his first report. The conclusive evidence only emerged when Dr Wright revealed the underlying files from his Maths (OLD) and Bitcoin folders.

(a) The Aspose blob

518. Amongst the documents present on the Maths (OLD) folder on the date of its creation (17 November 2023) was a blob file entitled "88933455f3f2a39eed5f2f1d6de8ac9167a83778" (the "Aspose blob") {See the chunks.json file from Maths (OLD) at **{L21/16.1/48}**}.

519. The Aspose blob was disclosed to the Developers on 16 February 2024. The file can be seen at **{L21/18.1**}. It is an Aspose output of the Bitcoin White Paper. It bears the tell-tale signs of such an output: for example, each letter of every word in the Bitcoin White Paper is placed individually on the page.

520. The Aspose blob had first been uploaded by Dr Wright to the ZZZ folder (over which privilege had been claimed): see **{L21/16.1/48**}. Dr Wright then deleted the file: see **{L21/16.1/59}**. Unfortunately for him, however, Overleaf had not removed the blob when the snapshot of Maths (OLD) was taken.

521. When cross-examined on Day 5, Dr Wright mentioned *en passant* that he had run Aspose and had a look at the output. When he returned to give evidence on Day 15, Dr Wright confirmed that the Aspose blob was "*one of the test files I did*". He also confirmed that the output of Aspose was so crazily precise that it would be ridiculous to use it to reverse engineer the Bitcoin White Paper:

"*204:22 Q. Now, the text output from Aspose would not create a very*
23 good forgery of the Bitcoin White Paper, would it?
24 A. A horrible one.
25 Q. Because no sane person would individually place letters
205: 1 in a word in this way when composing a LaTeX file from
2 scratch, right?
3 A. More than that. It also -- the way that it draws lines,
4 and all sorts of things, are crazy.
5 Q. And indeed, if we look here, we can see that the letters
6 are placed at what seem to be nanometric levels of
7 accuracy, right?
8 A. Yes.
9 Q. Which -- four decimal places of accuracy, some of them?

10 A. Yes.
11 Q. Five decimal places. So that is --
12 A. That's correct.
13 Q. That is probably 0.0035 nanometres, and that is an
14 insane level of accuracy, so insane that it's obviously
15 ridiculous, right?
16 A. Completely ridiculous, yes.
17 Q. So it would scream out forgery?
18 A. Sorry?
19 Q. It would scream out as a forgery?
20 A. It would scream that someone's used some sort of wacky
21 tool to do something."

522. In addition to setting out the text of the Bitcoin White Paper, the Aspose blob also included each of the images. Image 2 can be seen at {L21/18.1/63}. Image 2 appears as follows in the Bitcoin White Paper:

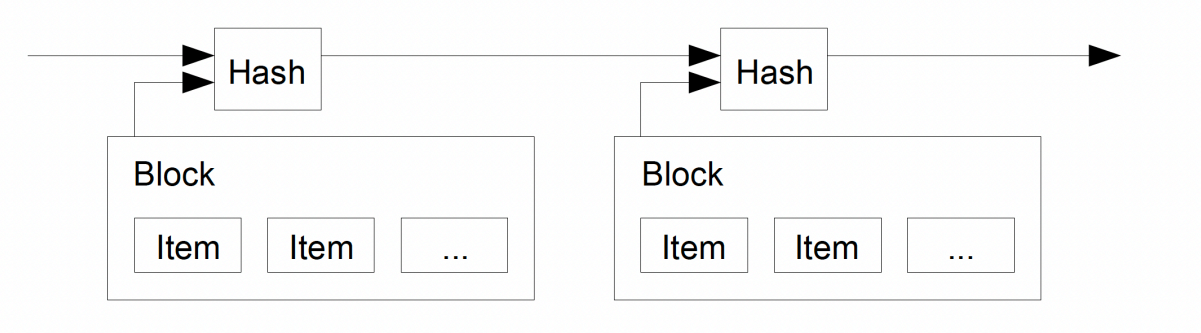


Image 2 from Bitcoin White Paper {L5/26/2}

523. There are certain anomalies with the coding of Image 2 in the Aspose blob:

523.1. colours are not identified by name (*e.g.* black), they are identified by number (*e.g.* color_29791);

523.2. font sizes are provided to unnatural levels (*e.g.* 7.144199 instead of 7 point);

523.3. unusual font names are used (*e.g.* usefont{T1}{uarial}{m}{n} instead of arialmt);

523.4. inconsistent line thicknesses are used (e.g. 1pt and 0.1pt).

Dr Wright acknowledged that it would be relatively easy to correct for these peculiarities of Aspose using a simple find and replace command {Day15/207-209}.

524. In any event, the coordinates of the lines from Image 2 are identified in the Aspose blob to a width of 0.1 point – a very precise level of accuracy {one point is 1/72.27 of an inch, i.e. 0.35 millimetres, so the coordinates are purportedly accurate to 0.035 millimetres: see **{Day15/206:12-24}**}.

(b) The identical co-ordinates

525. It emerged during Dr Wright's cross-examination that the .tex file for Image 2 in his so-called White Paper LaTeX Files used identical co-ordinates in the identical order, using identical syntax to those in the Aspose blob (subject to correction of the points mentioned in paragraph 523 above):

```
(174.8pt, -640.4pt) -- (407.6pt, -640.4pt)
 -- (407.6pt, -640.4pt)
 -- (407.6pt, -582.7pt)
 -- (407.6pt, -582.7pt)
 -- (174.8pt, -582.7pt) -- cycle
;
\filldraw[color_black][even odd rule]
(214.5pt, -588.5pt) -- (207.7pt, -590.8pt)
 -- (207.7pt, -590.8pt)
 -- (207.7pt, -586.2pt)
 -- (207.7pt, -586.2pt)
 -- (214.5pt, -588.5pt) -- cycle
;
\draw[color_black,line width=0.1pt]
(174.8pt, -588.5pt) -- (209pt, -588.5pt)
;
\filldraw[color_black][even odd rule]
(322.2pt, -594.2pt) -- (315.4pt, -596.5pt)
 -- (315.4pt, -596.5pt)
 -- (315.4pt, -591.9pt)
 -- (315.4pt, -591.9pt)
 -- (322.2pt, -594.2pt) -- cycle
;
\draw[color_black,line width=0.1pt]
(305.2pt, -594.2pt) -- (316.8pt, -594.2pt)
;
\filldraw[color_black][even odd rule]
(407.3pt, -588.5pt) -- (400.5pt, -590.8pt)
 -- (400.5pt, -590.8pt)
 -- (400.5pt, -586.2pt)
 -- (400.5pt, -586.2pt)
 -- (407.3pt, -588.5pt) -- cycle
;
\draw[color_black,line width=0.1pt]
(339.2pt, -588.5pt) -- (401.8pt, -588.5pt)
;
\filldraw[color_white][even odd rule]
(237.2pt, -640.3pt) -- (191.8pt, -640.3pt)
 -- (191.8pt, -640.3pt)
 -- (191.8pt, -605.7pt)
 -- (191.8pt, -605.7pt)
 -- (282.5pt, -605.7pt)
 -- (282.5pt, -605.7pt)
 -- (282.5pt, -640.3pt)
 -- (282.5pt, -640.3pt)
 -- (237.2pt, -640.3pt) -- cycle
;
\draw[color_black,line width=0.15pt,line join=round]
(237.2pt, -640.3pt) -- (191.8pt, -640.3pt)
 -- (191.8pt, -640.3pt)
 -- (191.8pt, -605.7pt)
 -- (191.8pt, -605.7pt)
 -- (282.5pt, -605.7pt)
 -- (282.5pt, -605.7pt)
 -- (282.5pt, -640.3pt)
 -- (282.5pt, -640.3pt)
 -- (237.2pt, -640.3pt) -- cycle
.
```

Wright's Image 2 {L21/22.2/2}

```
(174.8pt, -640.4pt) -- (407.6pt, -640.4pt)
 -- (407.6pt, -640.4pt)
 -- (407.6pt, -582.7pt)
 -- (407.6pt, -582.7pt)
 -- (174.8pt, -582.7pt) -- cycle
;
\filldraw[color_29791][even odd rule]
(214.5pt, -588.5pt) -- (207.7pt, -590.8pt)
 -- (207.7pt, -590.8pt)
 -- (207.7pt, -586.2pt)
 -- (207.7pt, -586.2pt)
 -- (214.5pt, -588.5pt) -- cycle
;
\draw[color_29791,line width=0.1pt]
(174.8pt, -588.5pt) -- (209pt, -588.5pt)
;
\filldraw[color_29791][even odd rule]
(322.2pt, -594.2pt) -- (315.4pt, -596.5pt)
 -- (315.4pt, -596.5pt)
 -- (315.4pt, -591.9pt)
 -- (315.4pt, -591.9pt)
 -- (322.2pt, -594.2pt) -- cycle
;
\draw[color_29791,line width=0.1pt]
(305.2pt, -594.2pt) -- (316.8pt, -594.2pt)
;
\filldraw[color_29791][even odd rule]
(407.3pt, -588.5pt) -- (400.5pt, -590.8pt)
 -- (400.5pt, -590.8pt)
 -- (400.5pt, -586.2pt)
 -- (400.5pt, -586.2pt)
 -- (407.3pt, -588.5pt) -- cycle
;
\draw[color_29791,line width=0.1pt]
(339.2pt, -588.5pt) -- (401.8pt, -588.5pt)
;
\filldraw[color_283006][even odd rule]
(237.2pt, -640.3pt) -- (191.8pt, -640.3pt)
 -- (191.8pt, -640.3pt)
 -- (191.8pt, -605.7pt)
 -- (191.8pt, -605.7pt)
 -- (282.5pt, -605.7pt)
 -- (282.5pt, -605.7pt)
 -- (282.5pt, -640.3pt)
 -- (282.5pt, -640.3pt)
 -- (237.2pt, -640.3pt) -- cycle
;
\draw[color_29791,line width=1pt,line join=round]
(237.2pt, -640.3pt) -- (191.8pt, -640.3pt)
 -- (191.8pt, -640.3pt)
 -- (191.8pt, -605.7pt)
 -- (191.8pt, -605.7pt)
 -- (282.5pt, -605.7pt)
 -- (282.5pt, -605.7pt)
 -- (282.5pt, -640.3pt)
 -- (282.5pt, -640.3pt)
 -- (237.2pt, -640.3pt) -- cycle
```

Aspose blob Image 2 {L21/18.1/63}

526. When that coincidence was drawn to Dr Wright's attention, his initial reaction was to argue that this was because "*it's a digital file*", rather than his use of Aspose.

> *210:14 Q. I mean, just keep that document up on screen but go back*
> *15 to page 63 {L21/18.1/64}, and then can we open up*
> *16 {L21/22.2/1} alongside it. So {L21/22.2/1}, that is*
> *17 the text file for image 2 from your White Paper LaTeX*
> *18 files, Dr Wright.*
> *19 Can we go to page 2 {L21/22.2/2}. Do you see it has*
> *20 exactly identical coordinates to your Aspose document?*
> *21 A. In these sections, they would. It's going into a lot of*
> *22 detail, so ...*
> *23 Q. Down to less than one twentieth of a millimetre.*
> *24 A. Because it's a digital file. So, if I've created*
> *25 something and it's using a digital file, then it's going*
> *211: 1 to come out with the same.*

2 Q. There's only one reason for this, Dr Wright. It's that
3 you used Aspose to forge your documents, didn't you?
4 A. No, I did not.

(c) The identical letter placement

527. In its rendering of Image 2, the Aspose blob characteristically set out the words in the image by placing each letter of the image individually.

528. Thus, in the Aspose blob the letters of each word in Image 2 were purportedly set to within 0.0001 of a point, a precision equivalent to 0.035 microns, or about one thousandth of the width of a human hair.

529. During Dr Wright's cross-examination it emerged that, whilst the Image 2.tex file had maintained the letter B in the word Block in the same position as in the Aspose blob, he had remembered to convert the placing of the remaining individual letters of the word Block after the letter "B" and as a full word. The relative coding of the Aspose blob and Dr Wright's Image2.tex file can be compared as below:

```
\begin{picture}(-5,0)(2.5,0)
\put(197.2,-616.1){\fontsize{7.144199}{1}\usefont{T1}{uarial}{m}{n}\selectfont\color{color_29791}B}
\put(201.9988,-616.1){\fontsize{7.144199}{1}\usefont{T1}{uarial}{m}{n}\selectfont\color{color_29791}l}
\put(203.6008,-616.1){\fontsize{7.144199}{1}\usefont{T1}{uarial}{m}{n}\selectfont\color{color_29791}o}
\put(207.4994,-616.1){\fontsize{7.144199}{1}\usefont{T1}{uarial}{m}{n}\selectfont\color{color_29791}c}
\put(211.1003,-616.1){\fontsize{7.144199}{1}\usefont{T1}{uarial}{m}{n}\selectfont\color{color_29791}k}
\end{picture}
```

Leftmost word "Block" of Image 2 in the Aspose blob {L21/18.1/63}

```
\begin{picture}(-5,0)(2.5,0)
\put(197.2,-616.1){\arialmt\fontsize{7}{1}\selectfont\color{color_black}Block}
\end{picture}
```

Leftmost word "Block" of Image 2 in the Dr Wright's Image2.tex file {L21/22.2/2}

530. When it was put to Dr Wright that he had achieved this outcome by manipulating the Aspose blob file, he denied it:

211: 5 Q. If we go to page -- if we look on page 2, do you see
6 where, on the left-hand side -- actually on
7 the left-hand side page, so page {L21/18.1/63}, we can
8 see the word "Block", right?
9 A. We can.
10 Q. On the right-hand side, we can see the letter "B" for
11 "block" is there; do you see? "Put" --
12 A. I do.
13 Q. Right. And the letter B is placed exactly where it
14 starts in the Aspose document, so you used Aspose to
15 place the beginning of that word, didn't you?
16 A. No, because that would actually end up producing
17 something slightly different to mine.
18 Q. But you have remembered that you needed to convert
19 the individual placing of letters into a full word,
20 right?

21 A. No.
22 Q. Because if you had placed each letter individually, it
23 would have screamed out that it was a forgery, right?
24 A. Again, it would show that an automated tool had created
25 it. But, no, I didn't do that.

531. Unfortunately, for Dr Wright, he had forgotten to make the same adjustment to the Aspose coding of the leftmost word "Item" in the Image2.tex file:

```
\begin{picture}(-5,0)(2.5,0)
\put(202,-631.7){\fontsize{7.144199}{1}\usefont{T1}{uarial}{m}{n}\selectfont\color{color_29791}I}
\put(203.9989,-631.7){\fontsize{7.144199}{1}\usefont{T1}{uarial}{m}{n}\selectfont\color{color_29791}t}
\put(205.8986,-631.7){\fontsize{7.144199}{1}\usefont{T1}{uarial}{m}{n}\selectfont\color{color_29791}e}
\put(209.8965,-631.7){\fontsize{7.144199}{1}\usefont{T1}{uarial}{m}{n}\selectfont\color{color_29791}m}
\end{picture}
```

Leftmost word "Item" of Image 2 in the Aspose blob {L21/18.1/64}

```
\begin{picture}(-5,0)(2.5,0)
\put(202,-631.7){\arialmt\fontsize{7}{1}\selectfont\color{color_black}I}
\put(203.9989,-631.7){\arialmt\fontsize{7}{1}\selectfont\color{color_black}t}
\put(205.8987,-631.7){\arialmt\fontsize{7}{1}\selectfont\color{color_black}e}
\put(209.8965,-631.7){\arialmt\fontsize{7}{1}\selectfont\color{color_black}m}
\end{picture}
```

Leftmost word "Item" of Image 2 in the Dr Wright's Image2.tex file {L21/22.2/3}

532. Thus, every letter of the word Item had been placed in the identical (to 0.035 microns) position in both the Aspose blob and Dr Wright's Image2.tex file.

533. When his use of the Aspose blob file to create the Image2.tex file in his White Paper LaTeX Files was put to Dr Wright, he veered between claiming that he had achieved this on his graphic tablet to blaming Mr Ager-Hanssen and Zafar Ali KC.

212: 1 Q. If we then go to page 3 {L21/22.2/3} and go to
2 {L21/18.1/64} on the left-hand side and let's go to
3 the word "item". You forgot to change the word "item"
4 from its Aspose encoding, didn't you, Dr Wright?
5 A. I did not.
6 Q. Every letter of that word has been positioned in exactly
7 the same position as your Aspose output, right?
8 A. Where is this document from?
9 Q. The document on the right is image 2.tex from your White
10 Paper LaTeX files.
11 A. Which particular?
12 Q. All of them, actually.
13 A. That's not --
14 Q. It doesn't change from 17 November, the earliest one
15 that we've got.
16 A. That's not how mine was, so ...
17 Q. This is down to 0.035 of a micron, right?
18 A. Possibly.
19 Q. Which is about the length of a short segment of DNA,
20 Dr Wright. It is tiny, right?

21 A. A digital file will do it, but mine -- none of mine have
22 that error, the originals.
23 Q. That is your LaTeX file, Dr Wright, on the right. That
24 is it.
25 A. Not necessarily. As I said, I had someone on my
213: 1 computer the whole time.
2 Q. Dr Wright, you cannot and would not have placed those
3 letters to that level of accuracy if you were composing
4 the Bitcoin White Paper in LaTeX from scratch.
5 A. No, I would, because what you do is you use a tool. So
6 the tool is a graphic tablet, and when you draw on
7 a graphic tablet it records, right down to the --
8 Q. Dr Wright, it's absurd to suppose that using a graphic
9 tablet you're going to get exactly the same level of
10 accuracy, down to 0.035 nanometres -- so 0.035 of
11 a micron, actually -- get it right -- sorry.
12 MR JUSTICE MELLOR: A schoolboy error.
13 MR GUNNING: Down to 0.035 of a micron, using your tablet.
14 A. No, actually, the other way round. What you're saying
15 is if you take a digital document and then analyse it.
16 But what I suspect, if this in my Overleaf,
17 unfortunately, Mr Ager-Hanssen already demonstrated that
18 he had access to all my things.
19 Q. That's not going to do either, because the syntax of
20 the code for your images is identical to the syntax of
21 this Aspose output, right?
22 A. It's similar in parts, yes.
23 Q. Every line break in the code is in the same place, every
24 command is in the same order, every line is in the same
25 order. You used Aspose, Dr Wright.
214: 1 A. No, I did not. What I had done before this is I'd said
2 how important this was to Mr Ager-Hanssen and Ali Zafar.

(d) Conclusions

534. I agree that Dr Wright cannot plausibly blame Mr Ager-Hanssen or Zafar Ali KC for the .tex image files in his so-called White Paper LaTeX Files. That suggestion is flatly contradicted by Dr Wright's own boasting about the technical artistry demonstrated by those self-same files set out in **Wright11** and at [514] to [516] above.

535. Every single one of the .tex files in Dr Wright's White Paper LaTeX Files is based on the Aspose blob.

Image	Aspose blob reference	.tex file reference
1	{L21/18.1/69}	{L21/20.2}
2	{L21/18.1/63}	{L21/22.2}
3	{L21/18.1/122}	{L21/23.2}
4	{L21/18.1/158}	{L21/11.2}
5	{L21/18.1/204}	{L21/24.2}
6	{L21/18.1/200}	{L21/26.2}

7	{L21/18.1/244}	{L21/27.2}

536. In relation to Image 1, it can be seen from page 2 of the Bitcoin White Paper that the words "Verify" and "Sign" are in slanted text **{L5/26/2}**. Aspose's output did not slant individual text characters; it placed each letter so that it ran horizontally rather than diagonally. The effect of compiling the Aspose output would accordingly be that the slanted text would be shown as a series of staggered horizontal letters, rather than slanted text. Dr Wright inserted new code for the slanted text at the top of the Image1 code **{L21/20.2/1}**. He would have encountered a difficulty with that code because his code set the position of the text relative to a specific point on the page. If he needed to move the slanted text he would have to change the coordinates – as a result he could not move the slanted text together with the rest of Image1: see the animation **{L21/13}** at Row 492. The Developers suggested it was a reasonable inference (and I agree) that that is why he replaced the .tex files with pdf images, as described in paragraph 481.4 above.

537. In short, as Counsel for the Developers submitted, it is clear that Dr Wright used Aspose to create his image files, sought to cover up his use of Aspose by placing the Aspose data in the ZZZ folder over which privilege was wrongly claimed and then concocted (probably with ChatGPT) a fantastical description in **Wright11** of the supposed exceptional craftsmanship in the creation of the files which he then used to claim that only he could be Satoshi Nakamoto.

e. Impossibility

538. Finally, it is necessary to mention Mr Rosendahl's evidence on Dr Wright's White Paper LaTeX Files.

539. Dr Wright had given a confusing account of the method by which he had supposedly compiled the White Paper LaTeX Files at **Wright8 [74-76] {E/23/22}**. He suggested that his "*Linux environment was integrated with Windows and supported Wine*". He went on to refer to MiKTeX being "*configured on Linux to use LaTeX packages and compilers including ... TeX Live: I used this as an alternative to MiKTeX on Linux*". He concluded by saying that "*These tools offered functionality similar to what MiKTeX provided on Windows*". This was more technobabble, for the reasons set out below.

540. It was suggested during the cross-examination of Mr Rosendahl **{Day17/26-27}** that the Court should understand that to mean that:

    540.1. Dr Wright used LaTeX with both Windows and Linux.

    540.2. When using Windows, he used MiKTeX as the TeX distribution on Windows.

    540.3. When using Linux, he used TeX Live as the TeX distribution as an alternative to MikTeX.

541. It is difficult to square that *ex post facto* rationalisation of Dr Wright's evidence with what he actually said in his witness statement. The real explanation for Dr Wright's evidence is that he did not know what he was talking about in **Wright8**, because he had not used LaTeX in the way that he was describing. In any event, Mr Rosendahl identified 6 characteristics of the White Paper LaTeX Files that demonstrated that they could not have been used to compile the Bitcoin White Paper.

i. fontspec

542. Dr Wright's White Paper LaTeX Files purport to call on a package entitled "*fontspec*" {*e.g.* at **{L21/9.1/2**}} to set custom fonts.

543. Dr Wright contended that he had compiled the Bitcoin White Paper in LuaLaTeX {**Wright8 [32-35] {E/23/13}, Wright8 [70-73] {E/23/20**}, Wright cross-examination **{Day5/143-146}** and Rosendahl cross-examination **{Day17/31:12-13}**}. As Mr Rosendahl noted, *fontspec* did not work with LuaLaTeX in March 2009 when Dr Wright had supposedly compiled the Bitcoin White Paper from the White Paper LaTeX Files {**Rosendahl1 [124] {G/7/43}**}.

544. It would accordingly not have been possible for Dr Wright to have used LuaLaTeX at the date of the Bitcoin White Paper, without a custom version of *fontspec* {**Rosendahl1 [126] {G/7/44**}}. Mr Rosendahl provided a detailed explanation of the difficulty that would have been involved in creating such a custom environment at **Rosendahl1 [127] {G/7/44}**.

ii. hidelinks

545. The "*hyperref*" package in LaTeX defines commands to add hyperlinks to a PDF file compiled in LaTeX. Dr Wright's White Paper LaTeX Files purport to call on a "*hidelinks*" option from that package {*e.g.* at **{L21/9.1/4**}. That option hides the fact that links within the document are hyperlinks, by displaying them without underlining {**Rosendahl1 [130] {G/7/45}**}. Mr Rosendahl explained that the "hidelinks" option was only added to the hyperref package in 2010 (*i.e.* after the Bitcoin White Paper) {**Rosendahl1 [130] {G/7/45}**}.

iii. unicode-math

546. The author of *fontspec* developed a companion package called "*unicode-math*". In 2009 it was in its infancy and supported very few fonts – and did not support Times New Roman, which was used for the formulae in the Bitcoin White Paper {**Rosendahl1 [134] {G/7/46}**}.

547. Further, the early versions of *unicode-math* suffered from a load-order problem: when used together with the "*amssymb*" package that defines additional mathematical symbols, the *unicode-math* package needed to be loaded before the *amssymb* package. Dr Wright's White Paper LaTeX Files load *unicode-math* after *amssymb*, meaning that TeX would have issued an error for every one of the 2307 mathematical symbols defined by the former package {**Rosendahl1 [136] {G/7/46**}}.

548. Mr Rosendahl acknowledged in his report that these features could *in theory* have been resolved by working on the source code privately. That was seized upon in his cross-examination in which it was suggested that "*it would have been technically possible in 2008/2009 for Dr Wright to have customised the code to … enable the use of Times New Roman*" **{Day17/30:22-24**}. In re-examination, Mr Rosendahl confirmed that this would have taken "*a matter of weeks, for someone with the technical knowledge*" **{Day17/35:15-16}**.

549. However:

549.1. Dr Wright has not produced a single document evidencing any private work on the source code for the *unicode-math* package;

549.2. Dr Wright lacked the capability to develop any such source code. The Developers reminded me of his evidence that "*I know LaTeX. I don't -- I'm not an academic, I don't teach it, so I don't know all the terminology*." **{Day15/132:13-14}.** There is also no reference to LaTeX in his contemporaneous CVs – an odd omission if he was developing related code at the time.

549.3. The *unicode-math* package was in the event only used by Dr Wright with Times New Roman in his so-called White Paper LaTeX Files for one thing: the Greek letter λ. {**Rosendahl1 [137] {G/7/46}**}. The Bitcoin White Paper uses the Times New Roman font in all its formulae, but Dr Wright's White Paper LaTeX Files wrongly do not: see **Rosendahl1 [153-154] {G/7/49}**. I agree that it beggars belief that Satoshi Nakamoto would have spent weeks working to revise the *unicode-math* package for the benefit of using a non-standard font on a single character.

iv. \AddToShipoutPictureBG*

550. The package "*eso-pic*" can be used to place pictures at specific coordinates on a page. In 2009 that could be done using a command called \AddToShipoutPicture*. The name of that command changed to \AddToShipoutPictureBG* in 2010 {**Rosendahl1 [139-140]{G/7/47}**}.

551. Dr Wright began to add the \AddToShipoutPictureBG* command to the BitcoinSN.tex file in the Maths (OLD) project from 18 November 2023 after he began to replace images with pdfs as described at paragraph 481.4 above {See the addition of the eso-pic package at Row 617 of the Maths (OLD)_chunks.xlsx file and addition of the \AddToShipoutPictureBG* command at Rows 6187, 625, 703, 825, 1065, 1067, 1072 and 1074}.

552. I agree that Dr Wright's use of that anachronistic command (together with the fact that he was only introducing it on 18 and 19 November 2023) shows that the White Paper LaTeX Files cannot have been the genesis of the Bitcoin White Paper.

v. The arrows.meta library

553. TikZ is a large package that is used to create graphics in LaTeX. It allows pictures to be defined programmatically and, given its complexity, is broken down into many different libraries with additional functionalities and features {**Rosendahl1 [143] {G/7/47}**}.

554. The White Paper LaTeX Files make use of the arrows.meta library in TikZ **{L21/9.1/3}**. That library was only released in September 2013 {**Rosendahl1 [145] {G/7/48**}}. Any file that loaded the arrows.meta library could not have been created in 2009 {**Rosendahl1 [146] {G/7/48}**}.

vi. luacode

555. The White Paper LaTeX Files purport to use a package called "*luacode*" **{L21/9.1/4}**. That package defines a few convenience functions to make it easier to use the Lua language from within LuaTeX {**Rosendahl1 [150]{G/7/48}**}. However, the package was

not issued until November 2010 {**Rosendahl1 [150] {G/7/48**}}, and so cannot have been used in the creation of the Bitcoin White Paper.

f. Summary

556. On the basis of all of the above, Counsel for the Developers submitted that Dr Wright's attempt to replicate the Bitcoin White Paper, oblivious to the fact that his activity was being recorded by Overleaf, his misunderstanding of the metadata of the Bitcoin White Paper, his reverse-engineering of the images using Aspose and his inability even to limit himself to contemporaneous LaTeX packages and commands make his claim to have compiled the Bitcoin White Paper in LaTeX seem laughable.

557. As Counsel also submitted, this is no laughing matter. The end-product of Dr Wright's activity in Overleaf was presented to the Court at the PTR as being capable of producing an "*exact replica*" of the Bitcoin White Paper. It was said to "*uniquely code*" for the Bitcoin White Paper and to contain Dr Wright's "*digital watermark*". All of that was untrue. The basis for Dr Wright's application to the Court on 1 December 2023 was a lie. I agree that his application was a fraud on the Court and a fraud on COPA and the Developers, bearing in mind that the possible consequences of this application included an adjournment of the trial, possibly for a year and a potential loss of counsel team for COPA.

558. Moreover, Counsel submitted that Dr Wright's incompetent and dishonest account of the production of the Bitcoin White Paper shows that Dr Wright does not know how the Bitcoin White Paper was produced. It shows that he is not Satoshi Nakamoto. I can only agree.

G. The true position as regards the Bitcoin White Paper

559. I agree there is no particular secret to the way in which the Bitcoin White Paper was produced. The metadata of the documents shows that it was produced in OpenOffice2.4 (see **{G/7/17}**). It was not produced in LaTeX.

560. That was common ground between both parties' experts: see **{Q/5/1}**. It was a conclusion based on sound foundations. Stroz Friedberg were able to recreate identical sections of the Bitcoin White Paper using OpenOffice 2.4 {**Lynch 1 [120] {I/5/35}**}. Even leaving aside the "aesthetic" considerations to which reference was made in cross-examination **{Day17/10-14**}, Mr Rosendahl was able to identify five specific features of the "innards" of the Bitcoin White Paper PDF which showed that it had been created in OpenOffice2.4 and not in LaTeX:

    560.1. The fonts included in the Bitcoin White Paper as subsets have names comprised of 16-letter string, followed by the character '+' and the name of the font {see the first column of Figure 2.1 at **{G/7/12}**}. If the PDF had been generated using a TeX engine, the 6-letter designations would have been chosen randomly {**Rosendahl1 [47] {G/7/16}**}. In the Bitcoin White Paper, they are chosen in a predictable manner (e.g. BAAAAA, CAAAAA etc) {**Rosendahl1 [47] {G/7/16}**}. That is consistent with how fonts are labelled when converting to PDF within OpenOffice {**Rosendahl1 [48] {G/7/16}**}.

560.2. All of the fonts included in the Bitcoin White Paper are TrueType fonts. That does not correspond to the output expected of any TeX engine even when TrueType fonts are used by the document. OpenOffice does, however, embed fonts in that way {**Rosendahl1 [49-50] {G/7/17}**}.

560.3. The page content stream of the Bitcoin White Paper involves individual characters being written into the PDF file one-by-one {**Rosendahl1 [52-53] {G/7/18}** and Figure 2.5 at **{G/7/18}**}. That is not consistent with the document being created with pdfTeX, in which words are built from printable characters or glue (i.e. spacing to account for kerning inside words) {**Rosendahl1 [53-55] {G/7/19}** and Figure 2.6 at **{G/7/18}**}.

560.4. The trailer of the Bitcoin White Paper contains an element "/DocCheckSum", which is unique to OpenOffice and is not output by any other PDF producer {**Rosendahl1 [60] {G/7/19}**}.

560.5. The header of the Bitcoin White Paper contains binary bytes that correspond to hexadecimal encoding (c3 a4 c3 bc c3 b6 c3 9f) that is only consistent with OpenOffice and software based on it such as *libreoffice* {**Rosendahl1 [62-63] {G/7/22}** and Figure 2.12 **{G/7/23}**}. The coding would be different if a TeX engine had been used {**Rosendahl1 [64]** and Figure 2.11 **{G/7/23}**}.

561. In short, the Bitcoin White Paper was produced by Satoshi Nakamoto in OpenOffice 2.4 and exported as a PDF. In my judgment, Dr Wright's elaborate attempt to carve an alternative narrative by forging documents in LaTeX mark him as a fraud and his claim in these proceedings as a fraudulent claim.

562. The documents produced by Dr Wright on 16 February 2024 provided irrefutable evidence of his forgery of the White Paper LaTeX Files ahead of their disclosure to COPA and the Developers.

563. For completeness, I return to the convoluted submissions made by Counsel for Dr Wright which I set out in [421] above. In light of the above analysis, they can be seen as a forlorn attempt to rescue something from the wreckage of the LaTeX files. I have no hesitation in rejecting all three submissions.

THE SECOND CHRONOLOGICAL RUN

564. I am now able to address those aspects of Dr Wright's positive case which do not depend entirely on documents which are alleged to have been forged. These aspects were succinctly summarised in section II of the written Closing Submission prepared by his Counsel, fully developed in sections III and IV and certain key aspects were developed by Lord Grabiner KC in his oral closing submissions. For ease of reference, I have labelled these key aspects A to J. These correspond to the parts in section III of Dr Wright's written closing, albeit not precisely, in two respects:

564.1. First, I have added additional sections to address points which did not really feature in the summaries in section II, including the writing of the Bitcoin Source Code and the events in 2011 when Dr Wright made his first public comments on Bitcoin. Under each heading I set out in italics the (accurate) summary of the point presented in section II of Dr Wright's written closing.

564.2. Second, certain matters have relevance under adjacent headings.

565. I address each of these aspects in turn. Although I have given careful consideration to the way these headline aspects were developed in written and oral argument on behalf of Dr Wright, and in Dr Wright's witness statements, it is not necessary for me to rehearse or address every point relied on. The principal reason for that is because Dr Wright's lying has been so extensive and pervasive on certain matters it is impossible to discern the dividing line between truth and lies, particularly in relation to events prior to the release of the Bitcoin White Paper but also certain of the events relied upon after that. I therefore focus on a few points of significance. Although I make findings on certain discrete matters in these sections and refer to findings I have made elsewhere (particularly as to forgery of documents), in large part I reserve my overall finding to the end.

566. For understandable reasons, in sections II, III & IV of their Closing, Counsel for Dr Wright focussed on points which they say support his claim to be Satoshi. It should be noted, however, that they did not focus upon and in many cases, did not even mention, a whole series of matters which indicate Dr Wright is not Satoshi.

567. Dr Wright's first witness statement was supposed to contain his evidence in chief on the Identity Issue. It is therefore not surprising that most of the elements A-J feature in that witness statement.

A. Skills, Knowledge and Experience

> *'3. Dr Wright has the required skills, knowledge and qualifications to have created the Bitcoin system and authored the White Paper. These qualifications include: (i) his master's degree in statistics from the University of Newcastle {e.g. {L1/337}} and his LLM from the University of Northumbria {Wright 1 [56]-[60] {E/1/12-13}}; (ii) his numerous other degrees and qualifications including his PhD in Computer Science and Economics and postgraduate degrees spanning many other disciplines, including statistics, game theory, finance, economics and law {Wright 1 [6] {E/1/3}}; and (iii) his cyber security certifications issued by the SANS Institute, including Global Information Assurance Certificates in forensics analysis, reverse engineering malware and the security of .NET code {{L1/327/1}, {L2/128/1} and {L2/282/1}}. This combination of skills and knowledge is consistent with the creation of a system that combines and applies a wide variety of pre-existing technologies and concepts, including cryptography, digital signatures, hash functions, distributed ledgers and game theory.'*

568. By way of background, I refer to the following sections in the Appendix which contain my findings that the following documents, relevant to these matters, were forged by Dr Wright:

568.1. Section 6: Statistics Assessment Homework.

568.2. Section 8: LLM Dissertation Proposal 2.

568.3. Section 12: False LLM Proposal 'Proposala.rtf'.

Coding experience in C++

569. In terms of his alleged coding experience, the foundation was laid in **Wright1** at **[25]** in the following terms:

> *'My fascination with coding and computing began when I dabbled with C and C++ around the age of eight or nine. By age 11, I had already started writing code for games. I used C and C++ because they were the languages that games were written in. As I discuss below, while I have worked extensively with various coding languages, C++ has remained a cornerstone of my expertise.'*

570. Professor Stroustrup's unchallenged evidence was that the name C++ was first coined in December 1983, when Dr Wright was 13 years old. When this was put to Dr Wright, he did not suggest he had made an error with the dates. Instead, he 'clarified' that he had been writing in precursor languages. He proceeded to refer to K&R C (K&R being the authors of an early version of C), 'Object C' (which is how Dr Wright referred to Objective C) and then Solaris C and that in 1989 a formal version of C++ and then ANSI C++, a year later, were developed. It was suggested to him that all of this was fabricated detail because he had been found out, to which his response was '*what I'm doing is simplifying so that people understand'*.

571. Although this is a small point in the great scheme of things, it is also revealing because it is an example of what became a very familiar sequence in Dr Wright's evidence:

    571.1. Dr Wright gives an account in his witness statement of something which might appear to be uncontroversial and of minor relevance, but is a foundation or building block of his case that he is Satoshi. It is in fact either wholly or partially fabricated.

    571.2. COPA produce evidence challenging Dr Wright's account.

    571.3. Dr Wright prepares his response or excuses, and these he deploys in cross-examination. Only very rarely does he accept he was mistaken. Instead, his response/excuses frequently rely on technical points never mentioned before but explained in some detail, so are difficult to deal with at the time they are deployed and not critical enough to warrant rebuttal evidence or any further questioning.

572. In this instance, it is highly likely that, having read Professor Stroustrup's statement, Dr Wright had researched the precursors to C++ and that his detailed account of the development to C++ was true. However, if he really had started with K&R C and had Knuth's book, it is most unlikely that he would have said what he said in **[25]**. There was no reason to 'simplify' these matters because anyone could have understood references to various different precursor languages.

573. Later in **Wright1**, Dr Wright said in **[71]** that '…**C++ continues to be** an integral part of my coding knowledge and skills, underscoring its enduring relevance in my professional career' (emphasis added). He went on to give four examples including:

    573.1. His extensive employment of C++ at Integyrz, a company he founded and ran from early 2009 to early 2011 which he said specialised in cryptographic code development.

573.2. His role as a BDO auditor involved conducing security reviews of code for prominent organisations including banks, necessitating in-depth exploration of various programming languages including C++.

573.3. His acquisition of 'numerous SANS/GIAC certifications that pertain to both C++ and C#.

573.4. Coding competitively, entering into a C++ coding competition with the SANS Institute and coming first, third, fourth and seventh (there being no limit to the number of times he could enter).

574. The SANS Institute competition was concerned with identifying flaws in certain passages of C++ code set out in various textbooks, and, according to Dr Wright, re-writing the sections of code more securely. Again, this is consistent with Dr Wright's role in IT security reviewing malware. It is a somewhat different skill to writing C++ code from scratch. In my judgment, the same point applies to Dr Wright's GSSP-C and GSSP.net certification by GIAC.

575. In their Closing Submissions, the Developers drew together a number of points which cast doubt on Dr Wright's proficiency in C++, but since all these points relate specifically to the Bitcoin Source Code, they are best considered below.

Academic qualifications

576. On several occasions, Dr Wright boasted of having numerous degrees, doctorates and qualifications in '*relevant disciplines*'. There was specific evidence of his MStat degree from the University of Newcastle, his LLM from the University of Northumbria and his PhD in Computer Science and Economics. He also spoke of his various certifications relating to coding (just mentioned) and his qualifications in IT Security matters.

577. It is true, as Dr Wright's Counsel submitted in closing, that COPA did not challenge his primary evidence as to his degrees and qualifications, although COPA and the Developers made it clear they did not mean he was Satoshi. The scope and extent of his knowledge was also challenged in three specific respects which I deal with below. However, at the general level, in other circumstances I would not have commented further on these matters. In the context of this case where Dr Wright has, in my judgment, engaged in wholesale forgery, fabrication and exaggeration, it would not come as a surprise to find that he had also engaged in significant exaggeration as to his degrees and qualifications. However, I will proceed on the basis that everything he said about his degrees and qualifications is true.

578. In their written closing, Counsel for Dr Wright addressed three specific topics on which Dr Wright's knowledge and expertise was the subject of challenge. These were (a) COPA's allegation of plagiarism by Dr Wright in his LLM Dissertation, (b) COPA's forgery allegation relating to his LLM Proposal and (c) Mr Hearn's evidence about the July 2016 dinner with Dr Wright.

579. I deal with the disputes over the dinner in its chronological context below. The significance of the first two topics lies in the fact that in **Wright1 [56]-[60]**, Dr Wright said (a) that from 2005-2007, in addition to his work at BDO, he pursued his LLM, (b)

over several months he 'painstakingly drafted and edited my LLM thesis' and (c) 'my exploration of these issues subsequently informed my vision for Bitcoin'.

580. Since his LLM Dissertation was a published document, Dr Wright was not able to manipulate its content. His LLM proposal was not a published document. In sections 8 and 12 of the Appendix, I have found that Dr Wright's LLM Proposal documents were forged by him to include references to concepts taken by him from the Bitcoin White Paper.

581. As for the content of his LLM Dissertation itself, in my judgment at [2023] EWHC 2642 (Ch) I refused permission to COPA to plead the alleged plagiarism by way of similar fact, on the basis that (see **[78 ii)]** '*the accusation that Dr Wright takes credit and passes off the work of others as his own pales into insignificance when viewed against the principal issue which is whether he is Satoshi and the evidence which has already been foreshadowed that the trial Judge is likely to hear*.' At **[78 i)]** in that Judgment I recorded the acceptance by the then leading counsel for Dr Wright that COPA would be entitled to cross-examine Dr Wright at trial about his copying of passages from the identified works of Hilary Pearson on the basis that he had identified his LLM thesis as containing work which contributed to his development of Bitcoin.

582. The extent of Dr Wright's copying from Ms Pearson's works was set out in an article she exhibited which was written by 'paintedfrog'. Ms Pearson (a former partner in Bird & Bird) confirmed the analysis was accurate and that the passages identified as copied from her own works copied were her own original work. The two opening paragraphs of her paper entitled '*Liability of Internet Service Providers*' (1996) were copied word for word. There were other instances of verbatim copying but the majority of the material was reworded, rather than copied verbatim. That paper contained 58 paragraphs, of which 45 were copied by Dr Wright, 25 in full and 20 in large part. I agree that the plagiarism was extensive and methodical.

583. Dr Wright also copied and reworded a paragraph from another of Ms Pearson's papers entitled '*Intellectual Property and the Internet: A Comparison of UK and US Law*' (1998). The paintedfrog article goes on to discuss copying of text and structure from other papers, including Mann & Beazley's '*The Promise of Internet Intermediary Liability*' (2005), which, unlike Ms Pearson's papers, is referenced in the dissertation, albeit with minimal credit.

584. Dr Wright was cross-examined on Day 6 about his copying from Ms Pearson's works on the basis of the paintedfrog article. His principal excuse was that in earlier versions of his dissertation, he had acknowledged Ms Pearson's work, but that his use of Endnote resulted in references to her paper(s) being removed. He also claimed that Ms Pearson's work did not '*come up properly because its not actually an academic thing, it's a blog'*. This was plainly untrue. He also claimed to have used an editing service and when the document was returned to him, he didn't notice the reference to Ms Pearson's paper(s) had been removed.

585. I found Dr Wright's evidence and excuses on this issue deeply unconvincing. He sought to reduce the whole issue to a referencing error, whereas the real point lay in just how extensive and deliberate his copying had been, which demonstrated that his evidence in **Wright1** that he had '*painstakingly drafted and edited my LLM thesi*s' was, at best, highly misleading. It also illustrated, in my judgment, that his LLM Dissertation really

had nothing to do with the genesis of Bitcoin. It also casts doubt on his assertions of having earned numerous degrees.

COPA's case as to Dr Wright's skills, knowledge and experience

586. In cross-examination, Counsel for COPA put to Dr Wright that his working history was as '*the IT security services guy'* **{Day5/177:1}** - **{Day5/178:1}**, and in submissions Counsel acknowledged that Dr Wright had taken great umbrage at this. These points were based on the following submissions, themselves based on passages in **Wright1**, his 2007 CV at **{L2/102/4}** and his 2015 LinkedIn profile at **{L11/130/16}**.

587. Counsel submitted that however competent Dr Wright may have been at IT security, he was not a visionary working at the cutting edge of designing digital payment systems. I summarised Dr Wright's employment prior to 2009 earlier (see [26]-[32] above).

588. COPA submitted that Dr Wright's 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. I agree.

589. As COPA submitted, 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*" {see **{Day6/35:25} - {Day6/38:11}}.

590. 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.

591. Thus, COPA's case provides some circumstantial evidence to suggest that Dr Wright is not Satoshi.

B. Investment in the evolution of digital cash systems

> *'4. Dr Wright has been deeply invested in the evolution of digital cash systems since the early 1990s. Examples include: his work at OzEmail, which involved the development of a payment protocol called "Millicent" that "used digital signatures" and an analogous scripting language to Bitcoin {Day 5/166/9 to 168/2}; and his work at DeMorgan, which involved extensive research and development in digital cash. The latter included project 'BlackNet', which Dr Wright described as "an encrypted internet based on crypto credits" that "morphed into Bitcoin and Metanet" {Day 5/171/17 to 173/11}.*

592. By way of background, I refer to the following sections in the Appendix which contain my findings that the following documents relevant to these matters were forged by Dr Wright:

592.1. Section 4: the BlackNet Abstract.

592.2. Section 5: the 'Project BlackNet Paper'.

Project Blacknet

593. In addition to the forged Blacknet documents, there are some authentic ones. These provide a very useful backdrop against which to assess Dr Wright's claims.

594. Dr Wright claims that he began his journey with working at OzEmail on the implementation of a payment protocol known as Millicent. 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. 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. He says little else in **Wright1** about Project BlackNet, but it features heavily in his Reliance Documents and is as prominent in **Madden1**.

595. The documents which appear to be authentic suggest that Project BlackNet 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", 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.*" **{L1/80/5}**. 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).

596. Cross-examination of Dr Wright confirmed that Project Blacknet had nothing to do with Bitcoin. Dr Wright's attempts to tie Blacknet to being "premised on crypto credits", suffer from the flaw that none of the authentic Blacknet documents says anything about such crypto credits.

597. As for the forged versions of Project Blacknet, these are addressed in section 5 of the Appendix. 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.

598. Other than the documents which I have found to be forged, my attention was not drawn by Dr Wright's Counsel to any other reliable contemporaneous document which has been shown to be authentic to support his evidence on these points. As I have already said, Dr Wright's lies have been so extensive and pervasive I do not find myself able to place any weight on something he has said unless it is corroborated by some other source which I find reliable.

599. Furthermore, the matters relied upon under this heading morph into those under the next heading, so I move to the next heading.

C. Precursor work and discussions

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

(a) At the Australian Stock Exchange (1996), Dr Wright built the "NIPPA network" that involved creating a distributed "peer network" protocol to send transactions across Australia. {Day 2/65/24 to 66/23}.

(b) At Lasseters online casino (1998), he developed "advanced security measures and logging systems" that were "an early precursor to the blockchain" {Wright 1 [38]-[44] {E/1/9}ff}

(c) At Vodafone (around 1998 to 2002), he worked on advanced logging systems that involved a "hash chain-based system" {Day 6/13/6 to 14/11}.

(d) At BDO (2004-2008), he discussed proposals for a network-based immutable ledger system with Mr Matthews (who at the time was CIO of Centrebet); and worked on projects with Dr Pang concerned with "small-world networks". {Wright 1 [53]-[55] {E/1/11}}.

(e) At the University of Northumbria (2005-2008), he produced his LLM Dissertation (2005-2008), the proposal for which contains passages that closely reflect passages in the White Paper. The LLM Dissertation itself was on the liability of internet intermediaries which are also known as 'trusted third parties' and are referenced in the White Paper. {The Impact of Internet Intermediary Liability: {L20/178/1}.' (emphasis added).

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

(a) Mr Jenkins had discussions with Dr Wright about "eGold" in around 2000-2002; about "grid computing" in around mid-2007; and about "achieving trust other than in a central bank" towards the end of 2007 or early 2008. {Day 9/54/5 to 65/24}; {Day 9/73/21 to 77/1}; Jenkins 1 [16]-[25] {E/6/5}ff.

(b) Mr Archbold had discussions with Dr Wright about digital currency in around 2004 or 2005, during his second stint at Lasseters. {Day 10/27-28}; {E/11/5} [15-16].

(c) Mr Yousuf had discussions with Dr Wright about digital currency and how the financial system was flawed as far back as 2006; and, prior to 31 October 2008, they spoke about the problem-solving capabilities of "distributed networks". {Yousuf 1 [8] and [15] {E/7/3-4}}.

(d) Dr Wright mentioned blockchain to Dr Pang on 1 August 2008, when Dr Pang purchased a Batman Lego set (for which he has the receipt). {Day 9/24-33} & the receipt dated 1 August 2008 is at {L3/57/1}.

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

600. In relation to paragraph 5(e), I refer to the following sections in the Appendix which contain my findings that the following documents, relevant to these matters, were forged by Dr Wright:

600.1. Section 8: LLM Dissertation Proposal 2.

600.2. Section 12: False LLM Proposal 'Proposala.rtf'.

601. I also refer to my findings above ([582] and following) in relation to his LLM Dissertation.

602. In relation to paragraph 5(c), Professor Meiklejohn observed in her first report that secure logging had been a standard recommended practice in the IT industry for decades, and she referred to guidance published in 1996.

Lasseter's and Vodafone

603. During his time working with Lasseter's Online Casino, Dr Wright claimed 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. It was his time at Lasseter's that he says "*planted the seeds that would later germinate into the idea of Bitcoin*". Similarly, Dr Wright charted his further career development working at Vodafone as being significant to how he would create Bitcoin. He said that, while there, he worked on the creation of secure logging and payment channels, with all system events and transactions being carefully tracked.

604. However, all the contemporaneous evidence of Dr Wright's work with Lasseter's and Vodafone (including in his own CV and profile cited above in [586]) 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. It would appear that 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 strained to characterise working on logging systems (totally normal for IT security) as being somehow a precursor to Bitcoin and suggested a continuing professional thread, ineluctably leading towards the creation of Bitcoin. I find that 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.

605. 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. 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.

BDO

606. 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. Dr Wright says that, in 2007, he introduced Mr Granger to what would become Bitcoin, though without that name. He also claims he discussed Bitcoin with Neville Sinclair. He has said on other occasions that he tried to interest BDO in investing in his nascent cryptocurrency project.

607. 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. 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 ("the Handwritten BDO Minutes"), but I have found the manuscript minutes are a forgery (see Section 9 in the Appendix).

608. Dr Wright's time at BDO also raises the point (see 5(d) above) about his proposal made to Mr Matthews at Centrebet. The only document purporting to support the claim is a supposed pitch document (not taken forward) **{L5/48}** which was found by Mr Madden to be unreliable **{Day11/88:25} - {Day11/89:17}; {Day11:107:8}**. In view of my finding as to Mr Matthews' credibility, I dismiss the suggestion that this alleged proposal was a founding part of Bitcoin.

609. More generally, it can be seen that the points relied on in paragraph 5 quoted above are put no higher than being '*relevant or related to the technology and concepts underpinning Bitcoin'*. Even taking these points at face value (i.e. assuming there is no exaggeration in them), I observe that, with the benefit of 20:20 hindsight, it is relatively easy to reach back into prior projects to pick out elements which *might* have something to do with what was utilised in either the Bitcoin White Paper or the Bitcoin system. These points therefore carry very little weight on their own. Furthermore, when viewed against the evidence of forgery pointing in the other direction, they are nothing more than unsupported assertion, from unreliable witnesses.

D. Drafting, sharing and releasing the Bitcoin White Paper

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

610. This point is put at about the highest that Counsel for Dr Wright could realistically put it, bearing in mind the evidence of forgery.

611. By way of background, I have already addressed the submissions in Section IV of Dr Wright's Closing. I refer to my conclusion above that the Bitcoin White Paper was drafted in OpenOffice 2.4. There is no evidence that it was drafted using LaTeX. It is likely that the first time that the content of the Bitcoin White Paper encountered LaTeX was in September 2023 when Dr Wright set about trying to create a forgery or forgeries which he thought (mistakenly) would not suffer from having metadata which would reveal it or them to be forged.

612. By way of further background, I refer to the following sections in the Appendix which contain my findings that the following documents, relevant to these matters, were forged by Dr Wright:

    612.1. Section 7: which concerns two documents presented by Dr Wright as precursor work to the Bitcoin White Paper.

    612.2. Section 9: the handwritten BDO Minutes which purport to set out a timetable for the development and launch of Bitcoin.

612.3. Section 10: ‘A Competing Transaction or Block Model’, presented as precursor work to the Bitcoin White Paper.

612.4. Section 11: The King2.rtf, also part of the alleged precursor work.

612.5. Section 13: ‘Hash Based Shadowing’, further supposed precursor work.

612.6. Section 14: ‘Secure and Trustworthy Voting’, further supposed precursor work.

612.7. Section 15: ‘Internal Controls and Immutable Logging in Auditing Backend Operations of Messaging Systems.rtf’, supposed precursor work on immutable logging.

612.8. Section 16: ‘NG3.tex and related files’, purporting to represent work on the Bitcoin system and/or Bitcoin related concepts.

612.9. Section 17: ‘LPA.tex’ and ‘LP1.tex’, two LaTeX documents on quorum systems, said by Dr Wright to have influenced his development of Bitcoin.

612.10. Section 18: ‘ESDT.tex’, further supposed precursor work created during Dr Wright’s time at BDO.

612.11. Section 20: Backdated White Paper PDF.

612.12. Section 21: OpenOffice 2.4 Document, a supposed precursor to the Bitcoin White Paper.

612.13. Section 22: the 12 March 2008 emails.

612.14. Section 23: Email: ‘I need your help editing a paper I am going to release’, a supposed email to Dave Kleiman in advance of publication of the Bitcoin White Paper.

612.15. Section 24: Timecoin ODT Whitepaper, purporting to be a precursor draft of the Bitcoin White Paper.

612.16. Section 25: ‘Block diffusion within bitcoin’, another supposed piece of precursor work.

612.17. Section 26: the SSRN submission, purporting to be a copy of the Bitcoin White Paper written on 21 August 2008, in which Dr Wright is named as the author.

612.18. Section 28: ‘Economics of BitCoin Nodes’, purported related work, supposedly created in September-October 2008.

612.19. Section 29: ‘Noncooperative finite games’, purported precursor work, dated to 10 September 2008.

612.20. Section 30: Coffee-stained printout of Bitcoin White Paper.

612.21. Section 31: ‘Economic Security.doc’, purported associated development work, referring to BitCoin in the future tense and dated to 5-7 November 2008.

612.22. Section 32: 'BitCoin: SEIR-C Propagation models of block and transaction dissemination', purported precursor work to the Bitcoin White Paper, dated 12 December 2008.

613. The number of those documents demonstrate that Dr Wright expended a good deal of effort in his attempts to lay a foundation in supposedly contemporaneous documents that he was Satoshi. There were also further alleged precursor documents which Mr Madden found to be inauthentic.

Dr Wright's evidence on drafting the Bitcoin White Paper

614. In **Wright1**, Dr Wright claimed to have started writing the White Paper by hand, between March 2007 and May 2008. He then claimed to have started the drafting process using voice recognition software known as Dragon. There was no mention in **Wright1** of the use of LaTeX, despite its central importance to the account he gave later. He said 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. As COPA pointed out, prior to raising LaTeX in this case in October 2023, neither in this action or in any of the other proceedings I mentioned above did Dr Wright ever claim that the Bitcoin White Paper was produced with LaTeX.

615. In **Wright4**, 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. There were 21 people on that list, of whom five are witnesses in this case and two are the subject of hearsay notices. Only two of the 21 have ever corroborated Dr Wright's account in this respect –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.

616. From March 2008 to May 2008 Dr Wright said that the draft started to look like the version that is now publicly known. Dr Wright also gave an account in the *Kleiman* proceedings of writing the White Paper which he has avowed for these proceedings, through his then solicitors, Ontier {letter of 7 March 2022, **{M/1/240}**}. Although Dr Wright has provided many drafts of the White Paper in his disclosure, in **Wright4** he said that he is unable to identify the order of production of the drafts, since he never used a versioning system. As listed above, I have found a series of White Paper drafts (and alleged precursor documents), including reliance documents, to have been forged by Dr Wright, including versions which give Dr Wright's details as author. I also note that further purported drafts of the Bitcoin White Paper were analysed by Mr Madden {see generally Appendix **PM3 to Madden 1 {H/20/1}**}. In their original 50 allegations of forgery, COPA pleaded that {**ID_000254}, {ID_000536}, {ID_000537}, {ID_000538}, {ID_003732}, {ID_004010}** and **{ID_004011}** were forgeries, all being purported drafts of the Bitcoin White Paper. As is clear from the Appendix, {**ID_000254}, {ID_000536}** and **{ID_004011}** were in the top 20 forgeries which COPA were allowed to pursue at trial.

617. Dr Wright claimed 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. According to Dr Wright, Mr Kleiman provided edits to the draft. There are several versions of the email by which Dr Wright supposedly sought Mr Kleiman's help in editing the draft ("**the Kleiman email**"). The version pleaded in the Particulars of Claim, **{ID_001318}**,

I have found to be a forgery in section 22 of the Appendix. Another version, **{ID_000465}**, I have found to be a forgery in section 23. One of the versions of this email was among the trove of documents leaked to Wired and Gizmodo in late 2015 {see the Gizmodo article of 9 December 2015 **{L11/213/4}**}.

618. Dr Wright said that, in around July 2008, he tried to communicate with Tuomas Aura, a computer science professor, but his efforts to contact him remained unanswered. Then in August 2008 he said he reached out to Wei Dei and Adam Back under the Satoshi pseudonym. He said he sent them a link to upload.ae where he had uploaded the draft. 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.

619. Dr Wright has suggested that he (as Satoshi) knew of Wei Dai's work well before August 2008, but the previously unpublished emails of Dr 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.

620. In **Wright1**, 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 first tried to deny the plain meaning of the emails, and then pivoted 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*". Dr Wright did not produce any of those "*extensive communications*". Dr Back's evidence was that he provided all of the emails he had with Satoshi {**Back, [9] {C/9/3}**} and Dr Wright's Counsel did not challenge him on that evidence.

621. 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 **{Day6/68:6} - {Day6/69:20}**:

> *"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" –"

622. 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, which tends to confirm that there is no supportive evidence for them.

623. Dr Wright then said that, while working on the White Paper, he presented his concepts to Microsoft under his own name but there was no interest in it. He claimed to have attended a series of business meetings at the Microsoft campus in Seattle in autumn 2008, but he said the specific names from those meetings "*have become hazy with time*". The few communications he has provided with Microsoft {see **{L3/247/1}** and **{L3/249/1}}** 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.

624. Dr Wright was taken through those communications in cross-examination {**{Day6/88:13} - {Day6/97:9}**}. 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. The emails that we do have appear to present a reasonably full picture of a set of communications about a regular job interview process and nothing more than that.

625. Dr Wright then claimed to have implemented the core of the Bitcoin system in Hoyts, a cinema chain in Australia, and for QSCU, a bank. However, in his dealings with the ATO, he said that he had dealt with Hoyts as a client "*in his security role*" **{L8/408/5}** and that he managed the company's firewalls **{L7/431/59 & 133}.** Meanwhile, his work for Qudos Bank (formerly known as QSCU) was done through BDO, where his work appears to have been straightforward IT security and audit work.

626. Dr Wright said that these events effectively 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. The evidence deployed to demonstrate purchase of that site Dr Wright agreed was inauthentic.

627. Dr Wright asserted that the essential elements of the code were already in place by the time of the upload, a point I pick up in the next section. Dr Wright then mentioned that he engaged with Hal Finney and Mike Hearn as Satoshi, but these were known contacts

of Satoshi derived from emails in the public domain {as Mr Hearn explained: **{C/22/4}**, at **[14]**}.

628. I have already found that I do not believe Mr Matthews's evidence about receiving a draft of the Bitcoin White Paper prior to its publication by Satoshi.

629. I have also rejected Mr Don Lynam's evidence from his Kleiman deposition about receiving a rough draft of a paper that he thought was a draft of the Bitcoin White Paper.

630. In his witness statement Mr Max Lynam spoke of Dr Wright's solicitors referring him to the evidence he gave at the *Granath* trial in Oslo in October 2022 to the effect that he '*had never read what is now known as the Bitcoin White Paper*.' He went on to say that his cousin's solicitors had proceeded to show him a copy of the Bitcoin White Paper (**{ID_000865}**, the document which Mr Madden used as the 'control copy') and said:

> *'I cannot recall whether I saw this exact paper or not, but what is written in the abstract is similar to the things that Craig sent through back then. What I do know is that in the late 2000s the papers Craig sent through covered, for example, the concept around hashing, and the secured keys pulling things through to authenticate transactions over a network. I can remember the concepts and what we were talking about, but whether it was that document or another document, I do not know as there was numerous documents with essentially the same information.'*

631. In cross-examination, Mr Max Lynam was taken to the transcript of his evidence in *Granath* in relation to his evidence about testing code for Craig. On the subject of whether he had seen a draft of the Bitcoin White Paper, he recounted that he had said we had received numerous documents and bits of information from him. The highest he was able to put it was that '*That could have been one of them*.' I found this evidence unconvincing at best. It carries no weight at all.

632. In my judgment, the evidence was overwhelming that the suggestion that Dr Wright drafted the Bitcoin White Paper or anything like it is pure fabrication. The account he gave in his witness statement(s), as summarised above, was pure fantasy. To the extent that others (such as Mr Matthews and Mr Don Lynam) were persuaded by Dr Wright to support his account, they unwisely went along with it.

E. The writing of the Bitcoin Source Code (in C++)

633. By way of background, I refer to the following sections in the Appendix which contain my findings that the following documents, relevant to these matters, were forged by Dr Wright:

633.1. Section 33: two pieces of C++ code.

633.2. Section 34: a source code flowchart.

633.3. Section 35: a hex-edited copy of bitcoin.exe.

Dr Wright's evidence about writing the Bitcoin Source Code

634. In **Wright1**, Dr Wright said he began working on the source code in 2007 using C++. He said he initially engaged in web testing and then progressed to coding a minimum

viable product prototype. 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. He said he created a repository on SourceForge to provide a centralized location for Bitcoin Source Code. All his evidence about writing the Bitcoin Source Code was expressed at a high level of generality.

635. He maintained 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. He claimed that, by early 2008, he had what he regarded as a preliminary version of the code. He said 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. He said 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. Mr Turner has never given evidence for Dr Wright.

636. COPA produced 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, based on the time zone for Sydney, Australia, where Dr Wright was living over this period. 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, Sydney time).

637. When the 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. This was just assertion on his part, and I did not find it credible, not least because 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.

638. It is notable that Dr Wright identified only a few documents which supposedly evidence his creation of the Bitcoin Source Code. In addition to those documents I found to have been forged in sections 33, 34 & 35 in the Appendix, there are **{ID_004014}** and **{ID_004015}**. The latter appears to be an edited version of the Bitcoin Source Code dating from 16 November 2008, which has been publicly available since December 2013 {see **{L20/206/1}**}. 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 **{L4/15/1}**.

639. Dr Wright said that the first email account he set up was the Satoshi GMX account in around December 2007, before later acquiring the Vistomail account. He also claimed 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 elsewhere, there are serious problems with Dr Wright's account of having acquired the Satoshi email account and web domain. Also, Mr Malmi said he first contacted Satoshi in May 2009, not February 2009 {see **Malmi1, [4a] {C/24/2}** and email of 2 May 2009 **{D/487/1}**}.

640. Dr Wright's Counsel challenged Mr Malmi in cross-examination suggesting 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 {**{Day13/6:19} - {Day13/6:24}**}. 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 suggestion. 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. 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.

The Developers cast doubt on Dr Wright's C++ coding proficiency

641. As I mentioned above, in their Closing Submissions, the Developers drew together a number of points which cast doubt on Dr Wright's proficiency in C++, and I consider these points here. As the Developers pointed out, there was little support for Dr Wright's supposed expertise in C++ in documents which can be reliably dated to 2008-2009. The section of his BDO CV which referred to 'computing skills' referred only to experience of 'C programming and Code audit' not C++. When he applied to Microsoft for a job in January 2008, he was asked '*Can you code (and do you want to)? What programming languages are you most proficient with?*' '*Please describe your experience writing code (incl. SQL queries) over the past 5 years*', and '*Which programming languages can you read, but not write*' to which he answered:

> *'Yes/Yes*
> *As for 2, yes some. I have a large amount of experiance* [sic] *decompiling C, C++, Java, script of various types, fortran, .Net, perl, Ruby and others.*
> *I have programmed in Java, though I prefer C (pure C, not even object). I used to be a C coder - way back - but I never was good at the graphics. I am not an artist and I never really liked high level languages for coding.*
> *I use R and C and occasionally C++ a fair bit for algorithmic coding and statistics work.'*

642. His decompiling experience is consistent with his role as an auditor and with malware research/analysis, looking at the decompiled code to see what the malware is trying to do, but decompiling is not coding. Bearing in mind Mr Andresen's evidence (in his Kleiman deposition {E/17/211}) that in his view Satoshi was in the top 10% of all programmers he had encountered (in the context of questions about Satoshi's actual source code written in C++), it is highly unlikely that Satoshi would have described himself as an *occasional* user of C++ in January 2008.

643. The Developers also point to Mr Hinnant's evidence in response to Dr Wright's claims about <chrono> (and the sleep_for function), <thread> and <random>, in that Mr Hinnant's evidence suggested a lack of real expertise in C++ on Dr Wright's part. They also point out that Satoshi did not use Dr Wright's 'sleep_for' function in the Bitcoin code, instead using the basic Sleep function from the Windows API, via inclusion of the headers.h file, which in turn included windows.h.

644. The Developers went on to cite three points which they submitted showed that Dr Wright cannot have written the Bitcoin Source Code:

644.1. First, his inability to describe the concept of an unsigned integer.

644.2. Second, his misunderstanding of the basic CheckBlock function in the code.

644.3. Third, his lack of knowledge regarding the proof-of-work function in the Bitcoin code which is said to have emerged in the approach taken in the cross-examination of Dr Back.

645. Counsel for Dr Wright objected to any reliance being placed on these points because (a) COPA had made it clear at an earlier hearing that they had not pleaded and were not advancing any case that Dr Wright misunderstood the technology of Bitcoin and (b) the Developers had not pleaded these points. They also submitted they should be given little, if any, weight. Notwithstanding that, they sought to downplay the challenge on the unsigned integer issue. The second and third points are somewhat related. I consider the second point in this section and what weight to give to it. The third point is closely bound up with the specific challenges made to Dr Back's evidence in cross-examination and addressed in some detail in Dr Wright's written closing.

646. I have considered Counsel's objection carefully, but I concluded that I should consider and take account of these points for several reasons: (i) partly due to Dr Wright's persistent boasting of his abilities; (ii) partly also because of Dr Wright's very extensive reply statement in Wright11 in which he raised all sorts of new points; (iii) perhaps most importantly, because he says he is Satoshi. Satoshi would be able to deal with these points. Finally, these points sit at a different level to the disputes over the technology of Bitcoin, as exemplified in Mr Gao's report.

Unsigned integer

647. The concept of an unsigned integer is simple: it cannot be negative. Satoshi often used unsigned integers in the Bitcoin code, he commonly referenced them in his emails and they are used in the Bitcoin File Format (the subject of alleged copyright which Dr Wright claims to have authored). Searches undertaken by the Developers indicate they were used 294 times across the entirety of the original Bitcoin code and over 100 times in the original main.cpp, main.h and bignum.h. Their point was that Satoshi would not have forgotten what an unsigned integer was, even after 15 years.

648. In a striking passage of cross-examination, Dr Wright was unable to explain the concept (at least until after he was taken to 'C++ for Dummies'). He was taken to the script.h file and to the declaration of a constant integer variable called *MAX_SCRIPT_ELEMENT_SIZE.* The cross-examination proceeded as follows:

4 Q. Just out of curiosity, do you know what unsigned means
5 in that?
6 A. I do. Basically it's unsigned variable, it's not an
7 integer with --
8 Q. With what?
9 A. It's larger. I'm not sure how -- I mean, on the stand
10 here, I'm not sure how I'd say it, but --
11 Q. Take a wild guess.
12 A. How I would describe it, I'm not quite sure. I know
13 what it is.
14 Q. Okay.
15 A. I'm not terribly good when I'm trying to do things like

16 this. Writing it down would be different.
17 Q. Well, do you recall you mentioned that you had a book by
18 Professor Stroustrup?
19 A. I do.
20 Q. You haven't disclosed that book, but you have disclosed
21 three other books about C++, so I want to take you to
22 one of those. It's {L1/199/1}, and could we go to
23 page 47 {L1/199/47}. Do you see that it explains that
24 "unsigned" means that it cannot be negative?
25 A. Yes, I do understand that. Would I have thought of
145: 1 saying it in such a simple way? No."

649. Some of the pauses are indicated in the transcript but on being invited to take a wild guess, there was a long pause (of about 8 seconds, albeit not referenced in one version of the transcript) before Dr Wright started his answer (a strong contrast with his usual immediate answer to any question).

650. Bearing in mind the care, effort and skill which Satoshi used in writing the Bitcoin Source Code, I agree that Satoshi would not have had any difficulty in explaining the concept of an unsigned integer, even 15 years later. Accordingly, I agree with the Developers that this evidence indicates that Dr Wright did not write the Bitcoin Source Code. Furthermore, this was a legitimate point on which to cross-examine, bearing in mind Dr Wright's much vaunted expertise in coding in C++, which he claimed still to be current. This claim has turned out to be one of many made by Dr Wright in this litigation which have common characteristics. A claim is made that he has a special (even unique) skill, knowledge or experience. The claim appears to be supported by some detail from the past which it is very difficult, if not impossible, to check or disprove, often because the detail is known only to him. Dr Wright is well aware of this. When he is challenged, he usually has some additional explanation which often involves some technical matters (which again are difficult or impossible to check or disprove during cross-examination). The claim is often either exaggerated or misleading or is simply untrue.

CheckBlock

651. As for the CheckBlock function, the Developers submitted this was one of the key functions in the Bitcoin Source Code, being the first stage in the processing of blocks under the ProcessBlock function in the main.cpp file, followed by AcceptBlock. I agree.

652. In the original source code, CheckBlock is comprised of six steps, each preceded with a single line comment as follows:

652.1. // Size limits

652.2. // Check timestamp

652.3. // First transaction must be coinbase, the rest must not be

652.4. // Check transactions

652.5. // Check proof of work matches claimed amount

652.6. // Check merkleroot

653. Each of those single line comments, save the fourth, provides a summary description of the checks that the relevant function undertakes that anybody with a basic understanding of Bitcoin could surmise. The fourth "Check transactions" is more ambiguous. Dr Wright was invited to explain what it comprised. He answered as follows:

> *"123: 6 Q. And then, fourthly, we can see that it checked*
> *7 transactions?*
> *8 A. Yes.*
> *9 Q. What was that?*
> *10 A. That it checks transactions?*
> *11 Q. Yes, what was the check of the transactions?*
> *12 A. Basically making sure that they are valid, that*
> *13 the transactions that have been received follow*
> *14 the rules, etc.*
> *15 Q. So what sort of thing?*
> *16 A. What sort of thing. So, basically, Bitcoin uses script.*
> *17 The way that you'd have to then check would be does*
> *18 the key work, does other policies work, are the output*
> *19 and script valid. It's a predicate. So, what we're*
> *20 functionally doing in here is ensuring that all of*
> *21 the input and output is structured correctly, that if*
> *22 there's a message with an ECDSA key that the correct*
> *23 previous block had been signed.*
> *24 Q. So I remember you talking the other day -- I can't*
> *25 remember which day it was -- about how, when you were*
> *124: 1 first running the Bitcoin Software, it hadn't been --*
> *2 the mining that had been absorbing all of your*
> *3 electricity, as it were, it was doing ECDSA checks in*
> *4 relation to the underlying transactions; is that right?*
> *5 A. And much more.*
> *6 Q. Okay, but when you're talking about ECDSA checking, is*
> *7 that what you're talking about in relation to --*
> *8 A. That particular part, yes."*

654. The Developers submitted that this description by Dr Wright of the "Check transactions" stage of the CheckBlock function (namely that the signature of transactions was checked) was hopelessly wrong, on the basis that the checks in "Check transactions" are set out in the main.h file at {L4/98.1/8}. Dr Wright was taken to them {Day8/124:18-p125:9}: they comprise just three basic checks of each transaction, namely checking that (a) there was at least one input and one output to a transaction, (b) the value of created UTXOs was not negative, and (c) if it was a coinbase transaction that the scriptSig was of the right size and, if it was not a coinbase transaction, that its input is not null.

655. However, Dr Wright persisted in suggesting that the CheckBlock function still checked the signatures of transactions in some mysterious, unexplained manner:

> *"125:10 Q. It did not involve checking ECDSA signatures, did it?*
> *11 A. Again, that then calls these other functions.*
> *12 Q. Dr Wright, you're wrong about that?*

13 A. I am not wrong about that. If you note this,
14 the diagram that you had is hierarchical. So, that
15 particular function calls the next function, and when
16 you're talking about checking CheckSig in that
17 particular one, then that's ECDSA, but it's not in that
18 core.
19 Q. You see, Dr Wright, this is a pretty central core point
20 in relation to the operation of the Bitcoin Software and
21 you don't know about it, do you?
22 A. Actually, I do, and you're not letting me explain it
23 properly.
24 Q. I'm going to explain it to you. Can we go, please, to
25 {L4/97.1/23}. Sorry, 98.1, I think, it is, page 23
126: 1 {L4/98.1/23}. No, 97.1, page 23 {L4/97.1/23}.
2 So, do you see here that we can see a function which
3 is described as "ProcessBlock"?
4 A. I do.
5 Q. And do you see underneath that, the preliminary check
6 that it does is called "CheckBlock"?
7 A. I do.
8 Q. And do you see that a secondary check, after CheckBlock
9 has been completed, is called "AcceptBlock"?
10 A. I do.
11 Q. Now, it is within AcceptBlock that the signatures are
12 checked, isn't it?
13 A. Basically what we have is a series of functions that
14 each of these call other functions. So, where you're
15 trying to say that each of these don't do all of that,
16 the diagram that these guys don't like is a functional
17 call mapping each of these areas down.
18 Q. I'm not asking you about any diagrams, I'm asking you
19 about what is in the CheckBlock function, and you told
20 me that within the CheckBlock function were checks of
21 ECDSA signatures.
22 A. If it's a header and everything else is underneath it,
23 then that is part of the entire function and you are
24 checking everything. So when you have one function
25 follow another to be correct, then all of those
127: 1 sub functions are part of the same function.
2 Q. I'm afraid you're wrong, Dr Wright. If we want to
3 explore how you get to signatures from the AcceptBlock
4 function, I can take you there. Do you want me to do
5 that?
6 A. Like I said, the block includes both the full check and
7 each of these. So when you have a transaction that you
8 have checked, it then goes into the block and it's put
9 into a binary tree structure. All of that is checked as
10 part of the entire function. What you're doing is
11 pulling out each individual call and saying that it's
12 separate. It isn't.

> *13 Q. We have looked at what the CheckBlock function contains*
> *14 and you have said it contains an ECDSA signature check.*
> *15 It doesn't, does it?*
> *16 A. That's not what I said.*
> *17 Q. Well, we can see what you said.*
> *18 A. What I said was, the function includes all of*
> *19 the processes in that. CheckBlock doesn't work unless*
> *20 each of the called functions are there."*

656. In summary, the check of signatures of transactions was not part of the CheckBlock stage of the ProcessBlock function. It was carried out in the AcceptBlock stage as was demonstrated to Dr Wright at **{Day8/127-129}**. I agree with the Developers that Satoshi would not have got these points wrong and so this is another indication that Dr Wright did not write the Bitcoin Source Code.

Proof-of-Work

657. The Developers' third point concerned the change (and improvement) in the proof-of-work system between what was proposed in section 4 of the Bitcoin White Paper and what Satoshi implemented in the original Bitcoin Source Code. This point is closely related to challenges made by COPA to parts of Dr Wright's evidence about the proof-of-work mechanism that he (as Satoshi) designed in the Bitcoin system and his interactions with Wei Dai and Dr Adam Back. It also relates to the counter-challenge by Dr Wright to Dr Back's evidence.

658. In **Wright1**, Dr Wright described those interactions in these paragraphs:

> *'91. In August 2008 1 reached out to a small number of individuals, including Wei Dai and Adam Back, by sharing the link to the White Paper via email as Satoshi Nakamoto, most likely using my satoshi@anonymousspeech.com address. I sent them a link to upload.ae where I had uploaded a single draft of the White Paper. ...*
>
> *92. Wei Dai was a distinguished academic who had previously proposed a digital currency concept called B-Money, which profoundly impacted my thinking. His work was highly influential and laid the groundwork for some ideas incorporated into the Bitcoin project. Notably, Wei Dai's contributions were the first that I acknowledged in the White Paper. After I provided him with a copy of the White Paper, he played a significant role in the development process, guiding me to various signature algorithm libraries, including his secure hash algorithm {SHA-256), which I successfully incorporated into the Bitcoin code base.*
>
> *93. Adam Back was known for his work on Hashcash (a proof-of-work algorithm different to that in bitcoin which he had proposed to combat email spam). He showed little interest in Bitcoin. His attitude was quite dismissive; he stated that digital cash had been attempted before and was bound to fail. At the time, I did not understand he was pointing at issues associated with creating a cryptocurrency and not digital cash.*
>
> *94. Contrary to popular belief, Bitcoin's proof-of-work system does not utilise Adam Back's Hashcash system. Instead, it more closely aligns with the methodologies described in Aura's paper. Due to Aura's lack of response, I felt it necessary to*

> *reference Adam Back in the Bitcoin White Paper due to the thematic parallels in our work and Back's notable presence in the field.'*

659. For the reasons which follow, this was all made up by Dr Wright, even though *some* of the technical details may have had some substance. These paragraphs appear to represent his deduction as to what happened, based on his study of the Bitcoin White Paper, the references in it and his other researches (e.g. into the earlier paper by Tuomas Aura et al). His deduction is wrong in a number of important respects. Satoshi would not have got these points wrong.

660. Understandably, COPA gathered various pieces of evidence to dispute these paragraphs in Wright1. I deal with several topics in turn.

Wei Dai

661. On 20 August 2008 Satoshi Nakamoto shared a link to a then draft of the Bitcoin White Paper with Dr Back **{L3/190}**, stating:

> "*I'm getting ready to release a paper that references your Hashcash paper and I wanted to make sure I have the citation right. Here's what I have:*
>
> *[5] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.*
>
> *I think you would find it interesting, since it finds a new use for hash-based proof-of-work as a way to make e-cash work. You can download a pre-release draft at http://www.upload.ae/file/6157/ecash-pdf.html Feel free to forward it to anyone else you think would be interested. I'm also nearly finished with a C++ implementation to release as open source.*"

662. Satoshi was clearly envisaging that Dr Back's Hashcash paper would be the fifth reference in the Bitcoin White Paper.

663. Dr Back responded the following day as follows **{L3/194}**.

> "*Yes citation looks fine, I'll take a look at your paper. You maybe aware of the "B-money" proposal, I guess google can find it for you, by Wei Dai which sounds to be somewhat related to your paper. (The b-money idea is just described concisely on his web page, he didnt* [sic] *write up a paper).*"

664. Two points emerge from that response. First, it was a perfectly friendly reply from Dr Back (he was not in any way dismissive). Second, and more importantly he drew Satoshi's attention to the "B-money" proposal made by Wei Dai (which was set out on a web-page, not in a paper).

665. Satoshi Nakamoto replied to Dr Back on 21 August 2008 as follows **{L3/192}**:

> "*Thanks, I wasn't aware of the b-money page, but my ideas start from exactly that point. I'll e-mail him to confirm the year of publication so I can credit him.*
>
> *The main thing my system adds is to also use proof-of-work to support a distributed timestamp server. While users are generating proof-of-work to make new coins for*

themselves, the same proof-of-work is also supporting the network timestamping. This is instead of Usenet."

666. Separately, Satoshi wrote to Wei Dai on 22 August 2008 in the following terms **{L3/195}**:

"*I was very interested to read your b-money page. I'm getting ready to release a paper that expands on your ideas into a complete working system.*

Adam Back (hashcash.org) noticed the similarities and pointed me to your site.

I need to find out the year of publication of your b-money page for the citation in my paper. It'll look like:

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, (2006?)."

667. Two points emerge from that email. First, it shows that the prompt for Satoshi Nakamoto's approach to Wei Dai, was Wei Dai's b-money page, rather than something else. Second, the effect of inserting a reference to Wei Dai's b-money page as the first reference in the Bitcoin White Paper would have been to lead to Dr Back's paper becoming the sixth reference – as in fact it was in the version published by Satoshi in October 2008: **{L3/231/8}**. Thus, it is clear that there was no reference in the Bitcoin White Paper to Wei Dai's b-money page until it was mentioned to Satoshi by Adam Back.

668. Wei Dai responded to Satoshi Nakamoto at some point afterwards as follows **{L14/99/3}**:

"Hi Satoshi. b-money was announced on the cypherpunks mailing list in 1998. Here's the archived post:
https://cypherpunks.venona.com/date/1998/11/msg00941.html
There are some discussions of it at
https://cypherpunks.venona.com/date/1998/12/msg00194.html.
Thanks for letting me know about your paper. I'll take a look at it and let you know if I have any comments or questions."

669. There were no further dealings between Satoshi and Wei Dai until the Bitcoin White Paper was published.

670. Wei Dai was unwilling to provide a witness statement but responded promptly to a request from COPA's solicitors to comment on [91] and [92] of **Wright1**. His email responses were the subject of a CEA Notice by COPA:

'1. I'm not a "distinguished academic" and has actually never worked in academia.
2. My understanding (from Satoshi's first email to me) is that Satoshi only became aware of b-money when he learned about it from Adam Back, which is after he had completed the draft of the whitepaper that he sent to Adam, so it seems wrong that I profoundly impacted Satoshi's thinking.
3. I did not play a significant role in the development process of Bitcoin. Specifically I did not guide Satoshi to "various signature algorithm libraries, including his secure hash algorithm (SHA-256)".
4. You can see the entirety of my communications with Satoshi at https://gwern.net/doc/bitcoin/2008-nakamoto.'

671. In further emails Wei Dai was asked to and did comment on some claims made by Dr Wright in one of his blog posts and an email sent by Dr Wright to Gavin Andresen on 4 March 2016. The relevant extract from the blog post is:

> *'Prof Wrightson knew of Wei Dai, and pointed me towards a paper titled Knowledge-Based Communication Processes in Building Design" that he knew of because of his work in machine learning. Both Adam Back and Prof Wrightson directed me to Wei Dai. 戴维 turned out to be another cypherpunk, and he was an incredibly helpful one. I used some of his code in the original release of Bitcoin — with his permission.'*

672. The relevant extract from the email reads as follows:

> *"Adam Back was not the source of the hashing algorithm within bitcoin. He was noted and referenced within the paper following my communications with him in mid-2008. The actual source of hash algorithm that is used for the proof or work is from the following authors:*
> *• Tuomas Aura, Pekka Nikander, and Jussipekka Leiwo:*
> *• http://www.tcs.hut.fi/old/papers/aura/aura-nikander-leiwo-protocols00.pdf*
> *It is my belief that you will recognise the algorithm on reading this paper.*
>
> *There are similarities in hashcash in that it searches for collisions, but the nature of the Bitcoin algorithm is derived from Aura et al. and not from Back. It also needs to be further noted that the code supplied by Wei Dai predates any communications with Adam by two months."*

673. Wei Dai said he did not write the paper mentioned in the blog post. He said it was someone else. He also said:

> *"I did not directly supply any code to Satoshi. (Again you can see the entirety of my communications with Satoshi at the link I gave earlier.) My understanding is that Satoshi did incorporate some of my code (specifically my implementation of SHA-256) into his Bitcoin code, but that code is in my open source Crypto++ library, and he probably just downloaded and used it without telling me."*

674. As I describe below, Wei Dai's evidence is strongly supported by the evidence of Dr Adam Back, to which I turn next. Suffice to say I found Wei Dai's evidence compelling and I accept it, despite the fact that he was unwilling to get involved beyond his email responses.

675. Before turning to consider Dr Back's involvement and evidence, I should refer to the development in Dr Wright's evidence on Wei Dai after Wright1. In **Wright11 [370] {CSW/1/69}**, Dr Wright further tried to suggest that he had been aware of Wei Dai's b-money proposal prior to his dealings with Dr Back, but was not aware of Wei Dai's b-money page. That might seem an odd point of detail for Dr Wright to persist with in light of the exchanges with Dr Back and Wei Dai I have already described. However, Dr Wright was compelled to argue the point because of prior publications by him asserting longstanding familiarity with Wei Dai's work.

676. In an article entitled "*Fully Peer-to-Peer*" published on 6 June 2019 **{L15/88/1}**, Dr Wright had referred to enrolling at the University of Newcastle in 2005 as a post-graduate researcher between 2005 and 2009. He stated that entering the university gave him access

to the work of Graham Wrightson and Andreas Furche **{L15/88/2}**. He went on to say at **{L15/88/3**}:

> "*I did not put down that I was Satoshi when I talked to them. I was just another postgraduate researcher and student. …*
>
> *… In a conversation that I had when I started my degree with Prof Graham Wrightson, I saw that the separate networks and communication infrastructure would end up merging. …*
>
> *Prof Wrightson knew of Wei Dai, and pointed me towards a paper titled "Knowledge-Based Communication Processes in Building Design" that he knew of because of his work in machine learning. Both Adam Back and Prof Wrightson directed me to Wei Dai. 戴维 turned out to be another cypherpunk, and he was an incredibly helpful one. I used some of his code in the original release of Bitcoin—with his permission. Andreas Furche knew of Hal Finney and Adam Back. So I emailed people. I was researching in 2005, and came to the conclusion that I could build something. By 2007, I was ready to start.*"

677. The Developers submitted that every element of that account was imagined for the following reasons:

677.1. Professor Wrightson had retired from the University of Newcastle on 9 August 2000 and had no further contact with it: **{C/17.1/4}** and **{C/17.1/11**}. He does not recall ever meeting, speaking or working with an individual named Craig Steven Wright **{C/17.1/11}** and does not know of Wei Dai **{C/17.1/11**}.

677.2. Andreas Furche left Newcastle University with Professor Wrightson (and halfway through his PhD) and completed it at Macquarie {**Furche1 [6-7] {C/13/2}** and **Furche1 [27] {C/13/6}**}. He had never heard of Adam Back: {**Furche1 [36] {C/13/7}**}.

677.3. The Wei Dai in question here had never written a paper entitled "*Knowledge-Based Communication Processes in Building Design"*: **{C/28/1}**. That seems to be a reference to a paper about the use of CAD systems in the construction industry written by someone else called Wei Dai from the Commonwealth Scientific and Industrial Research Organisation in Victoria, Australia **{L1/17/1}**.

677.4. As to the use of code from Wei Dai, I have already quoted Wei Dai's reply to Bird & Bird at [673 above] **{C/28/1}**.

678. I have to agree and so find that every aspect of Dr Wright's story as to his supposed dealings with Professor Wrightson, Andreas Furche and Wei Dai was untrue.

679. When Professor Wrightson's evidence was drawn to Dr Wright's attention on Day 6, his response was to say:

> *"81:14 A. I'm sorry if it's perfectly clear for you, but it's not.*
> *15 One, I'm not good with remembering people. The funny*
> *16 thing is, when it comes to code, when it comes to other*
> *17 things, I have a near eidetic memory; when it comes to*

18 people, I don't; I don't even remember faces very well.
19 But when it comes to recalling people, I'm horrible
20 with it.
21 I did have communications with him, I know that they
22 were valuable to me, more than that I can't say."
"84:12 Q. So your confident assertion in that paper, and
13 the anecdotes about Professor Wrightson pointing you to
14 Wei Dai and discussing Wei Dai with you, that could be
15 wrong?
16 A. Oh, definitely; I get people wrong all the time. I've
17 gone up to people I should know very well and called
18 them the wrong name many times; I do it at work all
19 the time. I have partial aphasia, which means I don't
20 actually recognise faces properly, so --"

680. The Developers characterised that as a laughable explanation for his false account of non-existent dealings with Professor Wrightson. Dr Wright has not been able to suggest anyone other than Professor Wrightson who might meet the bill. And far from having an "*eidetic*" (i.e. photographic) memory of code, Dr Wright could not even recall the CheckBlock function in Bitcoin.

681. When confronted with Andreas Furche's evidence that he had no recollection of Dr Wright, Dr Wright was left on Day 6 suggesting only "*I'm pretty sure it was him*" (emphasis added):

"84:21 Q. Page 1, please {L19/209/1}, an email from
22 Professor Furche. He, too, says that he has no
23 recollection of you, and that he left
24 Newcastle University in 1999. That latter bit is from
25 his witness statement. Do you dispute that he left
85: 1 Newcastle University in 1999?
2 A. No.
3 Q. So, he, too, could not have been there to have these
4 rewarding changes with you in 2005 to 2009, could he?
5 A. Possibly. I was there at that stage. But I was also at
6 the Australian Stock Exchange, where he developed
7 the signal process and some of the software for, and
8 also promoted.
9 Q. I'll come to that in a moment.
10 He also says -- we can take this document down.
11 He also says in his witness statement that he's
12 never heard of Hal Finney, with whom -- about whom you
13 supposedly had discussions with him. Is he wrong about
14 that?
15 A. I don't know. As I said, I'm not good with people, and
16 I could have had it wrong, but I don't think I am.
17 Q. He also agrees with Professor Wrightson that the group
18 didn't have a lot of resources, that it never lodged
19 a patent application and that he doesn't recognise
20 the patent paper hyperlinked to your article. Do you

21 accept he's right on those points?
22 A. Yes. I could have got the wrong person and linked
23 the wrong area. I'm not denying that.
24 Q. An awful lot of mistakes in your blogpost now, aren't
25 there?
86: 1 A. I told you, when it comes to people, I'm terrible. This
2 is the whole thing. When it comes to numbers, code,
3 writing things, a predicate system, I'm great; when it
4 comes to interacting with people ... This is why I work
5 from home, this is why I hide away from the world, this
6 is why I don't interact, why you're asking me about all
7 these people I'm supposed to remember.
8 Q. But you do dispute Professor Furche's claim not to
9 recall you, don't you?
10 A. I would find that difficult. I was at
11 the Australian Stock Exchange for a number of years, and
12 the only way I could put it was, I was a gadfly and
13 I was incredibly annoying to a lot of people, including
14 those in seats and other such systems. And some of
15 the other exchanges that he did stuff with as well,
16 I was involved.
17 Q. {CSW/1/82}, please.
18 A. Including Chi-X.
19 Q. Paragraph 433. This is your 11th witness statement,
20 isn't it, Dr Wright? Yes?
21 A. Yes.
22 Q. You claim that Dr Furche and you worked together on
23 the surveillance systems for the Australian Stock
24 Exchange from '97 to 2003, don't you?
25 A. I worked on those systems at that stage, yes, and
87: 1 I believe he was there, and he implemented those --
2 Q. Professor Furche --
3 A. -- systems at that time.
4 Q. Professor Furche's work on the ASX's surveillance
5 systems didn't start until after 2003, did it?
6 A. Well, I still remember him, and I definitely remember
7 him from the Perth Mint.
8 Q. So you worked together at Perth Mint in 2005 to 2008,
9 yes?
10 A. No, I was an auditor.
11 Q. "... then had a joint involvement at the Perth Mint,
12 where I was an auditor for BDO (2005-2008)."
13 Yes?
14 A. Yes.
15 Q. In fact, Professor Furche's work in relation to
16 the Perth Mint didn't begin until 2016, did it?
17 A. I don't know, but I'm pretty sure it was him there, and
18 I believe he was also involved with Chi-X.
19 Q. Just setting aside the thing you don't talk about in
20 your 11th witness statement, you couldn't have had

21 a joint involvement with him at the Perth Mint while you
22 -- in 2005 to 2008, because he didn't have a connection
23 with it at that time, did he?
24 A. I don't know, but I do remember him. As I said, I'm
25 terrible with people, but I remember him from something."

682. In light of the above, it is clear that the whole of Dr Wright's account concerning Wei Dai (from his 2019 blog, to **Wright1 [92]** to **Wright11**) was pure fabrication by Dr Wright and yet another strong indicator that he is not Satoshi.

Dr Adam Back

683. In his first witness statement, Dr Back described and exhibited his brief email exchanges with Satoshi Nakamoto in August 2008 and later in January 2009. He said these emails had never previously been published (as related above at [23.2]). These emails do not show Dr Back being dismissive at all.

684. In his second witness statement, Dr Back responded to the parts of **Wright1** in which he had been mentioned. His evidence shows the following:

684.1. That Dr Wright's claim to have been profoundly influenced by Wei Dai's b-money proposal was a lie, since Satoshi's first email to Dr Back shows that Satoshi was not previously aware of that proposal, a point confirmed by Wei Dai (see above).

684.2. That Dr Wright's claim that Dr Back was dismissive and had said that digital cash had been attempted before and was bound to fail, was a lie. Far from being dismissive, Dr Back points out he was one of the applied researchers who continued to work on making p2p electronic cash a reality, after the failure of Digicash in 1998. He also said that Hashcash was a building block used by others in their designs, including Wei Dai in 1998, Nick Szabo in 1998 and Hal Finney in 2004.

685. In addition, Dr Back responded to Dr Wright's claim in **[94]** of **Wright1** that Bitcoin uses an algorithm derived from Tuomas Aura's 2000 paper and not Hashcash. Dr Back gave a series of detailed chronological and other reasons why he did not think this was correct, not least the fact that his Hashcash paper is cited in the Bitcoin White Paper (reference [6]), but there is no reference at all to the paper by Aura et al. Dr Back also stated that the proposals in his Hashcash paper and that of Aura et al are different in that Aura's work is about an interactive client-server protocol, while Hashcash is a non-interactive proof. He pointed out that Bitcoin, being peer-to-peer, necessarily cannot involve a server. In this regard, it is relevant to note that Satoshi actually wrote, in the Bitcoin White Paper, '*we will need to use a proof-of-work system similar to Adam Back's Hashcash [6],'* and made no mention of Aura.

686. Professor Meiklejohn addressed proof-of-work systems in her first report at **[62]-[63]**, making the point that proof-of-work is not unique to Bitcoin. In respect of Bitcoin, she made the straightforward point that the specific type of proof-of-work used in Bitcoin is derived from a previous proposal called Hashcash, as proposed by Adam Back in 2002, as referred to in the Bitcoin White Paper.

687. Dr Wright then responded in **Wright11**. In **Wright11 at [387]**, Dr Wright responded to Dr Back's mention that Satoshi cited his Hashcash paper in the Bitcoin White Paper with this statement: '*I did so because I mentioned it in the White Paper, not because I used the algorithm'*, an explanation which I consider to be bizarre, given what Satoshi actually wrote. Dr Wright went on to refer to the algorithm used in Hashcash as being different from that implemented in Bitcoin, on the basis that '*the algorithm does not use a series of leading zeros as Bitcoin implements.*'

688. Similarly, later in **Wright11**, Dr Wright sought to respond to Professor Meiklejohn's first report at **[62]-[63]** and the first and second witness statements of Dr Back, saying:

> *'I will note that the initial Hashcash scheme and the Bitcoin Proof of Work (PoW) mechanism differ in their core concept and the specifics of their implementation, particularly in how the target for hash collision is defined.'*

689. In **[601**] he sought to summarise how he saw the differences. Under the sub-heading of 'Bitcoins's Proof of Work' he said this:

> *'e. Target with Leading Zeros: In Bitcoin's PoW, the goal is to find a hash that is below a particular target value, often visualized as a hash with a certain number of leading zeros. This target adjusts over time to maintain a consistent block time despite changes in computational power.*
>
> *f. Mechanism: Bitcoin miners compete to find a hash of the block header that meets the required difficulty level (i.e., has a sufficient number of leading zeros). The difficulty of this task adjusts dynamically with the network's collective hashing power to ensure that the average time to find a block remains consistent.'*

690. It is clear from these references that Dr Wright thought that the proof of work implemented in the Bitcoin system operated on the basis of finding a hash with a sufficient number of leading zeros.

691. Counsel for Dr Wright put to Dr Back that the Bitcoin code had retained the approach of simply checking leading zeros as described in the Bitcoin White Paper. Presumably this was done on instructions and/or the basis of what Dr Wright said in **Wright11**. Dr Back explained that although the Bitcoin White Paper refers to leading zeros, no released version of the Bitcoin code utilises that. As he explained,

> *48:20 the specification is not a number of leading zeros in*
> *21 Bitcoin, the specification is a difficulty which is the*
> *22 floating point number…."*
>
> *"50: 5 while the Bitcoin paper is expressed in that way, if you*
> *6 actually look into the details and the code and how it*
> *7 works, the difficulty is a floating point number, so*
> *8 it's a little more nuanced than leading zeros…"*

692. In re-examination, Dr Back confirmed that in the Bitcoin code there is no check for leading zeros:

> *"77: 20 Q. Okay. Does it deal with leading zeros, or …?*

21 A. No.
22 Q. Right.
23 A. So, I mean, I believe this end bit is a, sort of,
24 compact representation of -- it involves a compact
25 representation of the difficulty which, then, in turn,
78: 1 creates a target, and so it's checking if the hash is
2 as -- represented as a very large integer, is less than
3 the target, which is -- which is what I said. So that,
4 you know, superficially, if you look at the zeros, there
5 is a certain number of zeros, but, you know, even if you
6 look at it in binary, there are some more bits after it
7 where, you know, the next bit could be a zero or a one
8 and it could still be an invalid proof-of-work, because
9 it's really a floating point number, or a fraction or
10 something."

693. Although in Written Closing, Counsel for Dr Wright spent many paragraphs seeking to persuade me that **Wright1 [94]** was a fair and accurate description of a technically complex issue, I am not so persuaded. In fact, as I have mentioned, I find **[94]** (and the surrounding paragraphs) to be fabrication by Dr Wright.

694. It is unnecessary to get into the rather fine distinctions which were explored in cross-examination of Dr Back when comparing the methodologies of Aura et al, Hashcash and Bitcoin. Dr Back answered all the points put to him fairly and carefully. It may be true that when one conducts a detailed comparison of these three methodologies, the proof-of-work system described in the Bitcoin White Paper '*aligns more closely with the methodology described in Aura's paper than with Dr Back's original proposal'*. But that is an exercise using 20:20 hindsight. What Satoshi actually did appears to be much more straightforward. He referred to Adam Back's Hashcash paper because he was aware of it and, as he stated in the Bitcoin White Paper, his proposed proof-of-work system was similar to it. Either Satoshi was unaware of the proposal by Aura et al, or he considered it different, possibly for the reason given by Dr Back.

695. Dr Wright's explanation in [94] does not make sense. If Satoshi had based his proof-of-work algorithm on Aura et al, he would have cited that paper. The fact that Aura had supposedly not responded (per Dr Wright) would not have been a reason not to cite the paper.

696. In fact, there is a ready explanation as to why Dr Wright got all this wrong. It has become apparent to me that his *modus operandi* when pursuing his claim to be Satoshi is to do whatever he can to read and research all available materials so he is in a position to speak with authority on what happened/he did as Satoshi. This strategy is not foolproof. It comes unstuck if what Dr Wright thinks happened conflicts with (a) testimony from those who were actually involved at the time or (b) previously unpublished materials. This is yet another instance where Dr Wright has come unstuck. Furthermore, it appears he did not apply this strategy to the Bitcoin Source Code. Consistent with (a) the relatively few forgeries relating to the code and (b) the points he got wrong as regards the code, it would appear he had not analysed or familiarised himself with the code.

697. There is, of course, an additional problem with **Wright1 [94], Wright11 [387]** and **[601]**. In those paragraphs, Dr Wright got wrong the proof-of-work system which Satoshi

actually implemented in the Bitcoin Source Code, as Dr Back explained. Satoshi would not have got this point wrong.

698. Overall, there are a number of independent pieces of evidence which combine to present, in my judgment, an overwhelming case that Dr Wright did not write the Bitcoin Source Code, either by himself or with others. Once again, his evidence that he did is fantasy.

F. Launch of Bitcoin

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

699. By way of background, I refer to the following sections in the Appendix which contain my findings that the following documents, relevant to these matters, were forged by Dr Wright:

699.1. Section 27: False NAB Account Records, screenshots purporting to show the purchase of a vistomail address in 2008.

699.2. I also refer to Section 1 in the Appendix which sets out how Dr Wright's claims to have acquired the bitcoin.org domain were founded on those forged documents but then foundered or were abandoned.

Dr Wright's evidence on launching the Bitcoin system

700. In **Wright1**, Dr Wright said that he manually crafted the Genesis Block rather than mining it 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. He says that he chose this headline, which referred to the bank bailouts after the 2008 crash, because he strongly disagreed with the policy. Dr Wright was not in the UK at this time, but claims to have had access to The Times through a university portal. 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.

701. As COPA pointed out, Dr Wright strove to provide meaning and rationale to all aspects of how Satoshi chose to do certain things but he cited only publicly known matters.

702. Dr Wright's account of the Genesis Block in **Wright1, [107] {E/1/21}** and **Wright4, [102] {E/4/34}** now involves assertions that there is neither a public nor a private key linked to it. These assertions were rejected by both Professor Meiklejohn and Mr Gao. Professor Meiklejohn was clear that there is a public key for the Genesis Block and pointed out that that public key has never spent its content and cannot do so because the software does not treat this transaction output as UTXO. On that basis, she said it is not clear if anyone knows or has ever known the associate private key {**{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}**. I also note 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}**.

703. When confronted with Professor Meiklejohn's evidence in cross-examination **{Day7/54:13} - {Day7/57:4}**, Dr Wright could only refer to an unspecified blog by himself and say that the public key to the Genesis Block (as 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.

704. Dr Wright asserted that in the "*early days*" the only individuals involved in mining were himself, and his family (including Don and Max Lynam). He said Don and Max Lynam began operating a node from Don's farm. Concurrently, Dr Wright claimed to have been using his own mining set up in '69 racks' at his Australian residence, with 3 other laptops and 4 desktop systems in another location at Tumbi Umbi {**Wright 1, [116] {E/1/22}**}. He claimed 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. As Professor Meiklejohn explained, mining at that time would not have entailed such a cost. Dr Wright went 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 {**Wright1, [121] {E/1/23}**}. That 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.

705. I am satisfied that Dr Wright's evidence about launching the Bitcoin system was pure fantasy. Furthermore, his account of mining Bitcoin in the early days does not ring true.

G. Further circumstantial evidence post-dating the White Paper

'9. There is a significant body of other circumstantial evidence post-dating the White Paper that is consistent with Dr Wright's authorship, including:

(i) Dr Wright helping Qudos Bank to implement an immutable event logger system with similarities to blockchain technology in around November or December 2008;

(ii) Dr Wright pitching an alternative payment system to Qudos Bank that was based on a "decentralised ledger" and involved a "peer-to-peer payments network where transactions would be a fraction of the cost of the existing SWIFT payment system" in around late 2008 or 2009;

(iii) Dr Wright pitching to Centrebet a honeypot detection system with close parallels to Bitcoin/blockchain technology at some point in 2009;

(iv) Dr Pang's recollection of Dr Wright asking him and a number of other BDO colleagues whether they had heard of Satoshi Nakamoto "or something that sounds like that name" in late October or shortly thereafter;

(v) Dr Wright mentioning "blockchain" to Mr Jenkins in 2008 (probably around December 2008); and

(vi) Dr Wright showing Mr Jenkins a "Timecoin" paper in around 2009/2010; and

(vii) the fact that Satoshi used idioms and colloquialisms typical of Australia in his communications, which is consistent with Dr Wright's nationality. {See, for example, "wet blanket" {L19/11/2}; "bogged everything down" {L6/19/1}; "references galore" {L5/500/1}; and "bash the sockets" {L6/28/1}}.

706. Point (vii) is ridiculous, not least because there was no expert or any other evidence to support it. On point (vi), I have rejected Mr Jenkins' evidence that he was shown a 'Timecoin' paper in 2009/2010. On point (iv), I have explained above why that incident

suggests that Dr Wright is not Satoshi. The remaining points, even if I assume they are true, are similar to those I dealt with above, in that it is relatively easy, with the benefit of 20:20 hindsight, to reach back to pluck out some feature which might have some relation to Bitcoin. They are all generalised assertions.

707. However, there are a number of more concrete points going the other way which I must discuss.

708. The following five were submitted by the Developers:

    708.1. Dr Wright's evidence as to the 69 computers he claimed to have been operating on the launch of the Bitcoin system and their electricity consumption.

    708.2. Satoshi Nakamoto's disabling of opcodes in Bitcoin script.

    708.3. Dr Wright's failure to spot that in his pre-2009 reliance documents he had referred to concepts which were only introduced in 2011 and later.

    708.4. Dr Wright's claim to have transferred Bitcoin to Mr Zooko Wilcox-O'Hearn.

    708.5. What happened on Dr Wright's first public intervention on the subject of Bitcoin.

709. By way of background, I refer to the following sections in the Appendix which contain my findings that the following documents, relevant to these matters, were forged by Dr Wright:

    709.1. Section 32: 'BitCoin: SEIR-C Propagation models of block and transaction dissemination', purported precursor work to the Bitcoin White Paper, dated 12 December 2008.

    709.2. Section 36: the MYOB accounting screenshots, a series of disclosed screenshots purporting to show transfers of mined bitcoin and transfer to WIIL.

    709.3. Section 38: Spoofed email from Dr Wright, using satoshi@vistomail.com, in the name of Satoshi Nakamoto.

Dr Wright's 69 computers

710. Dr Wright first claimed to have operated a large number of computers (67) at his home in Australia at the start of the Bitcoin system in a blog on 6 April 2019 **{L14/420/2}** and in a CoinGeek interview on 6 June 2019 **{O4/12/13}** (this time with 69 machines). These claims were expanded upon in his evidence-in-chief in the *Kleiman* proceedings **{L17/327/105}-{L17/327/108**}. He suggested there that he was running 69 machines in four racks spread over his homes in Lisarow and Bagnoo at a monthly electricity cost of AU$11,000.

711. At **Wright1 [116] {E/1/22}** he appeared to suggest that he was in fact running 69 racks at those residences, but explained in cross-examination by COPA that he meant 69 computers in racks. At **Wright1 [117]** {E/1/22} he nevertheless went on to say that the "*considerable electricity consumption associated with Bitcoin mining represented a significant expense for me, amounting to thousands of Australian dollars*" and confirmed in cross-examination that he stood by the figures stated in *Kleiman*.

712. The Developers submitted there were two main problems with this evidence.

i. Problem 1: inconsistency with the known difficulty

713. First, Professor Meiklejohn pointed out that it would not have been necessary at that time for Dr Wright (if he were Satoshi) to run a setup of the kind that he described (69 computers), and in fact he could not have been running such a setup in early 2009 or early 2010 as, if he had, it would have increased the difficulty considerably to that which was observed at the time see {**Meiklejohn1 [74] {G/2/32**}}. Mr Gao appeared to quibble with Professor Meiklejohn's evidence in this respect at **Annex A [14]** to the Joint Statement {Q/3.1/5}, but when faced with the source data for Professor Meiklejohn's evidence at **{H/190/2**} Mr Gao was unable to sustain that criticism {Day18/58:1}-{Day18/59:3}.

714. Dr Wright responded to that at **Wright9 [23] {E/26/9}** by modifying his evidence to suggest that his machines were not dedicated to Bitcoin mining after all and that he was also validating blocks. In cross-examination, he sought to develop that answer as follows:

> *"146:20 Q. Now, I'm putting this to you on the basis of the expert*
> *21 evidence of Professor Meiklejohn. It wouldn't have been*
> *22 necessary to run a set up of this magnitude to mine*
> *23 Bitcoin in 2009 or early 2010, would it?*
> *24 A. Of course it would. Ms -- Professor Meiklejohn is*
> *25 misrepresenting Bitcoin mining and nodes. Section 5 of*
> *147: 1 the White Paper doesn't say that you solve hashing.*
> *2 Now, hashing is only one small component. The majority,*
> *3 at a low level like that, is actually validating ECDSA.*
> *4 ECDSA is a far more computationally intense process than*
> *5 hashing. So what we need to do is actually go through*
> *6 validation of blocks, checking, later running testnet as*
> *7 well, and ensuring that all of that process happens*
> *8 before you distribute the block. On top of that, I had*
> *9 to run multiple systems.*
> *10 Bitcoin was configured so that on a single C class,*
> *11 and I had a C class in each area, the 256 IP addresses*
> *12 in V4, or more in IP v6 would only act as a single node*
> *13 on the network. So even if you had 30 machines on*
> *14 a single location, they only broadcast as one node on*
> *15 the network. Now, that allowed me to have multiple*
> *16 systems, including the logging systems and the rest of*
> *17 the Timecoin server. All of that together was really*
> *18 the cost that I experienced."*

715. The account in **Wright9** and in cross-examination was significantly different to that presented in his blog, on CoinGeek, in his *Kleiman* evidence and in **Wright1**. Leaving that aside, there were three elements to Dr Wright's contention that Satoshi Nakamoto was using a setup such as that described by Dr Wright.

    715.1. First, that the setup was for the majority of the time "*validating ECDSA*", which is to say validating the signature of the transactions in each block.

715.2. Second, that the setup was "*running testnet*".

715.3. Third, that he was running "*the Timecoin server*".

716. On the first point, the evidence showed there were just 219 non-coinbase transactions (i.e. transactions containing ECDSA signatures) in the 32,489 blocks created up to the end of 2009. Typically, there were zero transactions per block. So the suggestion that Dr Wright's machines were mostly engaged in validating signatures for the transactions in blocks must be untrue **{Day8/177:11}-{Day8/179:7}**, and it was disclaimed by Mr Gao in his cross-examination **{Day18/60:10-12}**.

717. On the second point - Dr Wright running Testnet. Testnet did not exist until July 2010 **{Day8/175:20-23**}. Dr Wright suggested orally that he (as Satoshi) was running some previously undisclosed private version of Testnet **{Day8/175:25} - {Day8/176:1**}. That cannot be true. Testnet was an innovation introduced by Gavin Andresen: see **{L6/290.3/1}** in which Satoshi observed to Gavin Andresen on 30 July 2010: "*that test network was a really good idea of yours*". So his claim that the setup was running Testnet appears highly likely to be a lie.

718. On the third point, I agree that Timecoin appears to be a recent invention of Dr Wright's. It was not mentioned at all in the *Kleiman* proceedings. Furthermore, the incident in the re-examination of Mr Jenkins tends to confirm that. Moreover, Dr Wright's evidence as to his electricity consumption is almost certainly untrue for the reasons set out in the next section.

ii. Problem 2: inconsistency with known electricity consumption

719. The second problem with Dr Wright's evidence that he was spending AU$11,000 per month on electricity is that it is contradicted by the electricity bills that he submitted as part of his 2008-2009 personal tax return. Thus:

719.1. Lisarow: the electricity bills were as follows:

719.1.1. for the period from 8 December 2008 to 18 January 2009: AU$373.19 plus GST **{L4/485/23}**;

719.1.2. for the period from 18 January 2009 to 9 March 2009: AU$523.10 plus GST **{L5/70/8}**;

719.1.3. for the period from 9 March 2009 to 9 June 2009 was about AU$798.48: **{L5/70/79**}.

719.2. Bagnoo: the electricity bill for the period from 11 February 2009 to 8 May 2009 was less than AU$500: **{L5/70/50}**.

720. Dr Wright's answer to this evident contradiction was to contend that Lisarow was "*three-phase that was on a separate switch*" and billed separately to Information Defense Pty Ltd **{Day8/174:19-20}**. Although there was no documentary evidence either to support or contradict this, the Developers submitted it was 'vanishingly' unlikely to be true, for the following reasons:

720.1. There is no documentary evidence that his home in Lisarow was serviced by a three-phase electrical power distribution system. Although that it is not impossible, it was on a residential (not commercial or industrial) price plan **{L5/70/81}**.

720.2. As Dr Wright's sister confirmed, but Dr Wright denied, at the relevant time the computers in his Lisarow house were set-up in a spare bedroom or living area at the house {**DeMorgan1 [11] {E/8/4}**}. That being so, it seems highly implausible that it was "*on a separate switch*". Mr Bridges referred to the set-up being in Dr Wright's garage in early 2011: **Bridges1 [19] {E/9/6}**.

720.3. Information Defense Pty Ltd was only registered on 29 January 2009 **{L4/446/80}**, so cannot have been incurring the electricity consumption costs for the period prior to that date. Yet, the bills for the period prior to the registration of Information Defense are not consistent with AU$11,000 per month being spent on electricity.

720.4. In her deposition, Lynn Wright did not refer to any substantial set-up in Lisarow, suggesting that the main computer set-up (comprising just 4-5 laptops) was at Bagnoo {**{C/27/35} ll. 4-20**}.

721. When taken in combination with the first point (which is compelling) I find that Dr Wright was not incurring substantial expense as a result of his electricity consumption, and this was a further invention by Dr Wright to try to justify his initial boast of running 69 computers. The more pertinent point is that if he were Satoshi Nakamoto he would know that such an extensive computer set up with its enormous electricity consumption would not have been required anyway: a desktop or two would have mined a lot of bitcoin. Indeed, Mr Bohm's evidence was that he mined 100,000 bitcoins {**Bohm1 [16] {C/10/5}**, but I note that he said at [24] that he had spent all his bitcoin} on what was a normal HP Compaq computer **{L4/493/1}**.

opcodes

722. In **Wright11**, Dr Wright provided a lengthy critique of changes supposedly made "*by BTC*" to the original version of Bitcoin {**Wright11 [544] {CSW/1/100}**}. In particular, he complained that many "*OP_codes that are important to the functioning of the script have been disabled*" {**Wright11 [545] {CSW/1/100}**}.

723. Dr Wright's inconsistent and misspelling of the term "opcode" {see **Wuille2 [13] {C1/2/3}**} was a small indicator that he was expounding on something outside his knowledge or experience. More significantly, however, it appears that when Dr Wright prepared and filed **Wright11** he was not aware that the relevant changes to the Bitcoin code had been made by Satoshi Nakamoto.

724. The Developers relied on two examples of changes implemented by Satoshi Nakamoto namely (i) the change to size of data elements inside script and (ii) the disabling of OP_2MUL.

i. Script size

725. At **Wright11 [545.f] {CSW/1/102}**, Dr Wright stated that "*BTC has limited the ability to use script by placing a maximum size and enforcing this rigorously. The limit of 520 bytes gives very little ability to add data*".

726. Dr Wright's contention that "BTC" had "placed" a maximum size of 520 bytes was supported by a footnote which referenced **{L9/247.1}**, a version of the script.h file { version 0.10.0rc3 of the Bitcoin code: **Wuille2 [7] {C1/2/2}**} which at row 18 declared that a constant unsigned integer named "MAX_SCRIPT_ELEMENT_SIZE" had a value of 520 bytes. It is evident that at the time of writing his statement, Dr Wright thought that this change was "BTC" "placing" a maximum size on script.

727. In his second witness statement, Dr Wuille pointed out that the code referenced by Dr Wright did not introduce the 520 byte limit on script at all. Instead, Satoshi Nakamoto had introduced a limit on the size of data elements inside script in July 2010 and tightened it to 520 bytes in version 0.3.9 of the code on 15 August 2010 {**Wuille2 [9] {C1/2/2}**}. On 23 January 2013 the name MAX_SCRIPT_ELEMENT_SIZE was given to that limit {**Wuille2 [11] {C1/2/3}**}. Dr Wuille's evidence to this effect was not challenged by Dr Wright and I accept it.

728. In cross-examination, Dr Wright confirmed he had read Dr Wuille's statement but said 'Do I remember all of it off the top of my head? No.' It appears he sensed he was being trapped. It was pointed out to Dr Wright that he had not identified the commit that had named the limit MAX_SCRIPT_ELEMENT_SIZE, Dr Wright answered "*No, but it was actually one that I was behind*" **{Day8/145:5}**. Unfortunately for Dr Wright, that could not be true. The commit that had led to the introduction of the MAX_SCRIPT_ELEMENT_SIZE variable is at **{D1/28/1}**. It was made by Matt Corallo, aka TheBlueMatt on 23 January 2013. Dr Wright had to admit that he was not TheBlueMatt **{Day8/145:10}**. Indeed, TheBlueMatt is the tenth defendant in the BTC Core Claim, and one of the Developers.

729. Faced with the contradiction between Dr Wright's written evidence that the 520-byte limit had been "*placed*" by BTC and the factual record identified by Dr Wuille that it had been imposed by Satoshi Nakamoto, Dr Wright swerved to a suggestion that the limit had been introduced "*as a temporary measure*" as a result of a "*communication between multiple people, including Gavin and myself*" **{Day8/151:10-14}**.

730. However, there is no record of such a conversation in the documents disclosed by Gavin Andresen in the Kleiman proceedings. In any event, the change had been implemented by Satoshi Nakamoto many months before he left the Bitcoin project. Satoshi could have, but did not, reverse the limit. Dr Wright's explanation for this was evasive: "*I was building other systems*" **{Day8/151:18}**.

ii. OP_2MUL

731. At **Wright11 [545] {CSW/1/100}** Dr Wright complained that many opcodes that were important to the functioning of script had been disabled by BTC. He gave the specific example of "OP_2MUL".

732. As Dr Wuille explained at **Wuille2 [12-15] {C1/2/3}**, the opcodes in question (including OP_2MUL) had indeed been disabled, but they were disabled by Satoshi Nakamoto. Thus, Dr Wright was constrained to admit in cross-examination that the effect of the

changes made by Satoshi was that if one of the disabled opcodes was used in a script, it would return a false result – so that any transaction that used it would be invalid **{Day8/158:3-9}**.

733. Faced with this contradiction between **Wright11 [545]** and the evidence of Dr Wuille, Dr Wright suggested that he had "*pulled [these opcodes] temporarily*" **{Day8/157:17-18}** and that this was a "*temporary block*" **{Day8/158:15}** and **{Day8/158:24}**. These suggestions cannot be true: the change had been implemented by Satoshi Nakamoto many months before he left the Bitcoin project, but also because OP_2MUL had not even been re-enabled in BSV at the time of Dr Wright's cross-examination **{Day8/159:16}-{Day8/160:6}**.

734. The Developers invited me to re-read **Wright11 [545-545.e] {CSW/1/101}** with the knowledge that it was Satoshi Nakamoto that disabled OP_2MUL. They submitted that Dr Wright's speculation as to why BTC might have disabled OP_2MUL is generally incoherent, pointing out that Dr Wright had misunderstood the piece by Gregory Maxwell to which he refers at footnote 284. In that piece (at slide 22) Mr Maxwell was noting that Bitcoin Script had once been much more powerful and noting that this was "*not technically hard to fix*".

735. However the bigger point is that once it is understood that Satoshi Nakamoto disabled the opcodes, it is clear that Dr Wright cannot be Satoshi Nakamoto. If he were Satoshi Nakamoto, he would not be debating whether there was a possible justification for this change. He would be explaining why he made that change.

736. In short, Dr Wright's ignorance of Satoshi Nakamoto's imposition of limits on the size of script and ignorance of Satoshi Nakamoto's disabling of opcodes means that he cannot be Satoshi Nakamoto.

The anachronisms

737. The third respect in which Dr Wright's evidence shows a failure on his part to understand the history of the Bitcoin Software arises from the inclusion amongst his Primary Reliance Documents of documents purporting to date from before the release of the Bitcoin Software, but which refer to code and concepts that post-date Satoshi Nakamoto's involvement in the development of Bitcoin.

738. The Reliance Documents in question are challenged by COPA as forged or inauthentic. But the Developers submit the shortcoming in the content of those documents goes beyond merely showing that the documents are forged. They show that the forgery was by Dr Wright and that Dr Wright cannot be Satoshi Nakamoto.

739. The Developers confined themselves to four of the matters identified by Dr Wuille in his unchallenged first witness statement, namely CheckBlockHeader, BTC Core, UTXO and bootstrapping. Dr Wright was cross-examined on the first three points. The fourth is addressed in Dr Wuille's statement and corroborated by the documentary record.

i. CheckBlockHeader

740. The CheckBlockHeader function was introduced by Dr Wuille in March 2014 as part of a series of header synchronisation changes {**Wuille1 [24-25] {C1/1/6}**}.

741. CheckBlockHeader resulted from a split in the functionality present in the CheckBlock function described at [651] to [652] above, so that two of the six checks there described (the timestamp and proof-of-work checks) were prioritised ahead of the remaining four checks {**Wuille1 [25] {C1/1/6}**}.

742. By modularising CheckBlock into two stages, CheckBlockHeader and CheckBlock, nodes could quickly reject invalid blocks based on just their header, removing the need to download all of their transaction data.

743. When he was first taken to the CheckBlockHeader function in cross-examination, Dr Wright accepted that these changes were made by Dr Wuille (who had the username Sipa on GitHub) in 2013 and were not in Satoshi Nakamoto's original code **{Day8/132:23}-{Day8/133:6}**.

744. However, one of Dr Wright's reliance documents was a document entitled "*BitCoin: SEIR-C propagation models of block and transaction dissemination*" {L3/237} ("*the SEIR-C document*"). At **Wright11 AppendixB [14.2] {CSW/2/52}**, Dr Wright had stated that this document had been created between about Oct-Dec 2008 "*before I released the system in January 2009*". In section 32 of the Appendix, I have found this document to be a forgery.

745. At **{L3/237/13}** the SEIR-C document purported to provide a description of the Bitcoin system's block validation process. It stated as follows (and note the use of the present tense):

> *"Each node verifies a block before it propagates it to the connected peer nodes. In this way only valid blocks are propagated, and any invalid blocks are quickly isolated. The BitCoin Core client lists all of the validation requirements in the following functions:*
> *• CheckBlock*
> *• CheckBlockHeader"*

746. When this anachronism (i.e. the inclusion of a reference to a function from 2014 in a document purportedly from 2008) was put to him in cross-examination, the exchanges proceeded as follows:

> *"135: 9 Q. Do you want to carry on and we'll see that it then*
> *10 refers to two functions, the first is CheckBlock and*
> *11 the second is CheckBlockHeader, isn't it?*
> *12 A. Again, CheckBlock and CheckBlockHeader were meant to be*
> *13 implemented. CheckBlockHeader was a simple function for*
> *14 SPV. So in the client patches discussed with Gavin in*
> *15 2010, CheckBlockHeader was an implementation of*
> *16 a version of Bitcoin that does not have all of*
> *17 the checking. So that's different to the version Sipa*
> *18 put in, but that doesn't mean that there weren't*
> *19 functions. Again, CheckBlockHeader was about having an*
> *20 SPV, as defined in the White Paper, version of checking*
> *21 just the block headers.*
> *22 Q. There's no reference in the White Paper to*
> *23 CheckBlockHeader, is there?*

24 A. It has reference to SPV, which only checks Block Header.
25 There is no reference to any of the coding terms in
136: 1 the Bitcoin White Paper.
2 Q. When you say SPV checks -- "only checks Block Header",
3 what do you mean by "SPV" there?
4 A. Simplified Payment Verification.
5 Q. Right.
6 A. What that basically means is, like --
7 Q. To assist in the payment of individual transactions?
8 A. No, it's a -- basically what we're talking about is
9 a light node. So a node where an individual doesn't
10 need to download the entire blockchain. For instance,
11 I can just have the block headers and then I can have
12 a localised(?) path of where I'm checking an individual
13 transaction. I can keep each of those.
14 Q. Dr Wright, nobody referred to CheckBlockHeader until
15 the change that I took you to, did they?
16 A. No, that's wrong. That was actually part of building
17 SPV systems, that was basically the function I was
18 looking at at that time.
19 Q. There isn't a single document in which anybody refers to
20 CheckBlockHeader as a single function until Dr W[uille]
21 introduced it through GitHub, right?
22 A. I've no idea when he put it in that, but when I was
23 discussing the introduction of SPV, these concepts were
24 back there as well.
25 Q. Mr Andresen did not introduce CheckBlockHeader, did he?
137: 1 A. No, Mr Andresen got a patch from me initially. So
2 the patches for SPV were actually from Satoshi, me.
3 Q. Dr Wright, we've got the patches that Satoshi Nakamoto
4 sent to Mr Andresen; they do not include
5 CheckBlockHeader.
6 A. No, because I went off to develop things myself. So
7 where I was talking about work that I did in my other
8 companies, I didn't do everything publicly. The work on
9 Teranode now that was iDaemon that I've put in here, all
10 of those documents were based on our work, not his.
11 Q. Dr Wright, I know you want to talk about all of your
12 latest things. I'm actually trying to ask you about
13 things that Satoshi Nakamoto would know about, and that
14 is the original --
15 A. No, you're --
16 Q. -- Bitcoin code, right, and there was no reference in
17 the original Bitcoin code to CheckBlockHeader,
18 was there?
19 A. Again, difference between core, as in main nodes, and
20 those that are doing less, SPV, and there is a reference
21 to SPV. SPV nodes are those that only have to check
22 the headers across the network. If you read
23 the section, you will see that.

24 Q. Dr Wright, I am very confident that I can read any
25 section of anything and I will not see a single
138: 1 reference to CheckBlockHeader.
2 A. Because the code's not referenced in the White Paper at
3 all.
4 Q. And you're saying that -- when did you say then you
5 invented this? Was it in 2010, you said, when you were
6 talking to Mr Andresen?
7 A. No, I started working on SPV before I even released
8 Bitcoin. So, what I was doing is a combination of
9 Timecoin, which was a separate product, and Bitcoin.
10 Bitcoin was the main free product; Timecoin extended
11 everything."

747. The Developers submitted that that set of responses bears many of the common tell-tale signs of Dr Wright's dishonesty. I agree. They include:

747.1. An attempt to suggest that an optimisation introduced following Satoshi Nakamoto's departure was something that Dr Wright had thought of all along. Suffice it to say, that was not something that it had occurred to Dr Wright to mention when he was initially taken to the CheckBlockHeader function: see [743] above.

747.2. An attempt to suggest that the future optimisation was preordained in the Bitcoin White Paper. The Bitcoin White Paper simply does not engage in this sort of technical detail.

747.3. An attempt to suggest that the feature emerged in discussions for which there would be a reliable document trail, but of which no documentary record exists. Gavin Andresen disclosed all of his communications with Satoshi Nakamoto, including patches. None includes a function called CheckBlockHeader.

747.4. A vacuous reference to iDaemon and/or Terranode and/or Timecoin or other "*Star Trek-style technobabble*" (to quote Mr Hearn at **Hearn1 [28] {C/22/7}**).

ii. BTC Core

748. The passage from the SEIR_C document set out at paragraph 745 above contains a second anachronism. It refers to the "*Bitcoin Core client*".

749. As Dr Wuille explained at **Wuille1 [50] {C1/1/2**}, Bitcoin Core is the current name of the most commonly used fully-validating node software implementation. The name was introduced in March 2014 in version 0.9 of the software as follows **{L8/467/2}**:

> "*To reduce confusion between Bitcoin-the-network and Bitcoin-the-software we have renamed the reference client to Bitcoin Core.*"

750. When considering what Dr Wright said when this anachronism was put to him, one needs to keep in mind that Dr Wright seems to use the term 'BTC Core' as a catch-all to refer to the Developers. In the BTC Core claim, he and his companies sued 'BTC Core' as the first defendant, but there has never been any evidence that such an entity exists, other

than, perhaps, in Dr Wright's mind because **Wright11** is full of his complaints about what has been done or not done by 'BTC Core'.

751. Dr Wright's response was to suggest that:

751.1. The terminology of Bitcoin Core (capital B, capital C) had been used "*multiple times*" prior to March 2014 **{Day8/134:24}**, but there is nothing to support that contention. As Dr Wuille explained in his unchallenged evidence, the name was suggested by Gavin Andresen and was not used before version 0.9 of the software.

751.2. 'You adopted that name' i.e. that "*Bitcoin Core*" (i.e. the first defendant) had adopted the name Bitcoin Core from something else/someone else **{Day8/135:3-4}**, but this was an irrelevant diversion.

751.3. The term "Bitcoin Core" was being used in the SEIR_C document in contradistinction to Simplified Payment Verification (or SPV) **{Day8/135:7-8}**. Even if that were the case, and that does not seem to be so from just reading the document (the document had been edited to say that SPV had not been modelled at that time – see footnote4 at **{L3/237/7}**), it still would not explain the anachronism.

iii. UTXO

752. Bitcoin only allows nodes to accept a block if all transactions in it are valid and are not already spent {see the Bitcoin White Paper at [5.5] **{L5/26/3}**}. The initial release of the Bitcoin Software required there to be an index of historical transactions to enable nodes to check whether the output of a transaction had already been spent {**Wuille1 [30] {C1/1/7}**}. That index was called blkindex.dat **{L8/12/1}** and included information about all transactions that had occurred so far, including fully spent transactions, as well as transactions with unspent outputs. The index would point the software to the relevant block data from which the full raw transaction data could be obtained.

753. As a result of a patch authored by Dr Wuille, and placed by him on GitHub by pull request 1677 in August 2012, a significant optimisation was proposed to that approach. Because a spent transaction cannot be spent again, there was no need for nodes to check new transactions against spent transactions. It was sufficient that nodes confirm that any new transactions were of an unspent output from another transaction. As part of Dr Wuille's pull request he proposed replacing the transaction index with a database containing just the unspent transaction outputs {**Wuille1 [30-31] {C1/1/7}**}.

754. The change proposed by Dr Wuille was introduced in version 0.8 of the Bitcoin Software in February 2013 and resulted in a major performance improvement in the Bitcoin Software because (a) the unspent transaction database was much smaller given that it no longer contained information about spent transactions and (b) there was no need any longer to look up the full transaction data in the blockchain {**Wuille1 [30] {C1/1/7}**}. Dr Wuille's change accordingly introduced the concept of a pool of unspent transaction outputs. In addition, it introduced the concept of unspent transaction output caching, by which the software kept a subset of the unspent transaction output database cached in memory for faster access {**Wuille1 [31] {C1/1/8}**}.

755. It was in the context of the development of Bitcoin's treatment of unspent transaction outputs that the abbreviation "UTXO" came into being. Dr Wuille explains that Alan Reiner (who went by the name etotheipi) was the first person to use it. On 21 June 2012 he posted a message on the developers' chat that he was "*going to start using utxo to refer to unspent-txout*" {**{D1/6/11}** at Row 437}. Even some months later, however, the expression had not become well-established {see **Wuille1 [31] {C1/1/8}**}. In any event, there is no reference to the expression UTXO in the Bitcoin White Paper, in the Bitcoin Software or its updates released by Satoshi Nakamoto or in any of the voluminous emails and forum posts made by Satoshi Nakamoto.

756. Professor Meiklejohn and Mr Gao were in agreement that the term UTXO began to be adopted in 2012 or so {**Meiklejohn1, [45] {G/2/16**}, agreed by Gao at **{Q/3/2}**} and Dr Wright appeared to confirm the position in his eleventh witness statement at **Wright11, [578] {CSW/1/107}**. That, however, presented a difficulty for Dr Wright:

    756.1. The SEIR_C document refers explicitly to "UTXO caching" **{L3/237/13}**, to UTXO addresses **{L3/237/14}** and to the "UTXO pool" **{L3/237/15}**.

    756.2. A further reliance document alleged to come from 2008, Dr Wright's Non-Sparse Random Graphs paper **{L3/230}**, includes a sub-heading referring to UTXO **{L3/230/4}**.

    756.3. Even one of the documents on the BDO Image, which supposedly dates back to 2007 refers to the UTXO addresses and the "UTXO pool" **{PTR-F/39/1}**.

757. Dr Wright's response to this was to suggest that Satoshi Nakamoto had used the expression UTXO because Dr Wright used it in those three documents. However, the Developers estimated that around 1,000 emails or forum posts written by the real Satoshi Nakamoto are available to the parties and the Court. They submitted that not a single one uses the expression UTXO – and there was no contradiction on this point. Yet, according to Dr Wright, Satoshi is supposed to have used the expression UTXO in 2008 in the precise manner in which UTXO came to be used in 2012 – with UTXO caching and a UTXO pool - in those three documents. I do not find this to be credible.

758. On this point Dr Wright's evidence was nothing more than mere assertion:

> *"139: 6 Q. And if we go to the top of page 15 {L3/237/15}, we can*
> *7 see that this document refers to "the UTXO pool".*
> *8 A. Mm-hm.*
> *9 Q. That only came into existence after the Ultraprune*
> *10 request was updated, right?*
> *11 A. No, that's incorrect. Once again, the models that I'd*
> *12 been building include this. So, what you're assuming is*
> *13 that code and ideas that I'd already got in iDaemon, and*
> *14 other such things, are the only place they exist. And*
> *15 what a UTXO pool is, in my system, is very different to*
> *16 yours.*
> *17 Q. Now, if you were Satoshi Nakamoto, Dr Wright, and if you*
> *18 read this document before you purported -- or you chose*
> *19 to rely on it, before -- sorry, if you were*
> *20 Satoshi Nakamoto and you wanted to present the documents*

21 you wanted to rely on, you would have spotted those
22 three anachronisms, wouldn't you?
23 A. No, because they're not. That also goes into things
24 like the orphan block pool, which doesn't, I don't
25 believe, exist in BTC Core, but is something in my
140: 1 software. So when we're talking about that, what we
2 have are competing chains and we've made a pool for
3 that. So using a standard term, that one, you would
4 say, is an anachronism because it's not in core, but
5 it's in my paper."

759. Ignoring the irrelevant reference to iDaemon, Dr Wright's suggestion that he was referring to a different type of UTXO pool to that introduced by the Ultraprune pull request made by Dr Wuille is contradicted by the document to which he was actually referring. That document is specifically addressing the use of the UTXO pool for the purpose of checking double-spending:

> "*In a double spend, a client attempts to spend the same ledger entry in two places, and to separate end addresses, at the same time. The nature of the protocol is such that only one of these competing transactions can be allocated and recorded into the blockchain. Once an amount has been removed from the UTXO pool, it cannot be used again.*" **{L3/237/15}**

iv. Bootstrapping

760. A further area of anachronism was identified by Dr Wuille at **Wuille1, [13-23] {C1/1/3}** in the context of bootstrapping, which is the process by which a node connects to the peer-to-peer network {**Wuille1, [14] {C1/1/4}**}. It is convenient to take that topic in two parts:

760.1. First, by looking at the way in which a node first connects to the peer-to-peer network.

760.2. Second, by exploring how the Bitcoin Software then obtained the IP addresses of further nodes.

761. The process for first connection went through three phases:

761.1. **IRC seeding**: When the Bitcoin Software was first released, nodes would connect to an IRC channel on a particular IRC server (which was hardcoded into the software) to see which other nodes were in the channel. It then built a database of IP addresses {**Wuille1, [15] {C1/1/4}**}.

761.2. **Seeding from hard-coded IP addresses**: The software was then updated by Satoshi in June 2010 so that in addition to being able to connect to a particular IRC server, the IP addresses of some Bitcoin nodes was hardcoded into the software itself {**Wuille1, [16] {C1/1/4**}}. That can be seen at **{L6/182/4}** where the 47 seed IP addresses are identified in hex.

761.3. **DNS seeding**: In March 2011 Jeff Garzik (then one of the core developers) proposed DNS seeding in a pull request on GitHub **{L7/205}**. DNS seeding would

mean that nodes connected to a DNS server. The DNS server would record a number of Bitcoin node IP addresses {**Wuille1, [17] {C1/1/4}**}. Gavin Andresen recommended Jeff Garzik's proposal to Satoshi Nakamoto in March 2011 **{L7/204.4}**. Satoshi's response does not suggest that he accepted that there was a need for the change **{L7/204.7}**. However, the code was introduced into version 0.3.21 of the codebase in April 2011 **{L7/221/1**} (see fourth bullet point: "*A new method of finding bitcoin nodes to connect with, via DNS A records. Use the -dnsseed option to enable*"). The Bitcoin Software was then updated in version 0.3.24 in July 2011 to make DNS seeding the default: **{L7/343}** at point C1 ("*DNS seeding enabled by default*").

762. The process for a new node to obtain the IP addresses of additional nodes once it had connected to the network (which was undertaken through a "getaddr" request) also went through a number of stages {**Wuille1, [18] {C1/1/4}**}:

762.1. In the first release of the Bitcoin Software there was no limit on the number of IP addresses that a new node (a "receiving node") could receive from a node receiving that request (a "sending node").

762.2. In November 2009 Satoshi Nakamoto changed the Bitcoin Software to ensure sending nodes would only send 1,000 addresses in any one message. If there were more than 1,000 addresses to send, then the sending node would have to send more than one message {see **{L6/29/4}** final lines: if (VInventoryToSend.size() >= 1000) {pto->PushMessage("inv", vInventoryToSend);vInventoryToSend.clear()}.

762.3. In June 2010, Satoshi made a further change so that receiving nodes would not have to process more than 1,000 addresses at a time. Individual messages with more than 1,000 addresses would be rejected {see **Wuille1, [19] {C1/1/5**} and **{L6/181/2}**: "// receiver rejects addr messages larger than 1000"}. This brought the position of receiving nodes into line with that of sending nodes – and so assumed that sending nodes would have updated their software in line with the change in November 2009.

762.4. In October 2010, Satoshi made a further change so that if a sending node knew of 2000 or fewer active addresses, it would send all of them (albeit in messages of up to 1000 addresses at a time). If it knew of more than 2000 active addresses it would use a random number generator to send on average 2000 of them (again 1000 addresses at a time) {see **{L6/454/1**} green code passages}. Later that month, that was revised from 2000 to 2500 {see **{L6/456/4}** green code passage halfway down the page in which 2000 is replaced with 2500 and **Wuille1, [19] {C1/1/5}**.

763. This history of bootstrapping can be compared with another of Dr Wright's reliance documents, namely **{L3/184}**, which purports to date from December 2008. That document contains a section at the foot of **{L3/184/2}** that refers to "Node discovery" and purports:

763.1. to describe (at **{L3/184/2}**) the Bitcoin network finding nodes using DNS seeding (as well as other mechanisms), even though DNS seeding was not implemented

until April 2011. Moreover, the note does not even refer to IRC seeding, which is the system originally introduced by Satoshi.

763.2. to describe (at **{L3/184/3}**) the 1000 and 2500 limits on the number of addresses that would be sent by sending nodes, even though those limits were not introduced until mid-late 2010.

764. Those anachronisms show that the document cannot derive from December 2008, as the document's metadata purports to suggest. Satoshi Nakamoto would have been well aware of that shortcoming.

v. Summary

765. Each of the anachronisms identified above relate to documents that have been identified as manipulated or unreliable by Mr Madden and Dr Placks on grounds unrelated to the substance of their content. The anachronistic content corroborated those conclusions but, as the Developers submitted, also pointed to two more important conclusions.

766. The first is that the forgery of these documents must have been by Dr Wright himself. The reason for that is that on Dr Wright's own account some of the anachronistic content to which these documents refer was known only to himself as a result of his supposed personal development of Bitcoin and was written by him: (**emphasis** added)

> *"142: 5 Q. Now, my learned friend Mr Hough has been through*
> *6 the documents with you and made the point that*
> *7 the metadata of those documents is inauthentic, or that*
> *8 it's forged. But it's not just the metadata that's*
> *9 inauthentic, is it, it's the content as well?*
> *10 A. The metadata on that is not forged.*
> *11 Q. You wrote this content, didn't you?*
> *12 A.* ***Of course I wrote this content. This content was***
> ***13 created by me,*** *but not like you're saying. It was*
> *14 created by me in -- like, over 15 years ago.*
> *15 Q. Dr Wright, you forged these documents, didn't you?*
> *16 A. I did not. Again, what you're saying is that other*
> *17 terminology which I've used in multiple other things*
> *18 must have been shared with people. I create -- I've got*
> *19 several thousand documents, as in ones that are*
> *20 patented, and I have not discussed any of those*
> *21 terminologies outside of corporations where people have*
> *22 NDAs.*
> *23 Q. So nobody else could have forged these documents?*
> *24 A. They're not forged."*

767. The second is that each of these documents was separately considered by Dr Wright and included in his list of Reliance Documents. The person(s) who was Satoshi Nakamoto would not have made the mistake of relying on documents that contained anachronistic content to support their claim to that identity.

Satoshi's Bitcoin payments

768. It is apparent that in the development of his account to be Satoshi, Dr Wright has largely based it on known facts about Satoshi's work and communications. However, there are instances where Dr Wright's deductions about what he thinks happened have turned out to be wrong and some concern his assertions about transfers of Bitcoin.

769. In a fiery interview with GQ magazine conducted by Stuart McGurk with Dr Nicholas Courtois, Dr Wright asserted that he (as Satoshi) had only transferred bitcoins to Hal Finney and Zooko "*full stop*" **{{L14/67/1} at 5:17-5:21**}. Notwithstanding what Mr Zooko Wilcox-O'Hearn had said in his witness statement that he never received any bitcoin from Satoshi, in his cross-examination on Day 7 Dr Wright again asserted that Satoshi had transferred bitcoins to Zooko:

> *"157:18 Q. And in reality, Satoshi never transferred any Bitcoin to*
> *19 Zooko Wilcox-O'Hearn, did he?*
> *20 A. Actually, I did. Zooko was very interested because he*
> *21 had been working on a similar thing, MojoNation,*
> *22 beforehand.*
> *23 Q. So he's wrong in his witness statement when he says he*
> *24 didn't receive Bitcoin from Satoshi, is he?*
> *25 A. He is."*

770. I have set out my assessment of Mr Wilcox-O'Hearn as a witness above. His evidence in cross-examination on Day 14 on the matter of whether Satoshi had transferred bitcoins to him was as follows. Backed up by the detail in his witness statement, I found his evidence entirely credible:

> *"80: 4 Q. Right. You see, what I suggest is that you're in fact*
> *5 mistaken about that, and given what you've accepted is*
> *6 your very keen interest in Bitcoin, your perception that*
> *7 it was a revelation, that you were entranced and sucked*
> *8 in pretty early, that the reality is that you did in*
> *9 fact get more involved than you now remember: you*
> *10 downloaded, you ran the software and you were sent some*
> *11 Bitcoin by Satoshi.*
> *12 A. No, by the time of -- like I mentioned earlier, Bitcoin*
> *13 had gone from a curiosity to a breakthrough in my mind*
> *14 at some point, and Satoshi was totally my hero. Still*
> *15 is. I love what Satoshi means to me and to people. So*
> *16 if I had ever gotten bitcoins from Satoshi, I would*
> *17 definitely remember that. But again, my earliest use of*
> *18 Bitcoin was OTC trading. You know, "OTC" means "over*
> *19 the counter". I forget what it was called, but there*
> *20 was this thing where people could post, if they wanted*
> *21 to buy or sell bitcoins, and then they could get each*
> *22 other's contact from it. That's my earliest memory of*
> *23 using Bitcoin for anything myself.*
> *24 Q. So, again, I suggest that the fact that you regarded*
> *25 Satoshi as your hero, it beggars belief that you didn't*
> *81: 1 get more involved at the very earliest stage.*

2 A. You underestimate my laziness and procrastination."

771. This was not the only error in Dr Wright's prior assertions about Satoshi Nakamoto's transfer of bitcoins. Satoshi made transfers of Bitcoin to Nicholas Bohm, a former partner of Norton Rose who had developed an interest in cryptography {**Bohm1 [5] {C/10/2}** and **Bohm1 [15] {C/10/4}**}. Satoshi would have known of those transfers, but it would seem that Dr Wright only became aware of Mr Bohm's dealings with Satoshi when COPA served Mr Bohm's witness statement in these proceedings. When challenged on this point on Day 7, his answer presented a very striking contrast with the definitive statement in the GQ interview (to Hal Finney and Zooko "*full stop*")"

"158: 1 Q. And of course Satoshi transferred Bitcoin to Nick Bohm,
2 but you weren't to know that at that point, were you?
3 A. Oh, of course I did. But do I remember people? No.
4 I transferred to a lot of people in 2009."

772. It was striking that Dr Wright could not point by name to any of the "*lot of people*" to whom he was now saying Satoshi had transferred Bitcoin.

"158:23 Q. Can I just stop you. You have made the point – you've
24 made your point.
25 Let me ask this question then. You've said that you
159: 1 transferred Bitcoin as Satoshi to hundreds of people.
2 Can you name some of those to whom you transferred
3 Bitcoin whose receipt of Bitcoin from Satoshi is not in
4 the public domain?
5 A. God knows. I don't remember everyone now.
6 Q. So you can't remember any of the hundreds?
7 A. No.
8 MR JUSTICE MELLOR: Not even one?
9 A. I don't know who is and isn't in the public domain.
10 I know the funding stuff I did for Gavin, but he's
11 talked about that now. But, no, it had no value at the
12 time, my Lord. I just sent whoever asked, and most of
13 them were pseudonymous. The majority of people on
14 the forum didn't actually use their name."

773. Dr Wright's evidence about a transfer to Zooko was untrue, and his evidence in response to the fact that Mr Bohm had received bitcoin from Satoshi was, in my judgment, yet further fabrication. These matters provide further proof that he is not Satoshi.

The PGP key

774. If Dr Wright were Satoshi Nakamoto then he ought to have been able to sign a message using the PGP key associated with Satoshi Nakamoto that was on the bitcoin.org website. It can be seen at **{H/318/2}**.

775. The relevance of the key arises in two ways:

775.1. First, in his initial list of requests for proof on 29 March 2016 **{L11/449.1/1}**, Gavin Andresen requested that Dr Wright sign a message with that key. In the

Kleiman proceedings Mr Andresen vaguely recalled a conversation with Dr Wright about PGP signatures in which Dr Wright "*gave some reason why he either did not have the key, or it would not be good proof*" **{{E/17/42} at lines 11-14**}.

775.2. Second, in the backlash following Dr Wright's failed blogpost on 2 May 2016 (on which see below), efforts were made to get Dr Wright to sign using that key. Dr Wright sought to fob off those requests on the basis of an absence of relevant key slices: **{L13/297}, {L13/299}, {L13/304}, {L13/307}, {L13/308}, {L13/310}** and **{L13/313}**.

776. In their Particulars of Claim, COPA pointed out that Dr Wright ought to be able to show that he had control over Satoshi's private key. In his Defence, Dr Wright addressed the PGP key in question as follows {**Defence [83(2)] {A/3/24} and Wright4 [104] {E/4/34}**}.

> "*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 person or persons unknown. Therefore, control, command or ownership of that key has no probative value as to the identity of Satoshi Nakamoto.*"

777. Dr Wright had said almost exactly the same thing in an interview in 2021 {available in the webarchive, plus a transcript is at **{O4/14/36}**}, in which he directed the interviewer to a 2009 archive version of the bitcoin.org website, asked the interviewer to scroll down to and then click on the PGP key link (which takes the reader to a 28 February 2011 archive) before resolutely announcing: "*The first version was after I left*" **{O4/14/36}** and then continuing **{O4/14/37}**:

> *"RYAN CHARLES: So in fact when I look at what the URL is, it says if people can see on my screen, 2009, but then when you click it, the 2009 one is not there and it is a 2011 version instead.*
> *DR. CRAIG WRIGHT: Yes.*
> *RYAN CHARLES: So it does seem like the lack of version there could indicate that there was a different version at this time that has been excluded.*
> *DR. CRAIG WRIGHT: Yes. A different version has been ----*
> *RYAN CHARLES: Just to be clear then, are you saying you did that or did they do that?*
> *DR. CRAIG WRIGHT: I did not do that. I was not in control of the web page at this point."*

778. Dr Wright sought to distance himself from this in evasive answers in cross-examination at **{Day8/37:9}** to **{Day8/40:7}** and at **{Day8/42:2-24**}.

779. So the issue is whether Dr Wright's suggestion that the PGP key was "*created by a person or persons unknown*" "*in 2011*" is true or false. On this, the Developers relied on two points: first, the date of creation of the key and second, the nature of the key.

i. The date of creation of the key: not 2011

780. Dr Wright's contention that the PGP key was created in 2011 was addressed independently by both Mr Madden and by Martti Malmi.

781. Mr Madden described the key at **Madden4 [144 et seq] {G/6/46}**. He was able to verify the date of the key to 30 October 2008 in two ways:

781.1. First, using the X-Archive-Orig fields in the header of the relevant web page on the Wayback Machine, he identified that the key had been uploaded to the bitcoin.org website with a date of 30 October 2008 {**Madden4 [149] {G/6/48}**}.

781.2. Second, he was able to inspect the internal timestamp of the PGP key itself, which also gave a date of 30 October 2008 {**Madden4 [152] {G/6/50}**}.

782. Mr Malmi disclosed emails that he had exchanged with Satoshi Nakamoto in December 2010. On 6 December 2010 Mr Malmi had asked Satoshi to send his PGP key {L6/478/1}. Satoshi responded the same day, sending the PGP key and stating "*It's also at http://www.bitcoin.org/Satoshi_Nakamoto.asc*" **{L6/477/1**}. The key sent by Satoshi is identical to the key analysed by Mr Madden.

783. So the evidence from those two independent sources established that the key was not created in 2011.

784. Mr Malmi's emails were disclosed by COPA with his witness statement on 28 June 2023. They presented an immediate problem for Dr Wright's then account of events. His story changed in **Wright4**. He continued to state that the "*key was created by person or persons unknown*" (**Wright4 [104] {E/4/34}**) but now said:

> *"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 [sic] Malmi, so that they could send code updates to me. It was only published in 2011 by an unknown party (I suspect Marti [sic] Malmi), after I stopped the active use of the Satoshi Nakamoto pseudonym."*

785. Leaving aside the sudden reversal of the position previously taken by Dr Wright, his suggestion that the PGP key had been "*generated by Vistomail*" is wrong. As described in [788.1 below], the key was associated by Satoshi with his satoshin@gmx.com account (not his satoshi@vistomail.com address).

786. However, in addition Dr Wright had overlooked Satoshi's confirmation that the key that he had sent to Mr Malmi was already on the bitcoin.org website, i.e. that it had been on the bitcoin.org website no later than December 2010: see paragraph 782 above. Dr Wright repeated this error in **Wright9 [34] {E/26/12}**, continuing to contend that the PGP key was posted after he "*ceased to be active under the Satoshi Nakamoto identity*".

ii. The nature of the key: not "*person or persons unknown*"

787. In an attempt to escape the consequences of his inability to sign a message using Satoshi's public PGP key Dr Wright made two separate assertions regarding the technical capability of the key:

787.1. First, he suggested that "the PGP key is not specific to any individual but to a server at Vistomail" (**Wright4 [105] {E/4/35}**).

787.2. Second, he said that the key was "not a signing key" (**Wright11 [242] {CSW/1/46}**) and "Only for encrypting, never for signing" (**{Day7/143:10}**).

788. However, as the Developers submitted, the content of the key itself shows both assertions are wrong:

788.1. The key expressly identifies the user ID as "Satoshi Nakamoto <satoshin@gmx.com>" **{G/6/50}**.

788.2. The sigclass of the primary key is clearly identified as "*0x13*" **{G/6/50}**. That sigclass is defined in the OpenPGP Message Format as follows "*Positive certification of a User ID and Public-Key packet. The issuer of this certification has done substantial verification of the claim of identity*" **{L2/202.1/20**}. It ties the key directly to the satoshin@gmx.com address, not to "*a server at Vistomail*" or "*person or persons unknown*". Dr Wright had to admit this association: **{Day8/167:8}**.

788.3. The algorithm used in the generation of the primary key is clearly identified as "*algo 17*" {**{G/6/50}** – see next to "signature packet"}. Algo 17 is a DSA (i.e. a Digital Signature Algorithm) **{L2/202.1/62**}, that is to say an algorithm for digital signatures. It is not an encryption algorithm. So the primary key was not an encryption key: it was specifically for signing. Again, Dr Wright had to admit this at **{Day8/166:10-11}**.

788.4. The key flags for the primary key (noted against the reference "*hashed subpkt 27 len 1*" at **{G/6/50}**) are shown as "*03*". Key flags are binary flags {see OpenPGP Message Format at **{L2/202.1/33}** at **[5.2.3.21]**}. 03 corresponds to 11 in binary and marks the key as being "*used to certify other keys*" (0x01, or 01 in binary) and "*to sign data*" (0x02, or 10 in binary) {see OpenPGP Message Format at **{L2/202.1/34}** top of page}.

789. In short, I am satisfied that every element of Dr Wright's factual and technical explanation of Satoshi's PGP key was wrong. The Developers submitted that one inference to be drawn from that shortcoming in his evidence, and from the sharp change in that evidence following disclosure of Mr Malmi's emails, is that Dr Wright was telling these lies to avoid the inference to be drawn from his failure to sign a message using Satoshi's PGP key. I agree. However, Dr Wright's erroneous understanding of Satoshi's PGP key is yet a further indicator that he cannot be Satoshi Nakamoto.

Dr Wright's first public reference to Bitcoin

790. The Developers made a pertinent point about Dr Wright's first public reference to Bitcoin. To set the scene it is necessary to go back to a thread started by a user called genjix on bitcoin.org in November 2010 about using Bitcoin to make payments to Wikileaks. Robert Horning responded in a lengthy post **{L19/168/35}** concluding with the suggestion: "*Basically, bring it on. Let's encourage Wikileaks to use Bitcoins and I'm willing to face any risk or fallout from that act*". Satoshi Nakamoto responded to that suggestion on 5 December 2010 **{L19/168/49}**, stating:

> "*No, don't "bring it on".*
>
> *The project needs to grow gradually so the software can be strengthened along the way.*

> *I make this appeal to WikiLeaks not to try to use Bitcoin. Bitcoin is a small beta community in its infancy.*
>
> *You would not stand to get more than pocket change, and the heat you would bring would likely destroy us at this stage.*"

791. A few days later an article was published in PC World questioning whether the Wikileaks scandal might lead to a new virtual currency, and specifically naming Bitcoin **{L6/493}**. That led to a further thread on the bitcoin.org forum, concluding with Satoshi's response on 11 December 2010 at **{L19/49/2}**, which was one of his final postings on the forum.

> "*It would have been nice to get this attention in any other context. WikiLeaks has kicked the hornet's nest, and the swarm is headed towards us.*"

792. Dr Wright's first public reference to Bitcoin was on 28 July 2011. It was a response to some comments posted on an article that he had published for an online media outlet known as The Conversation. The article, entitled "*Are Anonymous and LulzSec about to hack PayPal for WikiLeaks?*", questioned whether PayPal's decision to withhold funds from WikiLeaks might lead to it being hacked.

793. In the comments beneath the article Dr Wright advanced the argument that, as a business, PayPal was entitled not to transact with WikiLeaks. Some of the commenters challenged that view on the basis that WikiLeaks did not have an alternative payment provider. Dr Wright observed that he knew of over 50 alternatives to PayPal and that WikiLeaks could have selected "*BitCoin*", but it did not. He noted that "*If you want to look at anything to blame, look to WL's stupidity in selecting PayPal as a provider over BitCoin and others like them when PayPal is known to shy away from contraversy [sic]*".

794. Dr Wright wrote a follow-up piece for the same website on 9 August 2011 entitled "*LulzSec, Anonymous … freedom fighters or the new face of evil?*" in which he referred to the vandalization by Anonymous of the home page of the Syrian Ministry of Defence. Dr Wright turned the conversation back to the position of PayPal, who he suggested represented freedom far more than groups such as LulzSec and Anonymous.

795. On the point about whether there were sufficient alternatives to PayPal he argued that there were. He responded to one commenter stating that "*WikiLeaks can get payments from other sources. It CAN get money transfers. It can get bit coins it can do many things if it wants. There are MANY options that allow people to send money to WL*" (emphasis added) **{L7/391/13**}. He responded to another commenter as follows (again, emphasis added) **{L7/391/17-18}**:

> "*Bit Coin (Bit Coin) is a digital currency. Bit Coin offers a full peer-to-peer currency solution. P2P transfer of funds is available using methods that can even be untraceable. They're a ways using this technology to transfer funds that cannot be intercepted or stopped.*
>
> *…*
>
> *That said, there are alternatives available in the marketplace such as Bit Coin that offer solutions to the problems that WikiLeaks faces……"*

796. The Developers submitted these exchanges showed the following:

796.1. First, that Dr Wright's first public foray into Bitcoin took a diametrically opposing view to Satoshi Nakamoto. Satoshi was seeking to discourage Wikileaks from adopting Bitcoin. Dr Wright seemed to think this would be a good idea.

796.2. Second, that by late July 2011 Dr Wright was aware of Bitcoin but he was uncertain about how it was spelled. On whether it should be one word or two, Dr Wright suggested in cross-examination that his use of two words was the consequence of auto-correct but this explanation is unconvincing in view of the fact that the 'error' appears three times in just 10 words in his post at **{L7/391/17-18}** – the point being that he was bound to spot the 'error' if he had meant to write a single word, whether BitCoin or Bitcoin.

796.3. On whether the c of coin should be capitalised or not, the Developers pointed out that the first release of Bitcoin was accompanied by a readme.txt file which referred to BitCoin. However, Satoshi Nakamoto moved the content of that readme file to build-unix.txt on 5 November 2009, see https://sourceforge.net/p/bitcoin/code/32/, in which the equivalent text referred to Bitcoin (without a capital "C"). All further releases of the Bitcoin Software referred to Bitcoin without capitalising the "C".

797. Faced with those inconsistencies on Day 8, Dr Wright was unable to explain them:

> *"189:11 Q. Dr Wright, more pertinently, you did not know that*
> *12 Satoshi was keen to discourage WikiLeaks from using*
> *13 Bitcoin, right?*
> *14 A. Again, I wanted people not to use the other. I'd seen*
> *15 all the sites, I'd gone through everything with people*
> *16 multiple times, so, no, I knew what I said. What you're*
> *17 trying to say is because, on a site, it comes up that*
> *18 way, which, "Bitcoin" and then "Bit Coin". It was meant*
> *19 to be cut and paste as a hyperlink and somehow that*
> *20 ended up funky."*

798. In July 2011, there is no reason to believe that Satoshi would have reversed his original view, having only relinquished his use of the pseudonym in April 2011. Furthermore, Satoshi would have had no reason to use any expressions other than 'Bitcoin'. He would not have used two words or capitalised the C. I also agree with the Developers that these posts show that Dr Wright had no significant familiarity with Bitcoin in July 2011, and that it is reasonable to suppose that all his familiarity was gained subsequently by careful study of the materials which had been made public.

Dr Wright's evidence as to his leaving the Satoshi persona

799. Dr Wright said that circumstances of late 2010 / early 2011 (including his marital problems and the ATO investigations) led him to decide to move away from the Satoshi persona, phasing out communications under the pseudonym in April 2011. Dr Wright recounted 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. He says

that he also granted Mr Andresen access to the Bitcoin code on SourceForge, though only on a lower-level administrator basis.

800. Dr Wright then painted a picture of disappointment. He said 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. There is no evidence that Dr van der Laan was involved at all, other than Dr Wright's account. Dr Wright claimed that these changes were against his wishes. However, the forum move did not alter the forum database, and (as noted above) it is clear from contemporaneous emails that Satoshi was perfectly content with the move to GitHub.

801. Dr Wright's account 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 he had wanted them, and (b) that Satoshi never requested such credentials. This latter point is unsurprising, as at that point Satoshi clearly knew he was going to leave the scene {see, on these points **{Day13/31:1} - {Day13/31:11}**.

802. 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 the 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 **{L/220/1}** urged Mr Andresen to make Bitcoin more an open source project and give more credit to developers. Dr Wright also maintained that Dr van der Laan had been involved in making the move to GitHub, without a shred of evidence.

The Investigations by the Australian Tax Office and the ATO Decisions

803. Dr Wright's dealings with the ATO formed a significant part of his life from 2010 to 2016, and they were important to his finances. Indeed, in August 2014, the ATO estimated that 94% of the income he had received in the previous two years had come from tax refunds to his companies {ATO Submission at **{L9/274/9}**, [36]}. This forms the backdrop for Dr Wright in 2015 needing money and receiving a bailout which involved him staking a claim to be Satoshi.

804. 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).

805. 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 Integyrs Pty Ltd) for sums totalling AU$ 2,235,000. The IP sale contract on which he relied in relation to 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 **{L4/462/1}**. This is significant because Dr Wright later produced documents (which I have found to be forged) to suggest that his Spyder and BlackNet projects involved elements of Bitcoin, whereas this and other contemporaneous documents show that they did not.

806. 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 {Interim Report at **{L7/431/119}**. Dr Wright submitted notices of objection, which were rejected by the ATO, including on the basis of failure to substantiate the IP sales {Reasons for Decision at **{L7/431/9}**. He applied for review to the Administrative Appeal Tribunal. The result was that the ATO agreed to lift the administrative penalty and to allow various expense deductions {letter from the ATO dated 15 January 2013 **{L8/117/1}**, but it does not appear that the CGT issue was specifically addressed.

807. 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.

808. 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 {decision letter dated 23 December 2013 **{L8/305/1}**}. 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 {letter of 28 February 2014 **{L8/422/1}**}.

809. 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 **{Day7/58:25}**. 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 **{L8/309/2}.** 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.

810. For the tax quarter ending September 2013, Dr Wright's companies submitted claims for GST refunds: AU$2.8 million in respect of Cloudcroft Pty Ltd; AU$3.7 million in respect of Coin-Exch Pty Ltd; AU$4.1 million in respect of Denariuz Pty Ltd; and AU$3.4 million in respect of Hotwire Pre-Emptive Intelligence Pty Ltd. These related to supposed acquisition of rights to software held by the Wright Family Trust (trading as DeMorgan). Dr Wright subsequently claimed that all consideration for the acquisition 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.

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

812. 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 **{L11/354/1}**. 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 Professor David Rees, a UK-based mathematician and veteran of Bletchley Park.

    812.1. 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.

    812.2. As to the latter claim, Dr Wright maintained that payment had been made to Professor Rees by way of Bitcoin rights. However, evidence from Professor 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 Professor Rees had made a Bitcoin transaction (after 28 June 2013), Professor 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 Professor Rees gave him notes which assisted in his work on Bitcoin more generally {see Dr Wright's book, "Satoshi's Vision", published in 2019, at **{L15/96/18}**}. In cross-examination, Dr Wright attempted to maintain his account that he had engaged Professor 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 Professor 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 **{Day7/61:15}** - **{Day7/65:20}**. It is also telling that Mr Yousuf, a director of C01N, had never heard of Professor Rees, who had supposedly provided valuable and costly consulting services to the company **{Day9/135:5}**.

813. 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, Denariuz Pty Ltd, Zuhl Pty Ltd and Integyrz Pty Ltd. 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. 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.

814. 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 {ATO Decision at **{L11/362/10}**, at **[52ff]**}. 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*", though he later accepted backdating the invoices {**{L9/140/29}** at line 8: "*I ended up doing the backdating because I thought it was correct".*}.

815. 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 {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}}.** 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*."

816. Under cross-examination, Dr Wright attempted to explain away the ATO's findings by saying that "*people sent in false information and fabricated documents to them*" **{Day7/98:10}**, but this explanation is not convincing at all bearing in mind that the problem with the emails 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 not consistent with the fact 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 **{Day7/98:6}** - **{Day7/102:3}**.

The Tulip Trust

817. Dr Wright claimed 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 he did this by putting in trust all these assets, including bitcoin he claims to have mined since 2009 {**Wright1, [138-140] {E/1/26}**}. He claimed 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.

818. It is not necessary to relate Dr Wright's various accounts about the Tulip Trust in full. Suffice to say that I agree with COPA's submission that his account of the Tulip Trust appears to have been refashioned successively in the ATO proceedings, in *Kleiman*, in *Granath* and in this action. His evidence about the Tulip Trust in cross-examination

{**Day6/179:2**} - {**Day6/182:9**} and {**Day7/8:5**} - {**Day7/54:12**} in particular} was very confused and contradictory and parts were incredible.

819. For example, 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 **{L7/382/1}** and 17 October 2014 **{L9/218/1}** 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 **{L8/17/1}**.

820. 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 {Decision concerning C01N Pty Ltd of 21 March 2016 **{L9/382/45}**, at **[247-261]**}. 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 {Decision concerning C01N Pty Ltd of 21 March 2016 **{L9/382/49}**, at **[266.2** and **fn. 241]**}. 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*" **{L17/382/46}**.

821. In *Kleiman,* Dr Wright was ordered (several times) to produce a complete list of all bitcoin that he mined prior to December 31, 2013. Dr Wright claimed he was unable to comply because the information was in the Tulip Trust, encrypted using a Shamir Sharing Algorithm, which he could not decrypt since he did not have all the necessary decryption keys. After an evidentiary hearing, Magistrate Judge Reinhart had to rule on whether Dr Wright had proved he was incapable of complying with the Court's Orders. His ruling dated 27 August 2019 **{L15/207/1-29}** relates how Dr Wright changed his evidence on (a) the creation of the Tulip Trust (and the Judge found the supposed Deed of Trust document presented by Dr Wright had been backdated), (b) the nature of the trust (that it was a 'blind' trust and he was not a trustee, yet three weeks later he stated in a sworn declaration that he was a trustee (of a blind trust!), (c) the trust assets (whether the trust contained bitcoin or, as he later asserted, the trust contained an encrypted file with the keys to the bitcoin, not the bitcoin itself), and (d) how the trust assets could be recovered. Dr Wright had given evidence that he had given away a controlling number of the key slices to David Kleiman (by then deceased), which was why he could not decrypt the file that controlled access to the Bitcoin. According to Dr Wright's evidence, unlocking the file depended upon a bonded courier appearing on an unknown date in January 2020 with the decryption keys, and if the courier did not appear, then Dr Wright would have supposedly lost billions of dollars' worth of bitcoin, a story which Judge Reinhart considered 'Inconceivable' **{L15/207/19}**. Generally, Judge Reinhart did not believe Dr Wright and also found that documents presented by Dr Wright to support his position in the litigation had been altered and were fraudulent. Other documents conflicted with his evidence. On the evidence he heard, Judge Reinhart found the Tulip Trust did not exist **{L15/207/21}**.

822. COPA made it clear that they did not rely (and did not need to rely) on Judge Reinhart's findings, but on his ruling as a record of Dr Wright's story.

823. By way of a further example, in a sworn declaration he made in *Kleiman,* Dr Wright identified David Kleiman as one of the trustees of the Tulip Trust **{L15/51/2, at [7]**}, yet

under cross-examination before me, he said he was not **{Day7:21:8}**. When I put the inconsistency to him, he came up with a story about being ordered by Judge Reinhart to answer the question even though he did not know **{Day7:21}**.

824. Other glaring inconsistencies in Dr Wright's evidence about the Tulip Trust were the following:

824.1. The existence of different Trust documents (mentioned above).

824.2. His claim 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) {**Wright1, [187] {E/1/33}}.** This claim was necessary to make his 'trust' story consistent with his participation in the 2016 proof sessions, yet is completely at odds with his evidence in *Kleiman* about having to wait until January 2020 for the bonded courier to arrive with the key slices.

824.3. The fact that the Trust document relied upon in Kleiman dated 23 October 2012 was supposedly between Wright International Investments Ltd and Tulip Trading Ltd, yet Dr Wright only acquired Tulip Trading Ltd as an aged shelf company in 2014.

824.4. His claim to have put all his assets (including bitcoin and IP in research documents) beyond his own use, yet, on his account, both he and the staff in his companies (including nChain) continued to have access and to use all these documents. For example, it was never explained how he and his staff could have continued to use (and thereby supposedly be responsible for altering the metadata of) the documents which Dr Wright produced as precursor work to the Bitcoin White Paper, when they necessarily would have been assets in the trust supposedly beyond his use.

824.5. Finally, if all the research prior to 2012 had been put beyond his use, one might have thought that he would have had to have mentioned this in 2015 when securing funding from Mr MacGregor for the continuation of his research activities at nChain. Of course, nothing to that effect was mentioned and the existence of the trust did not appear to have posed any barrier at all.

825. Mr Madden found a number of Tulip Trust and Tulip Trading Ltd documents to be 'inauthentic' or, as COPA put it, to bear signs of having been forged in 2014/2015 {see Appendix PM14}.

826. Overall, there is strong evidence and I find that the Tulip Trust was another invention of Dr Wright's, initially as part of an attempt to shield assets from a possible bankruptcy in Australia. Having invented it, he attempted to use it in *Kleiman* to avoid having to identify the bitcoin he supposedly owned, yet that attempt failed.

Conclusion under this heading

827. I can now return to the points relied upon by Dr Wright as confirming his claim to be Satoshi as summarised under the heading to this section G (see just above [706]).

828. I have already dismissed some of those points. However, taking them together, against the concrete detail of the points I have discussed in this section, plus all the evidence of forgery by Dr Wright, those mostly circumstantial points relied on for Dr Wright can have no weight. To the extent that the evidence went beyond circumstantial, I am entirely satisfied the relevant witness was mistaken or lying. All of them might well have been encouraged to embellish their evidence by Dr Wright.

H. Patent Research and Development

> *'10. Dr Wright's deeply held belief is that his identity as Satoshi should be proved through work and knowledge. In summary, "you prove by knowledge, who you are, what you create" {Day 7/144/13-14}. In Dr Wright's view, an important aspect of this approach to proving identity lies in his extensive portfolio of patent research and development. The breadth of that portfolio is not in dispute. Dr Wright was not challenged during cross-examination in relation to his evidence that nChain has amassed a substantial portfolio of patents, encompassing nearly 4,000 patent filings, which are the fruit of Dr Wright's prior research. {Wright 1 [172] {E/1/31}}. COPA's attempt to undermine that evidence by the back door, during cross-examination of Ms Jones (without putting the equivalent points to Dr Wright), was misguided.*

829. I can deal with the points under this heading relatively briefly.

830. In my judgment, Dr Wright's 'work and knowledge' argument was yet another convenient excuse in his attempts to avoid all the highly problematic metadata and other indicia of forgery.

831. As for the '*extensive portfolio of patent research and development*', Dr Wright was clear that in June 2015, he had the fruits of research but no patents had yet been applied for. He claimed to have a large number of research papers (some 1,300), each of which he claimed would give rise to multiple patents. It was not clear whether his count of patent filings was by patent family or individual patents. Whether all of this was exaggerated or not does not matter. The point is that starting from 2015, a well-funded business with a research focus could generate that number of patent filings, but this sheds no light whatsoever on events in 2008 and 2009. If anything, the generation of a multi-patent thicket which it is apparent Dr Wright (and nChain) wish to assert against anyone who does not share his view of Bitcoin appears to me to run entirely counter to the way Satoshi created and released Bitcoin as open-source material.

832. In closing, I asked when Dr Wright's first patent application was filed. The answer came back at the start of Day 22 that his first priority document was filed on 28 October 2011, but the documents produced **{X/85** and **X/87}** concerned claims to a registry in which entries were securely timestamped and digitally signed. Although I was not addressed on this document, a brief review indicated it had only a very tenuous connection to Bitcoin via the known concepts of timestamping and digital signing. In any event, this does not appear to have been one of the nChain portfolio.

833. Naturally, I say nothing about the validity of any of these patents. However, for present purposes, in my judgment there was nothing under this head to support Dr Wright's claim to be Satoshi.

I. The private proof sessions

'11. Dr Wright's demonstration during a number of private proof sessions in 2016 that he was in possession of private keys to certain of the original blocks (i.e. blocks 1 to 11) of the Bitcoin blockchain is highly probative of his claim to be Satoshi. These sessions included demonstrations with Mr Andresen and Mr Matonis, both of whom were central figures in the Bitcoin community, Andrew O'Hagan, an author who was chronicling the evolution of nChain, and journalists from the BBC (Rory Cellan-Jones) and Economist (Ludwig Siegele). In each demonstration, Dr Wright showed he had access to private keys associated with early blocks. The fact that Mr Andresen and Mr Matonis were persuaded by these demonstrations that Dr Wright was Satoshi is highly significant. Their recognition of Dr Wright as Satoshi is particularly credible. COPA's attempts to undermine the integrity of the private proof sessions are misplaced. There is no realistic basis for supposing that the sessions were deliberately subverted by Dr Wright and any case to that effect is in any event not open to COPA on its pleadings and was not fairly put to Dr Wright in cross-x.'

Summary

834. In all the detail which follows, it should be kept in mind that if Dr Wright really was Satoshi, a reliable private signing could have been performed very easily and simply. He could have signed a message on his computer, using the private key associated with the public key for block 9. That signed message could have been passed via a clean USB stick to, for example, Mr Andresen, who could then have run the Verify algorithm on his own laptop to determine if it was genuine. Nothing more complicated was required.

835. Against that simple point (on which the experts were agreed) there is a marked contrast with the complicated and elaborate procedures which seem to have been adopted by Dr Wright.

The position on the pleadings

836. I deal first with that last submission made on behalf of Dr Wright, clearly made in his written closing and amplified orally, as I explain below. On the pleadings, the position was as follows. In their Particulars of Claim, COPA referred to the GQ interview and the ensueing offer by Dr Wright of 'Extraordinary proof'. Their case is set out in [21]:

> *'Accordingly, Wright has publicly asserted that one of the ways he can prove he is Satoshi is by referencing his ability to make transactions associated with the Genesis Block and other early Blocks. To date, Wright has failed to do so.'*

837. In his Defence at [34], Dr Wright admitted that he had not publicly demonstrated that ability, but he alleged that he had in private demonstrations to Messrs Andresen & Matonis (re Blocks 1 and 9), and to Messrs Cellan-Jones and Siegele (re Block 9). COPA's reply put him to proof on these matters.

838. In his oral closing, Lord Grabiner KC submitted as follows:

838.1. First, that it was not open to COPA to run a case that any of the proof sessions was subverted by Dr Wright, on the basis that any such allegation was of fraud or dishonesty which must be clearly pleaded.

838.2. Second, that, in the absence of a specific plea of dishonesty, it is not open to the Court to make a finding of dishonesty, citing *Three Rivers, per* Lord Millett at [186].

838.3. Third, Counsel for COPA never put a case of subversion to Dr Wright in cross-examination. At most, he said, it was merely suggested to Dr Wright that it would have been feasible to create a malware program and 'straightforward for someone with Dr Wright's experience' to stage the signing session with Mr Andresen {see **{Day8/73:22 -74:23}**}.

838.4. Fourth, for completeness, the issue of subversion was nevertheless addressed in Dr Wright's written closing.

839. In response to the challenge, Mr Hough KC made COPA's position very clear. I can summarise it in the following:

839.1. First, Counsel reminded me of an exchange which took place with Dr Wright's then Counsel, Mr Flynn KC, during the hearing in October 2023 following which I gave COPA permission to plead 50 allegations of forgery. In the course of argument Mr Flynn KC made the point that Dr Wright cannot be negligently asserting that he is Satoshi and that '*Everything he does, on their case, is dishonest'*, to which I observed: '*Yes. They are saying his entire claim to be Satoshi is dishonest*.' '*And anything supporting or which purports to support that claim is dishonest*.'

839.2. Counsel also drew attention to the fact that in my Judgment from that hearing [2023] EWHC 2642 (Ch) at [15] and particularly [54] I acknowledged that '*the essential feature*' of COPA's claim was that Dr Wright's claim to be Satoshi was fraudulent and, consistently with that, the documents he relies upon in support of that claim have been forged.

839.3. However, this point proves too much. As Mr Flynn KC observed immediately after the exchange I mentioned above, those points do not take one anywhere because the cases are very clear. Allegations of fraud and dishonesty must be distinctly and properly pleaded. I do not think Mr Hough KC was denying that, he was simply making the point that everyone (including Dr Wright's legal team) understood what COPA's case was.

839.4. Second, Counsel referred to the pleaded case that Dr Wright never reliably proved his possession of the private keys and that they put in issue what happened at the signing sessions.

839.5. Third, Counsel submitted that COPA was not able to plead a positive case about what happened in the signing sessions, because that was outside their knowledge.

839.6. Similarly, in response to the point that it was incumbent on COPA to put to Dr Wright that the signing sessions were subverted in a particular way, for example by saying that he used DNS hijacking or typosquatting or use of malware to interfere with Electrum, Counsel submitted COPA was not able to do that.

839.7. Relatedly, Counsel submitted that what COPA were able to do (and did) was to challenge Dr Wright on his version of what happened at each stage as well as putting to him the ways in which the sessions could have been staged.

839.8. Accordingly, Counsel submitted that the finding that COPA seeks (and is entitled to seek) is a finding that Dr Wright did not possess the private keys (e.g. to any of the early blocks, but blocks 1 and 9 in particular) and that the signing sessions did not prove otherwise.

840. All of this was, in my judgment, a storm in a teacup. It was clear that Counsel for COPA did not put allegations to Dr Wright concerning the signing sessions which were speculative or for which they did not have material to substantiate them. There is no onus on COPA to prove that the signing sessions were subverted by Dr Wright. However, on the pleadings, Dr Wright was clearly challenged to prove that the signing sessions did prove that he was in possession of the private keys to the 'early blocks' and blocks 1 and 9 in particular.

The facts

841. The essential facts are as follows, and most of this is as related in **Wright1**. I deal later with the contentious aspects.

842. 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 Jon Matonis and Gavin Andresen (both subject to NDAs). 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.

843. Jon Matonis met Dr Wright in mid-March 2016 in a hotel in Covent Garden, as arranged by Mr MacGregor and Mr Matthews. Dr Wright then met Mr Andresen in London on or about 7 April 2016, having briefly corresponded by email. 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. Dr Wright claims to have signed messages using the keys associated with blocks 1 and 9. As noted below in relation to the signing sessions, there are some differences between Dr Wright's recollection and that of Mr Andresen in his *Kleiman* deposition (the latter given with reference to some notes). Based on the agreed expert evidence, these are important to whether the session was genuine.

844. 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. 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. Dr Wright was then interviewed by Stuart McGurk from GQ, with the reporter being accompanied by a cryptologist, Dr Nicolas Courtois. Dr Wright said he cannot "*recall the demonstrations exactly*" that were made to the journalists. However, he did say that he did at least demonstrate possession of the private key associated with block 9 in all his signing sessions {**Wright2 [24], [32] & [40]**}.

845. 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, 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.

846. 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. Mr Matthews accepted, grudgingly, that there was such a plan in place. 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.

847. 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.

Conclusions on the private signing sessions

848. It is clear that Dr Wright never publicly undertook 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). Prof Meiklejohn concluded: "*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*". In the Joint Statement, Mr Gao agreed with almost all parts of Prof Meiklejohn's report concerning the signing sessions, including with that conclusion. As Prof Meiklejohn explained, the signing sessions omitted key steps which would have been required to make them reliable. All these matters remained common ground between the experts in their oral evidence.

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

850. In **Wright2**, Dr Wright gave a complex explanation of the signing sessions, setting out various technical measures he took. Professor Meiklejohn disagreed with a number of technical points Dr Wright made:

    850.1. Dr Wright said that the first stage in verification entails installing the Bitcoin Core software. Prof Meiklejohn explained 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.

850.2. Dr Wright claimed that he underwent the time-consuming exercise of downloading the entire Bitcoin blockchain as a preliminary to each signing session. Professor Meiklejohn explained that this was 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. This was agreed by Mr Gao.

850.3. Dr Wright said 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 added that this element was "essential" for integrity of the exercise. Prof Meiklejohn explained that that was unnecessary and added 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. Again, there was no dispute about this between the experts.

850.4. Dr Wright insisted that the procedure he used, with a second system or computer used for verification, avoided the risk of exposing the private key. Prof Meiklejohn disputed that this procedure has such a benefit over other methods. Importantly, she explained 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. Mr Gao agreed in his evidence. This 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.

The Signing Sessions with Mr Matonis and the Journalists

851. 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. Dr Wright claimed 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 cited the command (starting "bitcoin-cli") which he used. He claimed that he then copied the signature across to the virtual machine and used a further command on the Bitcoin Core software to verify it.

852. As Prof Meiklejohn explained, 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. Mr Gao agreed with her on these matters. Dr Wright did 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 of these matters. 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, Dr Wright adopted an over-complex process.

853. Prof Meiklejohn also noted 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. On his account, she was indicating that he took *real* security risks while adopting complex steps to avoid *spurious* risks.

854. 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. This multiple hearsay statement was not even submitted under a CEA notice.

855. In the course of closing submissions, Dr Wright served a CEA notice dated 13 March 2024 relying on a blog post of Mr Matonis dated 2 May 2016 entitled 'How I Met Satoshi'. In that blog post, Mr Matonis related his encounters with Dr Wright, culminating with 'the London proof sessions'. Mr Matonis said 'the proof is conclusive'. Although posted on 2 May 2016, that blog post must have been written in advance, so that it was released as part of the planned 'Big Reveal'.

856. I am inclined to place very little weight on Mr Matonis' blog post, not least because we have no idea whether subsequent events caused him to change his mind or dent his conviction. We do not know Mr Matonis' reaction to the debacle of the Sartre blog. The dinner with Mr Hearn (see below) took place a couple of months later, at which time Mr Matonis seems to have been looking to Mr Hearn for confirmation of his view, something which indicates Mr Matonis was less sure of the position than when writing his blog. Equally, we do not know Mr Matonis' reaction to what Mr Hearn said to him after the dinner. In any event, Mr Matonis has not given evidence. The agreed expert evidence is that his proof session 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.

The Signing Session with Mr Andresen

857. As already mentioned, 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.

858. 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).

859. In **Wright2**, Dr Wright gave his version. He claimed 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 said 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 described that, for each of block 1 and 9, he produced a signed message on his laptop; that he transferred it via USB stick to the new laptop; and that he then performed the verification with the Electrum software on the new laptop while Mr Andresen watched. Dr Wright recalled 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.

860. Mr Andresen recalled that a hot-spot might have been used for internet access, a detail Dr Wright accepted in his *Granath* evidence. Mr Andresen was also clear that Dr Wright downloaded and installed the software on the new laptop, including the Electrum software. 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. 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.

861. 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 **{Day8/68:12}**. He admitted that Mr Andresen may well have been right in his recollection of the message and how the verification initially failed **{Day8/72:16}**.

862. Prof Meiklejohn addressed the possibility of this session being faked. She explained 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). COPA pointed out that Dr Wright's account diverges from Mr Andresen's on the key points of (i) who set up the laptop; (ii) who downloaded Electrum; and (iii) whether there was any verification of the Electrum software.

863. Once again, it is also important to note the point I made at the outset (see [834] above) 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. COPA submitted that the adoption of Dr Wright's complex process (involving the purchase of a new computer) in favour of that simple process spoke volumes. COPA invited the inference that the complex process was adopted because it could be staged.

<u>The Andresen Signing Session Reconsidered</u>

864. COPA also drew attention to 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 (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.*" He arrived at the Firmdale Hotel in Covent Garden at around 11:00 GMT. In his Kleiman deposition, Mr Andresen repeated that at this point he was "*very tired*" as it was a red-eye flight.

865. After landing, Mr Andresen got 1-2 hours of sleep. 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).

866. 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. According to Mr Matthews they spoke for around 1-1.5 hours on a number of topics, including "*eight or ten different aspects of the Bitcoin code*". 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.*"

867. The meeting moved towards the signing session itself, although Mr Andresen describes the session as "*one continuous meeting*" in the hotel room. 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. 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.

868. There was then a discussion that lasted around 15-20 minutes, following which a new laptop was "*procured*" by an assistant, which Mr Matthews has said was purchased from Curry's on Oxford Street. 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.

869. 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*".

870. 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, 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*".

871. 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:

> *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.*

872. In his evidence, 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 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.

873. Finally, it is clear from Mr Andresen's Reddit exchange with 'etmetm' that he wished (with the benefit of hindsight) that he had taken detailed notes of what happened. It seems he did not come prepared to take notes and therefore took none because they would be unnecessary '*because Craig would simply post a signature'* **{L14/354.1/1**}. In that exchange he also said '*We may now never know for certain if I was tricked somehow, and that might be for the best. (feel free to republish)'* **{L14/354.1/2**}. Furthermore, it is notable that Mr Andresen never said he and Dr Wright set up the laptop together, that was something inferred by etmetm in a summary of what happened - Mr Andresen responded saying he had got several details wrong.

J. The public proof session

> *'12. In relation to the public proof sessions, Dr Wright has explained how he was pressured by Mr MacGregor into doing something he did not want to do (i.e. use a private key to prove possession of an early block in the Bitcoin blockchain before his identity had been proved by other means). As he put it, "[t]he only way I would have signed was: first, prove my work" [{Day 8/19/3-16}]. Consistent with that mindset, Dr Wright's evidence is that the Sartre Message was not intended to provide proof of possession. It was instead an act of defiance, which Dr Wright says was intended to convey the message, "I'm not going to do it" [{Day 7/161/5 to 162/1}]. He saw his use of a quote from Jean-Paul Sartre as a profound demonstration of his rejecting and choosing not to engage in a particular action.'*

874. By way of background, I refer to the following section in the Appendix which contain my finding that the following document, relevant to these matters, was forged by Dr Wright, namely: section 39: the Sartre Message.

875. As above, I first set out the essential facts and then deal with the contentious issues.

The facts

876. The various articles arising out of the interviews described above 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*" **{L18/257/1}**. 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. 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).

877. 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 (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"). The Economist immediately published a piece saying that his proof had come under fire and that it had requested a corrected version. 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 {**Wright 1 [219] {E/1/37}**}. Dr Wright also said in {**Wright1 [223-224] {E/1/38}**} that his version of the Sartre post was edited by Mr MacGregor and that the version posted differed from what he had intended. Dr Wright's draft post (attached to an email of 29 April 2016) is available. Although the introduction is different, the technical content appears to be virtually identical.

878. 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. The email traffic shows that Mr Matonis and Mr Andresen reacted with a sense of betrayal. In his evidence in the *Kleiman* litigation, Mr Andresen said: *"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}**.

879. 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*". 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.

880. 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 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 me 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 reviewed for his first witness statement and which he did not think to mention featured false emails from someone impersonating him.

881. 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. 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*". 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. Moreover, contemporaneous emails show that Dr Wright was aware of this plan and at least initially appeared to support it.

882. 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. 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. 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.

883. Under cross-examination, Dr Wright disowned these emails, claiming that his wife's nCrypt email had been taken over just as his had been. However, in my judgment, 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 the 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.

884. 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 {**Wright1 [231] {E/1/39}**}. 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 {**Matthews1 [108] {E/5/23}**}. 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 **{L13/360/1}** and **{L13/361/1}**.

885. 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*". 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.

My findings in relation to the Sartre blog post.

886. 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 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.

887. It is common ground between the parties' experts that the Sartre blog post proved nothing. Prof Meiklejohn explained 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 added: "*This data is thus replayed from those transactions, which… means it provides no cryptographic evidence of the possession of the associated private key*." Mr Gao accepted this point.

888. Dr Wright 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 {**Wright 1 [217-220] {E/2/37}**}. As to the first of those points, his own draft of the blog post (sent on 29 April 2016) was largely the same as the published version, and his own team read it as intended to provide proof by a valid signature. As to the second, it is plain from the email correspondence from the time (summarised above) that it was intended to give such proof. Even Mr Matthews could only attempt to defend Dr Wright by saying that he was committing an act of "*sabotage*" to embarrass Mr MacGregor, which I consider to be a bizarre explanation and which conflicts with Dr Wright's own account {**Matthews1 [104] {E/5/22}**}.

889. 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*" **{L13/262/1},** 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.

890. 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 (which COPA estimated to be now 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 accurately described in his witness statement as a "*simple and comprehensive way for Wright to prove that he was Satoshi*". Mr Andresen made a similar transfer, which was also never returned.

891. 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). In the end, he did not provide any proof and the "big reveal" project fell apart.

892. This is a remarkable series of events. It might be said that Dr Wright had a dramatic loss of nerve when put under pressure to provide proof that he was Satoshi, but it is clear that he later regained his nerve to continue with his long-running project, notably in these proceedings, to establish that he is/was Satoshi. I do not consider it is necessary to make any detailed findings about these events or Dr Wright's state of mind over the period in question. It suffices for me to find that none of the events surrounding the Sartre blog provide any support for his claim to be Satoshi and the contrary is true: those events are entirely consistent with Dr Wright not being Satoshi. It must be remembered that these events took place before Dr Wright claims to have destroyed the hard drives on which he had stored the private keys for the early blocks or, at the very least, for blocks 1 and 9. As the experts agreed, Dr Wright could have proved his possession of one of the private keys to an early block easily and simply. In these circumstances, the natural inference is that Dr Wright was unable to do so because he has never had any of those private keys.

893. In my judgment, the suggestion that he took a principled stand against offering cryptographic proof is just another convenient excuse. It is also 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. Again, the inference is that Dr Wright came up with this excuse after the event.

Dr Wright's excuse for not having the private keys now

894. Dr Wright claims that, sometime 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. As COPA submitted, he has given inconsistent accounts on this, when one would expect him to have retained a clear recollection of such an important event. 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 {**Wright4 [33] {E/4/15}**}. 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 {**Wright4 [34] {E/4/16}**}.

895. 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 {**{O2/11/29}**, internal pages 108-110}. 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. Dr Wright's attempts in his oral evidence in cross-

examination to make these two different accounts reconcile were not impressive **{Day8/79:3} - {Day8/84:25}**.

896. Dr Wright's pleaded stance in this case is that he no longer has access to the keys associated with the early blocks in the Bitcoin blockchain. In *Granath* (in September 2022), he said that he could probably gain such access: "*In theory, I could probably track down Uyen [Nguyen] and get other people and do other thing that might give access, but I have not even tried to see whether I could do that*" {**{O2/11/31}**, internal page 119}. 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 any of his witness statements. The alternative, that he has not tried, or has chosen not to access the keys, is simply implausible in view of the pressure which Mr Ayre applied in his email of September 2023 **{L19/212/6}** and in view of what is at stake for him in this litigation, both personally and professionally. When he was cross-examined about this, he claimed to have discovered in 2019 that he could not access the keys. This conflicted with his evidence in *Granath*, but he then proceeded to deny the conflict **{Day8/85:1} - {Day8/87:8}**. These, in my judgment, were just more convenient (but conflicting) excuses.

The July 2016 Dinner with Mr Mike Hearn

897. As I mentioned above, under cross-examination Mr Hearn was the subject of robust challenge by Lord Grabiner KC on three points relating to this dinner: first, whether he requested to meet Dr Wright in 2016, or whether the initiative came from Jon Matonis; second, whether he was aware that the business for which he worked in 2016, R3, was a competitor of nChain and third, what occurred at the dinner. These challenges were developed in some detail in Dr Wright's closing.

898. My note made on the day Mr Hearn gave evidence was to the effect that Mr Hearn's evidence was clear, in no sense overstated and that he had recalled matters which were important to him and he had less recall about other matters. However, I have reconsidered the position in the light of the submissions made by Counsel for Dr Wright in their closing on these three points.

899. To assess them, it is necessary to say a little more about Mr Hearn's evidence.

900. First, he contacted Satoshi in April 2009 because he had a lot of questions about how Bitcoin would work out in the future. He corresponded with Satoshi between 12 April 2009 and 23 April 2011. He has posted 'almost all' of his emails with Satoshi on his website, so they have been publicly available for some considerable time. He was referred to the brief mentions of him in **Wright1**, but observed that all those events had been documented by him publicly.

901. Second, on searching his email inbox he found he had exchanged emails with Dr Wright in 2014 and 2016. The email exchange in 2014 (which Mr Hearn had forgotten about until the emails popped up from his search) related to funding for support of the core Bitcoin system. Essentially, Dr Wright had asked: 'can I fund you?'. This was not an unusual issue at the time as a common question was: 'how do we support the core system?'. Mr Hearn responded saying he could but heard nothing further.

902. Third, the key points in Mr Hearn's witness statement in relation to the dinner were as follows:

902.1. Jon Matonis wanted Mr Hearn to meet Dr Wright so Mr Hearn could reinforce Mr Matonis' belief that Dr Wright was Satoshi.

902.2. During the dinner Mr Hearn asked Dr Wright about things he had always wanted to know the answer to in relation to Bitcoin that only Satoshi would know, in respect of which Mr Hearn said '*He failed all of my check questions'*.

902.3. One of the specific points which Mr Hearn recalled asking about was what the SIGHASH_SINGLE mode was for in the signing protocol. He said it was easy to work out what it did, but why it was there and what it was intended for was much harder to work out. Mr Hearn said that was one of the answers where Dr Wright struggled and said '*I got the impression he didn't really know'*.

902.4. Mr Hearn also said that some of Dr Wright's answers were in the general area, but garbled. '*I didn't get the sense he knew that he was talking about*.' And

> *'...I got the sense that he was routinely talking about things he didn't deeply understand. I think there were additional technical questions I asked, I can't remember the exact details, but I remember feeling like the answers I got back were only slightly better than Star Trek-style technobabble in some cases. I was like, I don't get the sense at all that this guy designed the thing (Bitcoin) otherwise he'd be able to give a much more clear discussion of them.'*

902.5. As for Stefan Matthews, Mr Hearn found him a bit of an enigma, saying '*he didn't talk very much except to shut up Craig when he started struggling, well my perception was to give him an excuse to stop talking when he was about to dig himself a hole*.'

902.6. After the dinner, Jon Matonis said something to him along the lines of '*I think this guy is Satoshi, I want to know what you think..*'. Mr Hearn responded along the lines of '*I didn't get the impression I was talking to Satoshi, to be honest.*'

903. So the central issue which arises on the discussion at the dinner was whether Dr Wright struggled with some of the details which Mr Hearn would have expected Satoshi to explain, at which point Mr Matthews intervened, or whether Mr Matthews' interventions were to prevent Mr Hearn probing into technical details which were the subject of existing or future patent filings. In support of the latter interpretation, Dr Wright asserted that Mr Hearn had refused to sign an NDA prior to the dinner. Mr Hearn was asked in cross-examination whether he signed or was asked to sign a NDA before the dinner and he responded: '*Not that I can recall'* and '*No, I don't think so'* **{Day14/11:2-6}**.

904. Mr Hearn was asked by Bird & Bird for the purpose of preparing his witness statement how the dinner at Wild Honey, which took place on Saturday 9 July 2016, came about. Mr Hearn said he was speaking at a conference in London and Jon Matonis approached him and said something along the lines of '*Oh it's great you're in town, Craig Wright is too and he'd like to meet you*'. Mr Hearn exhibited the resulting email chain which starts with an email on Friday 1 July from Mr Matonis to Dr Wright and Mr Hearn, in which he said '*Hi Craig, I just met with Mike Hearn in central London. He asked if I could make an introduction. …*'

905. Further emails were exchanged on 1, 4 (in which Dr Wright introduced Stefan Matthews as the person who '*handles everything I don't*') and 6 July, with the dinner being arranged for Saturday 9 July. Mr Hearn was leaving London the next day.

906. Mr Hearn's recollection (both in his witness statement and in the witness box) was to the effect that Jon (Matonis) wanted him to meet Dr Wright and he was like '*fine, whatever*'. This alleged 'inconsistency' was developed into a major point because it suited Dr Wright's case to characterise Mr Hearn as wanting the dinner to take place so he could pump Dr Wright for information which would be of advantage to the company he was then working for, R3 (i.e. on the second and third points of challenge).

907. In **Wright11**, having seen Mr Hearn's witness statement, Dr Wright stated that Mr Hearn's company R3 was a competitor of nChain. In his usual style, Dr Wright devoted a number of paragraphs to putting some technical detail behind this allegation, much of which concerned the use of SIGHASH flags. Dr Wright also cited a particular GB application (which had been filed only weeks before the dinner) and said *'R3 was investigating and filing similar research'* and made reference to an application which he said was filed by Mr Hearn with a priority date of 22nd August 2016, which he said claimed a method which overlapped with an application filed by nChain with a priority date of 29th July 2016. This document was not put to Mr Hearn in cross-examination, although in closing US11,205,162 B2 was produced, in which Mr Hearn was one of the inventors and the applicant was R3 Ltd. That patent concerns a decentralised distributed ledger in which transactions are recorded by parties to the transactions *without* the use of a blockchain.

908. There was insufficient time (and, probably, inclination) at Trial to get into the detail of the alleged competition between R3 and nChain. Mr Hearn didn't think they were competitors but said he didn't really know what nChain's business was. This last point is not a surprise because one would have to conduct a detailed analysis of nChain's patent filings to understand where its business interests lay and the patent filings might cover a wide array of blockchain related subject-matter. It was put to him that one area of competition between the two entities concerned the scalability of blockchain transactions, but his response was that any company which makes software has to be concerned with scalability, which seems to me to be correct.

909. However, Mr Hearn's principal retort to the notion that he was trying to interfere with nChain's patent filings was this:

> *12:17 A. Well, I was asking questions that didn't -- didn't*
> *18 appear to me to involve any IP. I was asking questions*
> *19 about the core Bitcoin System, which of course is not*
> *20 patented. But, yeah, that was the justification*
> *21 I recall him giving for not answering any of my*
> *22 questions, yeah.*
> *18:19 A. Well, from my perspective, it was about Bitcoin. From*
> *20 his perspective, perhaps he felt it was related to*
> *21 patents they were filing, but I could not have known*
> *22 that at the time, so I think this is just a difference*
> *23 of opinion.*
> *19: 5 A. Well, Craig seemed to be stuttering, or struggling to*
> *6 answer and then he looked at Stefan, and Stefan was sort*

7 of like, "No, don't answer", and then I believe they --
8 they said this thing about the patents. "Patents",
9 sorry.
23: 1 A. …….I was
2 confused by his refusal to respond, because I didn't
3 believe you could really file patents on -- sorry,
4 "patents" on, you know, things that have been published
5 already, like Bitcoin had many years previously, and
6 certainly Satoshi had never expressed any interest in
7 patents to me previously, when I've communicated with
8 him, so it didn't really occur to me that I might get an
9 answer like that at all, to be honest.

910. The dinner occurred just under 8 years prior to the evidence at Trial, but some 7 years after the Bitcoin system had been launched. Mr Hearn's recollection was consistent with the passage of time since the dinner: he said parts of the dinner are a bit hazy, but the important parts that he remembered were the conversations about Satoshi and Bitcoin **{Day14/10}** and, I infer, the impressions he formed about Dr Wright. By contrast, some of the matters which Dr Wright said were discussed at the dinner in **Wright11** were unusually specific.

Analysis

911. There are some curiosities about the evidence concerning this dinner:

911.1. First, I have evidence from Mr Hearn, Mr Matthews and Dr Wright, but none from Mr Matonis on which I consider I can rely (who seems to have still believed that Dr Wright was Satoshi, at least prior to the dinner) or Ms Watts.

911.2. Second, even though this dinner took place just over 2 months after the Sartre blog, and the public comment in relation to that, there was no recognition of that in any of the evidence relating to the dinner.

911.3. Third, much was made at trial that the company for whom Mr Hearn was working at the time, R3, was a competitor of nChain. If that was the case, it is very curious that Dr Wright was happy not just to have a long dinner with Mr Hearn but to be prepared to answer a whole series of technical questions related to Bitcoin.

911.4. Fourth, the dinner occurred in circumstances where the issue as to whether Dr Wright's claim to be Satoshi was still very much live. By agreeing to dine and have a discussion with one of the developers, Dr Wright must have known that he would be questioned on technical details.

912. In addition, I was struck by the fact that the whole section in **Wright11** on this dinner at **[435]-[462]** was in Section VI where he gave his response to COPA's witnesses (other than Mr Malmi and Mr Gerlach). Thus, there were passages on Dr Back (and Wei Dai) [369]-[393], Steve Lee [394]-[404], Dustin Trammell [405]-[409], Zooko Wilcox-O'Hearn [410]-[430], Professor Wrightson and Dr Furche [431]-[434] and a section on Professor Stroustrup and Mr Hinnant [463]-[471]. For reasons explained elsewhere, I have found much of this evidence from Dr Wright to be pure fantasy on his part (so too, the earlier passages regarding Mr Malmi and Mr Gerlach), so the suspiciously specific

details set out in **Wright11** in relation to the technical discussion at the dinner could lie in a similar vein. Indeed, Mr Hearn's view that Dr Wright engaged in technobabble coincides with the impression I formed of a number of passages in Dr Wright's answers at trial, when he was under pressure.

913. I do not believe that I have sufficient detail to be able to reach firm findings as to precisely what occurred at this dinner. If I was to view the disputes in relation to this dinner in isolation (which was the implicit invitation in Dr Wright's submissions), I might well have concluded that there was some substance in the suspicions on both sides.

914. However, I am clear that it would be wrong to view this dinner in isolation. Dr Wright's submissions effectively invite me to find that Mr Hearn had some sort of axe to grind against Dr Wright and attended the dinner for that purpose. In his evidence, Dr Wright made a variety of allegations against the Developers, all of which I have found to be baseless.

915. In these circumstances and in the circumstances of this case more generally, on balance, I make the following findings as regards the dinner:

    915.1. It is likely that Mr Matonis was the driver of getting Mr Hearn and Dr Wright together at the dinner because Mr Matonis wanted Mr Hearn to confirm his own view that Dr Wright was Satoshi. Mr Hearn's evidence on that point rang true: in effect he was saying he did not have a burning desire to have a discussion with Dr Wright, but he said he would otherwise have had to eat on his own that evening if he didn't go to the dinner.

    915.2. Mr Hearn undoubtedly came away from the dinner believing that Dr Wright was not Satoshi and said so to Mr Matonis.

    915.3. The discussion at the dinner was between Mr Hearn, who had been involved as a developer of the Bitcoin code until the end of 2015, and Dr Wright who had gone public that he was Satoshi. I consider it is likely that Dr Wright did struggle with some of the technical details which Mr Hearn asked about. I also consider it is likely that Mr Matthews was primed to step in to shut down technical discussions if Dr Wright was struggling, with the excuse that it might endanger the nChain patent filings.

    915.4. Mr Hearn confirmed that Mr Matthews did deploy this excuse at the dinner, but he was clearly sceptical about it – he made the point that he was asking Dr Wright about Satoshi's original intentions for Bitcoin – in other words, the content of the Bitcoin White Paper, the original or very early versions of the Bitcoin Source Code, all of which was 7 years in the past by the time of the dinner. Mr Hearn made the obvious point that nothing in the public domain could be patented but he was asking Dr Wright about details which were not in the public domain. Taking the view which is most favourable to Dr Wright, it is therefore conceivable that there may have been some overlap and therefore conflict between what would have been full answers to Mr Hearn's questions and the areas which Dr Wright was seeking to develop in nChain patent filings.

    915.5. Let me assume that this conflict was perceived to exist on Dr Wright's side. I return to my initial assessment of Mr Hearn's evidence. I must balance that

against the evidence of Dr Wright and Mr Matthews. I have found Dr Wright to be a thoroughly unreliable witness who has engaged in forgery on a grand scale and, in his attempts to sustain his case, has lied extensively. I have found Mr Matthews to have been more careful in his evidence, but still to have lied in his bid to support Dr Wright's case. These are not circumstances in which I am inclined to reject Mr Hearn's evidence.

915.6. In conclusion, on all three points of challenge, I find that Mr Hearn's evidence was clear and in no sense overstated. He recalled matters which were important to him and had less recall about other matters. The implication underpinning these challenges was that Mr Hearn had some axe to grind against Dr Wright. I am entirely satisfied he did not and that he gave his evidence honestly and entirely fairly.

The other litigation involving Dr Wright as Satoshi

916. As part of the uncontroversial chronology, I mentioned how Dr Wright's claim to be Satoshi gave rise to the *Kleiman, Granath* and *McCormack* actions, and then this COPA claim, the two passing off actions and the BTC Core Claim. It is not necessary to discuss the *Kleiman, Granath* and *McCormack* actions any further.

917. There is one other claim which has been brought to my attention: the COBRA claim (IL-2021-000008) in which Dr Wright sued unnamed defendants as 'The person or persons responsible for the operation and publication of the website www.bitcoin.org (including the person or persons using the pseudonym 'C∅BRA''. The claim was for infringement of copyright in the Bitcoin White Paper. Dr Wright secured Judgment in default of acknowledgement of service and defence by the Order of HHJ Hodge QC dated 28 June 2021, which includes an injunction preventing the defendants from infringing copyright in the Bitcoin White Paper, whether by making the Paper available for download or in any other way. To the extent necessary, the status of that Order can be considered at the Form of Order hearing following hand down of this Judgment.

OVERALL CONCLUSIONS

918. Dr Wright's case that he is Satoshi clearly centred on the numerous documents he disclosed which purported to evidence precursor work to the Bitcoin White Paper and source code, along with his own testimony. This is why the status of those documents was so important in this Trial.

919. It is important to recognise the scale and scope of the documents in question. There are three aspects to this. First, the scope and importance of the documents is indicated by those dealt with in the Appendix, particularly those purporting to be precursor work or drafts of the Bitcoin White Paper.

920. The second aspect is the number of documents:

920.1. The reason why **Madden1** is so long and detailed is because he was asked to analyse a very considerable number of documents from Dr Wright's original disclosure. At the hearing in October 2023 when I had to rule on COPA's application to introduce allegations of forgery in addition to the 6 pleaded in the Particulars of Claim, Dr Wright's legal team estimated there was material in

Madden1 to support allegations that up to 400 documents had been forged. COPA filed a schedule which indicated they wanted to pursue 180. COPA were permitted, by my Order, to plead an additional 50 and did so.

920.2. After that, the Additional Documents were introduced into the case at the PTR in December 2023 comprising (a) the 97 documents from the BDO Drive and (b) the LaTeX files. This necessitated the existing 56 allegations of forgery being cut back to 26, with COPA selecting an additional 20 from the Additional Documents.

920.3. During Trial, one further allegation of forgery (the MYOB Ontier Email) was added.

921. I have dealt with numerous points of detail in relation to those 47 forgery allegations, both in the body of this Judgment and in the Appendix. I have found all of them proved.

922. However, for the case management reasons I explained above, there remained:

922.1. A number of documents which COPA pleaded as forgeries in October 2023 (including some of Dr Wright's Reliance Documents), but those allegations were not focussed on at Trial. Notwithstanding that, most if not all of these documents were necessarily the subject of cross-examination of Dr Wright because they were an essential part of the story.

922.2. A larger number of documents which were analysed in **Madden1** and which Mr Madden found to be inauthentic. These documents could not be accommodated within the limits I set for COPA's pleading of forgeries.

923. Due to the confidence I have in Mr Madden's evidence and analysis, I accept all of his findings of inauthenticity. In this regard, I note that many of the explanations (persistence, XCOPY, virtual machines etc) which Dr Wright put forward in response to the allegations of forgery were attempts to explain certain anomalous data identified by Mr Madden in **Madden1** when finding documents to be inauthentic. Dr Wright's explanations did not begin to meet the clear indicia of forgery and it is reasonable to infer that they do not explain Mr Madden's findings of inauthenticity, not least because (acting in accordance with his duty to provide independent objective expert evidence) he specifically considered whether there could be alternative explanations and concluded not.

924. The third aspect is the startling period of time over which Dr Wright forged documents:

924.1. As I 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 found a number of Tulip Trust and Tulip Trading Ltd documents to bear signs of having been forged in 2014/15{See Appendix PM14 **{H/73/1}**}.

924.2. COPA's October Schedule of Forgeries included some of those documents, namely: (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}**. None of those documents made the cut i.e. they were not among the 20 forgeries of original documents which COPA pursued at trial.

924.3. It is clear there is full documentary evidence showing that Dr Wright purchased Tulip Trading Ltd as an "*aged shelf company*" in October 2014 from Abacus Seychelles {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 Dr Wright's hands since 2011.

924.4. 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.

924.5. Through the documents 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 **{H/219/2}**.

924.6. The evidence showed that Dr Wright continued producing forged documents in advance of his original disclosure in this action and then throughout the remainder of this case, 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.

924.7. He then produced the forged MYOB Ontier Email in the middle of trial.

925. I have reflected on the classes into which these documents fall – 'forged' and 'inauthentic'. Although there is an important difference between those classes in terms of identifying allegations being made in a pleading, in the unusual circumstances of this case and after all the evidence has been heard, the distinction between the two classes seems to me to be artificial, particularly when all the evidence points inexorably to the fact that all the documents which Mr Madden found to be 'inauthentic' were forged by Dr Wright.

926. Overall, in my judgment, (and whether that distinction is maintained or not), Dr Wright's attempts to prove he was/is Satoshi Nakamoto represent a most serious abuse of this Court's process. The same point applies to other jurisdictions as well: Norway in particular. Although whether Dr Wright was Satoshi was not actually in issue in *Kleiman*, that litigation would not have occurred but for his claim to be Satoshi. In all three jurisdictions, it is clear that Dr Wright engaged in the deliberate production of false documents to support false claims and use the Courts as a vehicle for fraud. Despite acknowledging in this Trial that a few documents were inauthentic (generally blamed on

others), he steadfastly refused to acknowledge any of the forged documents. Instead, he lied repeatedly and extensively in his attempts to deflect the allegations of forgery.

927. Notwithstanding all that, as I was reminded (see [343] above) and had well in mind throughout, the issue for decision at this Trial is the Identity Issue.

928. Having (a) reached conclusions on COPA's allegations of forgery, (b) accepted the remaining allegations of inauthenticity which, as far as I am aware, cover Dr Wright's Reliance Documents, (c) not had my attention drawn to any other documents which appear to support Dr Wright's claim and which can be considered reliable, (d) considered the largely circumstantial evidence from the witnesses of fact called to support Dr Wright's case, (e) considered the evidence given in Dr Wright's own witness statements and (f) considered all the evidence adduced by COPA and the Developers, the case that Dr Wright is not Satoshi Nakamoto is overwhelming.

929. Although, at the conclusion of closing submissions at the Trial, I did not and could not have all the detail set out in this Judgment and Appendix in my head, I had been taken through it either in pre-reading or during the Trial. I tried to identify whether there was *any* reliable evidence to support Dr Wright's claim and concluded there was *none*. That was why I concluded the evidence was overwhelming. The preparation of this Judgment and Appendix has only confirmed that conclusion.

DECLARATORY RELIEF

930. As I said at the conclusion of closing submissions at the Trial, I was satisfied that it was in the interests of justice to make the four declarations I made orally on that occasion. Those declarations are repeated in [7] above.

931. I should explain my reasons for doing so in more detail, in view of the submissions which Lord Grabiner KC made on this topic on Day22.

932. On the basis that all the declarations sought by COPA were negative in nature, he referred me to the summary of the principles relevant to the grant of negative declaratory relief summarised by Cockerill J. in *BNP Paribas SA v Trattamento Rifiuti Metropolitani SpA* [2020] EWHC 2436 (Comm) at [78] which I set out, omitting citations:

> *'i) The touchstone is utility;*
> *ii) The deployment of negative declarations should be scrutinised and their use rejected where it would serve no useful purpose;*
> *iii) The prime purpose is to do justice in the particular case;*
> *iv) The Court must consider whether the grant of declaratory relief is the most effective way of resolving the issues raised. In answering that question, the Court should consider what other options are available to resolve the issue;*
> *v) This emphasis on doing justice in the particular case is reflected in the limitations which are generally applied. Thus:*
> *a) The court will not entertain purely hypothetical questions. It will not pronounce upon legal situations which may arise, but generally upon those which have arisen.*
> *b) There must in general, be a real and present dispute between the parties before the court as to the existence or extent of a legal right between them.*

c) If the issue in dispute is not based on concrete facts the issue can still be treated as hypothetical. This can be characterised as "the missing element which makes a case hypothetical."
vi) Factors such as absence of positive evidence of utility and absence of concrete facts to ground the declarations may not be determinative; Zamir and Woolf note that the latter "can take different forms and can be lacking to differing degrees". However, where there is such a lack in whole or in part the court will wish to be particularly alert to the dangers of producing something which is not only not utile, but may create confusion.'

933. Lord Grabiner KC stressed the points made at [78(v)] i.e. that the Court will grant declarations only to resolve real disputes relevant to the existence or extent of a legal right **between** the parties. He also relied on the passages cited below from the Judgment of O'Farrell J in *Office Depot International (UK) Ltd v UBS Asset Management (UK) Ltd* [2018] EWHC 1494 (TCC), [47], citing Lord Diplock in *Gouriet v Union of Post Office Workers* [1978] AC 435:

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

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

934. Based on these authorities, Lord Grabiner KC addressed the three declarations sought by COPA in their Particulars of Claim:

934.1. First, the declaration that Dr Wright is not the author of the Bitcoin White Paper. He characterised this as answer to a purely academic question which did not engage any legal right or interest of COPA 'not least because COPA does not claim to have authored the Bitcoin White Paper'.

934.2. Second, the declaration that Dr Wright is not the owner of copyright in the Bitcoin White Paper. Lord Grabiner KC submitted this declaration would have no practical utility going beyond the consequences of a Judgment determining the Identity Issue against Dr Wright and would be wholly unnecessary.

934.3. Third, a declaration that any use by COPA of the Bitcoin White Paper will not infringe any copyright owned by Dr Wright, which Lord Grabiner KC submitted would be entirely redundant.

934.4. In his oral submissions, Lord Grabiner KC also addressed the declaration which would arise out of my formulation of the Identity Issue, namely that Dr Wright is or is not Satoshi Nakamoto. I understood him to submit that I could make a declaration in his favour: that Dr Wright is Satoshi Nakamoto, but that it was not seriously arguable that I could make a declaration to the opposite effect: that Dr Wright is not Satoshi Nakamoto.

935. In considering these submissions, the first point to note is that this case has changed somewhat since it was first pleaded. In particular, this Trial of the Identity Issue has been the trial of a preliminary issue in the BTC Core Claim where the Developers and various members of COPA are sued by Dr Wright and two of his companies for infringement of copyright in the Bitcoin White Paper – the key point being that a copy of the Bitcoin White Paper is in the Bitcoin Blockchain, which, as I understand matters, is reproduced by every node. Furthermore, it is appropriate to keep in mind that in the BTC Core claim, Dr Wright is claiming database right in various manifestations of the Bitcoin Blockchain and, furthermore, the Kraken and Coinbase Defendants (to the passing off claims made against them in those actions) have agreed to be bound by the outcome of this Trial, those actions being stayed in the meantime. In mentioning these matters I am not changing the issue which is the subject of this Trial. The debate here is over what declarations would have utility in the circumstances which now present themselves. In this regard, Mr Hough KC for COPA also reminded me of the various claims for defamation which Dr Wright has brought against various people who have said or implied he is not Satoshi.

936. Second, it is clear, in my judgment, that in these circumstances COPA does not need a competing claim to be the author of the Bitcoin White Paper for a declaration that Dr Wright is not the author of it to have utility or to remove it from the realm of academic questions.

937. Third, in view of the extremely unpleasant threats which Dr Wright has made in the past against some of the individual Developers in particular, I was minded to make declarations to ensure that Dr Wright would not have any possible basis on which to threaten them with copyrights or database rights stemming from the work done by Satoshi Nakamoto.

938. Fourth, I found Lord Grabiner KC's submission to the effect that I should not grant any declaration to the effect that Dr Wright is not Satoshi Nakamoto (in the event that I so concluded) somewhat surprising, bearing in mind the huge effort and costs which have been expended on all three sides debating that very issue.

939. It was for those brief reasons that I very firmly concluded that the declarations I stated in open court on Day 22 (14 March 2024) had utility and were necessary to do justice between the parties.

FURTHER RELIEF

940. Beyond the declarations I have already made, there was and remains a significant dispute over what further relief I should grant, particularly as to the injunctive relief sought by COPA and the Developers. Initially, it appeared to be common ground that disputes over relief were best left to be addressed at a form of order hearing following the hand down of this Judgment. However, in Lord Grabiner KC's oral closing on Day 22, he urged me to decide all questions of relief in this Judgment and made submissions accordingly. Mr

Hough KC addressed the issues raised over declaratory relief but urged me to defer my decision on injunctive relief until after (a) this Judgment had been handed down and (b) further argument in the light of it.

941. I have concluded that I should defer the issues of injunctive relief. They will be argued at a Form of Order hearing to be appointed after the hand down of this Judgment.

942. What remains is for me to thank all Counsel, Solicitors and their teams for the immense amount of work which has gone into this case, and I commend all for their high standards of professionalism in this hard-fought litigation. I also pay tribute to the organisation and presentation of the documents on the Opus2 platform. There was a vast volume of documentation on that platform for this Trial. Many of the documents were long but the relevant part was frequently only one or two lines. If we had worked from hard copy bundles, I am sure this Trial would have taken weeks longer.

943. I should add that the respective teams conducted their respective cases with great efficiency. On Dr Wright's side, his team led by Lord Grabiner KC and Mr Craig Orr KC undertook Dr Wright's challenging case. As I mention on the title page, Mr Terence Bergin KC and Jack Castle represented the Claimants in the BTC Core claim, served short Skeleton Arguments and made brief oral submissions. Lord Grabiner KC and Craig Orr KC shared the cross-examination of COPA's witnesses.

944. As appears from my summary of the expert evidence above, COPA undertook all the heavy lifting on the expert evidence from their side and almost all of it on the evidence of fact, with the Developers serving no expert evidence of their own and evidence of fact from Dr Wuille alone. There was no overlap in the cross-examinations of Dr Wright conducted by Mr Hough KC for COPA and Mr Gunning KC for the Developers, even though COPA bore the burden of proving their allegations of forgery as set out in the Appendix. As I mentioned above, the challenges to Dr Wright posed by Dr Wuille's evidence were used to significant effect in support of the Developers' case that Dr Wright was not Satoshi, and they also provided significant support to COPA's case, both generally and on certain of the allegations of forgery. Finally, I should also add that Mr Hough KC and Mr Gunning KC were model leaders, giving their respective juniors, Mr Jonathan Moss and Ms Beth Collett, the opportunity to undertake some cross-examination in this major trial.

945. At the very start of the Trial, I mentioned that remote links to the proceedings had been provided (on individual request) to over 400 people from all over the world. By the conclusion of the Trial, that number had risen to over 1100, reflecting the wide interest in this Trial. All the recipients of those remote links owe a debt of gratitude to my clerk, Susan Woolley, and other court staff, for organising and providing those links, although I know that many thanked her personally by email and in generous terms. The vast majority of recipients abided by the conditions I imposed on each recipient of a remote link. In the very few cases where those conditions were breached, the breach was either swiftly remedied and an apology provided, or access was removed.