IN THE HIGH COURT OF JUSTICE **CLAIM NO. IL-2022-000069**

BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES

INTELLECTUAL PROPERTY LIST (CHD)

BEFORE: Mellor J

BETWEEN

DR CRAIG STEVEN WRIGHT & Ors

Claimants

—and—

BTC CORE & Ors

Defendants

CLOSING SUBMISSIONS OF THE DEVELOPERS

A. INTRODUCTION 4

B. THE BITCOIN SOFTWARE 5

1. COMPUTER SCIENCE 6
2. C++ PROGRAMMING 7
3. THE BASIC MECHANICS OF THE BITCOIN SOFTWARE 10
   - *a. Unsigned integers 10*
   - *b. CheckBlock 12*
   - *c. Leading zeroes 15*
   - *d. Summary of Dr Wright's awareness of the mechanics of the Bitcoin software 17*
4. IMPLEMENTATION OF THE BITCOIN SOFTWARE 18
   - *a. The 69 computers 18*
     - i. Problem 1: inconsistency with the known difficulty 19
     - ii. Problem 2: inconsistency with known electricity consumption 21
   - *b. opcodes 22*
     - i. Script size 23
     - ii. OP_2MUL 24
   - *c. The anachronisms 25*
     - i. CheckBlockHeader 26
     - ii. BTC Core 29
     - iii. UTXO 30
     - iv. Bootstrapping 33
     - v. Summary 35
   - *d. Satoshi's Bitcoin payments 36*

e. The PGP key *39*
i. The date of creation of the key: not 2011 40
ii. The nature of the key: not "*person or persons unknown*" 42
f. Wikileaks: Dr Wright's first brush with Bitcoin *43*
5. SUMMARY 46
C. THE BITCOIN WHITE PAPER 46
1. DR WRIGHT'S WEI DAI LIES 46
2. THE HISTORY OF (NON)-PRODUCTION OF DR WRIGHT'S LATEX FILES 53
a. The before phase *53*
b. The tease and reveal *54*
i. The tease 54
ii. The reveal 56
c. The (partly failed) cover up *58*
i. Dr Wright's Overleaf account 59
ii. The efforts made to resist providing metadata 61
iii Summary 66
3. THE INESCAPABLE EVIDENCE OF FORGERY 71
a. The animations *71*
b. Metadata command *74*
c. Text formatting *79*
d. The images *84*
i. Image 4 84
ii. Dr Wright's written evidence about the images 87
iii. Aspose 90
(a) The Aspose blob 90
(b) The identical co-ordinates 92
(c) The identical letter placement 94
(d) Conclusions 96
e. Impossibility *97*
i. fontspec 98
ii. hidelinks 99
iii. unicode-math 99
iv. \AddToShipoutPictureBG* 100
v. The arrows.meta library 101
vi. luacode 101
f. Summary *102*
4. THE TRUTH 102
D. RELIANCE DOCUMENTS AND FORGERY 104
1. THE RELIANCE DOCUMENTS 105
a. Reliance documents generally *105*
b. Dr Wright's jettisoning of the Reliance Documents *108*
i. Farewell Dr Placks and Mr Lynch 108
ii. Dr Wright's explanations 109
(a) xcopy 110
(b) Citrix 113
(c) Summary 118
iii. The state of things 119
2. THE DOCUMENTS PERTINENT TO THE TULIP TRADING CLAIM 122

a. The MYOB documents......123
i. Relevance to the Tulip Trading claim......123
ii. The .myox file in the Shadders email......123
iii. Dr Wright's Tulip evidence......124
iv. The Placks report – the new MYOB data......125
v. Madden2 – how the new MYOB data had been falsified......126
vi. The experts' joint statement......128
vii. Wright11......128
viii. Initial answers in cross-examination......129
ix. The first Ontier intervention......131
x. The email chain forgery......132
xi. Madden5......133
xii. Dr Wright's second cross-examination......133
xiii. The second Ontier intervention......134
xiv. The cross-examination of Mr Madden......135
xv. Further evidence......136
xvi. Dr Wright's last stand......137
xvii. Conclusions......139
b. The Tulip Trading incorporation documents......139
i. The incorporation form: ID_001930......140
ii. The Abacus invoice: ID_001421......141
3. THE UPDATED SCHEDULE......146

E. RELIEF......148

1. THE BTC CORE CLAIM......149
2. COPA'S CLAIMS......151
a. Dr Wright's threats......152
b. The relief sought......155
i. Declaratory relief......155
ii. Injunctive relief......156
iii. Summary......157

APPENDIX 1 – PROOF OF WORK AND LEADING ZEROES......159

A. WORKING OUT THE TARGET DIFFICULTY......159
B. CHECKING THE TARGET NUMBER......162
1. Ensuring that the minimum work requirement is met......162
2. Ensuring that the hash of the block is less than or equal to the target.......163

APPENDIX 2 – SCHEDULE OF FORGERIES......164

APPENDIX 3 – DR WRIGHT'S PRODUCTION OF DOCUMENTS......172

A. Introduction

1. Satoshi Nakamoto was the pseudonymous author of the Bitcoin White Paper and the original Bitcoin Code.

2. Dr Craig Wright is not Satoshi Nakamoto.

3. He has not come close to establishing that he is even a credible candidate for that role.

4. Instead, it has become overwhelmingly clear over the course of this trial that Dr Wright's claim to be Satoshi and his claims derivative upon that identity are fraudulent claims. The Court has directly experienced dishonesty from Dr Wright and forgery on a monumental level.

5. The consequences of Dr Wright's fraudulent attempt to portray himself as the pseudonymous inventor of Bitcoin have been profound and deleterious. The evidence in this respect has not even been challenged in cross-examination.

6. Two consequences must follow:
   a) First, the BTC Core Claim must be dismissed. It is common ground that the claim is predicated upon Dr Wright being Satoshi Nakamoto. Since he is not, the claim must fail.
   b) Second, the Court should grant COPA the relief that it seeks. This is a matter of direct interest to the Developers, who have been on the receiving end of Dr Wright's threats and lawfare.

7. In this written closing, the Developers adopt a slightly different approach to that taken in their opening. The focus of this closing is directly on the two points that must decisively resolve the case against Dr Wright, namely that he patently did not write the Bitcoin code (see Section B below) or Bitcoin White Paper (see Section C below).

8. The Developers do not in these submissions need to repeat their observations regarding his extravagant claims to the ATO from 2013 or in the Kleiman proceedings

which are set out at length in their opening skeleton. Those points have only been underscored during the course of the evidence – and can be taken as read. The Developers do, however, at section D below provide an updated overview of the forgeries (focussing on two matters of specific concern to the Developers) and finally (at section E) include some observations about the relief sought by COPA.

B. The Bitcoin software

9. It is central to Dr Wright's claim to be Satoshi Nakamoto that he wrote the Bitcoin code. Given that Dr Wright has not disclosed any reliable source documents evidencing his development of the code, that is a question that falls to be tested by reference to his written and oral testimony.

10. That evidence has fallen risibly short of the standard that would be expected of Satoshi Nakamoto. It is considered below in four parts by reference to his evidence regarding:
    a) his experience in computer science;
    b) his familiarity with C++;
    c) his understanding of the basic mechanics of the Bitcoin software; and
    d) his understanding of the running of Bitcoin.

11. Before turning to address those matters, the Developers would note that at the interlocutory stages of these proceedings, Dr Wright sought to diminish the role of the Developers in the defence of the proceedings against them to a mere watching brief.[1] That may have been driven by a determination to reduce Dr Wright's exposure to providing security for costs,[2] but the Developers cannot help feel that it was also designed to prevent his having to engage with questions as to the technical aspects of Bitcoin.

[1] See the BTC Core Claimants' submissions at the hearing on 17 October 2023 at p34 ll.3-4 ("*whoever is going to be attending is going to be on a watching brief*") {O/10.1/10} and the skeleton argument for the BTC Core Claimants ahead of the PTR at ¶15 {R/2.1/5}: "*Macfarlanes utterly fails to explain why this claim is not appropriate for a watching brief or minimal attendance*" and ¶30 "*Junior Counsel will be attending on a watching brief in any event*" {R/2.1/8}.

[2] A matter to which, seemingly, a substantial part of the cross-examination of Mr Lee (a COPA witness) was devoted: see {Day12/pp114-116}.

1. Computer science

12. In Dr Wright's opening submissions, he leant heavily into his "*educational background, his skills, his qualifications*"[3] as indicative that he might be Satoshi Nakamoto. He referred in particular in this context to his skills and knowledge of computer science.[4]

13. In his evidence and during his cross-examination, however, Dr Wright displayed an alarming ignorance of even a basic computer science concept, namely a binary search tree. In describing his supposed work at Lasseters and Vodafone he described using a "*Binary search tree structure (commonly termed a Merkle tree now)*".[5]

14. As explained during his cross-examination on Day 15,[6] a Merkle tree is <u>not</u> a form of binary search tree.

    a) A binary search tree is laid out according to an ordering rule that enables locating elements in the tree quickly: parent nodes contain data that sorts after all data elements in the left subtree, and before all data elements in the right subtree.[7]

    b) A Merkle tree associates a hash with each node, which is defined as the result of hashing the left and right child's own hashes together, recursively. This permits efficiently proving to someone who does not have the tree that a particular leaf is contained within the tree, without transferring the entire tree.[8]

    These are wildly different properties that serve very distinct purposes. The Merkle trees used in Bitcoin are not search trees.

[3] {Day1/p94/ll.5-7}.

[4] Wright opening¶5(1) {R/14/5} and ¶143 {R/14/44}. He also, of course, relied on his supposed expertise in law – even though his LLM thesis had been plagiarised from the work of Hilary Pearson: see Pearson1 {C/3} and Wright xx {Day6/pp23-35}. The plagiarism was observed in an article on medium by Paintedfrog. Dr Wright suggested that was one of the Developer defendants, namely Gregory Maxwell. Gregory Maxwell is not Paintedfrog.

[5] Wright11¶845.c {CSW/1/152} and Wright11¶859.a {CSW/1/155}. See too Wright9¶26 {E/26/10}.

[6] {Day15/pp180-187}.

[7] See *e.g.* {X/60/1}.

[8] See {Day15/pp182-185}.

15. This was not the limit of Dr Wright's apparent ignorance of relevant computer science concepts. He also failed to demonstrate the relevant capability in C++ and, more significantly still, failed to understand the operation of the Bitcoin code. Those are matters to which these submissions now turn.

16. It is possible that Dr Wright will seek to divert attention from the patent shortcomings in his computer science skills by drawing attention to his PhD from Charles Sturt University. His PhD thesis (entitled "*The Quantification of Information Systems Risk*"), however, dates from 2016, long after the release of the Bitcoin White Paper or the Bitcoin code. It is also an odd document, comprising a combination of papers apparently presented by Dr Wright at conference proceedings.[9] It does not demonstrate him to have been capable of writing the Bitcoin code.

2. C++ programming

17. The Bitcoin software is written in C++. Professor Stroustrup, the designer and original implementer of that language, described how he began to work on C++ in April 1979, with only a handful of users in 1980, and first named it C++ in December 1983.[10]

18. In his written witness evidence, Dr Wright made the absurd claim that he had "*dabbled*" with C++ around the age of eight or nine (i.e. in 1978 or 1979)[11] and started writing code for games in the language at the age of 11 (i.e. in 1981).[12]

19. Dr Wright went on to describe C++ as "*a cornerstone of my expertise*".[13] There is, however, little support for Dr Wright's supposed "*expertise*" in C++ in documents that can credibly be dated to 2008-2009. The section of his BDO CV referring to "computing skills" refers to his supposed experience of "*C programming and Code Audit*", not to C++.[14] Moreover, it appears that when Dr Wright applied to Microsoft

[9] {L14/17}.

[10] Stroustrup1¶3 {C/23/1}.

[11] Dr Wright's date of birth is 23 October 1970: {H/241/5}.

[12] Wright1¶25 {E/1/7}.

[13] Wright1¶25 {E/1/7}.

[14] {L2/102/6}. It only includes an inconsequential reference to C/C++ under the heading Unix application development at {L2/102/7}.

for a job in January 2008, he stated "*I use R and C* ***and occasionally C++*** *a fair bit for algorithmic coding and statistics work*" (emphasis added).[15] Satoshi Nakamoto could not have been an "*occasional*" user of C++ in January 2008.

20. More telling still was Dr Wright's evidently untruthful attempt to present C++ code fragments as part of the content of the BDO Image. That code contained anachronistic references to:

a) the <chrono>, <thread> and <random> headers from the C++ standard library: see Stroustrup1¶4 {C/23/2} (unchallenged) and Hinnant1¶9 {C/18/3};

b) the sleep_for function from the <chrono> header and std::chrono:milliseconds: see Hinnant1¶4 {C/18/1}.

21. Dr Wright sought to escape the consequences of his obviously botched forgery at Wright11¶465-471 {CSW/1/87}. That evidence was explored with Dr Wright at {Day5/pp113-119}, but more memorable was the attempt to suggest to Mr Hinnant that Dr Wright's evidence might possibly be true. That led to the following memorable exchanges with Mr Hinnant on Day14:

a) In cross-examination:

> "*34: 4 Q. And so in summary, it is right, isn't it, that from*
> *5 a technical perspective, there was nothing to prevent*
> *6 a C++ programmer doing what Dr Wright says he did?*
> *7 A. It is possible. It is -- does result in undefined*
> *8 behaviour, and it is highly, highly unlikely.*
> *9 Q. You say it's highly unlikely because it's something that*
> *10 you regard as unconventional?*
> *11 A. I say it's highly unlikely because telling me that you*
> *12 started with Project Chrono and ended up with*
> *13 std::chrono is -- is absurd from a technical*
> *14 perspective. It's like saying I started with a P51*
> *15 Mustang fighter plane to create a Ford Mustang car.*"

b) In re-examination:

> "4*3:10 Q. You then said that it was highly unlikely that somebody*
> *11 would start with Project Chrono and end with*

[15] {L3/252.1.1.1.1/2}. He also said that he had "*a large amount of experiance decompiling C, C++, Java, script of various types, fortran, .Net, perl, Ruby and other*s". Decompiling is not coding! It involves running a decompilation tool to (a) take the binary resulting from the compilation of source code and (b) convert that binary back into valid source code. It is a process undertaken in malware research/analysis, because you can look at the decompiled code and see what the malware is trying to do.

> *std::chrono. Do you recall saying that?*
> *A. Yes.*
> *Q. You agreed that that was your opinion; do you recall that?*
> *A. Yes.*
> *Q. What facts or considerations is that opinion based on?*
> *A. That opinion is based on the knowledge that Project Chrono has no similarity whatsoever to std::chrono besides the name "chrono". It's -- it's a statement that is technically so outrageous that it's -- it's literally unbelievable. I cannot believe it. The -- the mere fact that somebody says that they derived a date time library from a physics library indicates to me that they don't have the technical expertise to even write chrono from scratch, because it would actually take more work to write chrono from scratch than to derive it from a completely unrelated piece of software* [sic].[16] *Chrono did in fact derive from other libraries. It derived from the Boost.DateTime authored by Jeff Garland. And Jeff Garland and I worked on chrono together in the 2007/2008 time frame -- well, in the 2008 time frame, I'm sorry. In 2007, we were working together, but it wasn't called chrono at that point, it was called Boost.DateTime."*

22. The Developers adopt Mr Hinnant's observations, which accord with their own view of the code fragments and would simply add two further observations:

a) First, on a number of occasions it was posited in cross-examination of COPA's witnesses and experts that it was possible from a technical perspective that Dr Wright might have done something. But in none of these theoretical cases has Dr Wright provided any documentary evidence to show that he had done any such thing (*e.g.* the supposedly modified code).

b) Second, Satoshi Nakamoto did not use Dr Wright's fictional "Project Chrono" derived sleep_for function at any point in the Bitcoin code. Instead, he used the basic Sleep function from Windows' application programming interface (API).[17]

[16] Mr Hinnant clarified at Day14/p46 that it would take more work to derive it from a completely unrelated piece of software than to write it from scratch.

[17] This can be seen at, for example, {L4/97.1/31} of the main.cpp file, in which reference is made to "Sleep(100)". The Windows Sleep function was brought into the main.cpp file by its inclusion at {L4/97.1/1} of the headers.h file. The headers.h file in turn included windows.h {L4/92.1/1}.

3. The basic mechanics of the Bitcoin software

23. Dr Wright's cross-examination afforded the Developers an opportunity to test his awareness of basic elements of the Bitcoin software. In three remarkable respects it was clear that Dr Wright cannot have been involved in its development:

a) The first concerned his inability to describe the concept of an unsigned integer.

b) The second arose from his misunderstanding of the Bitcoin software's basic CheckBlock function.

c) Third, Dr Wright's lack of knowledge emerged from the approach that was taken on his behalf in cross-examination of Dr Back regarding the proof-of-work function in the Bitcoin code.

a. Unsigned integers

24. Satoshi Nakamoto often used "unsigned" integers in the Bitcoin code. The frequency of their use can be seen from a simple search in the principal software files for "unsigned int". That reveals that Satoshi used unsigned integers over 100 times in the original main.cpp {L4/970.1}, main.h {L4/98.1} and bignum.h {L4/89.1} files alone. Across the entirety of the original Bitcoin code they are used 294 times.[18] Unsigned integers were commonly referenced in Satoshi's contemporaneous emails.[19] They were even alleged to form part of the Bitcoin File Format over which Dr Wright claimed copyright.[20]

25. That being so, if Dr Wright was Satoshi Nakamoto he would know what an unsigned integer was. His blank expression when asked about the concept (in stark contrast to his immediate answers to other questions, he paused for about nine seconds after being

[18] There are 531 mentions of "unsigned" across the codebase, of which most are "unsigned char".

[19] {L4/328}, {L6/153}, {L6/155},{L6/282.2}, {L6/292.2}, {L6/464.4}, {L6/465.1}, {L7/204.3} and {L7/210.1}.

[20] See the notes against "nVersion", "nTime", "nOut", "nSequenceIn", "n" and "nSequence" in the (now deleted) Schedule 2 to the Amended Particulars of Claim in the BTC Core action at {A1/2/38} and following.

asked to take a wild guess) is captured in the following section of the transcript for Day8:[21]

"*143:21 Q. And we can find that at {L9/247.1/1}. So that's*
22 the GitHub reference that you have given and it's taken
23 us to the script.h file on GitHub; do you see that?
24 A. That is correct.
25 Q. And so we can see, at row 18, that is declaring
144: 1 a constant integer variable
2 called "MAX_SCRIPT_ELEMENT_SIZE"; do you see that?
3 A. I do.
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."

26. The book which Dr Wright had disclosed and to which he was taken was C++ For Dummies.[22]

[21] Dr Wright's inability to describe the coding function undermines his claim that: "*I'm better at code than words*" {Day2/p92/l.6}, though the Court will note that Dr Wright's claim is merely a clunking attempt to quote a well-known passage from a message from Satoshi to Hal Finney {L3/292/1} (final sentence).

[22] {L1/199/1}.

b. CheckBlock

27. CheckBlock was one of the key functions in the Bitcoin source code. It was the first stage in the processing of blocks under the ProcessBlock function in the main.cpp file. The second stage was AcceptBlock.

28. CheckBlock was comprised of six steps {L4/97.1/21} each of which is preceded by a single line comment as follows:

a) // Size limits

b) // Check timestamp

c) // First transaction must be coinbase, the rest must not be

d) // Check transactions

e) // Check proof of work matches claimed amount

f) // Check merkleroot

29. 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: Q. And then, fourthly, we can see that it checked transactions?*
A. Yes.
Q. What was that?
A. That it checks transactions?
Q. Yes, what was the check of the transactions?
A. Basically making sure that they are valid, that the transactions that have been received follow the rules, etc.
Q. So what sort of thing?
A. What sort of thing. So, basically, Bitcoin uses script. The way that you'd have to then check would be does the key work, does other policies work, are the output and script valid. It's a predicate. So, what we're functionally doing in here is ensuring that all of the input and output is structured correctly, that if there's a message with an ECDSA key that the correct previous block had been signed.
Q. So I remember you talking the other day -- I can't 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."

30. 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. The checks in "Check transactions" are set out in the main.h file at {L4/98.1/8}. 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,[23] (b) the value of created UTXOs was not negative,[24] and (c) if it was a coinbase transaction[25] that the scriptSig was of the right size and, if it was not a coinbase transaction, that its input is not null.[26]

31. It was a measure of how far Dr Wright was out of his depth when taken to this section of the code that he 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

[23] {Day8/p124/ll.18-24}.
[24] {Day8/p124/l.25}-{Day8/p125/lk.2}.
[25] i.e. the issue of the original mined coins.
[26] {Day8/p125/ll.3-9}.

> *is described as "ProcessBlock"?*
>
> *A. I do.*
>
> *Q. And do you see underneath that, the preliminary check that it does is called "CheckBlock"?*
>
> *A. I do.*
>
> *Q. And do you see that a secondary check, after CheckBlock has been completed, is called "AcceptBlock"?*
>
> *A. I do.*
>
> *Q. Now, it is within AcceptBlock that the signatures are checked, isn't it?*
>
> *A. Basically what we have is a series of functions that each of these call other functions. So, where you're trying to say that each of these don't do all of that, the diagram that these guys don't like is a functional call mapping each of these areas down.*
>
> *Q. I'm not asking you about any diagrams, I'm asking you about what is in the CheckBlock function, and you told me that within the CheckBlock function were checks of ECDSA signatures.*
>
> *A. If it's a header and everything else is underneath it, then that is part of the entire function and you are checking everything. So when you have one function follow another to be correct, then all of those sub functions are part of the same function.*
>
> *Q. I'm afraid you're wrong, Dr Wright. If we want to explore how you get to signatures from the AcceptBlock function, I can take you there. Do you want me to do that?*
>
> *A. Like I said, the block includes both the full check and each of these. So when you have a transaction that you have checked, it then goes into the block and it's put into a binary tree structure. All of that is checked as part of the entire function. What you're doing is pulling out each individual call and saying that it's separate. It isn't.*
>
> *Q. We have looked at what the CheckBlock function contains and you have said it contains an ECDSA signature check. It doesn't, does it?*
>
> *A. That's not what I said.*
>
> *Q. Well, we can see what you said.*
>
> *A. What I said was, the function includes all of the processes in that. CheckBlock doesn't work unless each of the called functions are there."*

32. The truth is more prosaic. 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 had to be demonstrated to Dr Wright at {Day8/pp127-129}. Such a demonstration would not have been necessary if Dr Wright was Satoshi Nakamoto.

c. Leading zeroes

33. Dr Wright's lack of familiarity with the Bitcoin code is also demonstrated by his lack of awareness of an improvement of the proof of work function in the original code that meant that it departed from the system described in the Bitcoin White Paper. This improvement had been flagged in the Developers' skeleton argument for the trial, but Dr Wright seems to have been unaware of it.

34. As described in the Developers' skeleton at paragraph 26.d {R/13/12}:

a) Assessment of whether the hash of the Block Header meets the requisite proof-of-work requirement is determined by reference to whether the hash is equal to or below a target number (*i.e.* when the Block Header is hashed using double SHA256, the output, when interpreted as an integer number, is equal to or less than the set target number).

b) Being equal to or below a long target number implies that there will be a number of leading 0s in the target number in binary (and in hex or any other base).

c) The Bitcoin White Paper: Section 4, second para {L5/26/3} contemplated that the target value would be set with leading zeroes – an approach that conforms to that suggested in Sections 3 and 5 of Adam Back's "Hashcash – a denial of service counter-measure" that is cited in the Bitcoin White Paper (http://www.hashcash.org/papers/hashcash.pdf).

d) However, the first available issue of the Bitcoin source code replaced the use of a target based on leading zeroes with a numerical comparison which did not refer to leading zeroes. This meant that the target number could be set precisely (*e.g.* the leading digits of the hash may have to be less than "0000000000000000000101..."), which in turn allowed the difficulty to be very precisely adjusted.

35. During his cross-examination, it was wrongly suggested to Dr Back (presumably on instructions from Dr Wright)[27] that the Bitcoin code had retained the approach of simply checking leading zeroes that had been described in the Bitcoin White Paper: see {Day13/p47/ll.16-18} and {Day13/p48/ll.6-9} and {Day13/p49/l.10}-{Day13/p50/l.1}.

36. Dr Back correctly answered that, although the Bitcoin White Paper appeared to refer to leading zeroes, no released version of the Bitcoin code does:

> "*47:19 A. It's a simplification. It's because the -- this paper*
> *20 and the Hashcash paper is concerning itself with a very*
> *21 coarse-grained type of work where the difficulty can*
> *22 only adjust by a factor of two, then it's leading zeros,*
> *23 but in the Bitcoin case, the precision is much higher,*
> *24 so that it's technically to find a hash which is less*
> *25 than a target. Now, because that is a small -- small*
> *48: 1 number relatively, it will have a lot of leading zeros,*
> *2 but technically it's a little more than that, which is,*
> *3 you know, the first digit of the -- that isn't zero has*
> *4 to be below the target and so on, as a kind of floating*
> *5 point number.*"

> "*48:14 …This paper appears to also use*
> *15 the factor of two simplification, but Bitcoin doesn't,*
> *16 and so Bitcoin is not just looking for leading zeros;*
> *17 it's looking for, you know, one number treated as*
> *18 a floating point to be less than another. And so*
> *19 leading zeros could result -- you know,*
> *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…"*

37. As the Developers pointed out in their skeleton, the relevant check is the following part of the CheckBlock function.

```
// Check proof of work matches claimed amount
if (CBigNum().SetCompact(nBits) > bnProofOfWorkLimit)
        return error("CheckBlock() : nBits below minimum work");
if (GetHash() > CBigNum().SetCompact(nBits).getuint256())
```

[27] This appears to be the case from Wright11¶387 {CSW/1/73} and Wright11¶601.e-g {CSW/1/112} and because Dr Wright made a garbled attempt to suggest that Dr Back was wrong at {Day15/p80/ll.1-5}.

```
        return error("CheckBlock() : hash doesn't match nBits");
```

38. An explanation of the precise way in which that function operates is appended to this closing. For present purposes it is sufficient to observe that the second stage of the function uses the operator > (which is highlighted in yellow above), *i.e.* it checks whether the hash (GetHash()) is "greater than" the proof-of-work target (CBigNum().SetCompact(nBits).getuint256())). If it is, the function returns an error. There is no check for leading zeroes, as Dr Back confirmed in re-examination by the Developers' counsel:

> "*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."*

d. <u>Summary of Dr Wright's awareness of the mechanics of the Bitcoin software</u>

39. In summary, in three elementary respects, Dr Wright was unaware of the content and meaning of the Bitcoin code. That being so, he cannot be the author of that code. Moreover, it is telling that faced with the opportunity to question a real Bitcoin developer, Dr Pieter Wuille, Dr Wright declined the opportunity (and indeed initially sought to exclude his evidence altogether).[28] Had Dr Wright taken that opportunity, the Developers are confident that the difference in skill-set between Dr Wright and a real Bitcoin programmer would have been abundantly obvious to the Court.

[28] The BTC Core Claimants wrongly contended that Dr Wuille's statement revealed a "*fundamental misunderstanding of the purpose of factual witness evidence in these proceedings*" and to "*not have anything to say that goes directly, or even indirectly, to the Identity Issue*": BTC Core Claimants' skeleton for the hearing on 17 October 2023 at ¶7.1 {R/23/3}. Orally it was said that it did not "*amount to a whole hill of beans*": see the BTC Core Claimants' submissions at the hearing on 17 October 2023 at p51 ll. 13-14 {O/10.1/14}.

4. Implementation of the Bitcoin software

40. There are five respects in which Dr Wright's evidence as to the implementation of the Bitcoin software and related concepts revealed his lack of understanding. The first arose from his evidence as to the computers that he claimed to be operating on the launch of the Bitcoin code and their electricity consumption. The second concerned his lack of knowledge about Satoshi Nakamoto's disabling of opcodes in Bitcoin script. The third arose from his failure to spot that within his purportedly pre-2009 (forged) reliance documents there were numerous references to concepts that were only introduced in 2011 and following. Fourth, he wrongly contended that he had transferred Bitcoin to Zooko Wilcox-O'Hearn. Fifth, and relatedly, there was his lack of awareness about Satoshi Nakamoto's PGP key. Finally, when Dr Wright first ventured into the debate about Bitcoin, his intervention was flatly at odds with him being Satoshi.

a. The 69 computers

41. Dr Wright boasted of the wide array of computers that he was running at his home in Australia in his evidence-in-chief in the Kleiman proceedings {L17/327/105}-{L17/327/108}.[29] 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.

42. 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.[30] 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.[31]

[29] He had previously made a similar claim (albeit of 67 computers) 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).

[30] {Day6/pp141-142}.

[31] {Day/8/p174/ll.12}.

43. There were two significant problems with this evidence.

i. Problem 1: inconsistency with the known difficulty

44. First, and most pertinently for his attempt to pretend that he was Satoshi Nakamoto, 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 (whether 69 racks or 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.[32]

45. Dr Wright responded to that setback 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.

46. 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*

[32] 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} was unable to sustain that criticism {Day18/p58/l.1}-{Day18/p59/l.3}.

> *the network. Now, that allowed me to have multiple systems, including the logging systems and the rest of the Timecoin server. All of that together was really the cost that I experienced.*"

47. Leaving aside the swerve in Dr Wright's evidence between his first and ninth statements and his oral evidence (and its flat inconsistency with his previous comments in his blog and on CoinGeek in 2019),[33] there were three elements to Dr Wright's contention that Satoshi Nakamoto was using a setup such as that described by Dr Wright.

    a) 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.

    b) Second, that the setup was "*running testnet*".

    c) Third, that he was running "*the Timecoin server*".

48. None of these contentions is true:

    a) 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 is manifestly false.[34] And it was disclaimed by Mr Gao in his cross-examination.[35]

    b) Nor can Dr Wright have been running testnet. Testnet did not exist until July 2010.[36] Dr Wright suggested orally that he (as Satoshi) was running some previously undisclosed private version of Testnet.[37] That cannot be true either. 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*".

    c) The latter contention can also be discounted. Timecoin is a recent invention of Dr Wright's (he did not mention it at all in the Kleiman proceedings), and one that he appears to have instructed his witnesses to corroborate artificially

[33] See {L14/420/2} (blog) and {O4/12/13} (CoinGeek interview).
[34] {Day8/p177/11}-{Day8/p179/7}.
[35] {Day18/p60/ll.10-12}.
[36] {Day8/p175/ll.20-23}.
[37] {Day8/p175/l.25} - {Day8/p176/l.1}.

in their own live evidence.[38] Moreover, his evidence as to his electricity consumption is plainly untrue for the reasons set out below.

ii. Problem 2: inconsistency with known electricity consumption

49. 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:

    a) Lisarow: the electricity bills were as follows:

        i) for the period from 8 December 2008 to 18 January 2009: AU$373.19 plus GST {L4/485/23};

        ii) for the period from 18 January 2009 to 9 March 2009: AU$523.10 plus GST {L5/70/8};

        iii) for the period from 9 March 2009 to 9 June 2009 was about AU$798.48: {L5/70/79}.

    b) Bagnoo: the electricity bill for the period from 11 February 2009 to 8 May 2009 was less than AU$500: {L5/70/50}.

50. 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.[39] That is vanishingly unlikely to be true.

    a) 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.[40]

    b) 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.[41] That being so, it seems highly implausible that it was "*on a separate switch*".

[38] {Day9/p94/l.5}- {Day9/p105/l.13}.
[39] {Day8/p.174/ll.19-20}.
[40] {L5/70/81}.
[41] DeMorgan1¶11 {E/8/4}. Mr Bridges refers to the set-up being in Dr Wright's garage in early 2011: Bridges1¶19 {E/9/6}.

c) Information Defense Pty Ltd was only registered on 29 January 2009,[42] 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.

d) 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.[43]

51. In short, Dr Wright was not incurring substantial expense as a result of his electricity consumption, but more to the point if he were Satoshi Nakamoto he would know that 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[44] on what was a normal HP Compaq computer.[45]

b. opcodes

52. In his eleventh witness statement, Dr Wright provided a lengthy critique of changes supposedly made "*by BTC*" to the original version of Bitcoin.[46] In particular, he complained that many "*OP_codes that are important to the functioning of the script have been disabled*".[47]

53. Dr Wright's inconsistent and mis-spelling of the term "opcode"[48] was a small indicator that he was expounding on something outside his knowledge or experience. More significantly, however, Dr Wright was evidently unaware at the time of filing his eleventh witness statement that the relevant changes to the Bitcoin code had been made by Satoshi Nakamoto.

[42] {L4/446/80}.
[43] {C/27/35} ll. 4-20.
[44] Bohm1¶16 {C/10/5}.
[45] {L4/493/1}.
[46] Wright11¶544 {CSW/1/100}.
[47] Wright11¶545 {CSW/1/100}.
[48] See Wuille2¶13 {C1/2/3}.

54. The Developers address two examples of changes implemented by Satoshi Nakamoto below: namely the change to size of data elements inside script and the disabling of OP_2MUL.

i. Script size

55. 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*".

56. Dr Wright's contention that "BTC" had "placed" a maximum size of 520 bytes was footnoted to {L9/247.1}, which was a version of the script.h file[49] 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.

57. 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.[50] On 23 January 2013 the name MAX_SCRIPT_ELEMENT_SIZE was given to that limit.[51] Dr Wuille's evidence to this effect has not been challenged by Dr Wright for the obvious reason that it is both true, and corroborated by the commits identified by Dr Wuille.

58. Dr Wright had read Dr Wuille's statement by the time that Dr Wright came to give oral evidence,[52] but had misremembered it. Accordingly, when 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/p145/l.5}. Unfortunately for Dr Wright, that could not be

[49] It is version 0.10.0rc3 of the Bitcoin code: Wuille2¶7 {C1/2/2}.

[50] Wuille2¶9 {C1/2/2}.

[51] Wuille2¶11 {C1/2/3}.

[52] {Day8/p145/ll.12-14}.

true either. 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.[53] Indeed, TheBlueMatt is the tenth defendant in the BTC Core Claim, and one of the Developers.

59. Faced with the absolute 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/p151/ll.10-14}.

60. Needless to say 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 typically evasive: "*I was building other systems*" {Day8/p151/l.18}.

ii. OP_2MUL

61. 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".

62. As Dr Wuille explained at Wuille2¶12-15 {C1/2/3}, the opcodes in question (including OP_2MUL) have indeed been disabled, but they were disabled by Satoshi Nakamoto. As Dr Wright was constrained to admit in cross-examination, 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.[54]

[53] {Day8/p145/l.10}.

[54] {Day8/p158/ll.3-9}.

63. Faced with this contradiction between Wright11¶545 and the evidence of Dr Wuille, Dr Wright suggested that he had "*pulled [these opcodes] temporarily*"[55] and that this was a "*temporary block*".[56] That is not a sustainable contention, both because 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.[57]

64. But even leaving those points to one side, the Developers would invite the Court to re-read paragraph Wright11¶545-545.e {CSW/1/101} with the knowledge that it was Satoshi Nakamoto that disabled OP_2MUL. Those paragraphs in which Dr Wright speculates as to why BTC might have disabled OP_2MUL are generally incoherent,[58] but once it is understood that Satoshi Nakamoto disabled the opcodes, it is quite obvious 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.

65. 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.

c. The anachronisms

66. 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 reliance documents of documents purporting to date from before the release of the

[55] {Day8/p157/ll.17-18}.

[56] {Day8/p158/l.15} and {Day8/p158/l.24}.

[57] See {Day8/p159/l.16}-{Day8/p160/l.6}.

[58] It is an irrelevant sideshow, but Dr Wright has completely 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*".

Bitcoin software, but which refer to code and concepts that post-date Satoshi Nakamoto's involvement in the development of Bitcoin.

67. It should be noted that the reliance documents in question are (rightly) challenged by COPA as forged or inauthentic. But 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.

68. For present purposes, it is sufficient to take four of the matters identified by Dr Wuille in his unchallenged first witness statement, namely CheckBlockHeader, BTC Core, UTXO and bootstrapping. The first three matters were taken orally with Dr Wright. The fourth is addressed in Dr Wuille's statement and corroborated by the documentary record.

i. CheckBlockHeader

69. The CheckBlockHeader function was introduced by Dr Wuille in March 2014 as part of a series of header synchronisation changes.[59]

70. CheckBlockHeader resulted from a split in the functionality present in the CheckBlock function described at paragraphs 27 to 28 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.[60]

71. 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.

72. When taken first 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.[61]

[59] Wuille1¶24-25 {C1/1/6}.
[60] Wuille1¶25 {C1/1/6}.
[61] {Day8/p132/l.23}-{Day8/p133/l.6}.

73. One of Dr Wright's reliance documents was, however, a document entitled "*BitCoin: SEIR-C propagation models of block and transaction dissemination*" {L3/237} ("*the SEIR-C document*"). At Wright11 AxB¶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*".

74. 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:

"*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"

75. Dr Wright's response to the anachronistic inclusion of reference (in the present tense!)[62] to a function from 2014 in a document purportedly from 2008 is informative:

"*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?

[62] {Day8/pp197-198}.

A. No, it's a -- basically what we're talking about is a light node. So a node where an individual doesn't need to download the entire blockchain. For instance, I can just have the block headers and then I can have a localised(?) path of where I'm checking an individual transaction. I can keep each of those.

Q. Dr Wright, nobody referred to CheckBlockHeader until the change that I took you to, did they?

A. No, that's wrong. That was actually part of building SPV systems, that was basically the function I was looking at at that time.

Q. There isn't a single document in which anybody refers to CheckBlockHeader as a single function until Dr W[uille] introduced it through GitHub, right?

A. I've no idea when he put it in that, but when I was discussing the introduction of SPV, these concepts were back there as well.

Q. Mr Andresen did not introduce CheckBlockHeader, did he?

137: A. No, Mr Andresen got a patch from me initially. So the patches for SPV were actually from Satoshi, me.

Q. Dr Wright, we've got the patches that Satoshi Nakamoto sent to Mr Andresen; they do not include CheckBlockHeader.

A. No, because I went off to develop things myself. So where I was talking about work that I did in my other companies, I didn't do everything publicly. The work on Teranode now that was iDaemon that I've put in here, all of those documents were based on our work, not his.

Q. Dr Wright, I know you want to talk about all of your latest things. I'm actually trying to ask you about things that Satoshi Nakamoto would know about, and that is the original --

A. No, you're --

Q. -- Bitcoin code, right, and there was no reference in the original Bitcoin code to CheckBlockHeader, was there?

A. Again, difference between core, as in main nodes, and those that are doing less, SPV, and there is a reference to SPV. SPV nodes are those that only have to check the headers across the network. If you read the section, you will see that.

Q. Dr Wright, I am very confident that I can read any section of anything and I will not see a single 138: reference to CheckBlockHeader.

A. Because the code's not referenced in the White Paper at all.

Q. And you're saying that -- when did you say then you invented this? Was it in 2010, you said, when you were talking to Mr Andresen?

A. No, I started working on SPV before I even released

> *Bitcoin. So, what I was doing is a combination of Timecoin, which was a separate product, and Bitcoin. Bitcoin was the main free product; Timecoin extended everything."*

76. That set of responses bears many of the common tell-tale signs of Dr Wright's dishonesty. They include:

    a) 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 paragraph 72 above.

    b) 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.

    c) 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. Happily, Gavin Andresen has disclosed all of his communications with Satoshi Nakamoto, including patches. None includes a function called CheckBlockHeader.

    d) A vacuous reference to iDaemon and/or Terranode and/or Timecoin or other "*Star Trek-style technobabble*" (to quote Mr Hearn).[63]

ii. BTC Core

77. The passage from the SEIR_C document set out at paragraph 74 above contains a second anachronism. It refers to the "*Bitcoin Core client*".

78. 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.*"

[63] Hearn1¶28 {C/22/7}.

79. Dr Wright's response to this anachronism was to suggest that:

a) The terminology of Bitcoin Core (capital B, capital C) had been used "*multiple times*" prior to March 2014 {Day8/p134/l.24}. There is no evidence to that effect. As Dr Wuille explains in his unchallenged evidence, the name was suggested by Gavin Andresen and was not used before version 0.9 of the software. Dr Wright's evidence that "*Bitcoin Core*" (the non-existent entity against which Dr Wright repeatedly rails in Wright11) had adopted the name Bitcoin Core from something else/someone else {Day8/p135/ll.3-4} was accordingly misplaced.

b) The term "Bitcoin Core" was being used in the SEIR_C document in contradistinction to Simplified Payment Verification (or SPV) {Day8/p135/ll.7-8}. Even if that were the case, and that does not seem to be so from just reading the document,[64] it still would not explain the anachronism.

iii. UTXO

80. Bitcoin only allows nodes to accept a block if all transactions in it are valid and are not already spent.[65] 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.[66] That index was called blkindex.dat[67] 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.

81. 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

[64] The document had been edited to say that SPV had not been modelled at that time – see footnote4 at {L3/237/7}.

[65] See Bitcoin White Paper at §5.5 {L5/26/3}.

[66] Wuille1¶30 {C1/1/7}.

[67] {L8/12/1}.

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.[68]

82. 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.[69] 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.[70]

83. 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*".[71] Even some months later, however, the expression had not become well-established.[72] 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.

84. Professor Meiklejohn and Mr Gao were in agreement that the term UTXO began to be adopted in 2012 or so[73] 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:

[68] Wuille1¶30-31 {C1/1/7}.

[69] Wuille1¶30 {C1/1/7}.

[70] Wuille1¶31 {C1/1/8}.

[71] {D1/6/11} at Row 437.

[72] Generally see Wuille1¶31 {C1/1/8}.

[73] Meiklejohn1¶45 {G/2/16}, agreed by Gao at {Q/3/2}.

a) 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}.

b) 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}.

c) 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}.

85. 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. That beggars belief. Something approaching 1,000 emails or forum posts written by the real Satoshi Nakamoto are available to the parties and the Court. Not a single one uses the expression UTXO. Yet Satoshi is supposed (by Dr Wright) 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.

86. Not even Dr Wright could sustain that obvious lie. His evidence went on as follows:

"*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."

87. Leaving the characteristically pointless reference to iDaemon to one side, 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 negatived 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

88. A further area of anachronism is 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.[74] It is convenient to take that topic in two parts:

a) First, by looking at the way in which a node first connects to the peer-to-peer network.

b) Second, by exploring how the Bitcoin software then obtained the IP addresses of further nodes.

89. The process for first connection went through three phases:

a) **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.[75]

b) **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.[76] That can be seen at {L6/182/4} where the 47 seed IP addresses are identified in hex.

[74] Wuille1¶14 {C1/1/4}.
[75] Wuille1¶15 {C1/1/4}.
[76] Wuille1¶16 {C1/1/4}.

c) **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.[77] 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*").

90. 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:[78]

a) 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").

b) 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.[79]

c) 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.[80] 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.

[77] Wuille1¶17 {C1/1/4}.

[78] Wuille1¶18 {C1/1/4}.

[79] See {L6/29/4} final lines: if (VInventoryToSend.size() >= 1000) {pto->PushMessage("inv", vInventoryToSend);vInventoryToSend.clear()}

[80] See Wuille1¶19 {C1/1/5} and {L6/181/2}: "// receiver rejects addr messages larger than 1000"

d) 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).[81] Later that month, that was revised from 2000 to 2500.[82]

91. 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:

a) 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.

b) 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.

92. 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

93. 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 corroborates those conclusions but points to two more important conclusions.

[81] See {L6/454/1} green code passages.

[82] See {L6/456/4} green code passage halfway down the page in which 2000 is replaced with 2500 and see Wuille1¶19 {C1/1/5}.

94. 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: Q. Now, my learned friend Mr Hough has been through the documents with you and made the point that the metadata of those documents is inauthentic, or that it's forged. But it's not just the metadata that's inauthentic, is it, it's the content as well?*
> *A. The metadata on that is not forged.*
> ***Q. You wrote this content, didn't you?***
> ***A. Of course I wrote this content. This content was created by me, but not like you're saying.*** *It was created by me in -- like, over 15 years ago.*
> *Q. Dr Wright, you forged these documents, didn't you?*
> *A. I did not. Again, what you're saying is that other terminology which I've used in multiple other things must have been shared with people. I create -- I've got several thousand documents, as in ones that are patented, and* ***I have not discussed any of those terminologies outside of corporations where people have NDAs.***
> *Q. So nobody else could have forged these documents?*
> *A. They're not forged."*

95. 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.

d. Satoshi's Bitcoin payments

96. It is a feature of Dr Wright's Satoshi role-play that he has tended to trim his evidence to fit known facts about Satoshi's work and communications. That was witnessed shortly before the trial by Dr Wright's tweeting of content from the Martti Malmi emails disclosed to him by COPA in August 2023.[83] Dr Wright presented that material in 2024 as if he was giving privileged insight into Satoshi's thinking – and his more

[83] {X/10/1} and {X/11/1}.

credulous supporters then took the subsequent public disclosure of Mr Malmi's emails as corroborative that Dr Wright was Satoshi.

97. Dr Wright has generally been more cautious about describing specific things that Satoshi did which are not in the public domain. No doubt that reflects a fear on his part that his claims might be rebutted. The Court will contrast this tendency on Dr Wright's part with his tendency to pontificate as to Satoshi Nakamoto's supposed philosophy, an inherently more nebulous concept.

98. A rare example of Dr Wright sticking his neck out concerns an assertion that he made in a tempestuous interview with GQ magazine in which he asserted that he (as Satoshi) had only transferred bitcoins to Hal Finney and Zooko "*full stop*".[84] He doubled-down on his assertion that Satoshi had transferred bitcoins to Zooko in cross-examination on Day 7:

> "*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.*"

99. The Court has had the opportunity to hear from Mr Wilcox-O'Hearn. He was a self-evidently honest (indeed, charming) witness. His evidence in cross-examination on Day 14 on the matter of whether Satoshi had transferred bitcoins to him was crisp and 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*

[84] {L14/67/1} at 5:19.

> *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."*

100. This was not the only error in Dr Wright's prior assertions about Satoshi Nakamoto's transfer of bitcoins. He had also overlooked the transfers made by Satoshi to Nicholas Bohm, a former partner of Norton Rose who had developed an interest in cryptography.[85] That was because Dr Wright would only have become aware of Mr Bohm's dealings with Satoshi when COPA served Mr Bohm's witness statement in these proceedings, but when presented with this oversight, Dr Wright responded on Day 7 as follows. The answer can be contrasted with his former claim to have transferred bitcoins 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.*"

101. Strikingly 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*

[85] Bohm1¶5 {C/10/2} and Bohm1¶15 {C/10/4}.

> *time, my Lord. I just sent whoever asked, and most of them were pseudonymous. The majority of people on the forum didn't actually use their name."*

e. The PGP key

102. 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}.

103. The relevance of the key arises in two ways:

a) 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*".[86]

b) Second, in the backlash following Dr Wright's failed blogpost on 2 May 2016, 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}.

104. In their Statement 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:[87]

> "*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.*"

[86] {E/17/42} at lines 11-14.

[87] Defence¶83(2) {A/3/24} and Wright4¶104 {E/4/34}. Dr Wright sought to distance himself from this in evasive answers in cross-examination (and in response to the Judge) at {Day8/p37/l.9} to {Day8/p40/l.7} and at {Day8/p42/ll.2-24}.

105. Dr Wright had said almost exactly the same thing in an interview in 2021,[88] 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[89] announcing: "*The first version was after I left*"[90] and then continuing:[91]

> "*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.*"

106. Dr Wright's suggestion that the PGP key was "*created by a person or persons unknown*" "*in 2011*" is demonstrably false. The fact that Dr Wright has advanced each of those propositions shows that he cannot be Satoshi Nakamoto. In this section of these submissions, the Developers take 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

107. Dr Wright's contention that the PGP key was created in 2011 was shown to be wrong both by Mr Madden and by Martti Malmi.

108. 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:

[88] The interview is recorded for posterity at: https://web.archive.org/web/20210206123702/https://www.youtube.com/watch?t=4326&v=_E7iuVM4CIA&feature=youtu.be, a transcript is at {O4/14/36}.

[89] The resolute tone can be seen at about 1:26:50 into the video.

[90] {O4/14/36}.

[91] {O4/14/37}.

a) 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.[92]

b) Second, he was able to inspect the internal timestamp of the PGP key itself, which also gave a date of 30 October 2008.[93]

109. 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.

110. That being so, the key was not created in 2011.

111. 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. In Wright4 he changed his story. 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.*"

112. 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 demonstrably wrong. As described further below, the key was associated by Satoshi with his satoshin@gmx.com account (not his satoshi@vistomail.com address).

113. But more importantly, Dr Wright had obviously 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 109 above. Dr Wright repeated this clumsy error in Wright9¶34 {E/26/12}, continuing

[92] Madden4¶149 {G/6/48}.
[93] Madden4¶152 {G/6/50}.

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*"

114. 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. First, he suggested that "*the PGP key is not specific to any individual but to a server at Vistomail*" (Wright4¶105 {E/4/35}). Second, he said that the key was "*not a signing key*" (Wright11¶242 {CSW/1/46}) and "*Only for encrypting, never for signing*" ({Day7/p143/l.10}).

115. Each of those points is demonstrably wrong by reference to the content of the key itself:

a) The key expressly identifies the user ID as "Satoshi Nakamoto <satoshin@gmx.com>".[94]

b) The sigclass of the primary key is clearly identified as "*0x13*".[95] 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*".[96]

c) The algorithm used in the generation of the primary key is clearly identified as "*algo 17*".[97] 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.[98]

d) 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.[99] 03

[94] {G/6/50}.

[95] {G/6/50}.

[96] Dr Wright had to admit this association: {Day8/p167/l.8}.

[97] {G/6/50} – see next to "signature packet".

[98] Dr Wright had to admit this at {Day8/p166/ll.10-11}.

[99] See OpenPGP Message Format at {L2/202.1/33} at ¶5.2.3.21.

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).[100]

116. In short, every element of Dr Wright's factual and technical explanation of Satoshi's PGP key was wrong. 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. But the greater and more obvious significance of Dr Wright's erroneous understanding of Satoshi's PGP key is that he cannot be Satoshi Nakamoto.

f. Wikileaks: Dr Wright's first brush with Bitcoin

117. On 10 November 2010, a user called genjix started a thread on the bitcoin.org forum about using Bitcoin to make payments to Wikileaks {L19/168}. 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.*"

118. 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 2020 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.*"

[100] See OpenPGP Message Format at {L2/202.1/34} top of page.

119. 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.[101] 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.[102]

120. 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]*". [103]

121. 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.[104] 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.[105]

122. Dr Wright waded into the ensuing debate in the comments in his characteristically outspoken manner.[106] On the point about whether there were sufficient alternatives to PayPal he argued that there were.

[101] https://theconversation.com/are-anonymous-and-lulzsec-about-to-hack-paypal-for-wikileaks-2582, currently available in illegible format at {L7/389.1/1}.

[102] {L7/389.1}.

[103] {L7/389.1}. Note, one characteristic of Dr Wright's postings is that they commonly contain spelling errors.

[104] {L7/391/1-20}, Wright11¶58 fn 27 {CSW/1/12}.

[105] Dr Wright explains that Anonymous and LulzSec stand "diametrically to what he believes in" Wright11¶36 {CSW/1/6}.

[106] Similar outbursts can be found on Dr Wright's contribution to other websites, including Seclists.org and his own blog.

123. 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). [107] He responded to another commenter as follows (again, emphasis added): [108]

> "*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.….*"

124. Thus, Dr Wright's first 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. And, although by late July 2011 Dr Wright was aware of Bitcoin, he was uncertain about how it was spelled (one word or two, [109] capitals or not). [110] 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.*"

[107] {L7/391/13}.

[108] {L7/391/17-18}.

[109] Dr Wright suggested in cross-examination that the use of two words was a consequence of "auto correct", but the error appears twice in just 4 words in his post at {L7/391/17} at not at all at {L7/389.1}.

[110] 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".

5. Summary

125. Any one of the shortcomings in Dr Wright's evidence regarding the Bitcoin code and the implementation of the Bitcoin system might reasonably disprove any claim he could make to be Satoshi Nakamoto. Taken together, his lack of basic computer science knowledge, his inexperience with C++, his unawareness of unsigned integers, his ignorance of the CheckBlock function, his erroneous belief about the use of leading zeroes, his misunderstanding of the computing power applied in Bitcoin's initial mining activities, his ignorance that Satoshi had limited the data element size in script and disabled opcodes, his reliance upon documents with anachronistic content, his lack of awareness of Satoshi's bitcoin transactions and his misunderstanding of Satoshi's PGP key lead ineluctably to the conclusion that Dr Wright's claim to have written the Bitcoin code is a brazen lie. Dr Wright's first foray into the Bitcoin debate came in late July 2011 and showed that he was not Satoshi.

C. The Bitcoin White Paper

126. Dr Wright's attempt to claim that he authored the Bitcoin White Paper is inescapably linked to his evidence about the so-called White Paper Latex Files. As became clear during Dr Wright's evidence, those documents are a crude forgery. Accordingly, it is necessary to take the so-called White Paper LaTeX Files at some length in this section of these submissions. There is, however, a preceding indicator that Dr Wright was not involved in production of the Bitcoin White Paper, namely the mess that he made of his dealings with Wei Dai. That point is taken first.

1. Dr Wright's Wei Dai lies

127. On 20 August 2008 Satoshi Nakamoto shared a link to a then draft of the Bitcoin White Paper with Dr Back {L3/190}. He stated as follows:

"*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."

128. Stopping there, Satoshi was clearly envisaging that Dr Back's Hashcash paper would be the fifth reference in the Bitcoin White Paper.

129. 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).*"

130. Two points emerge from that response. First, it was a perfectly friendly reply from Dr Back. Second, and more importantly he drew Satoshi's reference to the "B-money" proposal made by Wei Dai (which was set out on a web-page, not in a paper).

131. 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."

132. 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?)."

133. 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 a first reference to 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.

134. 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.*"

135. There were no further dealings between Satoshi and Wei Dai until the Bitcoin White Paper was published.

136. Nevertheless, Wright1¶92 {E/1/18} took a wild guess as to what Satoshi's dealings with Wei Dai might have been, stating:

> "*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.*"

137. Wei Dai was asked by Bird & Bird to comment on that evidence and has confirmed that was not what happened {C/28/3}:

> "*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.*"

138. At Wright11¶370 {CSW/1/69}, Dr Wright further tried to suggest that he had been aware of Wei Dai's b-money <u>proposal</u> 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 described above. However, Dr Wright was compelled to argue the point because of prior publications by him asserting longstanding familiarity with Wei Dai's work. Regrettably that story of longstanding familiarity with Wei Dai is a further pack of lies.

139. 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."

140. Every element of that account was imagined:

a) 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}.

b) 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}.

c) Wei Dai 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}.

d) As to the use of code from Wei Dai, Wei Dai has stated {C/28/1}:

> "*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.*"

141. In short, every aspect of Dr Wright's story as to his supposed dealings with Professor Wrightson, Andreas Furche and Wei Dai was untrue. 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 --"

142. That is 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.

143. Similarly, 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,

> *I was involved.*
>
> *Q. {CSW/1/82}, please.*
>
> *A. Including Chi-X.*
>
> *Q. Paragraph 433. This is your 11th witness statement, isn't it, Dr Wright? Yes?*
>
> *A. Yes.*
>
> *Q. You claim that Dr Furche and you worked together on the surveillance systems for the Australian Stock Exchange from '97 to 2003, don't you?*
>
> *A. I worked on those systems at that stage, yes, and I believe he was there, and he implemented those --*
>
> *Q. Professor Furche --*
>
> *A. -- systems at that time.*
>
> *Q. Professor Furche's work on the ASX's surveillance systems didn't start until after 2003, did it?*
>
> *A. Well, I still remember him, and I definitely remember him from the Perth Mint.*
>
> *Q. So you worked together at Perth Mint in 2005 to 2008, yes?*
>
> *A. No, I was an auditor.*
>
> *Q. "... then had a joint involvement at the Perth Mint, where I was an auditor for BDO (2005-2008)." Yes?*
>
> *A. Yes.*
>
> *Q. In fact, Professor Furche's work in relation to the Perth Mint didn't begin until 2016, did it?*
>
> *A.* ***I don't know, but I'm pretty sure it was him there,*** *and I believe he was also involved with Chi-X.*
>
> *Q. Just setting aside the thing you don't talk about in your 11th witness statement, you couldn't have had a joint involvement with him at the Perth Mint while you -- in 2005 to 2008, because he didn't have a connection with it at that time, did he?*
>
> *A****. I don't know, but I do remember him. As I said, I'm terrible with people, but I remember him from something.”***

144. Given the central importance that Dr Wright has attributed to the influence of Wei Dai on the Bitcoin White Paper, the fact that his account of how he came to learn of Wei Dai is riddled with lies is sufficient for the Court to conclude that Dr Wright could not have written the Bitcoin White Paper. And that is before Dr Wright blundered into suggesting that the Bitcoin White Paper was written in LaTeX.

2. The history of (non)-production of Dr Wright's LaTeX files

145. The emergence of the so-called White Paper LaTeX Files can be conveniently divided into 3 phases: the "before" phase, the "tease and reveal" and the "cover up".

146. The history of their production reveals three key points which substantiate the direct evidence that the documents are a recent creation by Dr Wright. First, Dr Wright never thought to mention the files until a few months before trial. Second, Dr Wright described those files to the Court at the PTR in a thoroughly misleading manner. Finally, Dr Wright deleted and tampered with relevant files right up until the moment of their production.

147. The content of the files themselves is dealt with in sub-section 3 below.

a. The before phase

148. Dr Wright did not mention LaTeX at all until after the service of Mr Madden's first expert report, which 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, on 1 September 2023 {G/1/1}.

149. Thus, LaTeX was not mentioned by Dr Wright:

a) 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;

b) 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;[111]

c) in his lengthy evidence given in the Granath proceedings in Norway on 14 September 2022, which included evidence about the way in which he had

[111] See Dr Wright's Amended Reply¶¶13 et seq {L16/342/14}. 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}.

supposedly composed the Bitcoin White Paper from handwritten form to the printed page: see {O2/11/9} (internal transcript pages 29-31); or

d) 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.

150. It is a feature of PDF documents compiled from LaTeX code that the PDF file's internal metadata properties may be defined by the document author. It is likely no coincidence, therefore, that faced with Mr Madden's report in September 2023, Dr Wright started searching the internet to see whether Satoshi Nakamoto having used LaTeX might be a possibility. In particular, he accessed a closed Q&A on the TeX StackExchange entitled "*Was anything in Satoshi Nakamoto's original Bitcoin paper compiled in LaTeX?*", in which somebody had speculated that this might be possible.[112]

151. That would have been a bizarre thing for Satoshi Nakamoto to have searched. Nevertheless, it seems to be the thing that launched Dr Wright's White Paper LaTeX Files.

b. The tease and reveal

152. Dr Wright's first mention of LaTeX came in his fourth witness statement dated 23 October 2023. He suggested at Wright4¶6.c {E/4/5}, for the first time, that the development of the Bitcoin White Paper involved a "*complex workflow utilising various software platforms, including LaTeX, OpenOffice and Microsoft Word*".

i. The tease

153. 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

[112] See {P1/18/24} and Wright xx {Day5/pp122-123}.

Overleaf, (b) to seek to impose stringent limitations on their disclosure and (c) asking adjourn the trial {AB/2/2}.

154. 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. The application was heard at the PTR.

155. The burden of the evidence in relation to the White Paper LaTeX Files was placed on a partner of Shoosmiths, but she made clear that she was simply reporting what she had been told by Dr Wright – and Dr Wright filed a (sixth) witness statement confirming her evidence. The evidence repeated and amplified claims Shoosmiths had made (on instructions) in their 27 November 2023 letter. It was said that:

a) 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},[113] and the LaTeX code on Overleaf did not "*have a metadata date*". That evidence was confirmed at Wright6¶4 {E/21/3}.

b) 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}.[114] That evidence was confirmed at Wright6¶4 {E/21/3}.

c) Exact replica: the White Paper LaTeX Files compiled into an "*exact replica*" of the Bitcoin White Paper, Field1¶48 {E/24/16}.[115] The words "*materially identical*" were used at Field1¶19.2.6 {E/24/8}. At Field1¶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}.

[113] See also Shoosmiths' letter at ¶15 {AB/2/5}.

[114] See also Shoosmiths' letter at ¶16 {AB/2/5}. The other material was said to relate to Dr Wright's academic and personal interests post-dating 2020.

[115] See also Shoosmiths' letter at ¶19 {AB/2/5}.

d) <u>Unique position</u>: 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}).

e) <u>Digital watermark</u>: 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*".

<u>ii. The reveal</u>

156. Having teased the content of the White Paper LaTeX Files, 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, when it came,[116] that it was not "*materially identical*" to the Bitcoin White Paper, let alone an "*exact replica*".

157. 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:

a) 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 Nakamoto*" (see {AB/2/67} at ¶2).

b) 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).

158. 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

[116] It is at {L20/248.2}.

potentially determinative of the identity issue (see Wright skele¶57-57(1) {R/2/19}), as impossible to reverse engineer (see Wright Skele¶57(2) {R/2/20}) and as uniquely coding for the published form of the Bitcoin White Paper (Wright Skele¶57(3) {R/2/20}).

159. The Judge ordered that Dr Wright should provide COPA and the Developers inspection of the so-called White Paper LaTeX files in native form on standard Patents Court confidentiality terms: see Order¶5 {B/22/4}. In addition, the Judge ordered that Dr Wright should request Overleaf to give access to metadata and current and historic information regarding document activity, revision and edit history and account creation information: see Order¶7 {B/22/4}. Further, Dr Wright was ordered to produce the advice from Ontier upon which had he relied: see Order¶3 {B/22/3}.[117]

160. 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)*"

161. Thus, Dr Wright's account as to why the White Paper LaTeX Files had not been disclosed previously, fell apart on contact with an officer of the Court. Dr Wright has hinted that Ontier might have some motivation for lying about his LaTeX files, but the truth is more simple. As explained at paragraph 167 below, Dr Wright's Overleaf account did not exist at the time of Ontier's instruction.

162. 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 so-disclosed had been received by Shoosmiths on 24 November 2023.118 It was the same folder that had been used to produce the

[117] Tellingly, Dr Wright had objected to Ontier addressing this issue on grounds of privilege.

[118] See Shoosmiths' letter of 10 January 2024 at {AB/2/199} ¶3.

compilation that had been disclosed on 13 December 2023.[119] The main document path that had been used to create the compilation was a file in the TC subfolder and called main.tex.[120]

c. The (partly failed) cover up

163. Dr Wright has provided only very limited information concerning his Overleaf account(s), and then only reluctantly. He appears to have believed that the Overleaf platform recorded little or no metadata or document editing history (see {Day15/p148/ll.4-9}) and, 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, has made every effort to prevent the production of that information to the Developers and COPA.

164. Dr Wright's undoing lay in his inability to tell the truth about even his interactions with Shoosmiths and the consequential disclosure that had to take place on 16 February 2023, mid-way through the trial. Even now, the Court only has a window into Dr Wright's activity in 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). That window, however, comprehensively destroys any credibility that the so-called White Paper LaTeX Files might otherwise have had.

165. The Developers set out below the history of Dr Wright's Overleaf account, pieced together as best one can in light of the fragmentary information Dr Wright has provided. That is then contrasted with Dr Wright's efforts to avoid the truth of the account coming out.

[119] See Shoosmiths' letter of 29 December 2023 at {AB/2/141} ¶2 and 4 January 2024 at {AB/2/175} ¶2.

[120] 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}.

i. Dr Wright's Overleaf account

166. Dr Wright professes to have held multiple Overleaf accounts associated with multiple (21) universities since 2020.[121] However, his relevant account for present purposes is that associated with his craig@rcjbr.org address.[122]

167. Although Shoosmiths stated that Dr Wright's Overleaf account was created in June/July 2023,[123] the account number[124] incorporates a Unix timestamp in hex[125] that can easily be converted[126] to a precise date and time of 8 August 2023 at 8:21am. That may explain 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.

168. 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.[127] 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.[128]

169. 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.[129] No earlier folders have been disclosed. The main document used by Dr Wright was titled BitcoinSN.tex. He created that file at 17:29

[121] See Shoosmiths' letter of 10 January 2024 at {AB/2/199}. No evidence of those other accounts has been provided.

[122] See Shoosmiths' letter to Overleaf of 10 January 2024 at {M1/2/39}.

[123] See Shoosmiths' letter of 8 January 2024 at {AB/2/187} at ¶11.

[124] 64d1faf729c18d6984405691: see "lastUpdatedby" in the Project.json files at {L21/15.1/1} and {L21/17.1/1}.

[125] 64d1faf7.

[126] The hex number 64d1faf7 corresponds to the decimal number 1691482871 (this can be confirmed using the HEX2DEC formula in Excel). That decimal number represents the number of seconds since 00:00:00 UTC on 1 January 1970 (see Madden1¶59.b.i {G/1/26}) and so corresponds to 8 August 2023.

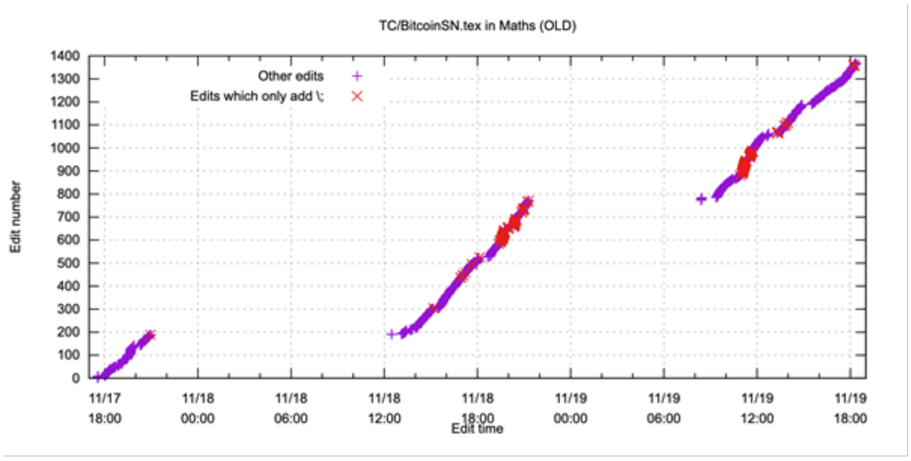
[127] {M/3/48}.

[128] See Shoosmiths' letter of 16 February 2024 {M/3/15} at ¶8.a.

[129] See Shoosmiths' letter of 20 February 2024 {M1/2/210}.

on 17 November 2023[130] 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.[131] He appears to have then given another demonstration to Shoosmiths between 17:00 and 17:30.[132]

170. 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}.



171. 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.[133]

172. 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.[134] Only four inconsequential changes were made during those demonstrations; and then only in the latter session.[135]

[130] {L21/16.1/92}.

[131] {L21/17.1/2}.

[132] See Shoosmiths' letter of 16 February 2024 {M/3/15} at ¶8.a.

[133] {L21/14.1/44}

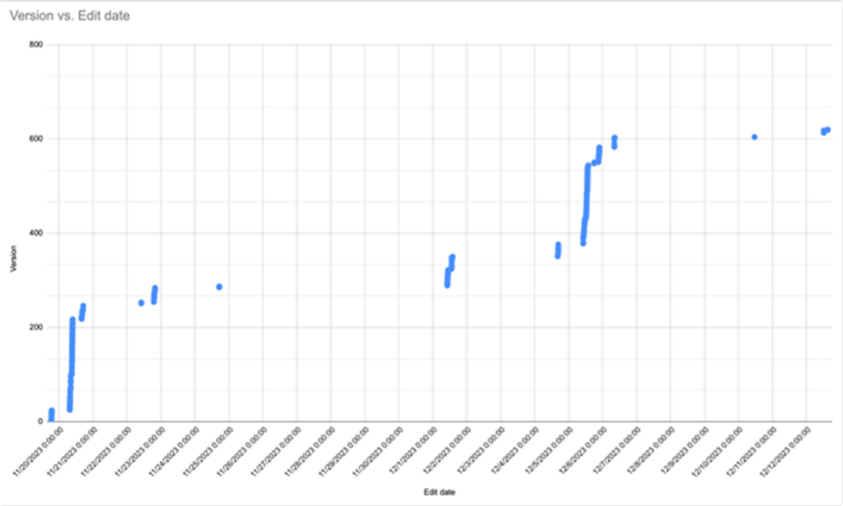
[134] See Shoosmiths' letter of 16 February 2024 {M/3/15} at ¶8.b-8.c.

[135] 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}.

173. 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).[136] The covering emails made no reference to Dr Wright having made any changes, or to him planning to do so.[137]

174. Dr Wright continued to make changes to the main.tex file between 20 November and 24 November 2024. 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*".[138]

175. 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}.



<u>ii. The efforts made to resist providing metadata</u>

176. 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.

[136] See Shoosmiths' letter of 16 February 2024 {M/3/15}.
[137] {L20/252.86}, {L20/252.87} and {L20/252.88}.
[138] {L20/252.89}.

177. Dr Wright had numerous opportunities to tell the truth to the Court – 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 (see [{E/1/1} and {E/4/1}]) – but signally failed to take them:

a) He said nothing to that effect when asking for an adjournment of the trial at the PTR.

b) 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}.

c) 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*".[139] 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.

d) Nor did he provide any such description in Wright14, served on 30 January 2024 and produced in response to the Court's order that Dr Wright identify the chain of custody in relation to the so-called White Paper LaTeX Files {E/33}.[140]

[139] {AB-A/2/68} at ¶5.

[140] 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 explains 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. That 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 has faded from attention in the present proceedings.

178. Although the Judge ordered at the PTR that metadata be obtained from Overleaf, Dr Wright dragged his feet in providing any useful metadata:

a) By January 2024 no metadata had been provided – and Dr Wright had not even provided Shoosmiths with the login credentials to his Overleaf account.[141]

b) Accordingly, COPA wrote to Overleaf directly on 3 January 2024.[142] Overleaf responded to say that they had provided information to Shoosmiths,[143] and separately wrote to Shoosmiths directing them to the Project History feature on Dr Wright's Overleaf account.[144]

c) 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.[145]

d) The Developers wrote to Overleaf on 10 January 2024 requesting that they produce the relevant files.[146] That same day, Shoosmiths wrote to advise that Overleaf had emailed to Dr Wright "*an export of the project history*" for his account.[147] In the event, Overleaf declined to provide information to the Developers.

e) 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.[148] That application prompted Shoosmiths to confirm that they would be "*in a position to provide the materials requested*" on 22 January 2024.[149]

179. On 22 January 2023, Shoosmiths finally produced four zip files, including one containing a redacted version of the data that had been supplied by Overleaf.[150] Even

[141] See Shoosmiths' letter of 8 January 2024 {AB/2/189} at ¶1.
[142] {AB/2/169}.
[143] {AB/2/171}.
[144] {AB/2/180}.
[145] {AB-A/2/187}.
[146] {AB-A/2/197}.
[147] {AB-A/2/201} at ¶18.
[148] {AB-A/1/1} and {AB-A/3/1} at ¶2.
[149] {AB-A/5/24}
[150] {AB-A/5/52}.

now it is not clear who had decided on the relevant redactions or why. The files included:

a) 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.[151]

b) 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 175 above.

180. 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*".[152] Put another way, Dr Wright had never intended to reveal the existence of the Maths (OLD) project to the Developers.

181. 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:

a) 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 and paragraph 192 above;

b) 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.

[151] {AB-A/5/58}.

[152] {M1/2/153}.

182. On Day 5 of the trial, COPA's leading counsel 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 175 above and suggested that Dr Wright was responsible for the edits shown in that document. Dr Wright admitted that he was, but then pretended 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?"*

183. Although Dr Wright's counsel then observed that issues of privilege were being traversed, Dr Wright's answers put Shoosmiths in an impossible position. It plainly was not true that Dr Wright had made the changes in demonstrations to Shoosmiths. Indeed, as noted at paragraphs 173 to 174 above, he had not even mentioned any changes in his emails to Shoosmiths enclosing the Bitcoin folder.

184. The only way forward was for there to be a waiver of privilege in relation to the Maths (OLD) and Bitcoin folders – and that was what 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

185. The Developers turn in section 3 below to the evidence that has emerged from production of the metadata underlying the White Paper LaTeX Files. However, before doing so, it is necessary to underscore four points which emerge from the above history.

186. First, Dr Wright deleted the previous folders on Overleaf from which he derived the Bitcoin folder. [153] In Shoosmiths' letter dated 20 February 2024,[154] 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.*"

187. 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

[153] The Developers had sought deleted data in their application to the Court on 16 January 2024. It has never been provided – and may no longer be available.

[154] {M1/2/210}.

the destruction of documents in this way: {L1/470/8}-{L1/470/9} and {Day15/pp114-117}.

188. When Dr Wright was challenged on the deletion of the previous files, he lied:

"*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.”

189. 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.

190. 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 dishonesty 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 (an excuse which will be explored further below):

“*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.

Q. It contained material that was directly relevant to your creation of the White Paper LaTeX files, right?

A. No, it didn't. It had where I loaded, on the 17th, files from a different directory so that I could demonstrate the changes. That is directly loaded on the 17th. As you already know, I had meetings with my solicitors demonstrating Overleaf and those files, so they had to exist before the 17th. They were there at my house."

191. And, when challenged as to his inadvertent disclosure of the Maths (OLD) project, he was typically evasive:

"*190: Q. Now, we know that it was inserted inadvertently by you because we see that at {M1/2/153}. This is a letter from Shoosmiths of 1 February 2024. 2(c):*

"We understand from our client that the content of the 'Maths (OLD)' project was inadvertently put into this folder by our client."

Do you see that?

A. That's not what it's saying. It was a copy of the -- the thing. If you're saying a redaction, that's a different thing. So I'm --

Q. The only Maths (OLD) project-related file that we received, when you produced materials to us on 22 January, was that json file that I've just taken you to?

A. I've no idea. I didn't actually open the file. KLD came out, I clicked the link, we downloaded it, I gave it to them. That's all I know.

Q. "We understand from our client that the content of the 'Maths (OLD)' project was inadvertently put into this folder by our client."

Right? It was you?

191: A. No, that's not the downloaded file. The Maths (OLD) file, what we're talking about, is Overleaf. I inadvertently copied the Bitcoin stuff into the Maths (OLD). That's what that there is describing.

Q. It's talking about the opposite. It's about content of the Maths (OLD) project inadvertently being put into something, right?

A. No, not at all. The download was done by either Stroz or KLD at my house when we clicked on the file, and they captured it.

Q. Now, if we --

A. I had no interaction with that process.

Q. If we hadn't immediately spotted the existence of the project json file in relation to the Maths (OLD) project in your Bitcoin folder, we would never have

> *known of all of the changes that you had made to the White Paper LaTeX files, would we?*
>
> *A. As I said, they were all part of the demonstration process, so all that happened was I clicked the download and all that comes across.*
>
> *Q. So when saying that you had inserted it inadvertently, what that actually means is that you had intended to suppress that file from disclosure to us, right?*
>
> *A. Not at all."*

192. Third, as contrasted with Dr Wright's failed attempt to suppress the truth of his editing of the files, 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*".

193. Fourth, Dr Wright 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.[155]

194. 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.

[155] {M/3/15}.

3. The inescapable evidence of forgery

195. The documents produced by Dr Wright on 16 February 2024 provide irrefutable evidence of his forgery of the White Paper LaTeX Files ahead of their disclosure to COPA and the Developers. In this section of these submissions, the Developers describe the process of forgery demonstrated in the animations prepared by the Developers, address Dr Wright's misleading evidence about the metadata entry in the files, describe the nature of his revisions to the text formatting, before showing how Dr Wright forged the images using Aspose and lied about that repeatedly.

a. The animations

196. 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 in the chunks.json files. The animations produced by the Developers showing the output of those alterations graphically demonstrate the process by which Dr Wright forged the White Paper LaTex Files. They are the digital equivalent of a video capturing Dr Wright in the act of forgery.

197. The animations can be found 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.

198. The following information emerges from the animations themselves:

a) 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 169above) 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. The rest of the document was a mess.

b) 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.

c) 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.[156] 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.

d) 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.[157] 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 can be advanced individually by using the right-arrow key on a keyboard).

199. 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).[158] That explanation could not have been more misleading.

200. Instead what was happening was that Dr Wright was desperately 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

[156] This can be seen in row 535 at {L21/5}.

[157] 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.

[158] See 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}.

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*".[159]

201. 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:[160]

> "*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*".

202. 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.

203. Dr Wright leant in to 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*

[159] See Field1¶27 {E/24/10} confirmed by Wright6¶4 {E/21/3}.

[160] Shoosmiths' letter dated 16 February 2024 at ¶14 {M/3/16}.

> *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.*"

204. Dr Wright's "*demonstrations*" excuse is demonstrably false. The period of the demonstrations is illustrated in the animations by changing the background colour to red. It occupies just 4 frames of the animations: see further paragraph 172 Above. 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.

205. 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

206. 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, the Developers are only concerned with the relevant command used in the White Paper LaTeX Files.

207. 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}.

208. There were three problems with that evidence.

209. 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}. In other words, Dr Wright had identified the wrong time zone in his supposed LaTeX code.[161] When presented with that error on Day 15, Dr Wright dissembled, including in response to questions from the Judge:

> “*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*

[161] He might have been in a muddle arising from the fact that the October version of the Bitcoin White Paper used at -7 hours time zone: PM3¶22 {H/20/8}.

20090324113315 minus 6, right?

A. Minus 7, in the statement, when you add summer time becomes minus 6, plus one hour, so minus 7 plus one is minus 6.

Q. Dr Wright, I perfectly well understand that if you were trying to state the relevant time at a minus seven-hour time zone that you would have put 103315, but actually, Satoshi didn't use a minus 7-hour time zone for this version of the White Paper, did he?

A. No, you're incorrect once again. Time zones. If you compile it and you change, like, that not to be that part of the year, it will be different.

Q. Dr Wright, the whole point of this section of your witness statement is for you to describe the -- is to describe what you were saying was the way in which you could configure the metadata properties, right?

A. Yes.

Q. But you put in duff metadata properties in your 11th witness statement, didn't you?

A. Again, time zones. I know you seem not to understand it on purpose, but when you have a plus one on a time zone, it changes. So time zone plus one means negative 7 plus one, which comes out on the final document as negative 6.

Q. If you're manually configuring the Bitcoin White Paper to identify -- and you're doing it in LaTeX, which Satoshi did not do, if that's what he had done, he would have had to put minus 6 to get the output that we're seeing here as the creation --

A. No, if you did it on minus 6, because of plus 1, you'll actually get negative 5. So again, it's like London time. We keep adding an hour, subtracting an hour, making people change clocks --

MR JUSTICE MELLOR: Hang on, Dr Wright. As I understand your evidence, in LaTeX, it's nothing to do with any clock, you put in these numbers.

A. Ah, but the system will still use the timestamp information. So you put in those numbers --

MR JUSTICE MELLOR: How? Which bit of this creation date field does the system change then?

A. You still have to put in the time zone information if you want it not to change naturally on the system clock, my Lord. So the system clock, when it compiles, will recognise if it's a plus one and add that and modify it. So, when you do this, unless you do something like specify GMT, or Eastern Standard Time specifically, then it's going to take the natural sort of changes and drifts.

MR JUSTICE MELLOR: Mm. I think I've previously asked you about whether there was a default or whether you had to *put all this in manually.*

A. If --

MR JUSTICE MELLOR: And I recall you answered it's manual.

A. Yes, but what I'm saying here is the difference between the negative 7 and the time zone information, my Lord. They're actually two different settings.

MR JUSTICE MELLOR: Yes, I mean, I'm afraid, Dr Wright, I simply don't understand that answer. So if you want me to understand it, you're going to have to explain precisely how this works.

A. Yes, my Lord.

All right, so what happens is you set a default, and if you put negative 7 and the --

MR JUSTICE MELLOR: Where do you set the default in LaTeX?

A. In a command.

MR JUSTICE MELLOR: In this command?

A. Yes.

MR JUSTICE MELLOR: But I thought you said earlier it's just what you type in?

A. The negative 7, though, is different to the time. The time is what you type in. Now, you also either set explicitly whether you have time zones changing for summer time, etc, or not. If you don't, then it goes to your clock time, as you're doing it.

MR JUSTICE MELLOR: Okay, but I don't understand why you would be worrying about summer time, plus 1, minus 1, etc.

A. That's why it comes out, if you put 7 in --

MR JUSTICE MELLOR: No, no, no, why wouldn't -- okay, we'll assume Satoshi is putting in the creation date.

A. Yes.

MR JUSTICE MELLOR: Why would he worry about whether it was summer time or not?

A. No, it's a time zone negative 7. At the time, I was doing a lot of work with American and Caribbean companies, so my default when I printed things was negative 7. The reason for that is, in Antigua, various other islands, a lot of gaming happens. So when I was doing, you know, documents, etc, I used standards for either South American or Caribbean time. Now, that comes with certain plus 1 minus or plus 10 type adjustments. Now --

MR JUSTICE MELLOR: Adjustments from when?

A. I'm not exactly sure when summer time does or doesn't start.

MR JUSTICE MELLOR: No, no, no, but if you're talking about Antigua and Caribbean saying plus 1/minus 1, that's adjusting relative to which time zone?

A. To the negative 7. So it will take negative 7 and add 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."

210. 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 2024, they showed a pdfcreationdate of "20090324173315": see {L21/9.1/4}.

211. The third problem with Dr Wright's evidence was that the command to which he referred <u>had</u> 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. I'm not going to waste time going into it, but it isn't.*
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.

> *Q. It's the PDF creation date that's entered in the Bitcoin project up to 24 November is not the -- doesn't include the time and time zone that you've provided there.*
>
> *A. The one that I demonstrated when they were over at my house in October had all this, and when I demonstrated, I demonstrated how that worked.*
>
> *Q. And we can see where it comes in by looking at the chunks file and this command goes in on 1 December, right?*
>
> *A. No, you can see the demonstrations I did after they'd already come out to my house.*
>
> *Q. Dr Wright, we can take that up in closing, but you're lying.*
>
> *A. No, I'm not."*

212. He was.

c. Text formatting

213. As noted at paragraph 155.e) above, 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.[162] 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 and Granath.

214. 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. He was probably inspired to promote that theory by the fact that his repeated entry of \; and spaceskip commands was an obvious sign of forgery. At that point he chose to post mysterious references to watermarking on his Slack channel,[163] 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.[164]

[162] {Day5/pp139-140}.

[163] {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/pp122-123}. The obvious inference from the timing is that it was him.

[164] See {L21/16.1/696} and {L21/16.1/698}.

215. 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.

216. 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[165] and can be seen at {L21/29.1/4}: see the command "*\spaceskip=0.3em plus 3.4em minus 0.10em*".

217. As Dr Rosendahl explained spaceskip is a somewhat arcane LaTeX command.[166] Dr Wright did not seem entirely clear what the figures in its syntax meant.[167] 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.[168]

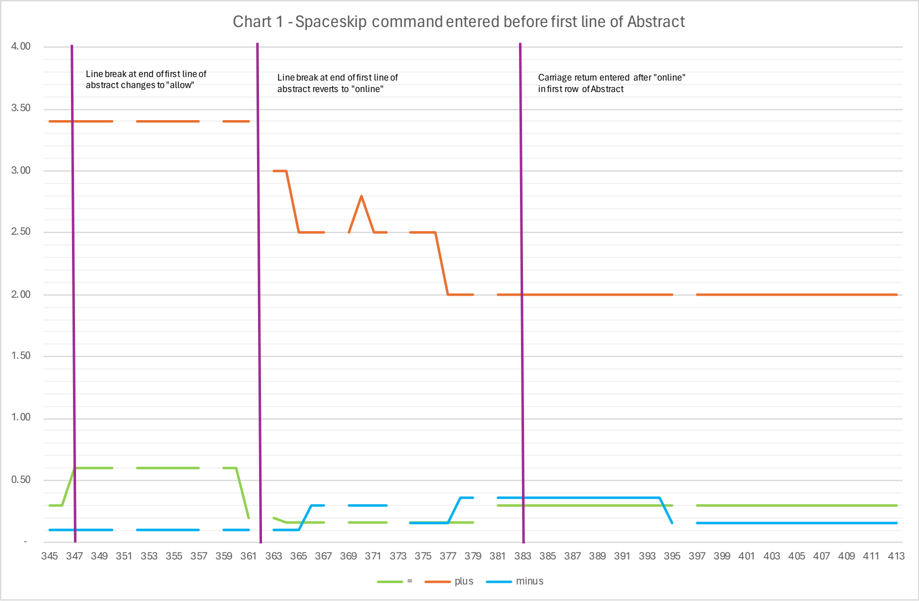
218. Having inserted the spaceskip command described above, Dr Wright spent a little over half an hour on 17 November 2023 adjusting its parameters to try to get the spacing of the first line of the abstract to fit. During the course of those changes, he mucked up the line-break at the end of the first 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}:

[165] {L21/5}.

[166] Rosendahl2¶42 {G/8/10}.

[167] Wright xx {Day15/pp131-133}.

[168] Wright xx {Day15/p133/ll.8-25}.



219. 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}*".[169] 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.[170] The former command had set the vertical space above the abstract. The second had set the width of the abstract.

220. 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.

[169] {Day15/p136/ll.3-14}.

[170] This can be seen by carrying out the tedious exercise of examining page 4 of each of the compilations at {L21/29.1/4} to {L21/90.1/4}.

Q. Yes, but none of this is being done on one of your demonstrations to Shoosmiths?
A. This was actually part of what I was documenting at the time.
Q. How were you documenting it?
A. I had files.
Q. What files?
A. I had screenshots, etc, for some of the --
Q. Sorry, you were taking screenshots every time you made a change to your Overleaf files?
A. Some of these, yes. Not every single time, but when I was making differences. I also had other conversations even before this. Shoosmiths were at my house --
Q. I'm not interested in your discussions with Shoosmiths. What I'm going to explore is how spaceskip changes and we've seen how the first parameter changed, right?
A. Mm-hm.
Q. The second parameter was the max stretch that LaTeX would permit to that base spacing, right?
A. Yes.
Q. And it started at 3.4?
A. Mm-hm.
Q. And we can see you then reduced that in a number of stages, right?
A. Yes, to demonstrate --
Q. A minor tweak upwards we can see at around 370 or 371?
A. It's a bit more than that. You'll notice that there are three values. So it was demonstrating, like a three body problem, just how difficult it is to actually find something that matches. But you can't just, like you're suggesting, go, "Oh, I'm going to guess a value" and it's going to match --
Q. The third --
A. -- because if you do that it's going to be way, way out.
Q. The third parameter was the shrinkage parameter, right?
A. Mm-hm.
Q. And that's depicted in blue and it starts at 0.1, yes?
A. I'm not sure where it starts, but ...
Q. Well, it's -- take it from me, it's at 0.1.
A. Yeah.
Q. You then increased it to 0.3?
A. Mm-hm. Yeah.
Q. Before reducing it?
A. Yes.
Q. And then increasing it, before finalising it at 0.16?
A. Mm-hm.
Q. Now, so you had in fact at one point set the shrinkage to a level that was lower than the base spacing?
A. Yes.

Q. Which doesn't make any sense, does it?

A. That's the whole point. By doing this, I'm demonstrating just how sort of many changes can occur from a simple little tweak.

Q. You're not showing it to anybody, Dr Wright. We know the times when you're showing it to Shoosmiths. This can only be something that you're doing for yourself?

A. No, actually, it's not, because I also created documents and I also documented the changes I was doing in what they wanted.

Q. We're going to come to the documents that were produced, but standing back from this, we don't see that you were making adjustments to reintroduce known parameters from the Bitcoin White Paper, do we? That's not what you're doing?

A. No, I'm actually adjusting it to show how different it can be.

Q. What you're doing is tweaking parameters to try to get them to fit the layout of the Bitcoin White Paper, aren't you?

A. No, actually, you wouldn't do that. And what you're actually -- you're saying --

Q. It's not a question of what I would do --

140: A. Well --

Q. -- that's what you did.

A. No, I demonstrated how these changes worked. Now, what you're saying in the thing you said, it would be ridiculous, and yes, I noted so how ridiculous some of these things could end up and how different. You notice some of them, the whole structure changes just by a small change.”

221. Three points emerge from this:

a) First, Dr Wright’s answers were absurd. 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. [171]

b) 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*”.

[171] The final version of the relevant command in the White Paper LaTeX Files read “*\spaceskip=0.30em plus 2.0em minus 0.16em*”: {L21/9.1/7}.

c) 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, it is simply the smudge of Dr Wright seeking incompetently to reverse-engineer the Bitcoin White Paper.

d. The images

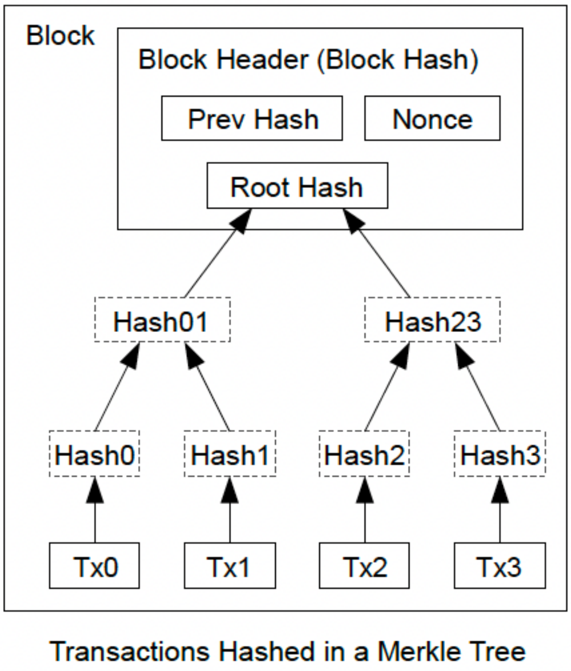
222. The Bitcoin folder disclosed by Dr Wright contains a subfolder entitled "Images" which contains the seven images from the Bitcoin White Paper in two formats. They were stored as .tex files in which specific drawing commands were entered in LaTeX code: see e.g. {L21/22.2}. In addition, they were provided as PDF files. As described at paragraph 198.d) above, Dr Wright ultimately used the PDF files in his production of the White Paper LaTeX Files.

223. 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 useful first to draw attention to that evidence, before exploring the unmistakable evidence that they were produced by Dr Wright using an online PDF-LaTeX conversion tool called Aspose.

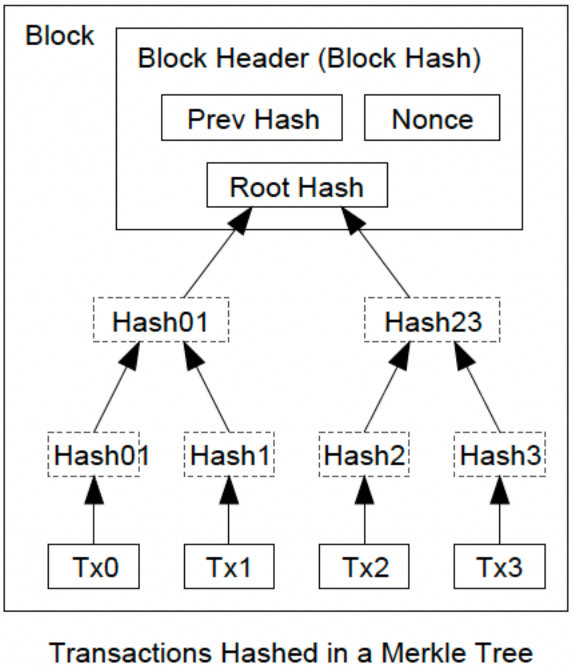
224. Before doing that, the Court may recall that Dr Wright had made a clumsy error in the production of Image 4 in his White Paper LaTeX Files.

i. Image 4

225. 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

226. That comparison reveals two parts to Dr Wright's error:

a) 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 at paragraph 245 below.

b) Second, and as a consequence of the first error, the related text overflowed its bounding box.

227. Oddly, 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, confusion, denial, dissembling and Teranode (coloured for effect):

177: Q. And do you see that, in the second row up, above "Tx0",
the text "Hash01" overflows the bounding box, right?
A. I do.
Q. And that's obviously an error, isn't it?
A. Yes, in this version.
Q. Any other comments on that?
A. Not off the top of my head, no.
Q. Isn't there something rather strikingly obvious?

A. I don't memorise every part of my diagram, no.

Q. Okay, well, let's go back to the Bitcoin White Paper. It's at {L5/26/1}. Let's go to page 4 of that {L5/26/4}. Perhaps we could put that up alongside -- yeah, sorry. So, do you see, if we look at those two things, in the original Bitcoin White Paper, which is on the left, the error isn't one of overflowing the bounding box, the mistake is that in your image, you've identified the hash of transaction 0 as "Hash01", right?

A. Yes. There's a typo in it, yes.

Q. And that is an error in your LaTeX code, right?

A. No, it's not an error in the LaTeX code, it's an error in the diagram that's been introduced at some point.

Q. It's an error in your code. If we go to {L21/11.2/7}. This is the code for image 4. Do you see, about ten lines down from the top, it says, "put(154.8, -548.3)"?

A. Yes, and I've typed in "Hash01" instead of "Hash0".

Q. Right. Because it doesn't make any sense to describe the hash of transaction 0 as Hash01, does it?

A. It does in certain other versions of the document.

Q. No, no, no.

A. Well, yes, it does in other versions. This isn't the only time I've used that.

Q. As a hash of transaction 0?

A. As I said, this diagram has been used in multiple things, so where it says "Hash01", others were 00011, etc.

Q. Oh dear. Shall we go back to {L5/26/4}. You understand how Merkle trees work, right?

A. Of course I do.

Q. Right. So the way that they work is that you take a hash of each of the transactions at the bottom, right?

A. Mm-hm.

Q. And a hash of transaction 0 is going to be hash 0, right?

A. That's one way of naming. In a binary tree structure, you could also do other structures and names. Now, in my diagram, I've noticed I've put "Hash01" there and I've got an error in one of the versions, yes.

Q. Because it doesn't make any sense to refer to the hash of transaction 0 as hash 0[1], because hash 01 is the hash of both hash 0 and hash 1, right?

A. No, not necessarily. If you have Tx01 and you have other naming, then it's going to be different. So there's an error in my diagram because I've used it in multiple things. So I know you want to sort of try and make out that I don't know anything about this stuff, despite the fact that we have -- BSV are now doing 1.1 million transactions a second on a public testnet, which is about a million times what you guys can do, but -- and actually faster than Oracle.

MR JUSTICE MELLOR: We're talking about the original White Paper.

A. This is part of the original White Paper, my Lord. I said it scaled undoubtedly. That's what I worked on doing and that's what these guys want to stop.

228. In a way, the error in Image 4 of Dr Wright's White Paper LaTeX Files, is relatively inconsequential, but Dr Wright's response to it evidenced his detachment from the real content of the Bitcoin White Paper and set the scene for his absurd written evidence about the images in the White Paper LaTeX Files.

ii. Dr Wright's written evidence about the images

229. 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).*"[172] That point was emphasised at paragraph 57(2) of Dr Wright's skeleton argument for the PTR {R/2/20}.

230. Dr Wright warmed to that theme in his eleventh witness statement. 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}).

[172] Field1¶30 {E/24/10}, confirmed at Wright6¶4 {E/21/3}.

"*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})

231. The Developers strongly suspect 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.[173] 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.[174] The Developers proposed code to enable Stroz Friedberg to check that text for content from Dr Wright's witness statement.[175] Shoosmiths responded to suggest that they "*understood*" that those checks had not resulted in any findings suggesting the use of ChatGPT,[176] but declined to respond to a request for clarification of what that meant (in particular, whether there had been any hits).[177] Thus, contrary to the evidence of Dr Wright,[178] he has not provided his ChatGPT data to COPA or the Developers.

232. 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})

[173] {M1/2/133}.

[174] See Shoosmiths' letter at {M1/2/149}.

[175] See Macfarlanes' letter at {M1/1/151}.

[176] See Shoosmiths' letter 1t {M1/2/161}.

[177] See Macfarlanes' letter at {M1/1/162}.

[178] {Day15/p85/ll.12-17}.

"*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

233. Aspose is an online tool that converts PDF files to LaTeX. It encodes images using TikZ.[179] 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,[180] rather than in the manner described by Dr Wright. Mr Rosendahl was not able to confirm that point conclusively at the time of that report. The conclusive evidence only emerged when Dr Wright revealed the underlying files from his Maths (OLD) and Bitcoin folders.

(a) The Aspose blob

234. 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").[181]

235. 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. Each letter of every word in the Bitcoin White Paper is placed individually on the page.

236. 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

[179] Rosendahl1¶196 {G/7/60}.

[180] Rosendahl1¶201 {G/7/61}.

[181] See the chunks.json file from Maths (OLD) at {L21/16.1/48}.

{L21/16.1/59}. Unfortunately for him, however, Overleaf had not removed the blob when the snapshot of Maths (OLD) was taken.

237. When cross-examined on Day 5, Dr Wright mentioned *en passant* that he had run Aspose and had a look at the output.[182] When he returned to give evidence on Day 15, Dr Wright confirmed that the Aspose blob was "*one of the test files I did*".[183] 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*
> *good forgery of the Bitcoin White Paper, would it?*
> *A. A horrible one.*
> *Q. Because no sane person would individually place letters*
> *205: in a word in this way when composing a LaTeX file from*
> *scratch, right?*
> *A. More than that. It also -- the way that it draws lines,*
> *and all sorts of things, are crazy.*
> *Q. And indeed, if we look here, we can see that the letters*
> *are placed at what seem to be nanometric levels of*
> *accuracy, right?*
> *A. Yes.*
> *Q. Which -- four decimal places of accuracy, some of them?*
> *A. Yes.*
> *Q. Five decimal places. So that is --*
> *A. That's correct.*
> *Q. That is probably 0.0035 nanometres, and that is an*
> *insane level of accuracy, so insane that it's obviously*
> *ridiculous, right?*
> *A. Completely ridiculous, yes.*
> *Q. So it would scream out forgery?*
> *A. Sorry?*
> *Q. It would scream out as a forgery?*
> *A. It would scream that someone's used some sort of wacky*
> *tool to do something."*

238. 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:

[182] {Day5/p152/ll.6-10}.
[183] {Day5/p203/l.13}.

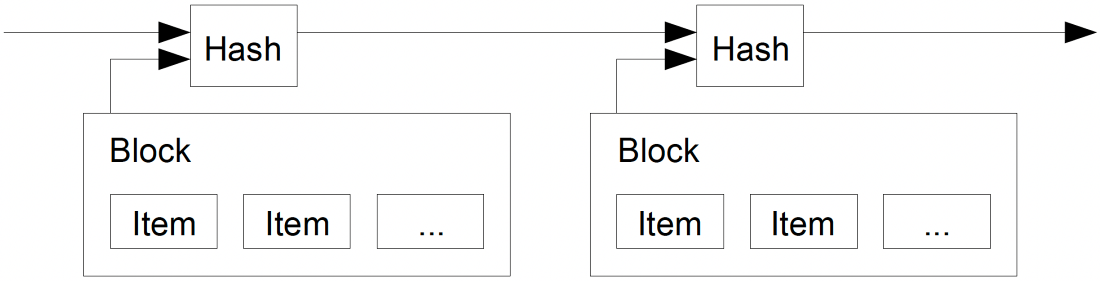


Image 2 from Bitcoin White Paper {L5/26/2}

239. There are certain anomalies with the coding of Image 2 in the Aspose blob:

a) colours are not identified by name (*e.g.* black), they are identified by number (*e.g.* color_29791);

b) font sizes are provided to unnatural levels (*e.g.* 7.144199 instead of 7 point);

c) unusual font names are used (*e.g.* usefont{T1}{uarial}{m}{n} instead of arialmt);

d) inconsistent line thicknesses are used (e.g. 1pt and 0.1pt).

Dr Wright acknowledged, however, that it would be relatively easy to correct for these peculiarities of Aspose using a simple find and replace command.[184]

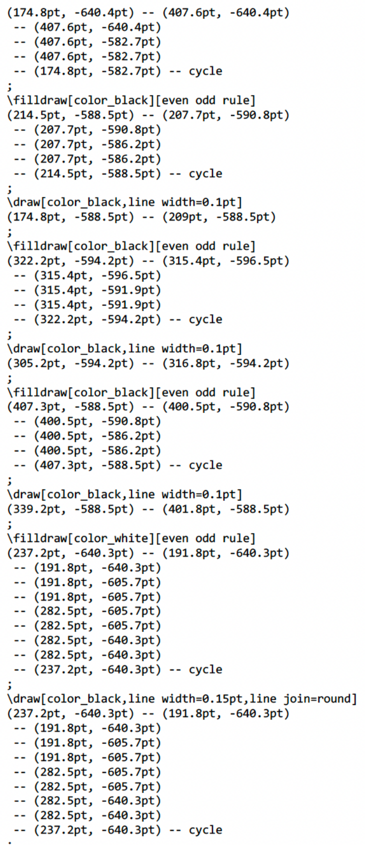
240. In any event, the coordinates of the lines from Image 2 are identified in the Aspose blob to a width of 0.1 point – a very precise level of accuracy.[185]

(b) The identical co-ordinates

241. 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 239 above):

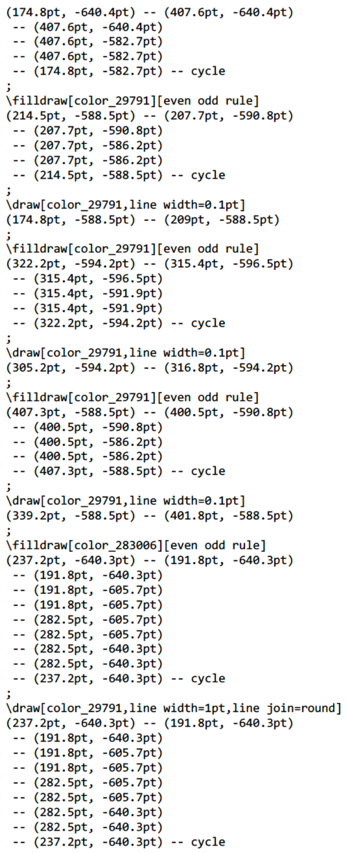
[184] {Day15/pp207-209}.

[185] 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/p206/ll.12-24}.



```
(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}

242. 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.

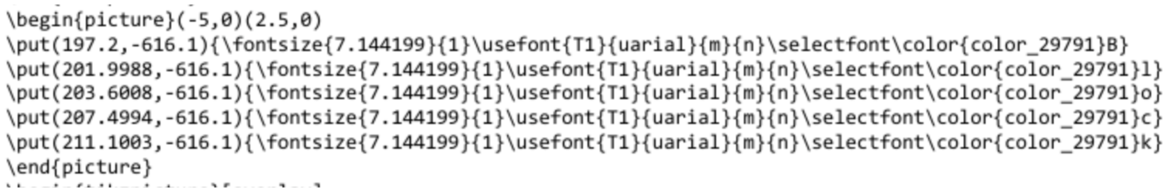
210:14 Q. I mean, just keep that document up on screen but go back
15 to page 63 {L21/18.1/64}, and then can we open up
16 {L21/22.2/1} alongside it. So {L21/22.2/1}, that is
17 the text file for image 2 from your White Paper LaTeX
18 files, Dr Wright.
19 Can we go to page 2 {L21/22.2/2}. Do you see 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

243. 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.

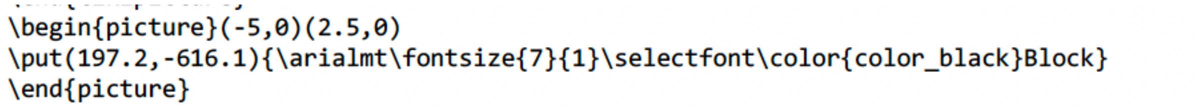
244. Thus, in the Aspose blob the letters of each word in Image 2 were purportedly set to within 0.0001 of a point, a precision equivalent to 0.035 microns, or about one thousandth of the width of a human hair.

245. 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}
```

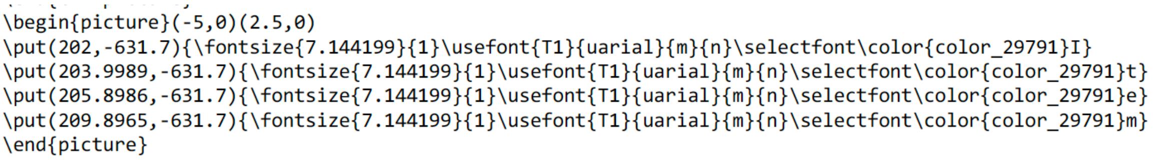
Leftmost word "Block" of Image 2 in the Dr Wright's Image2.tex file {L21/22.2/2}

246. When it was put to Dr Wright that he had achieved this outcome by manipulating the Aspose blob file, he denied it:

211: Q. If we go to page -- if we look on page 2, do you see
where, on the left-hand side -- actually on
the left-hand side page, so page {L21/18.1/63}, we can
see the word "Block", right?
A. We can.
Q. On the right-hand side, we can see the letter "B" for
"block" is there; do you see? "Put" --
A. I do.
Q. Right. And the letter B is placed exactly where it
starts in the Aspose document, so you used Aspose to
place the beginning of that word, didn't you?

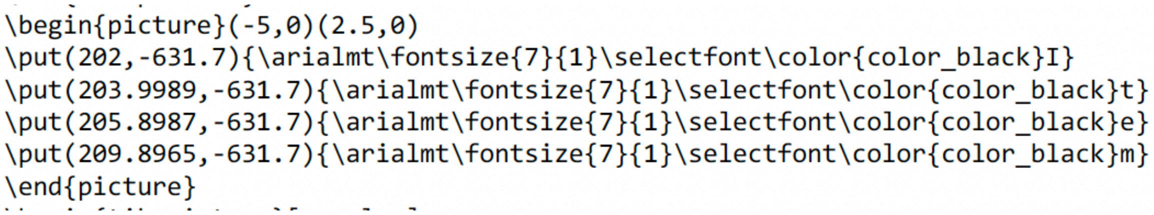
A. No, because that would actually end up producing something slightly different to mine.
Q. But you have remembered that you needed to convert the individual placing of letters into a full word, right?
A. No.
Q. Because if you had placed each letter individually, it would have screamed out that it was a forgery, right?
A. Again, it would show that an automated tool had created it. But, no, I didn't do that.

247. 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}

248. 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.

249. When his blatant 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-Hansen and Zafar Ali KC.

212: Q. If we then go to page 3 {L21/22.2/3} and go to {L21/18.1/64} on the left-hand side and let's go to the word "item". You forgot to change the word "item" from its Aspose encoding, didn't you, Dr Wright?
A. I did not.
Q. Every letter of that word has been positioned in exactly the same position as your Aspose output, right?
A. Where is this document from?
Q. The document on the right is image 2.tex from your White Paper LaTeX files.

A. Which particular?

Q. All of them, actually.

A. That's not --

Q. It doesn't change from 17 November, the earliest one that we've got.

A. That's not how mine was, so ...

Q. This is down to 0.035 of a micron, right?

A. Possibly.

Q. Which is about the length of a short segment of DNA, Dr Wright. It is tiny, right?

A. A digital file will do it, but mine -- none of mine have that error, the originals.

Q. That is your LaTeX file, Dr Wright, on the right. That is it.

A. Not necessarily. As I said, I had someone on my computer the whole time.

Q. Dr Wright, you cannot and would not have placed those letters to that level of accuracy if you were composing the Bitcoin White Paper in LaTeX from scratch.

A. No, I would, because what you do is you use a tool. So the tool is a graphic tablet, and when you draw on a graphic tablet it records, right down to the --

Q. Dr Wright, it's absurd to suppose that using a graphic tablet you're going to get exactly the same level of accuracy, down to 0.035 nanometres -- so 0.035 of a micron, actually -- get it right -- sorry.

MR JUSTICE MELLOR: A schoolboy error.

MR GUNNING: Down to 0.035 of a micron, using your tablet.

A. No, actually, the other way round. What you're saying is if you take a digital document and then analyse it. But what I suspect, if this in my Overleaf, unfortunately, Mr Ager-Hanssen already demonstrated that he had access to all my things.

Q. That's not going to do either, because the syntax of the code for your images is identical to the syntax of this Aspose output, right?

A. It's similar in parts, yes.

Q. Every line break in the code is in the same place, every command is in the same order, every line is in the same order. You used Aspose, Dr Wright.

A. No, I did not. What I had done before this is I'd said how important this was to Mr Ager-Hanssen and Ali Zafar.

(d) Conclusions

250. Dr Wright cannot plausibly blame Mr Ager-Hansen 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 paragraphs 230 to 232 above.

251. 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[186]	{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}

252. In short, 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 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

253. Finally, it is necessary to mention Mr Rosendahl's evidence on Dr Wright's White Paper LaTeX Files.

254. 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

[186] The words "Verify" and "Sign" in Image 1 were 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 infer that is why he replaced the .tex files with pdf images as described at footnote 157 above.

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*".

255. It was suggested during the cross-examination of Mr Rosendahl[187] that the Court should understand that to mean that:

a) Dr Wright used LaTeX with both Windows and Linux.

b) When using Windows, he used MiKTeX as the TeX distribution on Windows.

c) When using Linux, he used TeX Live as the TeX distribution as an alternative to MikTeX.

256. 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. <u>fontspec</u>

257. Dr Wright's White Paper LaTeX Files purport to call on a package entitled "*fontspec*"[188] to set custom fonts.

258. Dr Wright contended that he had compiled the Bitcoin White Paper in LuaLaTeX.[189] As Mr Rosendahl noted, fontspec did not work with LuaTeX in March 2009 when Dr Wright had supposedly compiled the Bitcoin White Paper from the White Paper LaTeX Files.[190]

[187] {Day17/pp26-27}.

[188] See *e.g.* {L21/9.1/2}

[189] Wright8¶32-35 {E/23/13}, Wright8¶70-73 {E/23/20}, Wright xx {Day5/pp143-146} and Rosendahl xx {Day17/p31/ll.12-13}.

[190] Rosendahl1¶124 {G/7/43}.

259. 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.[191] 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

260. 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.[192] That option hides the fact that links within the document are hyperlinks, by displaying them without underlining.[193] Mr Rosendahl explained that the "hidelinks" option was only added to the hyperref package in 2010 (*i.e.* after the Bitcoin White Paper). [194]

iii. unicode-math

261. 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.[195]

262. 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.[196]

[191] Rosendahl1¶126 {G/7/44}.

[192] See *e.g.* {L21/9.1/4}

[193] Rosendahl1¶130 {G/7/45}.

[194] Rosendahl1¶130 {G/7/45}.

[195] Rosendahl1¶134 {G/7/46}.

[196] Rosendahl1¶136 {G/7/46}.

263. 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*".[197] In re-examination, Mr Rosendahl confirmed that this would have taken "*a matter of weeks, for someone with the technical knowledge*".[198]

264. That obviously did not happen:

a) Dr Wright has not produced a single document evidencing any private work on the source code for the unicode-math package;

b) Dr Wright plainly lacked the capability to develop any such source code. The Court will recall 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/p132/ll.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.

c) The unicode-math packages 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.[199] 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*

265. 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.[200]

[197] {Day17/p30/ll.22-24}.

[198] {Day17/p35/ll.15-16}.

[199] 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}.

[200] Rosendahl1¶139-140 {G/7/47}.

266. 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 198.d) above.[201]

267. His 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

268. 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.[202]

269. The White Paper LaTeX Files make use of the arrows.meta library in TikZ.[203] That library was only released in September 2013.[204] Any file that loaded the arrows.meta library could not have been created in 2009.[205]

vi. luacode

270. The White Paper LaTeX Files purport to use a package called "*luacode*".[206] That package defines a few convenience functions to make it easier to use the Lua language from within LuaTeX.[207] However, the package was not issued until November 2010,[208] and so cannot have been used in the creation of the Bitcoin White Paper.

[201] 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.

[202] Rosendahl1¶143 {G/7/47}.

[203] {L21/9.1/3}.

[204] Rosendahl1¶145 {G/7/48}.

[205] Rosendahl1¶146 {G/7/48}.

[206] {L21/9.1/4}.

[207] Rosendahl1¶150 {G/7/48}.

[208] Rosendahl1¶150 {G/7/48}.

f. Summary

271. Dr Wright's blundering 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 blatant 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.

272. However, 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. His application was a fraud on the Court and a fraud on COPA and the Developers.[209]

273. Moreover, 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.

4. The truth

274. In the final reckoning, it is Dr Wright's ignorance of the way in which the Bitcoin White Paper was produced – and his need, based on that ignorance, to forge the White Paper LaTeX Files – that is dispositive of any attempt by him to claim to be Satoshi Nakamoto.

275. However, 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.

[209] The court will remember 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.

276. 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.[210] Even leaving aside the "aesthetic" considerations to which reference was made in cross-examination,[211] 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:

a) 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.[212] If the PDF had been generated using a TeX engine, the 6-letter designations would have been chosen randomly.[213] In the Bitcoin White Paper, they are chosen in a predictable manner (e.g. BAAAAA, CAAAAA etc).[214] That is consistent with how fonts are labelled when converting to PDF within OpenOffice. [215]

b) 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.[216]

c) The page content stream of the Bitcoin White Paper involves individual characters being written into the PDF file one-by-one.[217] 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).[218]

d) 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.[219]

[210] Lynch1¶120 {I/5/35}.

[211] {Day17/pp10-14}.

[212] See the first column of Figure 2.1 at {G/7/12}.

[213] Rosendahl1¶47 {G/7/16}.

[214] Rosendahl1¶47 {G/7/16}.

[215] Rosendahl1¶48 {G/7/16}.

[216] Rosendahl1¶49-50 {G/7/17}.

[217] Rosendahl1¶52-53 {G/7/18} and Figure 2.5 at {G/7/18}.

[218] Rosendahl1¶53-55 {G/7/19} and Figure 2.6 at {G/7/18}.

[219] Rosendahl1¶60 {G/7/19}.

e) 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.[220] The coding would be different if a TeX engine had been used.[221]

277. In short, the Bitcoin White Paper was produced by Satoshi Nakamoto in OpenOffice 2.4 and exported as a PDF. 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.

D. Reliance documents and forgery

278. Given that Dr Wright is not Satoshi Nakamoto, documents that purport to show Dr Wright in the role of Satoshi Nakamoto will be forgeries. And so has proved to be the case.

279. Dr Wright was (not for the first time) provided with the opportunity in these proceedings to adduce documentary evidence to establish that he was Satoshi Nakamoto ("**the Reliance Documents**"). None of the Reliance Documents that he put forward that could conceivably support his claim to that identity are authentic or reliable:[222] and ultimately Dr Wright appears to have disclaimed the reliability of his documents' metadata, which deprives them of any material probative value.

280. The Developers understand that COPA will address the allegations of forgery in greater detail in their closing and so limit this section of these submissions to (a) a description of the background to Dr Wright's reliance documents (b) two particular categories of document (the MYOB documents and the Tulip Trading documents) that are of particular pertinence to the parallel proceedings brought by Dr Wright against the Developers and (c) an update to the schedule at paragraph 140 of their opening.[223]

[220] Rosendahl1¶62-63 {G/7/22} and Figure 2.12 {G/7/23}.

[221] Rosendahl1¶64 and Figure 2.11 {G/7/23}.

[222] Reliance Documents that are not forged or inauthentic do not corroborate his claim to be Satoshi Nakamoto.

[223] {R/13/60}.

1. The Reliance Documents

281. On 2 September 2022, at the CCMC in the COPA claim, Dr Wright was ordered to provide to COPA a list of the 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.[224] He provided that list on 4 April 2023.[225] That process ought to have placed Dr Wright on the front foot in the COPA claim. Instead, ever since his list of Reliance Documents was provided Dr Wright's case has been in retreat. In this section of these submissions, the Developers identify the history of Dr Wright's Reliance Document disclosure, before turning to the back-pedalling that was experienced in these proceedings.

a. Reliance documents generally

282. The present proceedings are not the first occasion upon which Dr Wright has been afforded an opportunity to identify the documents that might make good his claim to be Satoshi. It is the third.

283. Dr Wright was first directed to identify the documents upon which he primarily relied in relation to the factual issue of whether or not he is Satoshi Nakamoto on 30 July 2020 in the libel proceedings that he brought against Peter McCormack.[226] In the event, Mr McCormack lacked the funds to defend Dr Wright's claim and so withdrew his defence of truth and public interest.

284. There was no equivalent Order in the Kleiman proceedings, because the claim there was predicated upon Dr Wright being one of the people that had contributed to the creation of Bitcoin. Nevertheless, over 40 of Dr Wright's documents were alleged to be forgeries by Dr Edman of Berkeley Research Group – and the closing submissions made on behalf of Dr Wright appeared to confirm that many of those documents had indeed been forged by Dr Wright: see paragraphs 105-110 of the Developers' opening skeleton {R/13/45}.

[224] {B/7/2}.

[225] {K/5/1}.

[226] See paragraph (2) at {L17/18/2}.

285. In parallel with the Kleiman proceedings, Dr Wright was asked in the Granath proceedings in Norway whether he possessed or could access evidence to prove his claim to be Satoshi. Wikborg Rein on Dr Wright's behalf presented 71 documents on 27 August 2021 which were said to "*substantiate that Craig Wright is Satoshi Nakamoto*".[227] Many of those documents were identified as forgeries by KPMG in a report dated 12 December 2021.

286. In theory, if his claim was a good one, by the time Dr Wright came to nominate his Reliance Documents in the present proceedings he should have had available a track-record of reliable documents that he could bring to bear in support of his claim. In reality, Dr Wright faced an ever-decreasing pool of forgeries to which he could turn.

287. Indeed, on Day 4 of the present proceedings, Dr Wright first attempted to disclaim reliance on his Granath documents, by making the bizarre suggestion that the documents were nominated by him to show that others had been manipulating his documents:[228]

> *"91: 25 A. No, there's no reliance documents in the Norway Court.*
> *92: 1 What this was was a demonstration, like, as it says,*
> *2 documents from other court cases. So, basically, as*
> *3 with the other court case, this is a demonstration of*
> *4 people editing files basically to manipulate things and*
> *5 show that they're part of my history. So, when you're*
> *6 talking about this as a reliance document, the reason*
> *7 I would rely on it is to demonstrate that there are*
> *8 forgeries occurring, that simple things that I could*
> *9 rebuild are being altered to make it look like I'm*
> *10 incompetent, and that happened multiple times."*

288. Dr Wright even tried to claim (patently untruthfully) that the Granath proceedings were not about his identity as Satoshi Nakamoto:[229]

> *"93: 14 MR JUSTICE MELLOR: Dr Wright, can I just ask. If these 71*
> *15 documents were not being presented to substantiate that*
> *16 you were Satoshi in the Norwegian proceedings, what were*
> *17 they being presented for?*
> *18 A. Actually, the first lawyers I had in the Norwegian*
> *19 proceedings went down a complete different path as*
> *20 the way I wanted, which is why I dismissed them. What*

[227] {L17/202/8}.

[228] {Day4/p91/ll.25} – {Day4/p92/ll.10}

[229] {Day4/p93/ll.14} – {Day4/p94/ll.2}.

> *21 I wanted to do and what happened were two different*
> *22 things. They didn't want to bring a case about being*
> *23 Satoshi, and rather wanted to make it about human right*
> *24 violations and hate crime on Twitter. The incitement*
> *25 aspect was where they put things. So, I didn't actually*
> *94: 1 want a Twitter hate case, but that's what I ended up*
> *2 with."*

289. Moreover, the bleak position facing Dr Wright following his emergence from the judgment against him in the Granath proceedings was worsened when the Reliance Documents in the present proceedings fell for consideration by Mr Madden and Dr Placks. In his first report, dated 1 September 2023, Mr Madden identified a catalogue of forgeries amongst both Dr Wright's Reliance Documents and the remaining disclosure. Dr Placks reached similar conclusions in relation to many of the documents in his first report on 23 October 2023.

290. That prompted the sequence of events that led to Dr Wright's production of a further 97 documents (supposedly derived from a BDO Image that was presented as a form of time capsule) and the White Paper LaTeX Files, that is described in the Developers' written opening at Section E.2 {R/13/54} and that led to the application to adjourn the trial at the PTR.

291. As the Developers said at the PTR, having adduced forged and/or falsified documents as his Reliance Documents to show that he was Satoshi Nakamoto, Dr Wright should not have been permitted to rely on further documents to dig himself out of that hole.[230] But in circumstances where Dr Wright swore blind that the documents were reliable and authentic, the Court had little alternative but to accede to their admission.

292. Needless to say it swiftly emerged that the BDO Image had itself been forged – as had the White Paper LaTeX Files, the latter in the manner set out at Section C above.

[230] Developers' Skeleton for PTR at ¶21 {R/3/8}.

b. Dr Wright's jettisoning of the Reliance Documents

293. Dr Wright's case on the Reliance Documents in the present proceedings has had three characteristic features. First, a jettisoning by him of his experts. Second, a retreat into general and theoretical justifications of the spurious metadata in his documents. Finally, as a result of his first and second points, a jettisoning of reliance on the metadata of his documents.

i. Farewell Dr Placks and Mr Lynch

294. Dr Placks is an experienced digital forensic practitioner, who had led the Digital Forensics teams at Deloitte LLP and Ernst & Young LLP. He holds a B.Sc. and Ph.D. in Computer Science from the University of Durham (not, so far as the Developers are aware, psychology as Dr Wright wrongly alleged)[231] and has held CCE and EnCE qualifications. His first expert report, served on 23 October 2023, fairly identified a number of concerns with Dr Wright's Reliance Documents. On 8 December 2023 he reached extensive agreement with Mr Madden as to documents that had manipulated timestamps or were otherwise unreliable.

295. At the PTR, the Court was told that Dr Placks was struggling with the workload arising from the vast amount of material that Mr Madden had had to consider.[232] That burden was said to justify alone the need for an adjournment – and so Dr Wright asked also to appoint Stroz Friedberg.[233]

296. Mr Lynch of Stroz Friedberg was instructed to focus on the BDO Image and the White Paper LaTeX files. He is also a very experienced expert in matters of digital forensics and he worked with a team of examiners whose certification by EnCase, GIAC and CREST he set out at some length.[234]

[231] {Day2/p128/ll.15-16}.

[232] {PTR/pp36-37}.

[233] {PTR/pp177-178}.

[234] Lynch1¶7 {I/5/4}.

297. Dr Placks and Mr Lynch issued further expert reports on 18 January 2024. They concluded that there was further widespread forgery, including of the BDO Image and other Reliance Documents and nominated forgeries. They reached extensive agreement to this effect with Mr Madden on 22 January 2024.[235]

298. This appears to have infuriated Dr Wright, who promptly cut them loose, accusing them of incompetence and lacking independence.[236] Neither expert was called to give evidence, but:

a) COPA and the Developers are permitted to refer to and rely upon their expert reports (CPR Part 35.11) and the agreement reached between the experts.

b) The Court might note that neither Dr Placks nor Mr Lynch has withdrawn from the case pursuant to ¶27 of the Guidance for the Instruction of Experts.[237] That being so, it can be assumed that there was no conflict of interest requiring them to withdraw.

c) The Court can draw adverse inferences from Dr Wright's failure to call Placks and Lynch – and should attach little or no weight to the contrary views of Dr Wright.

ii. Dr Wright's explanations

299. In the absence of any expert evidence, Dr Wright cast himself as the expert and sought to justify the anomalous nature or content of his documents on the basis of his supposedly complex computer environment.

300. Dr Wright's evidence in this respect was predominantly focussed on two characteristics of his supposed technical setup that it is convenient to take in turn, namely xcopy and Citrix.

301. Before turning to those, however, it is important to recall that on 23 June 2023 COPA served a request for further information, including about the operating systems Dr Wright used in relation to the documents in his DRD. Dr Wright's response, served

[235] {Q/4} and PQ/6}.

[236] {Day2/p128/ll.4-24} and {Day3/pp1-7}.

[237] See White Book Vol. 1 ¶35EG.7, p1153.

on 11 September 2023 (10 days after Mr Madden's report) was that the operating systems that he used were irrelevant {A/13/23}.

(a) *xcopy*

302. Xcopy is a file copying utility in Windows. Dr Wright suggested in Wright8¶9 {E/23/5} that he might have used the utility to copy file between servers and at Wright8¶42 {E/23/16} suggested that he had used it to copy between virtual machines. At Wright9 AxA¶2.2(a) {E/26/35}, he suggested that its use might have accounted for apparent anomalies in his documents – and suggested at AxA¶2.2-2.9 {E/26/37} that it could result in "*unusual file times where the create time is after the modified date*".

The Reliance Documents/nominated forgeries

303. At Wright11 AxB, Dr Wright appeared to rely on the use of xcopy for the purpose of explaining metadata in ID_000254 (Wright11 AxB¶7.20 {CSW/2/29}), ID_000396 (Wright11 AxB¶11.21-11.23 {CSW/2/42} – see too {Day2/p127/l.24}) and ID_000550 (Wright11 AxB¶14.3). In his oral evidence, Dr Wright also referred to xcopy in connection with ID_000199 {Day3/p76/l.2} ID_000258 {Day3/p26/ll.14-15}) and ID_004011 {Day4/p17/l.11}}.

304. Dr Placks considered the use of xcopy in his second report in connection with ID_000739 (Bitcoin.exe) (see Placks2¶8.05 {I/6/13}) and ID_000848 (debug.log) (see Placks2¶9.05 {I/6/15}}. He noted that xcopy "*can allow the user to exercise control over the OS (external) timestamps that are updated during a copy operation which can lead to apparent inconsistencies between OS Created, Modified and Accessed timestamps (as opposed to internal timestamps which would remain unaffected by these tools).*"

305. Mr Madden confirmed in cross-examination that the typical footprint of xcopy was that the creation date of a document appears to post-date the last modified date {Day16/p45/ll.9-15}. It was suggested to him that if a computer system had been

configured to disable the updating of its last accessed time metadata then, were xcopy used, its use would not result in an update to the last accessed file timestamp on the file. Mr Madden confirmed that this would be true of the source file (i.e. the file of which the copy was being made), but that the destination file would have a new timestamp {Day16/p46/ll.11-16}.

306. But none of this is to the point.

a) The anomalies in the relevant documents are not related to apparently conflicting created and last file timestamp modified dates[238] – and they are certainly not limited to that.

b) Importantly, Xcopy affects external file timestamps, not any internal properties.[239] It is a feature of Dr Wright's evidence that he conflates these two sources of metadata, whereas Dr Placks and Mr Madden had been careful to focus predominantly on the documents' internal properties.[240]

c) COPA has not presented and Dr. Wright has not nominated any documents with unreal edit durations in his disclosure that lack other indicators of forgery, as would be expected if fantastical edit durations were a true artifact of his environment.

d) The fact that there are theoretical ways that documents might end up with long edit times without forgery does not change the fact that forgery is the most probable reason for them. Thus, Dr Placks and Mr Madden were able to agree, following discussion of Dr Wright's technical infrastructure, that the information that he had supplied did not change any of their conclusions: (JS¶8.c {Q/4/6}).

[238] In relation to ID_000254 just one of COPA's points is an inconsistency between its creation and last accessed date and for ID_000258 and ID_000396 they rely (amongst many other things) upon the period of editing. And ID_000550 is the document containing reference to CheckBlockHeader, Bitcoin Core and UTXO that contains hidden, embedded text from an article posted by Dr Wright on 2 April 2018 {H/15/1}.

[239] See Placks2¶8.05 {I/6/13}.

[240] See, for example, Madden2¶16-19 {G/3/8}.

BDO Image

307. In Wright12 he suggested that he used xcopy to create the BDO Image (Wright12¶11 {CSW/7/4}). He repeated that evidence at {Day5/p48/l.25} and relied on xcopy in relation to the anomalies in that drive at {Day5/p59/ll.13-17}, {Day5/p103/ll.21-25} and{Day15/p62/l.19}.

308. Mr Lynch explained that transaction files are system files that are generally not accessible to a user and, as such, timestamps on them would not be affected by the use of xcopy: Lynch1¶77 {I/5/21}. He went on to explain at Lynch1¶126.f {I/5/38}:

> "*Xcopy or other software to copy or manage files can be configured to reset timestamps to the time actions occurred, or to preserve timestamps when files are moved or copied. I am very familiar with those types of software and took those types of activity into account when conducting my analysis. XCopy is generally not used to copy Recycle Bin or transaction log files, and in normal usage, it cannot be used to copy those files as they are system files that are not accessible to a user. To the extent Xcopy is used to cause impact to other files and their timestamps, it does so on the resultant copy, not the original source. The BDO Image is purportedly a contemporaneous source of material, not the resulting copy of material. If data was copied from the BDO Image either before or after 31 October 2007, it would not account for the evidence presented herein. If data was copied to the BDO image before (or during) 31 October 2007, it would not account for the evidence presented herein. If data was copied to the BDO Image after 31 October 2007, it would mean that the data in the BDO Image was manipulated after 31 October 2007 (and still would not account for the timestamps of the transaction logs that show clock manipulation).*"

309. Dr Wright mischaracterised that evidence at {Day5/p60/ll.1-7} and {Day5/p104/ll9} as Mr Lynch refusing to check Xcopy. It was no such thing.

310. Mr Madden and Mr Lynch agreed that the use of xcopy, or other similar tools could not account for the manipulating and backdating artefacts identified on the BDO Image (Joint Statement¶9.f {Q/6/4}). Moreover, Mr Lynch and Mr Madden's conclusions in relation to the BDO Image are amply corroborated by the presence on that drive of documents that plainly post-date 2007. Those documents include the C++ code that was debunked by Mr Hinnant and include the image.tex files that Dr Wright had created using Aspose.

(b) Citrix

311. At Wright8¶3-7 {E/23/3}, Dr Wright contended that he used Citrix and Xen as part of his computing environment to run "*remote desktops and applications*". In Wright9 AxA¶2.2(4) {E/26/35}he explained that this enabled him "*to work from remote locations using computer virtualisation*". At Wright10, building on this theme, he said that the servers running Citrix and virtual machine-based systems were configured to be accessed across multiple systems (Wright10¶74 {E/31/16}) and implied that multiple users had access to the files in his Citrix environment and could work on documents collaboratively (Wright10¶82-88 {E/31/18}).

312. Dr Wright appeared to rely on Citrix to explain three particular characteristics of documents:

a) apparently long edit times;

b) the merger of documents; and

c) anomalies arising from template updates.

<u>Long edit times</u>

313. At Wright9 AxA¶2.12 {E/26/41}, Dr Wright contended that Citrix could provide one explanation for "*apparently long editing times*" of some documents. He explained there that:[241]

> "*if a Microsoft Word document is opened in a Citrix session and the session is then closed but the Microsoft Word document is still open and the session is left to continue before being accessed again some time later, Microsoft Word considers that the document has been edited throughout the time between sessions, resulting in an apparently long editing time whereas in fact the document may have been worked on for only a relatively short period of time.*".

314. At Wright11 AxB he seemed to rely on these Citrix-effects for the purpose of explaining anomalies identified in connection with ID_000217 (see Wright11 AxB ¶5.13 {CSW/2/19} and {Day3/p60/ll.1-19}) , ID_000258 (see Wright11 AxB ¶8.12-8.13 {CSW/2/31}) and ID_000550 (see Wright11 AxB ¶14.10 {CSW/2/53}). He also relied on it in his oral evidence in respect of ID_000462, where he suggested that this

[241] He repeated the point at Wright10¶126 {E/31/25}.

might account both for the long period without saving {Day5/p130/ll.7-11} and (incongruously) that it might explain the anachronistic formatting of equations {Day5/pp130-132}. He said a similar thing about ID_000504 at {Day3/p48/ll.3-22}.

315. It is notable that the long edit times is the most inconsequential of the oddities with those documents – and the use of Citrix is accordingly unlikely to explain the long edit time. As Mr Madden freely confirmed, as a matter of theory, leaving a document open and untouched on a virtual machine (as leaving it open on a standard desktop) could lead to it having a long edit time {Day16/pp28-30}. That would not, however, work if the server was restarted or patches or other updates were applied to it. Nor would this explanation apply if autosave was configured on the system, in which case each time the document was autosaved the file-internal modified timestamp would be updated.[242] It is noteworthy that some of the edit times are recorded in excess of a year.

Merger

316. At Wright10¶35-52 {E/31/7}, Dr Wright sought to draw attention to alleged potential consequences arising from his supposed use of symbolic linking (i.e. using a link to connect to a folder held somewhere else on his system) and the use of SAN storage infrastructure. He suggested that in a virtualised environment this could lead to data crossover or corruption, "*potentially leading to a situation where data from different files gets combined or overwritten*" (Wright10¶47(4) {E/31/11}).

317. Dr Wright seemed to rely on this supposed characteristic of Citrix/Xen to explain the embedded text in ID_000227 (Wright11 AxB¶6.12-6.18 {CSW/2/22} and {Day15/pp23-24}), ID_000077 (Wright11 AxB ¶4.11 {CSW/2/14}), ID_000396 (Wright11 AxB ¶11.4 {CSW/2/40}) and ID_000550 (Wright11 AxB ¶14.14 {CSW/2/54} and {Day5/p136/ll.12-14}).

318. Mr Madden explained at Madden4¶156 {G/6/51} why Dr Wright's evidence about symbolic links was a red-herring:

[242] {Day16/p126/ll.9-18}.

"*though I observe that Dr Wright talks a great deal about the use of symbolic links, those do not work in a way that would cause the irregularities that I have observed, particularly where I have gone to pains to make sure that my opinions are formed in view of multiple streams of analysis. In the case of symbolic links, they are simply a term for a file or record that acts as a pointer, 'alias', or 'shortcut' to another file. The actual data is contained in the file that is being pointed to, and a symbolic link just contains text that specifies the path to that file, which is often used for convenience. The presence of symbolic links does not affect how the ultimate file is handled by the operating system.*"

319. He went to explain the position concerning the supposed combination of files at Madden4¶159 {G/6/52} as follows:

"*a. The minimum storage unit assignable from a hard disk is 512bytes (for older hard drives) and 4096bytes (for newer hard drives) - called a 'sector'.*

b. On a 40GB hard disk, there would be room for over 78 million 512byte sectors.

c. If a storage error led to data from different files being blended together, it would be spliced together in chunks of at least 512bytes.

d. In data terms, 512 bytes is a great deal of information: It would be enough to store 512 text characters (within an MS Word document), or 2048 characters (if stored in hexidecimal).

e. If text data were spliced together, it would be expected to be assigned in large detectable chunks which would stand out from the rest of the document structure very clearly, because it would be out of context.

f. While in theory it is possible for documents to become corrupted if data for a sector or some sectors has been incorrectly drawn from the wrong place on a hard disk, it would result in a "Frankenstein's document". This would not be expected to result in healthy documents that could be interpreted by a reader e.g. MS Word. It would instead be likely to result in a corrupted document.

g. In my view (given the size of storage devices on computing devices) the chances are vanishingly unlikely, that a document would become corrupted in a way that led to a healthy document which did not immediately show signs of corruption - especially taking into account the number of available sectors on a hard drive, which encompasses many different types of document.

h. Going further, it would be something miraculous for such merging of unrelated data from random parts of a disk to result in not only a healthy document, but also a healthy document with sensible, legible text inside a well-defined structure.

i. Even in the case of documents such as ID_000550, (which contains extensive content from previous revisions embedded within slack portions of the file), the content in slack portions is human-readable, coherent, text which appears in precisely the same place of the file as would be expected in such circumstances.

j. It reminds me of the idea of drawing 13 cards from a shuffled deck of 52 and expecting the outcome to be a perfectly organised sequence of Clubs: However in this case it is even more unlikely, since given the size of files concerned it is not just drawing a sequence of 13 from a deck of 52, but drawing a sequence of 16-32 (data clusters to make one file) from a deck of several million - and doing that repeatedly, in each case resulting in hundreds of documents that I have examined."

320. Unsurprisingly, therefore, Dr Placks and Mr Madden agreed:

a) Content in redundant areas of files, that was not presented on their face, was likely to indicate the content of previous versions of the file. Where that content included indicators that contradict the metadata timestamps, e.g. changed tenses/references to events that had not occurred/anachronistic hyperlinks) that was an indication of backdating (Joint Statement1¶8.c {Q/2/3}).

b) The possibility of data recovery tools or a misconfigured SAN being responsible for the splicing of different documents resulting in the collection of functioning documents (as was the case here) was highly unlikely and would result in recognisable indicators of corruption in discrete 512-byte blocks within those files (Joint Statement2¶8.b {Q/4/6}).

321. That evidence was not challenged in cross-examination[243] – and hence Dr Wright's explanation for the anomalies cannot stand. The Court will recall in particular the obviously bogus CheckBlockHeader/Bitcoin Core/UTXO content of ID_000550 which is addressed at paragraphs 66 and following above.

<u>Template anomalies</u>

322. Dr Wright suggested at Wright9¶2.15-2.18 {E/26/42} that three kinds of anomaly exhibited by some of the apparent forgeries could have been caused by the effect of "group policy settings" on Microsoft Word's "normal" template, namely anachronistic fonts,[244] anachronistic versions of MathType software[245] and anachronistic Grammarly timestamps.[246] He seemed to suggest that a system-imposed update to a Word template would lead to the application of fonts and embedding of references to new software versions as soon as a file was opened: Wright9¶2.27

[243] The only point that was put in cross-examination was that the content of ID_000077 (a document with multiple independent indicia of manipulation) could have come from a predecessor document that contained the content of the Bitcoin White Paper: {Day16/pp72-74}.

[244] See further Wright9¶2.45-2.55 {E/26/51}.

[245] See further Wright9¶2.56-2.64 {E/26/53}.

[246] See further Wright9¶2.31-2.44 {E/26/46}.

{E/26/44} and Wright9¶2.65-2.72 {E/26/55}– and that this explained the anomalies experienced in a number of documents.

323. He relied on this to explain the anomalies with ID_000199 {Day3/pp74-76}, ID_000217 (see Wright11 AxB ¶5.5-5.6 {CSW/2/17} and {Day3/pp60-61}), ID_000395 {Day3/p89/ll.8-17}, ID_000525 {Day2/pp109-115}, ID_000550 {Day2/p143/ll.1-9} and ID_04516 {Day2/pp99-100}: see too {Day3/p102/ll.10-22}.

324. In his first report, Dr Placks had noted that timestamped artefacts such as Grammarly timestamps, MathType versions and contemporary font references were strong indicators of inauthenticity.[247] He plainly held that view at the time of his second report too.[248]

325. Mr Madden explained at Madden4¶158.b that

> "*the inclusion of elements in templates does not explain the observations made in respect of Dr Wright's documents. For example, adding a Grammarly reference to a Normal template could, in theory, cause future documents (created after that date) to incorporate the same reference. However, in each case the reference would be identical, and would encode the same identical information including the same identical timestamp. That is not what I have observed. I have not observed one Grammarly timestamp being repeated across multiple later-created documents: To the contrary, I have observed many different Grammarly timestamps embedded within documents which would otherwise appear as if they were created in the past, at a time before Grammarly was first created. I have also explained in my First Report that Grammarly does not interact with documents automatically, but only when interacted with by a user's explicit command.*"

326. That evidence was explored with Mr Madden at {Day16/pp36-42}. It was suggested to him that it would be possible to configure a system so that default styles and customisations in the normal.dotm template would be automatically applied to all documents opened by a user and not only newly created documents. Mr Madden made clear that when you open a Word document you do not immediately, as you start to type, start updating the pre-existing file – updates will only be committed to the file if you save the file or have an autosave configured {Day16/pp36-37}. Indeed, the Microsoft support page presented to Mr Madden in cross examination[249] in relation to

[247] Placks1¶6.43 {I/1/17}.

[248] Placks2§25 {I/6/33}.

[249] {X/46/2}.

Normal.dotm files included the explicit note: "***Note**: Any changes that you make to Normal.dotm will be applied to documents that you create in the future*".

327. At {Day16/pp38-42} he was asked directly about Grammarly. Dr Wright had asserted that Grammarly tags could only be embedded into documents using the Grammarly Enterprise version, where multiple users could access the file simultaneously (Wright9¶2.33 {E/26/46} and {Day3/pp66-67}). The questions to Mr Madden seemed to be predicated on Dr Wright's evidence being true and the tags shown by Mr Madden at Madden1¶64 {G/1/28} having been generated by the Enterprise version. When Mr Madden confirmed that to be incorrect, since the tag had been generated by him using his standard version, the questioning moved on {Day16/pp.41-42}.

328. Mr Madden's evidence should not have been controversial. Dr Placks and Mr Madden had agreed that the use of Grammarly/MS Schemas/MathType versions or timestamps that post-dated document internal metadata was an indicator of backdating (Joint Statement1¶8.a {Q/2/3}). They confirmed too that MS Word does not behave in the manner summarised by Dr Wright in his ninth witness statement, with respect to how updating template files might result in the ingestion of post-dated artefacts into existing files (Joint Statement2¶8.a {Q/4/6}).

329. That being so, Dr Wright has no answer to these indicia of forgery. Indeed, his explanations do not begin to grapple with the observation of both (a) one Grammarly timestamp being repeated across multiple later-created documents, and (b) many Grammarly timestamps embedded with the same document.

(c) Summary

330. At the conclusion of his cross-examination, and slightly *in dolore*, it was put to Mr Madden that the anomalies he had identified with documents and files on the Samsung Drive and BDO Image can be attributed to and explained by a hacker obtaining access to Dr Wright's computer system during September 2023 using Trojan malware. This, Mr Madden confirmed, "*might be a bit of a leap*".[250] Needless to say, no corroborative

[250] {Day16/123/ll.11-16}.

evidence of any such hack has been provided by Dr Wright – and such evidence as he has given of the supposed hack is incoherent: see, for example, paragraph 394 below. Indeed, the supposed hacker seems to have specialised in manufacturing documents that were supposedly supportive of Dr Wright's claims – and that Dr Wright advanced as Reliance Documents despite knowing of the hack.

331. In respect of each of these matters, the lone voice consistently disagreeing with Mr Madden's conclusions is that of Dr Wright. Mr Madden's conclusions are not challenged by any independent expert.

iii. The state of things

332. As a result of his disintegrating technical case, both in Wright11 and during the course of his evidence, Dr Wright attempted to disavow his Reliance Documents, as well as other documents that he had disclosed, as being an untampered documentary record.

333. By Day 3, Dr Wright was saying that none of those documents have untampered metadata; they had all been edited, altered and amended: (**emphasis** added)

> *"16: 5 What I need to clarify , though, is ,* ***you seem to be***
> ***6 implying that my case is about proving metadata, or that***
> ***7 these are reliance because of metadata.*** *I'm going to*
> *8 very simply say, I put these in in support of what I do,*
> *9 the research I do. These documents are maintained on*
> *10 corporate servers . None of the ones you have have come*
> *11 from me directly; they've been taken from staff laptops*
> *12 and images, all of which were given over when I sold*
> *13 IP to nChain in 2015. So, while you're saying this ,*
> *14 the thing to remember is, I never set up a time capsule,*
> *15 nor said that I did. What I said was I have files that*
> *16 I give to my staff members. I do that so that they can*
> *17 take my ideas. The way that I work is, I create*
> *18 the research, I have an idea. That idea is then fleshed*
> *19 out. Sometimes, when I say "I created a document", I,*
> *20 on a voice recorder, speak to it , sometimes I write*
> *21 handwritten notes, and then my staff do this for me.*
> *22 So, what I'm basically saying, these are the origins*
> *23 of the 350 White Papers that I've completed. These are*
> *24 the origins of the 1,900 OI papers, which are original*
> *25 idea papers. These are the origins of*
> *17: 1 the 1,040- something granted patents that I've created.*
> *2 These are the origins of the 4,000 plus filed patents*

that are now public and the other ones that are in the 18-month, as my Lord will know, secret period where we can change them.

So, what I’m saying is, this is not a time capsule and I’m not saying it was and I never claimed that.

Q. Dr Wright, we agreed yesterday that the court had ordered you to nominate those documents on which you primarily relied in support of your claim to be Satoshi, yes?

A. Yes.

Q. You’re aware that this, among many others, featured in that list ?

A. I am.

Q. And you’re aware that this, like many others in that list , contain metadata dating it to before the creation, or certainly the release of the Bitcoin System?

A. Yes, I am.

Q. And you’re aware, aren’t you, that your solicitors on your behalf said nothing to suggest that the metadata should be expected to be inaccurate, or that the documents had in fact been subject to alteration, deliberate and accidental, for many years since their creation?

18: “A. Well, actually , if you check Relativity and other platforms that you have access to, what you’ll see is the majority of these come from either corporate servers or staff laptops; they don’t come from me. ***There are very few documents, apart from the later ones, that came from me directly, so that was all in the chain of custody and it’s in Relativity .*** *So at no point have I ever said otherwise.*

In the Kleiman case, I explicitly said that all of these came from file servers . The QNAP server that was taken and not imaged well is - - was, when it was taken, a several hundred thousand pound rack system that was unfortunately taken with 250 terabytes worth of data that I can’t access at the moment.

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

We, last year, did 79 patents at nChain.”

“53: Q. Can you at least agree that this document in this form is not authentic to 2008?

A. None of them are from 2008, if you’re going to look at it that way, because they have all been accessed and all used.

> *Q. So would you accept, on the basis of what you've just said, that none of your primary reliance documents are authentic to their stated dates where they're 2008?*
> *A. No, I would not. Again, you're - -*
> *Q. Well, what did the last answer mean?*
> ***A. You're misrepresenting what I said. I 've said I drafted documents in 2008. I created systems and I'm using these documents to show what I started researching before the 350 White Papers that they led to, several thousand patents, etc. These are the documents I gave to my staff members to work on that and to do that project ."***

334. In line with his taking that position, so far as the Developers have been able to tell, Dr Wright has expressly accepted that the following documents are not authentic to the dates on their face (Reliance Documents are shown in green):

a) ID_000260.[251]

b) ID_000395.[252]

c) ID_000465.[253]

d) ID_000549.[254]

e) ID_000550.[255]

f) ID_000739.[256]

g) ID_000848.[257]

h) ID_001318.[258]

i) ID_001386.[259]

j) ID_001421.[260]

k) ID_001546.[261]

l) ID_001925.[262]

[251] {L15/131/71}.

[252] {Day3/p87/l.8} – {Day3/p92/l.21}.

[253] Wright4¶98 {E/4/33} and {Day4/p74/l.6} – {Day4/p89/l.13}.

[254] {Day3/p50/l.17} – {Day3/p55/l.5}.

[255] {Day2/p132/l.20} – {Day2/p144/l.15}, {Day8/p133/l.23} –{Day8/p140/l.13}, {Day8/p196/l.6} – {Day8/p198/l.7}.

[256] {Day4/p43/l.22} – {Day4/p53/l.8} and {Day4/p90/l.1} – {Day4/p96/l.18}.

[257] {Day4/p53/l.8} – {Day4/p60/l.8}.

[258] {Day4/p68/l.25} – {Day4/p73/l.18}.

[259] {Day4/p114/l.6} – {Day4/p124/l.13}.

[260] {Day4/p127/l.12} – {Day4/p129/l.18}.

[261] {Day4/p60/l.9} – {Day4/p68/l.2}.

[262] {Day4/p124/l.14} – {Day4/p129/l.18}.

m) ID_001930.[263]

n) ID_002586.[264]

o) ID_003455.[265]

p) ID_004011.[266]

q) ID_004687.[267]

r) ID_004715.[268]

s) ID_004719.[269]

t) ID_004723.[270]

u) ID_004733.[271]

v) ID_004734.[272]

335. Even though Dr Wright falsely denies forging those (or any document), his position overall leaves any case built on his Reliance Documents in a state of collapse. On the one hand he has presented the Reliance Documents as the materials upon which he primarily relies in relation to the factual issue of whether or not he is Satoshi Nakamoto and has presented them with metadata which indicates a date of creation that is typically contemporaneous to the development of Bitcoin in 2008-2009. On the other, he now recognises that the metadata is unreliable and that the documents might have been interfered with by third parties. The contradiction between those two positions is unbridgeable.

2. The documents pertinent to the Tulip Trading claim

336. There are two particular sets of forgeries that are of direct relevance to the Tulip Trading proceedings. The first concerns accounting data. The other concerns the documents relating to the incorporation of Tulip Trading itself.

[263] {Day4/p129/l.19} – {Day4/p133/l.13}.
[264] {Day4/p68/l.3} – {Day4/p68/l.24}.
[265] {Day2/p43/l.10} – {Day2/p44/l.19}.
[266] {Day4/p9/l.6} – {Day4/p24/l.2}.
[267] {Day5/p106/l.6} – {Day5/p112/l.20}.
[268] {Day5/p79/l.24} – {Day5/p84/l.18}.
[269] {Day5/p85/l.16} – {Day5/p86/l.13}.
[270] {Day5/p91/l.10} – {Day5/p93/l.6}.
[271] {Day5/p100/l.8} – {Day5/p102/l.20}.
[272] {Day5/p95/l.9} – {Day5/p100/l.7}.

a. The MYOB documents

337. Amongst Dr Wright's reliance documents were three groups of screenshots of entries in the MYOB AccountRight accounting software ("**MYOB**"). The screenshots ("**the Reliance Screenshots**") were presented in PDF files that had an internal creation date of 9 March 2020. These documents are of particular importance, both because the conclusions in respect of them carry across to the Tulip Trading claim and because of the depth of dishonesty by Dr Wright that his attempt to excuse himself from their forgery revealed.

i. Relevance to the Tulip Trading claim

338. When Dr Wright had applied for permission to serve the Tulip Trading Ltd proceedings out of the jurisdiction he relied on MYOB records to prove his acquisition of one of the two Bitcoin addresses to which that claim related, namely 1Feex. Dr Wright had described the MYOB records as "*contemporaneous accounting records*": Wright2¶26 {S1/1.10/31}.

339. Although the Reliance Screenshots do not include any entry recording the acquisition of 1Feex, they were accompanied by a "Purchases & Payables Journal" {L5/128} which purported to include the accounting entries shown in the screenshots, together with an additional entry supposedly showing the purported purchase from WMIRK.com that had formed the basis for the claim made by Tulip Trading Ltd in respect of the 1Feex address: see Cain1¶106 {S1/1.16/47}. The subsequent native MYOB files provided by Dr Wright also include that purported acquisition.

ii. The .myox file in the Shadders email

340. In Mr Madden's first report, he identified that the Reliance Screenshots corresponded to entries in a .myox file that had been included in a .zip file (MYOB03022012.zip), that was itself contained with a .zip file (WII.zip), that had been attached to an email that Dr Wright had sent from his craig@rcjbr.org email address to s.shadders@nchain.com on 17 April 2020 ("**the Shadders email**").

341. Mr Madden observed that the .myox file in the Shadders email is the only possible document within Dr Wright's disclosure dataset from which the Reliance Screenshots could have come. The content of the Reliance Screenshots precisely matches the content of that .myox file in every respect.[273]

342. Analysis by Mr Madden of the .myox file revealed that it contained an audit trail showing that the relevant accounting entries had been made in a two-day period between 6 March and 7 March 2020, but were ascribed dates ranging from 2009 to 2011: PM7 ¶64 {H/47/34}. As such, it appeared that the Reliance Screenshots were a crude forgery made in 2020.

iii. Dr Wright's Tulip evidence

343. Given the significance of the disclosure of the Shadders email for the Tulip Trading Ltd claim, the Developers sought permission to use it in those proceedings. In response to that request, on 6 September 2023, Travers Smith, Dr Wright's then solicitors advised that "*the .myox file is merely an incomplete, not forensically extracted file from the live cloud-based MYOB accounting data, as opposed to the latter itself, downloaded by Dr Wright for a different purpose to that which you contend*" {M1/1/263}. They repeated the same explanation in a letter to Enyo (for the Developers) on 20 September 2023 {S1/1.32/20}.

344. On 18 October 2023, Dr Wright filed a witness statement in the Tulip Trading Ltd claim in which he purported to respond to the concerns that had by then been raised by the Developers about the MYOB data. Dr Wright suggested for the first time that the MYOB records that he had produced in Tulip were not contemporaneous: Wright5¶21 {S1/1.13/8}, thereby contradicting the sworn evidence in support of his application for service out.

345. Dr Wright stated that the MYOB records in the Tulip claim (which he described as "*indicative records*") "*were generated by my previous solicitors Ontier LLP and*

[273] PM42¶12.a-12.b {H/209/3}.

without the involvement of TTL or me It is therefore not TTL's case that the MYOB records represent contemporaneous records of the transaction": Wright5¶39 {S1/1.13/13}. He stated that the "*live MYOB data should … be the definitive source of information*": Wright5¶23 {S1/1.13/8}.

iv. The Placks report – the new MYOB data

346. Just a few days after Dr Wright's evidence in the Tulip Trading case, on 22 October 2023, Dr Placks served a report in which he confirmed Mr Madden's conclusion that the accounting entries in the .myox file from the Shadders email had been created between 6 March 2020 and 7 March 2020: Placks1¶9.12 {I/1/30}.

347. Dr Placks had, however, also received two emails giving him access to the live MYOB databases. The invitation emails were from Dr Wright.[274] Dr Placks describes the approach that he took to access the live MYOB data as follows:

> "*In an email that same day to Travers Smith LLP, I confirmed my approach to downloading data from these databases using my forensic workstation. That approach stated that:*
> *Once I receive the credentials, I will do the following.*
> *• Open the online company file from my AccountRight App (current Build 2023.8.1.2) on my forensic workstation.*
> *• Select the option 'File=>Back Up…' from the Menu.*
> *• I will then use the dialog to save a full copy of the database to a local evidence hard drive.*
> *• I will then exit the application.*"

348. Dr Placks followed that approach and duly downloaded two files, one for Wright International Investments Ltd, the other for Ridges R&D. Dr Placks presented the results of his analysis at Placks¶9.25 et seq {I/1/32}.

349. Dr Placks's attempt to replicate the Reliance Screenshots was not entirely successful. For example:

a) the Description of the Item in the Reliance Screenshot at {L5/150/1} and its Ship to address do not match Dr Placks' printout at {J/7/1}.

[274] Placks1¶9.18 {I/1/31}.

b) the Description of the Item in the Reliance Screenshot at {L5/471.1/1} and its Ship to address do not match Dr Placks' printout at {J/8/1}.

350. Moreover, Dr Placks noted that, when the MYOB files were worked on offline, timestamps in security logs were taken from the clock of the local computer. He noted that as a result, a company file edited offline, with spurious timestamps, could be imported/restored into the online environment with backdated timestamps. On that basis, he was unable to confirm or challenge the authenticity of any of the data that he had downloaded.[275]

351. On 8 November 2023, Bird & Bird noted that Dr Placks had referred to having access to the live databases and to the various back-up files and observed those documents had not been provided to COPA.[276] Shoosmiths responded to that request producing Dr Placks' documents and stating as follows:[277]

"*With reference to paragraph 9 of his report, Dr Placks has confirmed that Dr Wright's previous solicitors, Travers Smith, arranged access for Dr Placks to the online version of MYOB on 22 September 2023. Dr Placks on that day used freely available imaging software (FTK Imager) to create a forensic image containing the two copies of the live MYOB databases accessible through the online version of MYOB, which produced a small forensic image file of approximately 2MB ("the Forensic Image File"). Dr Placks has confirmed that his analysis was conducted using the Forensic Image File alone and that the scope of his work was conducted over those databases contained within the Forensic Image File. The Forensic Image File contains the relevant logs including transaction and security logs along with other data contained within the MYOB live company files and was locked down into a Forensic Image File (the ad1) after download.*"

352. It will be noted that there is no hint of a suggestion in that evidence that Dr Placks had somehow considered irrelevant, or incomplete or misleading material or that Mr Madden should access the live MYOB data instead.

v. Madden2 – how the new MYOB data had been falsified

353. Mr Madden considered the newly disclosed materials in Appendix PM42 to his second report on 17 November 2023 {H/209}.

[275] Placks1¶9.45-9.47 {I/1/39}.
[276] {M/2/447}.
[277] {M/2/451}.

a) He noted that MYOB recorded <u>off</u>line entries in a different format to <u>on</u>line entries. For offline entries the username was displayed as a single name, whereas for <u>on</u>line entries the format username/email address was used. Mr Madden noted that the MYOB files considered by Dr Placks included both offline and online entries: see PM42¶26-27 {H/209/8}. The entries for the period before 7 June 2023 (including those covering the period of the entries replicating the reliance documents) were all <u>off</u>line logins. Those from 7 June 2023 were online: see PM42¶29 {H/209/9}.

b) He also observed that the sessions when the MYOB files were in use were designated with a unique identifier, which enabled login and logout data to be related: see PM42¶28 {H/209/8}. Mr Madden observed anomalous login and logout data, including one session that had purportedly begun at 20:29 on 31 August 2010, but finished on 6 June 2023 at 20:35 (the time on the clock having moved forward by 6 minutes, whilst the years, months and days had leapt forward by over a decade). In the meantime numerous other sessions were shown to have been undertaken by the same user.[278]

c) He found that the versions of the MYOB software that had been available in 2009/2010 did not track the same level of information that was found in the logs that were disclosed by Dr Wright.[279] Put another way, had Dr Wright really been using MYOB in 2009/2010 there would have been much less information available to analyse that activity.

354. In addition, Mr Madden noted that MYOB used an underlying SQL database. That SQL database kept more data in relation to individual accounting entries than was directly visible through MYOB's user interface. The information extracted from the SQL database by Mr Madden:

a) enabled him to confirm:

i) the sequence of offline and online activity described at paragraph 353.a) above. [280] He was able to determine that this indicated that the offline entries had been uploaded online on 7 June 2023.[281]

[278] PM42¶31-36 {H/209/9}.

[279] PM42¶40 {H/209/11}.

[280] See PM42¶65-70{H/209/21}.

[281] See PM42¶69 {H/209/22}.

ii) the anomalous login and logout data described at paragraph 353.b) above. [282] He observed that this was redolent of the use of clock manipulation to backdate records.[283]

b) included information as to the version of MYOB AccountRight that had been used to input the data. In every case a version from 2023 had been used: see {H/212/1} and PM42¶56 {H/209/18}. The user audit logs were consistent with the backdated entries in the database having been created between the release of AccountRight versions 2023.4 and 2023.5.[284]

vi. The experts' joint statement

355. Following the service of Madden2, Dr Placks and Mr Madden were able to reach agreement on the MYOB documents on 8 December 2023 as follows:

a) The reliance screenshots had manipulated timestamps: {Q/2/9}.

b) The .myox file from the Shadders email was not authentic to the recorded accounting dates. Its journal audit logs indicated that the records were created on 6 and 7 March 2020: {Q/2/9}.

c) The new MYOB files to which Dr Placks was given access live were not authentic to the stated accounting period. They were created at some point after 10 May 2023 on computing equipment that had its clock set back to various dates between 2007 and 2013 while the database was populated with information. The records generated from those accounts did not contain any accounting records created in any period before May 2023 {Q/2/9}.

vii. Wright11

356. Dr Wright responded to these developments at Wright11¶298-312 {CSW/1/55} and Appendix B §23 {CSW/2/69} and in cross-examination.

357. Dr Wright devoted nearly the entirety of the MYOB evidence in the main body of Wright11 to a contention that live users of MYOB who either upgrade their software

[282] See PM42¶51 {H/209/16}.

[283] See PM42¶52 {H/209/16}.

[284] See PM42¶74 {H/209/23}.

or who apply automatic updates, experience updated schema, and that might explain the anomalies that are described at 354.b) above.[285]

358. So far as the .myox file in the Shadders email was concerned, he suggested at AppendixB¶¶23.8 to 23.15 {CSW/2/69} that:

a) someone had organised an extract from the online MYOB accounting system to be provided to him in a Quicken Interchange Format (QIF) file; and

b) he opened up a local version of MYOB on his computer and then on 6 and 7 March 2020 transferred entries from the QIF file into MYOB.

That same explanation is provided in Tulip Trading's Amended Reply¶99A.4.2 {S1/1.6/24}.

359. On any view, Dr Wright's evidence was an inadequate response to the clear evidence of forgery:

a) First, it overlooked the undisputed evidence that the Reliance Screenshots were derived from the .myox file in the Shadders email that Dr Wright accepts to be a recent invention. That file in the Shadders email is the only possible document within the disclosure dataset from which the reliance screenshots could have come. The content of the Reliance Screenshots precisely matches the content of that .myox file in every respect: see paragraph 341 above.

b) Second, it failed to engage with the undisputed evidence that even the new MYOB files had been created offline, before being uploaded to the MYOB live system in June 2023 – and that as a result they contained log files that would not exist in relation to data that had been entered contemporaneously: see paragraphs 353 to 354 above.

<u>viii. Initial answers in cross-examination</u>

360. In cross-examination on Day 3 (7 February 2024), Dr Wright sought to elaborate on the evidence that he had provided in Wright11:

[285] See Wright11¶303-312 {CSW/1/56}.

a) He suggested that the .myox file in the Shadders email had been produced offline so that he could make sure that no online copy of anything from Tulip Trading would go into the American case – as he feared that otherwise the supposed Tulip transactions would an "*extra opportunity for Mr Kleiman to seek money from me*".[286] That is nonsensical. The .myox file contains the 1Feex transaction: see {H/53/2}.

b) He denied that the .myox file in the Shadders email had been used to generate the Reliance Screenshots,[287] even though that file was the only match for the Reliance Screenshots.

c) He suggested that the Reliance Screenshots were produced "*as a result of Ontier downloading the software with the credentials given to them in late 2019*"[288] and in response to the following question answered as follows:

"*127:22 Q. Now, just to be clear, the findings of Mr Madden, agreed*
23 by Dr Placks, were that the entries shown on these
24 documents which we have just seen were as a result of
25 your entries on 6 and 7 March 2020. You dispute that,
128: 1 do you?
2 A. I do, because both of these -- or all of those images
3 were taken by Ontier prior to that date, so that can't
4 be true."

As emerged later (and is described below) that was a lie designed to cover up the .myox file attached the Shadders email as the source of the Reliance Screenshots.

d) He sought to explain the length of the anomalous session identified by Mr Madden as being referable to the fact that "*the companies were put into a sleep or dormant position awaiting 2020*".[289] That is incoherent on two bases. First, a computer user will not remain logged into a terminal because an associated company becomes dormant. Second, Dr Wright has wholly overlooked the fact that he was logging into and out of other sessions over the very same purported period: see paragraph 353.b) above.

e) He suggested that the schema updates (which he suggested had led to anomalous 2023 AccountRight versions being accredited to data) had also

[286] {Day3/p123/l.21}-{Day3/p124/l.2}.
[287] {Day3/p124/l.22}-{Day3/p125/l.22}.
[288] {Day3/p126/l.25}-{Day3/p127/l.2} and {Day3/p127/ll.8-10}.
[289] {Day3/p132/ll.17-19}.

somehow backfilled the log files with information that would not exist in relation to data entered in 2009.[290]

361. Dr Wright's contention (at paragraph 360.c) above) that the Reliance Screenshots had been produced by Ontier in 2019 was untenable. The Reliance Screenshots were not the only screenshots from MYOB that he had provided. He had also provided a related screenshot showing the same transactions at {L16/252/1}. Although it is obscured by the page reference on Opus, that screenshot recorded the clock time on the computer that was being used as 14:44 on 9 March 2020[291] and its related PDF file had been authored using the same creator software as the Reliance Screenshots.[292]

362. Dr Wright was taken to that evidence on Day 4 (8 February 2024) and dug into his suggestion that Ontier had prepared the Reliance Screenshots prior to the creation of the .myox file in the Shadders email:

> " *5:21 Now, bearing in mind that we'll say this can be*
> *22 further confirmed with Ontier if necessary, would you*
> *23 now accept that these screenshots were created on*
> *24 9 March 2020?*
> *25 A. No. I will accept that this other one was done. Those*
> *6: 1 or screenshots are not screenshots, they're pdfs in --*
> *2 produced. So Ontier had earlier produced a series of*
> *3 documents. They then converted those into PDF documents*
> *4 at a later date. They also reaccessed at a later date.*
> *5 So they had downloaded into a local version and they had*
> *6 taken multiple screenshots.*
> *7 Q. So you insist that those other screenshots, those other*
> *8 documents were created before 9 March 2020?*
> *9 A. Yes.*"

ix. The first Ontier intervention

363. Unfortunately for Dr Wright, Shoosmiths confirmed on 9 February 2024{M/2/1000} that Ontier had written to them the previous evening to contradict the evidence given by Dr Wright. Ontier stated:[293]

[290] {Day3/p133/ll.12-21}.

[291] PM42¶13 {H/209/4}.

[292] {H/209/5}.

[293] {X/55/1}.

> "*Dr Wright first provided this firm with log-in details for the MYOB accounting software on 9 March 2020 and we first accessed the software on that same date. We did not have access to MYOB in "late 2019" (line 8, page 2 of Bird & Bird's letter). We created a series of screenshots from that system on 9 and 10 March 2020, including screenshots that correlate with the screenshots which appear at Doc IDs: ID_004076; ID_004077; ID_004078; and ID_004079.*"

364. This was drawn to Dr Wright's attention on Day 5 (9 February 2024):

> "*44: 9 It's right, isn't it, that, as Ontier say, they were*
> *10 not provided with log-in details in late 2019, as you*
> *11 said yesterday?*
> *12 A. No, and I'm going to be instructing them to release*
> *13 information that is already in the disclosure platform,*
> *14 including 2019 emails to AlixPartners and Ontier, giving*
> *15 those access details. So, no, those emails are already*
> *16 in disclosure.*
> *17 Q. And it's correct, isn't it, that they took*
> *18 the screenshots on 9 and 10 March 2020?*
> *19 A. I wasn't involved with them taking the screenshots.*
> *20 What I do know is that they received the log-in details*
> *21 in 2019.*
> *22 Q. You were very firm yesterday that those screenshots were*
> *23 not taken as late as 9 March 2020, weren't you?*
> *24 A. I know what I was told by my solicitors at the time, and*
> *25 I also know, and I have the emails in disclosure stating*
> *45: 1 that they had access from 2019.*
> *2 Q. So you're saying that you understood from your*
> *3 solicitors that those screenshots had been taken before*
> *4 9 March 2020?*
> *5 A. That is correct.*
> *6 Q. On that basis, they were either lying to you then or*
> *7 lying to the court now; correct?*
> *8 A. I have no idea. I know most of the people at Ontier who*
> *9 were there are no longer there."*

x. The email chain forgery

365. On Sunday, 18 February 2024 at 11:39, Dr Wright emailed his wife attaching an email which purported to record an exchange between him and Simon Cohen of Ontier on 2 December 2019. Ms Watts forwarded that email to Shoosmiths at 12:56 that day {X/56/1}. The attached email (which was not brought to the attention of COPA or the Developers at that time) purported to corroborate the account that Dr Wright had provided to the Court in his oral evidence of his dealings with Ontier.

xi. Madden5

366. At 10:29 on 19 February 2024 Mr Madden issued his fifth report. It made three points:

a) First, Dr Wright's suggestion that he had exported the entries in the .myox file in the Shadders email from QIF was contradicted by the fact that each entry had clearly been separately entered – and was timed accordingly. [294] Moreover, edits had been made to those entries[295] and had the entries been made in one go, they would have appeared as a separate entry. [296]

b) Second, Dr Wright had failed to explain the anomalous sequence of logins. The sequence in which accounting entries had been made could be assessed from their Record IDs in the underlying database. Sorting the entries in that way showed entries made in 2023 sitting in the middle of entries supposedly made in 2010.[297]

c) Third, software updates in MYOB do not have the effect of changing the content of the database tables that identify the version of the software applicable at the time of a relevant accounting entry.[298]

xii. Dr Wright's second cross-examination

367. Dr Wright returned to give evidence on Day 15, 23 February 2023, and was cross-examined about the matters raised in Mr Madden's fifth report between 10:30am and 11:18am.

368. On this occasion:

a) Dr Wright sought to excuse the fabrication of the .myox files attached to the Shadders email on the footing that he was "*doing a legally privileged exercise*".[299] Dr Wright's attempt to use the cloak of legal privilege to excuse forgery echoes his approach to the White Paper LaTeX Files addressed at

[294] Madden5¶11 {G/9/6}.
[295] Madden1¶64 {H/47/34}.
[296] Madden5¶12-14 {G/9/6}.
[297] Madden5¶16-17 {G/9/6}.
[298] Madden5¶25 {G/9/9}.
[299] {Day15/p12/ll.19-25}.

paragraphs 193 and 236 above. It also suggests that Dr Wright has a tenuous grasp on the law of legal professional privilege.

b) Perhaps fortified by the email exchange referred to at paragraph 365 above (which at that point was unknown to COPA or the Developers), Dr Wright dug in on his evidence that he had provided access to MYOB to Ontier in 2019:

> "*14:23 Q. You told the court that Ontier received MYOB log-in*
> *24 details in late 2019, didn't you?*
> *25 A. I did, and I have the emails for it.*"

c) Dr Wright reiterated his evidence that he had made the accounting entries in the .myox file attached to the Shadders email from a QIF file using "*an automated process. You click a button*".[300] That is flatly contradicted by the journal entries at {H/53/1} and {H/55/1}.

d) In a pointlessly truculent series of answers, Dr Wright disputed that he had been involved in giving access to Dr Placks to the live MYOB database.[301]

e) He otherwise continued to reject Mr Madden's findings, without support either from Dr Placks or any corroborating material.

xiii. The second Ontier intervention

369. At 11:51am on 23 February 2023, about 30 minutes or so after Dr Wright had been cross-examined about his MYOB files, Shoosmiths (very sensibly) thought to check the authenticity of the email sent to them by Ms Watts with Ontier {X/57/2}. Shoosmiths asked whether Ontier could locate that email on their systems, the exact date that they were sent a link to the MYOB data and whether anyone logged in on receipt of the link.

370. Ontier's response the same day was as follows {X/57/1}:

> "*We confirm as follows:*
> *1. We have searched our systems. We can confirm that we have located the attached email which, on its face is dated 2 December 2019 and contains the same text as the email attached to your email timed 11.51. However, our attached email was in fact received on our systems on Sunday 18 February 2024, this is confirmed by the email metadata which can be reviewed by viewing the properties of our attached email. For the avoidance of doubt, we have compared the email properties of the email on our*

[300] {Day15/p16/ll.21-22}.

[301] {Day15/p21/l.6}-{Day15/p22/l.5}.

systems to those of the email attached to your 11.51am email and they substantially differ.
2. We also attach for your information an email saved on our systems from Dr Wright dated 2 December 2019 timed 15.56, which was received on that date and sent in response to the same email chain starting on that same date and which forms part of the email attached to your 11.51 email.
3. We confirm that no link to the MYOB database was received in 2019, whether from Dr Wright or any other third party and that therefore no login took place at this time. We repeat and confirm the contents of our email of 8 February 2024 in this regard.
In light of the above, we are of the view that the email attached to your 11.51 email is not genuine.
Understandably, we are keen to ensure that the Court is not misled. Please provide us with a copy of the transcript of today's proceedings and confirm by return how you intend to proceed."

xiv. The cross-examination of Mr Madden

371. Mr Madden attended for cross-examination on 26 February 2024. His cross-examination on MYOB lasted all of five minutes and occupies 3½ pages of transcript ({Day16/p80}-{Day16/p83}).

372. The only point made to Mr Madden in cross-examination was that he had not accessed Dr Wright's live MYOB system. As Mr Madden explained, the availability of that system had only been revealed in Dr Placks' report. And in any event, as he had made clear in his reports, he had set up a live MYOB system himself and checked how it operated.

373. None of Mr Madden's evidence as to the damaging content of the MYOB files produced by Dr Wright was challenged. The conclusions reached by Mr Madden that:

a) the Reliance Screenshots had been derived from the .myox file attached to the Shadders email;

b) the accounting entries shown in the Reliance Screenshots had been input in March 2020; and

c) the entries then shown in the live MYOB system to which Dr Placks had been afforded access had been input in June 2023

were not challenged.

374. Following Mr Madden's cross-examination, Dr Wright's legal team, very properly, drew the Court's attention to Ontier's correspondence and to the related email exchanges.

xv. Further evidence

375. On 28 February 2024, Mr Madden served a sixth report in which he reviewed those emails, namely:

a) the purported 2019 email to Ontier that Dr Wright had sent to his wife on 18 February 2024 ("**the Ramona version**");

b) the version of that email that had been received by Ontier on 18 February 2024 ("**the 18 Feb 2024 Received Version**"); and

c) the genuine email exchange from 2019 that Ontier had provided ("**the Ontier Version**").

376. Mr Madden was able to confirm that:

a) The nChain logo image in the Ontier Version had an embedded timestamp dating it to 2019, whereas both the Ramona Version and the 18 Feb 2024 Received Version had 2024 timestamps dating them to 18 February 2024.[302]

b) The transmission header for the Ontier Version was internally consistent and contemporaneous to 2019, The 18 Feb 2024 Received Version contained conflicting timestamps. Its header was consistent with an email being composed and sent on 18 February 2024 with the local clock backdated to 2 December 2029 (something Mr Madden had confirmed could be done).[303]

c) The ESMTPSA (Extended Simple Mail Transfer Protocol Secure Authentication) identifier in both the 18 Feb 2024 Received Version and the Ramona Version were of a length that marked the messages out as having been created later than January 2022.[304] As such they could not be authentic to 2019. Worse still, Dr Wright had manipulated the overlong ESTMPSA identifier in the Ramona Version to insert a 2019 date.[305]

[302] Madden6¶8-13 {G/11/7}.

[303] Madden6¶15-23 {G/11/8}.

[304] Madden6¶30 {G/11/12}.

[305] Madden6¶27 {G/11/12}.

377. Dr Wright responded to that evidence in a witness statement served on 29 February 2024 {E/34}. That statement appeared to contend that the Ontier Version (i.e. the email that Ontier had presented as the real email that Dr Wright had sent them in 2019) had been spoofed.[306] His basis for saying that seemed to be that the header contained an SPF indication[307] – which he suggested was precluded by the settings on his tuliptrading.net and RCJBR.org domains.[308] In addition, he suggested that it was "*not possible*" that Mr Madden had sent an email with his local clock backdated in the manner that Mr Madden was contending had occurred with the 18 Feb 2024 Revised Version.[309]

xvi. Dr Wright's last stand

378. Dr Wright returned to give evidence about the Ramona Version, the 18 Feb 2024 Received Version and the Ontier Version on 1 March 2024 (Day 19).

379. Contrary to his evidence served the day before, during his oral evidence, Dr Wright disclaimed any suggestion that the Ontier Version might have been spoofed. Instead, he acknowledged that it was a real email,[310] albeit one that he thought might have ended up in Ontier spam folder.[311] However, it emerged that the basis upon which Dr Wright was claiming that the Ontier Version might have been treated as spam, namely the settings on his tuliptrading.net and RCJBR.org domains, had been adjusted by Dr Wright within the previous week.[312] His evidence in this respect was accordingly based upon a document trail that he had recently created.

[306] Wright15¶11 {E/34/5} addressed Madden6¶17 {G/11/9}, which concerns the Ontier Version. For the allegation of spoofing: see Wright15¶16 {E/34/6}.

[307] Wright15¶9-10 {E/34/5}.

[308] Wright15¶12-13 {E/34/6}.

[309] Wright15¶15 {E/34/6}.

[310] {Day19/p14/ll.8-9}.

[311] {Day19/p36/ll.16}-{Day19/p38/l.16}.

[312] See {X/78}. Dr Wright sought to cast doubt on the form of the "." character at {X/78/3} – and to suggest that it was an asterisk: {Day19/p41/l.9}. That is not correct. The format of the "." character is the same in Wright15 at {E/34/4} and is simply a consequence of its formatting on the DNSHistory website, as Mr Madden confirmed: {Day19/p66/ll.9-20}.

380. Instead of challenging the Ontier Version, Dr Wright asserted that it was the 18 Feb 2024 Received Version that had been spoofed.[313] In support of that contention Dr Wright tumbled out a fanciful conspiracy theory in which:

a) A conspiracy was committed by someone unknown out of the "*100 people that I know of, if not more, [that] have access to all of my files now*"[314] who "*want BTC to win and me to fail and the BTC Ponzi to keep going*".[315]

b) That person sent the spoofed 18 Feb 2024 Received Version to Ontier very shortly before Dr Wright sent an email with the same content to Ms Watts, who then sent it on to Shoosmiths.[316] It is unclear how the person knew to do this at that very time, let alone how they knew that Ontier did not have the email that Dr Wright says he sent in 2019. Dr Wright suggested the person may have planted a bug in his house.[317]

c) Oddly, the email sent by that person appeared to support Dr Wright's case as to MYOB records that had been advanced by Dr Wright in his oral evidence on 9 February 2024 and which he then repeated on 23 February 2024. But Dr Wright suggested it was in fact sent to fabricate an excuse to bring Dr Wright back to Court.[318]

381. Leaving aside the absurd implausibility of this account, it suffers from two fatal shortcomings, namely that the Ramona Version (which is supposed to be the true version of the relevant email) contains:

a) the identical 18 February 2024 nChain image that appears in the 18 Feb 2024 Received Version: see Madden6¶12 {G/11/8}. As such, the Ramona version cannot be from 2019. Dr Wright sought to contend that the dating of the image was a consequence of the way Google works,[319] but the Ontier Version (i.e. the real 2019 email) does not suffer from that shortcoming – and Dr Wright's contention was not even put to Mr Madden; and

[313] {Day19/p30/ll.13-16}-{Day19/p34/l.10}.

[314] {Day19/p32/ll.20-22}.

[315] {Day19/p55/ll.18-19}.

[316] {Day19/p57/ll.3-21}. The 18 Feb 2024 Received Version has a timestamp of 11:06 on 18 February 2024 {G/11/10}. The email from Dr Wright to Ms Watts is timed at 11:39 on 18 February 2024 {X/56/1}.

[317] {Day19/p57/l.23}-{Day19/p58/l.7}.

[318] {Day19/p56/l.5-6}.

[319] {Day19/p17/ll.4-17}.

b) the same anachronistic ESTMPSA ID that afflicts the 18 Feb 2024 Received Version. Dr Wright did not dispute that,[320] but suggested that this might have been a consequence of email migration.[321] Mr Madden confirmed that an account migration could not result in that anachronism.[322]

xvii. Conclusions

382. The depth of mendacity revealed by Dr Wright's evidence in relation to the Reliance Screenshots is on a par with his dishonest evidence about the so-called White Paper LaTeX Files. Dr Wright's botched attempt to cover his tracks by faking a document trail with his former solicitors should not, however, be permitted to distract from the underlying truth, namely that the Reliance Screenshots and the related accounting data that he produced in support of his claim in relation to 1Feex are forgeries.

b. The Tulip Trading incorporation documents

383. There are two related documents amongst Dr Wright's disclosure set that have been identified as forgeries by COPA in its list of 50 forgeries (although not their Top 20) and explored in cross-examination. The documents were not identified by Dr Wright as Reliance Documents, but are pertinent to his claims in the Tulip Trading case.

384. The first is an incorporation form purportedly completed by Dr Wright on 21 July 2011 to acquire Tulip Trading Limited {L7/357}. The other is a purported invoice from Abacus Seychelles for Tulip Trading Limited which bears a date of 17 October 2014, but purports to refer only to payment for management and trust accounting {L9/214}. The story underlying both of these documents – and explaining why they are forgeries (or, at least, inauthentic) – is that Dr Wright only acquired Tulip Trading Ltd as an off-the-shelf company in October 2014. These documents were falsified to make it appear that he had acquired Tulip Trading Ltd in 2011.

[320] {Day19/p19/l.25}.

[321] {Day19/p20/ll.11-16}.

[322] {Day19/p62/ll.1-2}. It was suggested in cross-examination that Mr Madden had not tested to see whether this was the case: but no substantive basis for challenging his evidence was identified: {Day19/p91/ll.7-17}.

i. The incorporation form: ID_001930

385. ID_001930 {L7/357} purports to be an application by Dr Wright for the incorporation of a company called Tulip Trading Limited (or two other names) on 21 July 2011. The document corresponds to Dr Wright's evidence at Wright11¶292 {CSW/1/54} that he had asked Denis Mayaka to register a new company for him called Tulip Trading Ltd in 2011.

386. It is common ground between Mr Madden and Dr Placks that the incorporation form has been manipulated.[323]

a) Mr Madden explained that the document is a scanned hard copy document that has been processed in order to make the text content editable.[324] Both Mr Madden and Dr Placks noted that it includes a metadata tag indicating an 'editedScannedDoc' event on 24 November 2015 at 15:59:01 +11:00, indicating edits made to pages 3, 4 and 5.[325]

b) Using the Winking PDF analyser, Mr Madden was able to compare embedded picture items within the PDF of ID_001930 with the text that was readable on its face.[326] Inconsistency between the space occupied by the text and the underlying images revealed that edits had been made to the Ultimate Beneficial Owner, the director's name and address, the accounting records, the address for dispatch of corporate documents and the email details for the person completing the form.[327]

c) Mr Madden was also able to locate another Tulip Trading Ltd incorporation form amongst Dr Wright's disclosure, namely ID_001395 {L9/183}. That form was dated 17 October 2014[328] and had been attached to an email sent by Dr Wright to Denis Mayaka on 17 October 2014 {L9/182}. Thus, ID_001395 reveals Dr Wright applying to incorporate Tulip Trading Limited over 3 years later than he has suggested was the case.

[323] See {Q/4/4}.
[324] PM14¶148 {H/73/56}.
[325] PM14¶150-151 {H/73/57} and Placks2¶18.03 {I/6/25}.
[326] PM14¶152 {H/73/58}.
[327] PM14¶155-159 {H/73/61}.
[328] PM14¶163 {H/73/65}.

d) The text in ID_001395 matches the underlying images of ID_001930. But more importantly, ID_001395 contains a document ID <d76872058027f958e6e5d124e9416254>, which has been retained in ID_001930. Both Mr Madden and Dr Placks agree that this indicates that ID_001930 was created by editing ID_001395.[329]

e) In short, the incorporation form for Tulip Trading was actually completed and submitted by Dr Wright on 17 October 2014, but was edited by him in November 2015 to make it appear that he had applied for it to be incorporated in July 2011.

387. In cross-examination Dr Wright accepted that ID_001930 (the 2011 form) was "*doctored*"[330] – that "*the whole thing's edited*".[331] However, to escape the obvious consequences of such a finding, he suggested that ID_001395 (the 2014 form) was also doctored. Strikingly neither Mr Madden nor Dr Placks identified any indicia of doctoring of ID_001395 and Dr Wright has not provided any alternative supposedly un-doctored version of an application form to Abacus Seychelles.

388. The only reasonable conclusion is that Dr Wright edited ID_001930 in 2015 to support his (false) account that he had purchased Tulip Trading Limited in 2011. That is corroborated by the falsification of the Abacus invoices to which these submissions now turn.

ii. The Abacus invoice: ID_001421

389. ID_001421 {L9/214} purports to be an invoice (numbered 39388) from Abacus Seychelles dated 17 October 2014 for "*Management and trust accounting Seychelles company*" in respect of Tulip Trading Ltd in the sum of US$3,650.

390. It is common ground between both Mr Madden and Dr Placks that this document was also manipulated,[332] by editing an invoice of the same date and with the same

[329] PM14¶166-168 {H/73/67} and Placks2¶18.04-18.05 {I/6/25}.

[330] {Day4/p132/l.12}.

[331] {Day4/p131/l.1}.

[332] See {Q/4/4}.

reference and in the same sum that had been disclosed as ID_001397 {L9/185/1} , but which referred to "*Purchase of Seychelles 2011 shelf company*". That was clear because:

a) ID_001397 had a created and modified timestamp of 17 October 2014 at 05:27:25 BST.[333] That corresponds to the created timestamp of ID_001421, but ID_001421 had a modified timestamp of 18 October 2014 at 02:21:17 BST.[334] Thus, ID_001397 came first in time.

b) The internal PDF identifier for ID_001397 (<B2D67099F798F94AABE7A1F5679D688D>) is recorded as a prior document id within the PDF trailer for ID_001421.[335]

c) ID_001421 had Touchup_textedit tags which showed that it had been edited from a prior document.[336] Those tags are an artifact of editing a PDF using Adobe Acrobat products.[337] The changes had been made so crudely that what should have been a single line of text, was shown in ID_001421 as being comprised of two portions.[338]

391. Consistently with its timestamp, ID_001397 (the original invoice) had been sent to Dr Wright by Abacus by email dated 17 October 2014 {L9/184/1}. ID_001421 had not. Thus, ID_001421 had been prepared in an apparent attempt to cover up that in October 2014, Dr Wright was paying for the purchase of a 2011-incorporated Seychelles shelf company, that he has subsequently said he purchased in 2011.

392. In cross-examination, as with the incorporation form, although Dr Wright accepted that ID_001421 was a fake (something that he had not thought to mention when disclosing it), he also suggested that ID_001397 was a fake.[339] Unlike the incorporation form, however, Dr Wright purported to produce a "real" invoice for the purchase of Tulip Trading Limited. That "real" invoice had a peculiar provenance. It

[333] PM14¶44 {H/73/15}. Not, in fact the PDF has timestamps consistent with an Australian time zone: PM14¶50-51 {H/73/17}.

[334] PM4¶116 {H/29/37}.

[335] Placks2¶13.04 {I/6/20} and PM14¶45-46 {H/73/16}.

[336] PM4¶121 {H/29/39}.

[337] PM4¶7 {H/29/2}.

[338] PM14¶47-48 {H/73/17}.

[339] {Day4/p129/l.18}.

was sent to Dr Wright by papa.neema@gmail.com on 10 September 2023 together with some other supposed invoices.

393. Dr Wright had not thought to mention the papa.neema emails when making his application for an adjournment at the PTR. Instead, he produced them with Wright11 and sought to provide a convoluted explanation for them at Wright11¶269-297 {CSW/1/50}. Much as Denis Mayaka had miraculously come to Dr Wright's assistance in the Kleiman proceedings by producing the (fake) CSW list at the eleventh hour in place of the mysterious bonded courier,[340] so Dr Wright suggested the Kenyan lawyer had come to his aid in these proceedings by producing the real Tulip Trading invoice.[341]

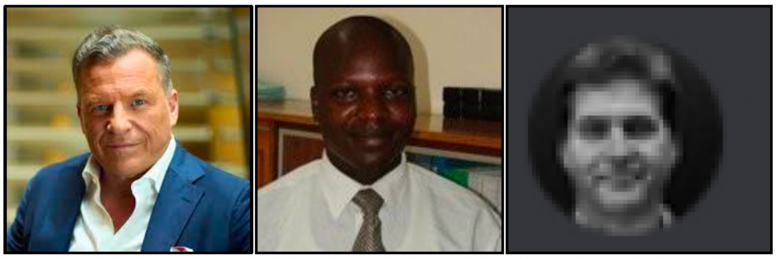
394. Dr Wright's story in this respect was yet another nonsensical fiction:

a) First, and regrettably for Dr Wright, Mr Mayaka had sent screenshots of the invoices which at least appeared to be photographs of a computer monitor that bore the hallmarks of the set-up in Dr Wright's home.[342] According to Dr Wright, Mr Ager-Hansen had installed monitoring software on Dr Wright's computer.[343] At this point, however, the story lost all semblance of coherence. How Mr Ager-Hansen would have the real invoices, when Dr Wright had to ask Mr Mayaka for them is unclear. And instead of putting the (real?) invoices on Dr Wright's computer by means of his supposed monitoring software, Mr Ager-Hansen then mocked up Dr Wright's set-up, took photographs of that set up showing the (real?) invoices and sent them to

[340] See the Developers' opening skeleton at ¶103(h) at {R/13/43}.

[341] Wright11¶292 {CSW/1/53}.

[342] See Sherell20¶22 and following {P1/20/8}, including the memorable comparison of the visible Google Chrome profile picture visible in the photographs, which was contrasted at Sherell20¶39 {P1/20/20}.



Comparison: Mr Ager Hanssen (Left) vs Mr Mayaka (Middle) vs Dr Wright (Right)

[343] Wright11¶280 {CSW/1/52}.

Mr Mayaka to send them on to Dr Wright.[344] To what end any of this could plausibly have occurred is unclear.

b) Second, and in a misstep reminiscent of Dr Wright's history of typographical inexactitude, Mr Mayaka made two bungling errors.

i) Instead of putting a 2011 date on the Tulip Trading invoice, he dated it to 30 July 2009 {CSW/15/1} – which was some years prior to the off-the-shelf company's incorporation. Dr Wright acknowledges that this was "*the wrong date*" and hypothesised that Mr Mayaka had "*simply copied a WIIL invoice as a template and did not update the date*".[345] Again, that is no explanation at all – not least given that it is unclear when Dr Wright thinks Mr Mayaka might have made this error. September 2023, perhaps?

ii) Each of the four invoices, although notionally issued years apart, had filenames in which the word "invoice" had been spelt as "invoive".[346]

c) Third, when sending the email, Mr Mayaka had failed to send the email using his native Kenyan time zone. Instead, he appeared to be sending the emails from a UK time zone[347] (and the invoices had been created on a UK time zone).[348] That might seem an anomaly, but on Day 15 Dr Wright was able to identify one other person who adopted this peculiar working habit: himself:

"*49:24 Top of the first page {CSW/25/1}, would you accept*
25 the recorded time zone offset for this email and
50: 1 the others, including both those on 10 September and
2 those on 29 September was GMT plus one hour?
3 A. Yes, Denis works on London time. Most of his clients
4 are English.
5 Q. So you say that he had his system set to be at that
6 time, although he worked in Kenya?
7 A. Yes, because most of his clients are English.
8 The majority of clients he sets up companies in
9 the Seychelles, Panama and everything like that, happen
10 to be British. Most of them related to large British
11 companies as well. British seem to like having these
12 sort of companies.
13 Q. But the time zone is certainly consistent with somebody

[344] Wright11¶275-278 {CSW/1/51}.

[345] Wright11¶292 {CSW/1/54}.

[346] Madden5¶135 {G/9/41}

[347] Madden5¶94-99 {G/9/32}

[348] Madden5¶137.c {G/9/43}.

> *writing from the UK as well, isn't it?*
> *A. No, it's consistent with someone doing work in the UK. I used to have my time zone set to America when I was doing American work.*"

d) Fourth, both Stroz Friedberg in their report dated 29 January 2024[349] and Mr Madden concluded that the digital signatures found in the invoices cannot be relied upon for an accurate timestamp and that they could have been manipulated or backdated by changing the clock time on the computer concerned.[350]

e) Fifth, the invoices bear a logo that bears the exact same dimensions (down to a single pixel) as the logo on Abacus's website on the Wayback Machine.[351]

f) Sixth, Mr Mayaka had purportedly touchingly declared "*You know, I have been loyal and I am always going to be. I have worked for you for 14 years and I know to be loyal*".[352] That loyalty had apparently extended to sending Dr Wright supposedly forged screenshots from Mr Ager-Hansen. There is no reason to suppose the invoices are any more credible.

395. Recognising the numerous oddities of Dr Wright's story, the Developers wrote to Shoosmiths in relation to the papa.neema emails on 18 January 2024 {M1/2/78}. They asked a series of pertinent questions about the document, including for present purposes asking at {M1/2/79}:

"*E1. When and how was Dr Wright informed that papa.neema@gmail.com was an email address associated with Mr Mayaka?*
E2. Please obtain the necessary consents to allow Google to provide to us the information provided when the email address papa.neema@gmail.com was registered, including the name, phone number, date of birth, gender and recovery email address in relation to that account."

396. No answer has been received to those modest requests. The obvious inference is that Dr Wright has himself produced or procured the producing of the papa.neema emails. Whether that is right or not, though, the papa.neema emails cannot corroborate Dr Wright's story as to his acquisition of Tulip Trading Ltd.

[349] Section IV {F/170/8}.
[350] Madden5¶136-137 {G/9/42}.
[351] Madden5¶144 {G/9/44}.
[352] {CSW/27/1}.

397. On the contrary, it is overwhelmingly obvious that Dr Wright purchased Tulip Trading Ltd as an off-the-shelf company in October 2014. That story is corroborated by the true versions of the incorporation form (ID_001395) and the invoice (ID_001397). There is ample corroborating material to support that fact, including:

a) The email exchange between Dr Wright and Abacus seeking an Aged Shelf Company on 16 October 2014, in which Dr Wright chose Tulip Trading Ltd.[353]

b) The email sending the invoice on 17 October 2014.[354]

c) The registrant name of the tuliptrading.net domain being changed to Dr Wright on 17 October 2014.[355]

d) The sending of the corporate documents for Tulip Trading on 20 October 2014.[356]

e) The letter of non-activity from Abacus of 21 October 2014.[357]

f) The provision of documentation for Tulip Trading on 23 October 2014.[358]

398. The consequences of the inevitable conclusion that Tulip Trading Limited was only acquired in 2014 are significant. It falsifies Dr Wright's parallel evidence about the Tulip Trust, which the Developers understand is being addressed by COPA.

3. The updated schedule

399. At paragraph 140 of the Developers' opening they provided a schedule of references to the forgeries alleged by COPA. The current position on the evidence in relation to those documents is now set out in Appendix 2 to these submissions.

400. Every one of the documents has been accepted by the experts as having been manipulated or otherwise being unreliable. The Developers understand that COPA is providing an updated schedule of Dr Wright's forgeries, so they do not comment further on those documents here.

[353] {L9/190/3}.

[354] {L9/184/1}.

[355] Madden5¶182-185 {G/9/54}.

[356] {L9/225/1}.

[357] {L9/230/1}.

[358] {L9/234/1}.

401. Suffice it to say, as anticipated at paragraph 141 of the Developers' opening skeleton:

a) First, the forgeries cover a wide range of types of documents: from supposed drafts of the Bitcoin White Paper, to alleged raw code, to accounting documents, to corporate incorporation information. They have one thing in common. They purport to support Dr Wright's case to be Satoshi. The only candidate for their forgery is Dr Wright.

b) Second, some of the documents are the evidence that Dr Wright has been promoting outside of these proceedings as solid proof that he is Satoshi. An example is ID_004019 {L2/245} which Dr Wright has literally held up to camera as the origin of where he chose the name Satoshi: https://www.youtube.com/watch?v=tel8aUEUe0U.[359] Another example is ID_003455 {L15/100}, which is the only document that has been produced by Dr Wright that could amount to the "*bank statements and credit card statements*" that Dr Wright has asserted he has evidencing his supposed original purchase of the bitcoin.org domain name and which he has indicated that he would be producing (in preference to using a private key as evidence): https://www.youtube.com/watch?v=dC0wwFJ7cHM (at 1m40s).[360] Dr Wright also relied on that document as proof of payment in Wright11¶171 footnote 112 {CSW/1/34} despite acknowledging that it is a forgery.[361]

c) Third, the documents cover the full period over which Dr Wright claims to have been involved in the development of Bitcoin. They are not limited to one particular period, or one particular issue. Indeed, they extend into the trial itself. In short, they contaminate the entire documentary record.

d) Fourth, the forgeries include documents produced after (1) Dr Wright was aware of COPA's allegations of forgery and (2) after Dr Wright had sight of Mr Madden's expert report which identified the indicia and methods by which documents might be falsified and how best to conceal such falsification. The Court will have noted the late flurry of metadata-light materials including LaTeX files.

[359] See{L16/86} for the video and {L16/83.1} for the transcript.

[360] {O4/25/36-37}.

[361] See Wright11 AxB §19 {CSW/2/62}.

e) Fifth, many documents are additional to those previously identified by the ATO or Dr Edman or KPMG (in the Granath proceedings) as being forged. That is not surprising. Although were the ATO/Edman/Granath documents arguably authentic they would doubtless be relied upon by Dr Wright as evidence of his being Satoshi, he has shied away from nominating those documents as his Reliance Documents.

f) Sixth, Dr Wright has subverted the disclosure process. The Developers have prepared a summary table of the relevant dates of documents disclosed by Dr Wright at Appendix 3, which emphasises the lackadaisical process of production. Further, the Developers did not have the opportunity to fashion the search terms that were applied to Dr Wright's documents; and when they have proposed additional searches, those were turned down by Dr Wright.[362] But Dr Wright has not even applied the basic search terms required by Part II of the DRD to his more recent disclosure, namely the BDO Image or his Overleaf account. Nor did he disclose the Andresen documents, even though those were produced to him in the Kleiman proceedings.[363]

402. The Developers invite the Court to adopt the conclusions pressed by COPA. The consequence is that Dr Wright has committed forgery on a monumental scale. He had embarked on that process before these proceedings commenced. Indeed, as explained at Appendix 1 to the Developers' opening skeleton {R/13/79}, that process began when he started advancing fraudulent claims to the ATO in 2013. It has continued persistently ever since, including in the immediate lead-up to the PTR (see the White Paper LaTeX Files) and during the trial itself (see the Ontier email forgery).

E. Relief

403. The consequences for Dr Wright's claims of the exposure of the facts that (a) he is not Satoshi Nakamoto, (b) he has committed forgery on an industrial scale and (c) he has

[362] See by way of example the Request from Macfarlanes ¶2 Letter of 13 November 2023 {M1/1/709-710} and the refusal to engage incorrectly on the basis that Macfarlanes had been involved in the DRD process {M1/1/1160}.

[363] The Developers have had to obtain these at their own expense themselves from the Relativity folder in Kleiman, following an initial refusal by Dr Wright to produce them.

given false evidence, should be profound. The Developers address here the effect on the BTC Core Claim and on the relief sought by COPA.

1. The BTC Core Claim

404. The Developers face claims in the BTC Core proceedings with an estimated financial value of "*hundreds of billions of pounds*".[364]

405. When asked to confirm whether that was what he was claiming, Dr Wright equivocated. On Day 3, when taken to that claim Dr Wright responded as follows:

> "*MR HOUGH: Dr Wright, when you said you're not suing people for hundreds of billions of dollars, you're wrong, aren't you?*
> *A. No, actually, if I'm correct -- which I am -- and all of the different aspects, including the patented material that is granted patents that are in BTC Core's products, aren't there, then this isn't I get that money, this is how the market reacts. Right now, if it is found out, as I'm saying, that nodes, aka pools, can be put under a legal constraint that the Sinaloa cartel can't pass money through them, that North Korea can't pass money through BCC, that it can be seized, that's worth hundreds of billions of dollars, not to me, to the industry.*
> *Q. Dr Wright --*
> *A. So my claim is worth that, not that I get it, but the value of BTC will diminish.*
> *Q. Dr Wright, this is a statement of value in a court claim form in which a party who is bringing a claim says how much they want to recover. Did you not understand that that was the significance of the statement of value when you endorsed this and other similar claim forms?*
> *A. The value has that in what I will personally lose, not that I get from you.*
> *My Lord --*
> *MR JUSTICE MELLOR: Can you answer the question, Dr Wright.*
> *A. I'm trying to, my Lord.*
> *What I'm saying is, I will lose, potentially, hundreds of billions of dollars, because if I'm right and I didn't do everything the way that I'm doing and I did the BTC Core way of doing it and I was an anonymous Satoshi, I would be worth lots more money. The value is what diminishes.*

[364] See the Claim Form at {A1/1/2}.

> *17 MR HOUGH: So is your position now, Dr Wright, that,*
> *18 the statements of value saying that your claims,*
> *19 including this one, are put at hundreds of billions of*
> *20 pounds do not mean that you are trying to recover sums*
> *21 of that amount, contrary to what anyone would understand*
> *22 the court statement of value to mean?*
> *23 A. No, I don't think I would recover hundreds of billions*
> *24 of dollars. I don't think that would be possible. In*
> *25 fact, the value would go down."*

406. When the Developers returned to the question on Day 8, naturally curious whether Dr Wright was claiming anything from them, Dr Wright indicated that a substantial claim would be pursued, unless the Developers agreed to some unspecified "*changes*":

> "*115:25 Q. So let me ask you this. Are you claiming any monetary*
> *116: 1 remedies other than the recovery of legal costs in*
> *2 the BTC Core claim?*
> *3 A. Not directly. What I will do is, every single cent*
> *4 I get past my costs goes to Burnside and other*
> *5 charities. I'm categorically stating, under oath,*
> *6 I will accept no money, not a cent, from recovered BTC.*
> *7 Q. I just want to understand your answer. Are you saying*
> *8 that you are seeking monetary remedies against*
> *9 the defendants to the BTC Core claims or not?*
> *10 A. I will seek to cover any damages people have had from*
> *11 losses, not to me. I will not accept any money from*
> *12 BTC. I will accept money that goes to third parties.*
> *13 Q. Are you making any claim, on your own behalf or on*
> *14 behalf of your companies, for the payment of a monetary*
> *15 remedy in the BTC Core claim?*
> *16 A. Not to me. If you basically agree to follow British*
> *17 law, and I don't even care if you like me or not, if you*
> *18 agree to admit that you've changed Bitcoin from*
> *19 the White Paper, pay my original offer, I would be*
> *20 happy. Not to me. If you give that money to a charity*
> *21 that's part of my church, I'm signed off.*
> *22 MR JUSTICE MELLOR: Dr Wright, it's a simple question.*
> *23 Leave the question of costs aside. What you're being*
> *24 asked about is, are they going to have to write a cheque*
> *25 for any money at all other than costs? It doesn't*
> *117: 1 matter who it's going to, are you going to insist on*
> *2 them writing a cheque for money as a result of*
> *3 the BTC Core claim, if you win it?*
> *4 A. My Lord, if they implement the required changes so that*
> *5 the British legislation as it is now is supported,*
> *6 I will forego any money. That would be the value*
> *7 I would accept. If the current legislation that has*
> *8 passed is implemented and supported by the developers,*
> *9 that one thing, I want no money.*

> *MR JUSTICE MELLOR: And where are these required changes set out?*
>
> *A. British legislation. There's cryptocurrency --*
>
> *MR JUSTICE MELLOR: Have you explained the required changes you need to the defendants in the BTC Core claim?*
>
> *A. They know what I want, but I would sit down with them and have these explained in full. I would very happily sit in a room and go, you need to do X, Y and Z, no more money laundering, no building Taproot for enabling secret transactions, the facility -- micropayments can be anonymous, large payments, like million pound ones to Hamas, stop. If that -- if that's agreed, I'm good.”*

407. In light of the obvious fact that Dr Wright is not Satoshi Nakamoto, his (and his companies’) claims in the BTC Core action must be dismissed. Given the flagrant abuse of process in Dr Wright’s forgery of documents and false evidence, the Court would be entitled to strike the proceedings out for the reasons set out at paragraphs 116 to 123 of the Developers’ opening skeleton {R/13/51}. However, as Mummery LJ noted in Zahoor v Masood [2009] EWCA Civ 650 at [73]:

> “*One of the objects to be achieved by striking out a claim is to stop the proceedings and prevent the further waste of precious resources on proceedings which the claimant has forfeited the right to have determined. Once the proceedings have run their course, it is too late to further that important objective. Once that stage has been achieved, it is difficult see what purpose is served by the judge striking out the claim (with reasons) rather than making findings and determining the issues in the usual way. If he finds that the claim is based on forgeries and fraudulent evidence, he will presumably dismiss the claim and make appropriate orders for costs. In a bad case, he can refer the papers to the relevant authorities for them to consider whether to prosecute for a criminal offence: we understand that this was done in the present case.*”

2. COPA’s claims

408. COPA makes claims for both declaratory and injunctive relief. Although not a party to those claims, the Developers (who have been on the receiving end of Dr Wright’s claims and threats) support them.

a. *Dr Wright's threats*

409. The court has heard unchallenged evidence of the direct impact of Dr Wright's bullying of and threats against individuals and businesses within the Bitcoin community.[365]

410. Those threats have ranged from threats of physical violence, economic hardship, and legal action against people who have either refused to accept Dr Wright is Satoshi Nakamoto, and/or somehow been involved (or perceived to be involved) with BTC or BCH.[366]

411. The court is invited to re-read both paragraphs 142 – 157 of the Developers' Opening Skeleton Argument[367] and Mr Lee unchallenged witness statement[368] in this respect.

412. Mr Lee spoke directly and authoritatively as to the litigation commenced by Dr Wright predicated upon his being Satoshi. That has included:

a) His proceedings against the people who own bitcoin.org.

b) Defamation claims against Peter McCormack and Magnus Granath.

c) His claims against the Developers (and others) in the present proceedings.

413. Mr Lee has provided multiple examples of individuals who have either stopped or minimised their involvement with Bitcoin development, notwithstanding the open-source nature of Bitcoin. Mr Lee cites five named former Bitcoin Core Maintainers who have been affected by Dr Wright's threats; namely

a) Jonas Schnelli, who was directly threatened by Calvin Ayre and stepped down in October 2021 (see Lee1¶20.a {C/12/7}). He is the third Defendant Developer in the BTC Core Claim;

b) Wladimir van der Laan, the former Lead Maintainer of Bitcoin Core and second Defendant Developer, who stepped down after takedown notices from Dr Wright's lawyers (see Lee1¶20.b {C/12/8}) and who Dr Wright has

[365] Lee1¶¶17-25{C/12/5}.

[366] See ¶¶142-157 Developers' Opening Skeleton for Trial {R/13/69}.

[367] Developers' Opening Skeleton for Trial {R/13/69}.

[368] Lee1 {C/12/1}.

wrongly alleged to have been involved in the setting up of the GitHub platform for Bitcoin;[369]

c) Greg Maxwell, an early Bitcoin developer and the twelfth Defendant Developer in the BTC Core Claim, who stopped contributing to bitcoin entirely after Dr Wright's lawsuits began (see Lee1¶20.c {C/12/9}) and who Dr Wright has falsely named on multiple times during his witness evidence;[370]

d) Marco Falke, the former Bitcoin Core Maintainer who had the record for the highest number of commits to the project, who resigned citing legal risks following Dr Wright's litigation (see Lee1¶20.d {C/12/9}) and who is the fifth Defendant Developer; and

e) Samuel Dobson, another former Bitcoin Core Maintainer of Bitcoin Core, who expressed his concerns of Dr Wright's legal activities prior to quitting: (see Lee1¶20.e {C/12/9}) and who is the [371] Mr Lee explained that many others have been scared away from the Bitcoin community by Dr Wright's threats.[372]

414. Having had the benefit of live evidence from Dr Wright, the Court has experienced at first hand, Dr Wright's unrestrained and unjustified attacks on a variety of individuals, from unspecified 'COPA members', to COPA witnesses, to the expert witnesses (including Dr Placks and Mr Lynch) and to his former solicitors. By way of example, when Mr Rosendahl, COPA's LaTeX expert was asked whether the accusation Dr Wright had made during his cross examination that Mr Rosendahl had attended a number of BTC Conferences and would lose a lot of money if Dr Wright was successful in this case, he politely pointed out none of it was true.[373] Even Mr

[369] Dr Wright made this false allegation at Wright1¶136 {E/1/26}. The documents clearly show that it was Gavin Andresen who proposed setting up the GitHub platform {L6/282.7}, {L6/500.1}, and that he did so with the approval of Satoshi {L6/500.2}. Mr Andresen then announced the development on the Bitcoin forum {L17/57}. Mr van der Laan was not involved.

[370] Including falsely accusing him of (a) compromising his server {Day6/p52/ll.8-15}, (b) sending documents to the ATO {Day7/p111/ll.2-15} (c) fabricating an invalid response to Dr Wright's PGP keys {Day2/p23/ll.4-8} and {Day7/p124/ll.9-17} and (d) being PaintedFrog, the person who (rightly) identified the plagiarism in Dr Wright's LLM dissertation {Day6/p31/l.23}.

[371] Lee1¶20 {C/12/7}.

[372] Lee1¶19 {C/12/4}.

[373] {Day17/p6/ll.16} – {Day17/p8/ll.23}.

Matthews, Dr Wright's number 1 supporter, commented that he had seen a lot of posts that Dr Wright had made, that he "*personally wouldn't have made*".[374]

415. The only answer that Dr Wright seemed to advance to Mr Lee's evidence in cross-examination was that a number of community-minded people had set up and funded the Bitcoin Legal Defense Fund, to help open source developers in Bitcoin defend themselves against litigation.[375] It cannot seriously be suggested that such protection as that fund had afforded to developers against their costs of defending Dr Wright's claims is a reason for Dr Wright to be permitted to continue to make those claims after the judgment against him in these proceedings.

416. Yet that seems to be precisely what Dr Wright intends. He has made clear that he "*will keep doing this, and no matter what the outcome of this case is, I'll hit 10,000 patents and then I'll keep going*."[376] Dr Wright expressly confirmed that he will not stop his campaign of litigation if he loses this case on Day 8:

"*112:10 Q. If this court decides that you are not Satoshi, you'll*
11 still want to make claims, here and around the world,
12 based on Satoshi's supposed IP rights, won't you?
13 A. Again, I don't actually need to be Satoshi to have those
14 rights. A Champagne case, which my lawyers wanted to
15 run, would not require anything other than a change to
16 the protocol. So --
17 Q. But the claims you are currently making are based
18 explicitly upon Satoshi's IP rights and contingent on
19 you being Satoshi?
20 A. Only because if I ran a Champagne case, the first thing
21 your side would ask is, "You're Satoshi", and you would
22 have me do this.
23 Q. So the question again, if this court decides you are not
24 Satoshi, you would still want to make claims, here and
25 around the world, based upon you being Satoshi and
113: 1 having IP rights as such, wouldn't you?
2 A. No, I'd move to patents. Taproot is based on three
3 nChain patents, which is integrated into the core of
4 BTC. We would actually pull the plug on that, and we
5 have already investigated, and we would have
6 the European courts start patent action on that. We
7 would then --

[374] {Day12/p86/ll.14-18}.

[375] {Day12/p113/ll.21} – {Day12/p117/ll.2}.

[376] {T8/103/1-104/6}

> *8 Q. And Dr Wright --*
> *9 A. -- go -- we would then start patent action in the US*
> *10 and, if I had to, I'll basically force them to shut*
> *11 down. We will go to vendors, such as AWS, who we're*
> *12 partnered with, and we will notify of the patent*
> *13 violations and it will be a patent case. So if I lose*
> *14 this, there are approximately 80 patent cases already*
> *15 waiting.*
> *16 Q. If this court decides that you're not Satoshi, you will*
> *17 still want to threaten those who dispute that claim,*
> *18 the claim to be Satoshi, with legal action, won't you?*
> *19 A. No, it's not that I'm Satoshi that I care about.*
> *20 I don't give a rats whether you believe I'm Satoshi.*
> *21 I don't care. I would prefer if you ignored the fact.*
> *22 I didn't want it out there. I would love everyone just*
> *23 to ignore the fact and just leave me alone and let me*
> *24 invent.*
> *25 So what I would say is, as long as they stop and*
> *114: 1 they leave me alone, I will leave them alone."*

417. The court should not be fooled by Dr Wright's protestations that he only cares about his patents; each of the BTC Core Claim, the Kraken Claim, and the Coinbase Claims has been brought in respect of unregistered IP rights. His protestations that he has only ever cared about his patent portfolio is in stark contrast to these current live High Court Claims, and the number of letters before action received by companies in respect of their use of the Bitcoin White Paper.[377]

b. <u>The relief sought</u>

418. COPA's claims are for declaratory and injunctive relief. Both are well justified. The claims may require some tweaking in light of the judgment (in particular, to ensure that they cover the Bitcoin code).

i. <u>Declaratory relief</u>

419. COPA claims declarations that Dr Wright is not the author of the Bitcoin White Paper, not the owner of the copyright in the Bitcoin White Paper and that any of the Bitcoin White Paper by the claimant would not infringe any copyright owned by Dr Wright.[378]

[377] Lee1¶11 {C/12/3}.

[378] Re-AmendedPoC¶68 {A/2/22}.

420. The principles as declaratory relief do not appear to be in dispute. They are conveniently set out in Financial Services Authority v Rourke [2002] CP Rep 14, per Neuberger J at {T/17/3} and following and per Cockerill J in BNP Paribas SA v Trattamento Rfiuti Metropolitani SpA [2020] EWHC 2436 (Comm) at [78] {T/46/21}. As noted by Lord Woolf MR in Messier Dowty v Sabena [2000] 1 WLR 2040 at [41]: "*The approach is pragmatic. It is not a matter of jurisdiction. It is a matter of discretion*."

421. It is clear that, even with dismissal of the BTC Core claim, there will remain a genuine commercial need for declaratory relief of the kind sought by COPA. Merely recording that Dr Wright is not the author of the Bitcoin White Paper and Bitcoin code nor the owner of the copyright in the Bitcoin White Paper and Bitcoin code in the judgment will not be sufficient. As the Court has seen, interest in COPA's claim extends far beyond those who may be trained in the reading of any legal judgment.

ii. Injunctive relief

422. COPA also claims injunctive relief preventing Dr Wright from claiming he is the author and/or owner of copyright in the Bitcoin White Paper and/or taking any steps which would involve him asserting the same. Such relief is well-justified in relation to both the Bitcoin White Paper and the Bitcoin code.

423. The court is more than familiar with the breadth and flexibility of injunctive relief. It is an equitable remedy that is purposefully broad and reactive to the relevant situation. The four objections raised by Dr Wright in his Opening Skeleton Argument[379] are matters which are most appropriately resolved at the Form of Order hearing in due course.

424. In summary, the position is this. Dr Wright's claims to be Satoshi Nakamoto and subsequently the author of the Bitcoin White Paper are not made in isolation. They are the precursors to the campaign of threatening and harassing behaviour

[379] Dr Wright Opening Skeleton Argument for Trial ¶¶186- 192 {R/14/67}.

particularised by Mr Lee. The injunction to restrain Dr Wright from making those claims is the way to prevent the latter campaigns, and to stop him from relying on a lie to cause harm and distress to others.

425. Dr Wright's misguided libel proceedings against Peter McCormack and Magnus Granath only serve to highlight the justification for restraining Dr Wright. And Dr Wright's repeated and mendacious forgery and brazen lying to the Court underscore the justification for granting injunctive relief. Moreover, the Court may of its own motion need to intervene to overturn the Order of HHJ Hodge in the COBRA claim {L17/168}, pursuant to which bitcoin.org has been prevented from making the Bitcoin White Paper available for download in the UK: see Developers Opening Skeleton ¶145.[380]

426. It is absurd to suggest (as Dr Wright did in his opening skeleton at ¶189{R/14/69}) that there would be no useful purpose to an injunction. Dr Wright has mounted a global campaign of aggression against those who disagree with him, and has made it clear both in this trial and in his approach to other findings made against him that he will not accept a view that is contrary to his own.

iii. Summary

427. This is not Dr Wright's first rodeo. His false and mendacious claims have been observed and noted in a series of decisions, from the Kleiman proceedings,[381] through

[380] {R/13/70}.

[381] Judge Reinhart observed that "*During his testimony, Dr. Wright's demeanor did not impress me as someone who was telling the truth. When it was favorable to him, Dr. Wright appeared to have an excellent memory and a scrupulous attention to detail. Otherwise, Dr. Wright was belligerent and evasive. He did not directly and clearly respond to questions. He quibbled about irrelevant technicalities. When confronted with evidence indicating that certain documents had been fabricated or altered, he became extremely defensive, tried to sidestep questioning, and ultimately made vague comments about his systems being hacked and others having access to his computers. None of these excuses were corroborated by other evidence.*" {L15/207/19}.

the McCormack claim,[382] to the claim by Magnus Granath. [383] Adverse findings against Dr Wright have not acted as a sufficient restraint. The Court should grant COPA the declaratory and injunctive relief that it seeks.

ALEXANDER GUNNING KC
BETH COLLETT
8 March 2024

[382] In Wright v McCormack [2022] EWHC 3343 (KB), Mr Justice Chamberlain observed as follows at [4]-[5]: "*Ordinarily, a claimant in Dr Wright's position would be entitled to substantial damages. In this case, however, I decided that he should have only nominal damages of £1. The reason was that, in an attempt to establish that Mr McCormack's publications had caused serious harm to his reputation, an essential element of a defamation claim, Dr Wright had advanced a deliberately false case until shortly before trial. When the falsity was exposed, he changed his case, explaining that he had made inadvertent errors. I rejected that explanation as untrue.*
As I noted in my judgment, this was not the first occasion on which Dr Wright's evidence to a court has been found to be unreliable. I set out at [87]-[88] of my judgment some excerpts from the decisions of two United States federal judges, who came to the same conclusion. Since I gave judgment, my attention has been drawn to the observations of Butcher J, sitting in the Commercial Court in this jurisdiction, who found Dr Wright to be an unsatisfactory witness in many respects: Ang v Relantco Investments [2020] EWHC 3242 (Comm), at [49]. ..."

[383] District Court Judge Helen Engebrigtsen of the Oslo District Court in Norway held on 20 October 2022 "*The court believes that Granath had sufficient factual grounds to claim that Wright had lied and cheated in his attempt to prove that he is Satoshi Nakamoto.*" {L18/66/19}.

Appendix 1 – Proof of work and leading zeroes

1. The CheckBlock function at {L4/97.1/22} includes two steps for ensuring that the relevant proof of work difficulty has been met under the comment "// Check proof of work matches claimed amount".

2. Both steps require the identification of the target for the block. Accordingly, one needs to work out the target first and then carry out the comparison exercise required by CheckBlock.[384] This appendix describes first how the target is identified, before describing the two checks of the proof of work against that target.

3. As will be seen below, the check of the proof of work against the target is not merely a counting of the number of leading zeroes.

A. Working out the target difficulty

4. The target that is used in the CheckBlock function is obtained from the object "CBigNum().SetCompact(nBits)".

5. That target is itself identified by converting a compact representation of the target ("nBits") which is included in the Block Header into a CBigNum object using the "SetCompact" function.

6. The SetCompact function is defined in the bignum.h header file {L4/158.1/5}. That function enables the decoding of numbers stored in a compact form into an expanded format. The numbers stored in a compact format are referred to as "nCompact" in the function. [385] When the SetCompact function is applied to nBits, nBits is nCompact.

7. The nCompact format is a 32-bit (4-byte) number. The first byte (or 8 bits) represents the length of the full uncompacted number in bytes. The remaining bytes represent the

[384] It is not until AcceptBlock that it is checked that the target is correct: see {L4/97.1/22}.

```
// Check proof of work
if (nBits != GetNextWorkRequired(pindexPrev))
return error("AcceptBlock(): incorrect proof of work");
```

[385] `CBigNum& SetCompact(unsigned int nCompact)`

first three bytes of the actual number. As such the nCompact (i.e., in the case of the CheckBlock function, nBits) can be understood as a floating-point number[386] with an 8-bit exponent, a sign bit and a 23-bit mantissa.

8. The SetCompact starts by producing a multiprecision integer (or "MPI") in four stages.

   a) The first stage essentially extracts the size of the full number (i.e. the exponent) from the first byte of nCompact. As such it identifies how many bytes are required to hold the expanded MPI. The size of the full MPI is extracted by shifting the compact number 24 bits to the right ("unsigned int nSize = nCompact >> 24").[387]

   b) The second stage prepares a vector ("vch") that is big enough to hold the full MPI. The vector can be thought of as a list that encodes the MPI by setting out its size and then the target number. The size of the vector (in bytes) is 4 plus the size extracted earlier ("std::vector<unsigned char> vch(4 + nSize);").

   c) In the third stage the size of the decoded target number is stored in the first 4 bytes of the vector. Because the size of that number has been identified in a single byte of nCompact, this size can only take up one of those 4 bytes. The line "vch[3]=nSize" sets the fourth of the initial bytes of the vector to represent the size.

   d) In the fourth to sixth stages the next three bytes of nCompact (which represent the most significant bytes of the full number) are extracted and placed into the vector. The SetCompact function does that:

      i) First, by shifting each "carriage" of bytes of nCompact along, so that it can be isolated.[388]

      ii) Second, the 0xff operation has the effect of isolating the byte at the end and ignoring the rest.

[386] This was the terminology used by Dr Back {Day13/p48}. It is also used by BSV: https://archive.is/GNEIn.

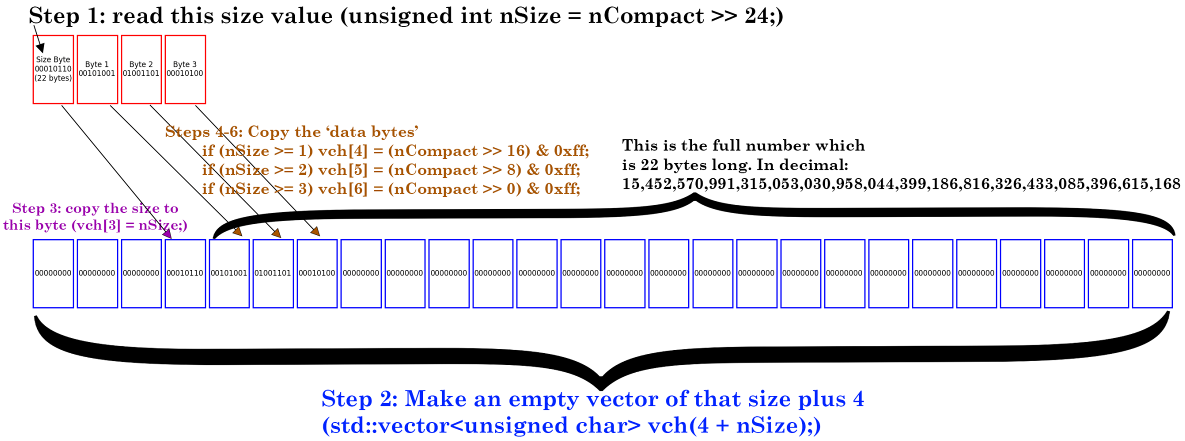
[387] You can think of each byte in the nCompact format as the carriage of a train which can only be examined if it is right at the end of the train. Given that there are 4 bytes (with 8 bits to the byte), if you want to examine the first byte, you need to move it 3 bytes (i.e. 24 bits) along the train so that it then sits at the end of the train. If you want to examine the second byte, you need to move it by 2 bytes (i.e. 16 bits) along the train - and so on.

[388] See footnote 387 above.

iii) Third, the isolated bytes are placed into the relevant part of the vector.

Thus, the lines read "if (nSize >= 1) vch[4] = (nCompact >> 16) & 0xff;" and so on. In this step, for each condition (if (nSize >= 1), etc.), the code is essentially doing this "shift and isolate" process to pick out the second to fourth bytes from nCompact one by one and place them into the correct position in the vector (vch).

9. This process can be illustrated as follows. The nCompact/nBits number is identified in the red boxes and the target is the (in this illustration, 22-byte) number represented in the 5th to 26th blue boxes:


Step 1: read this size value (unsigned int nSize = nCompact >> 24;)
Size Byte 00010110 (22 bytes)
Byte 1 00101001
Byte 2 01001101
Byte 3 00010100
Steps 4-6: Copy the 'data bytes'
if (nSize >= 1) vch[4] = (nCompact >> 16) & 0xff;
if (nSize >= 2) vch[5] = (nCompact >> 8) & 0xff;
if (nSize >= 3) vch[6] = (nCompact >> 0) & 0xff;
This is the full number which is 22 bytes long. In decimal: 15,452,570,991,315,053,030,958,044,399,186,816,326,433,085,396,615,168
Step 3: copy the size to this byte (vch[3] = nSize;)
00000000
00000000
00000000
00010110
00101001
01001101
00010100
00000000
00000000
00000000
00000000
00000000
00000000
00000000
00000000
00000000
00000000
00000000
00000000
00000000
00000000
00000000
00000000
00000000
00000000
00000000
Step 2: Make an empty vector of that size plus 4 (std::vector<unsigned char> vch(4 + nSize);)

10. In the final stage of SetCompact, the MPI which now contains each of those bytes is rendered into a CBigNum object. That is done using the BN.mpi2bn function from the OpenSSL library. Converting the vector of bytes into a CBigNum allows the programmer to simply treat the target in the MPI as a normal (albeit large) integer. Because it is now being treated as a normal integer it can be subject to common mathematical operations.

11. It will be noted from the above that the target (i.e. the CBigNum object) represents a normal integer, not merely a number of leading zeroes.

B. Checking the target number

12. As noted at paragraph 1 above, having identified the target number that target is subject to two checks. The first is to ensure that the minimum work requirement has been met. The second is to ensure that the hash of the block is less than or equal to the target.

1. Ensuring that the minimum work requirement is met

13. In the CheckBlock function, the code "if (CBigNum().SetCompact(nBits) > bnProofOfWorkLimit)" compares the target derived from nBits to "bnProofOfWorkLimit".

14. bnProofOfWorkLimit is a constant defined by the Bitcoin code to represent the highest possible target (i.e. easiest difficulty), to ensure that the minimum work is maintained.

15. The bnProofOfWorkLimit is set in the main.h file {L4/98.1/1} as 32 bits of zero followed by 224 bits of one.[389]

16. Accordingly at this first stage the target shown in the Block Header is checked to make sure that it is lower than 32 bits of zero followed by 224 bits of one.

17. If the target derived from nBits does not meet the minimum work requirement, an error is returned.

18. The bnProofOfWorkLimit is set as a number, not as simply a number of leading zeroes. So at this stage, the target specified in the Block Header is not simply checked by reference to its inclusion of a number of leading zeroes.

[389] This is a massive number. In decimal it would be represented as follows: 26,959,946,667,150,639,794,667,015,087,019,630,673,637,144,422,540,572,481,103,610,249,215.

2. Ensuring that the hash of the block is less than or equal to the target.

19. The second stage of the proof of work check in the CheckBlock function reads as follows:
“if (GetHash() > CBigNum().SetCompact(nBits).getuint256())
return error("CheckBlock(): hash doesn't match nBits");”

20. At this stage the hash of the block (“GetHash()”) is compared to the CBigNum which has been derived as set out above.

21. Because the hash has been derived using a SHA-256 hashing function, it will be a 256-bit integer.

22. Accordingly, for the purposes of this check, the CBigNum target is first converted into a 256-bit integer using the operation "getuint256()".

23. This conversion allows the block's hash (a 256-bit number produced by the SHA-256 hashing function) to be directly compared to that target.

24. The comparison is being made between one 256-bit integer and another. It is not simply a check of leading zeroes.

Appendix 2 – Schedule of Forgeries

Document Bundle Ref (Pleading)	Short document description	Reliance doc	Wright evidence	Wright XX Refs	Other witness evidence	Madden	Placks/Stroz	Madden XX	Joint report	Other Transcript Refs
ID_000073 {L1/323} ({A/2/29})	University of Newcastle Master of Statistics Assignment Poisson competing process…	No	Wright11 AxB §4 {CSW/2/13}	{Day2/p154} – {Day2/p166}	Gerlach¶5 {C/20.1/1}	PM24¶8 {H/116/3}, PM24¶29 {H/116/10}, PM24¶33 {H/116/10}, PM24¶37 {H/116/13}, PM38 {H/145/1}, Madden3 fn5 {G/5/38}	Placks2§3 {I/6/6}	{Day16/p68} – {Day16/p75}	M&P: Manipulated {Q/4/4}	
ID_000199 {L2/130} ({A/2/31})	Northumbria University LLM Dissertation Proposal Payments Providers and Intermediaries as defined in the Law of the Internet LLM_PROP.DOC	Yes	Wright1¶58 {E/1/12}, Wright11¶60 fn29 {CSW/1/12}, Wright11¶140-169 {CSW/1/27}, Wright11¶1021 fn418 {CSW/1/180}	{Day3/p74 } – {Day3/p76}	Pearson {C/3/1}	PM3¶6-7 {H/20/2}, PM3¶11 {H/20/5}, PM24¶8 {H/116/3}, PM24¶28 {H/116/10}, PM24¶37 {H/116/13}, PM25 {H/118/1}, Madden2¶57 {G/3/23}, PM43¶55 {H/219/24}, PM43¶61 {H/219/26}, PM43.17 {H/237N/1}	Placks1¶4.01 {I/1/7}, 6.01 {I/1/11}, 6.05 {I/1/12}, 6.09 {I/1/13}, 6.32 {I/1/16}, 6.36 {I/1/16}, 6.38 {I/1/16}		M&P: Manipulated {Q/2/6}	JHOp {Day1/p34}
ID_000217 {L2/131} ({A/2/34})	Northumbria University LLM Dissertation Proposal Payments Providers and Intermediaries as defined in the Law of the Internet LLM_ProposalA.doc	Yes	Wright11¶60 fn29 {CSW/1/12}, Wright11¶140-169 {CSW/1/27}, Wright11 AxB §5 {CSW/2/17}	{Day3/p55} – {Day3/p68}	Pearson {C/3/1}	PM3¶6-7 {H/20/2}, PM3¶11 {H/20/5}, PM24¶25.b {H/116/8}, PM25 {H/118/1}, PM43¶6 {H/219/3}, PM43¶36-54 {H/219/16}, PM43¶55 {H/219/24}, PM43¶58 {H/219/25}, PM43¶61 {H/219/26}, PM43.17 {H/237N/1}	Placks1¶4.01 {I/1/7}, 6.01 {I/1/11}, 6.05 {I/1/12}, 7.16 {I/1/21}		M&P: Manipulated {Q/2/6}	JHOp {Day1/p34}
ID_000227 {L3/219} ({A/2/37})	The Economics of central Core Bitcoin Nodes	Yes	Wright1(List) {E/1/41}, Wright11 AxB §6 {CSW/2/20}	{Day3/p7} – {Day3/p25}		PM24¶8 {H/116/3}, PM24¶37 {H/116/13}, PM24¶41 {H/116/14}, PM26 {H/121/1}, PM40¶1-2 {H/156/1}, PM40¶32 {H/156/13}, PM40¶42 {H/156/16}, PM43¶6 {H/219/3}, PM43¶13-14 {H/219/5}	Placks1¶4.01 {I/1/7}, 6.01 {I/1/11}, 6.09 {I/1/13}, 6.32 {I/1/16}, 6.34 {I/1/16}, 6.40 {I/1/17}		M&P: Manipulated {Q/2/6}	

ID_000254
{L2/441}
({A/2/39})
	Time Coin: Peer-to-Peer Electronic Cash System	Yes	Wright11 AxB §7 {CSW/2/26}	{Day3/p139} – {Day3/p160}, {Day15/p64} – {Day15/p91}		Madden1¶14.a {G/1/8}, 147 {G/1/51}, PM2 {H/17/1}, PM3¶6-7 {H/20/2}, PM3¶10 {H/20/4}, Madden2¶65-77 {G/3/25}	Placks1¶4.01 {I/1/7}, 7.01-7.02 {I/1/19}, 7.04 {I/1/19}, 7.09-7.10 {I/1/20}, 7.14 {I/1/21}		M&P: Manipulated or unreliable {Q/2/6}	JHOp {Day1/p24} – {Day1/p26}, {Day1/p31}, {Day1/p8} –{Day1/p9},
										XXRJ {Day9/p94} – {Day9/p107}
										{Day9/p171} – {Day9/p172}

ID_000258 {L3/286} ({A/2/41})	Economic Security	Yes	Wright1(List) {E/1/41}, Wright11 AxB §8 {CSW/2/30}	{Day3/p25} – {Day3/p32}		PM1¶14 {H/1/4}, PM24¶8 {H/116/3}, PM24¶37 {H/116/13}, PM24¶41 {H/116/14}, PM29 {H/126/1}, Madden2¶53.b {G/3/22}, PM43¶6 {H/219/3}, PM43¶13-14 {H/219/5}	Placks1¶4.01 {I/1/7}, 6.01 {I/1/11}, 6.09 {I/1/13}, 6.12 {I/1/13}, 6.20 {I/1/14}		M&P: Manipulated {Q/2/6}	
ID_000260 {L2/294} ({A/2/43})	POISSONC.ODT	Yes	Wright1(List) {E/1/41}, Wright11 AxB §9 {CSW/2/33}	{Day3/p38} – {Day3/p47}, {Day16/p75} – {Day16/p80}	Joost Andrae Letter to Bird & Bird {L18/313}	Madden1¶147 {G/1/51}, PM2¶58 {H/17/24}, PM23¶1-6 {H/107/1}, PM23¶10-45 {H/107/5}, Madden2¶78 {G/3/28}	Placks1¶4.01 {I/1/7}, 7.01 {I/1/19}, 7.17 {I/1/21}		M&P: Manipulated {Q/2/6}	
ID_000367 {L3/185} ({A/2/44})	Block diffusion within bitcoin	Yes	Wright1(List) {E/1/41}, Wright11 AxB §10 {CSW/2/36},	{Day2/p144} – {Day2/p153}		PM24¶8 {H/116/3}, PM24¶37 {H/116/13}, PM24¶41 {H/116/14}, PM30 {H/129/1}, Madden2¶53.a {G/3/22}, PM43¶13 {H/219/5}	Placks1¶4.01 {I/1/7}, 6.01 {I/1/11}, 6.09 {I/1/13}, 6.12 {I/1/13}		M&P: Manipulated or unreliable {Q/2/6}	

Document Bundle Ref (Pleading)	Short document description	Reliance doc	Wright evidence	Wright XX Refs	Other witness evidence	Madden	Placks/Stroz	Madden XX	Joint report	Other Transcript Refs
			Wright11 AxC §3 {CSW/3/6}							
ID_000371 {L3/200} ({A/2/46})	Phase transitions in block propagation networks	Yes	Wright1(List) {E/1/41}, Wright11 AxB ¶11.11-11.13 {CSW/2/41}, 11.15 {CSW/2/42}	{Day2/p118} – {Day2/p125}		PM24¶8 {H/116/3}, PM24¶37 {H/116/13}, PM24¶41 {H/116/14}, PM27 {H/122/1}, PM40¶1-2 {H/156/1}, PM40¶4-10 {H/156/2},PM40¶22-30 {H/156/10}, PM40¶32 {H/156/13}, PM40¶35 {H/156/14}, PM40¶42 {H/156/16}, Madden2¶50 {G/3/20}, PM43¶13 {H/219/5}	Placks1¶4.01 {I/1/7}, 6.01 {I/1/11}, 6.09 {I/1/13}, 6.40 {I/1/17}		M&P: Manipulated {Q/2/6}	
ID_000395 {L3/202} ({A/2/48}	Northumbria University Documentary Credits under the UCP 500	Yes	Wright1(List) {E/1/42}, Wright11¶140-169 {CSW/1/27}, Wright11¶955 fn390 {CSW/1/172}, Wright11¶969 fn397 {CSW/1/174}, Wright11¶1015 fn407 {CSW/1/179}, Wright11¶1024 fn420 {CSW/1/181}, Wright11 AxC §7 {CSW/3/12}	{Day3/p87} – {Day3/p92}		PM24¶8 {H/116/3}, PM24¶37 {H/116/13}, PM24¶41 {H/116/14}, PM27¶36 {H/122/14}, PM31 {H/132/1}, PM43.17 {H/237N/1}	Placks1¶4.01 {I/1/7}, 6.01 {I/1/11}, 6.09 {I/1/13}, 6.38 {I/1/16}		M&P: Manipulated {Q/2/6}	
ID_000396 {L3/203} ({A/2/50})	Noncooperative finite games	Yes	Wright1(List) {E/1/42}, Wright11 AxB §11 {CSW/2/40}	{Day2/p125} – {Day2/p129}		PM24¶8 {H/116/3}, PM24¶37 {H/116/13}, PM24¶41 {H/116/14}, PM27 {H/122/1}, Madden2¶47.c {G/3/19}, Madden2¶50.a {G/3/20}	Placks1¶4.01 {I/1/7}, 6.01 {I/1/11}, 6.09 {I/1/13}, 6.12 {I/1/13}, 6.19{I/1/14}		M&P: Manipulated {Q/2/6}	
ID_000462 {L2/149} ({A/2/52})	Defining the possible Graph Structures	Yes	Wright1(List) {E/1/42}	{Day2/p129} – {Day2/p132}		PM24¶8 {H/116/3}, PM24¶28 {H/116/9}, PM24¶37 {H/116/13}, PM24¶41 {H/116/14}, PM27¶33 {H/122/13}, PM27¶36.c {H/122/14}, PM28¶9 {H/124/4}, PM28¶13 {H/124/5}, PM32 {H/137/1}, PM43¶13 {H/219/5}	Placks1¶4.01 {I/1/7}, 6.01 {I/1/11}, 6.09 {I/1/13}, 6.12 {I/1/13}		M&P: Manipulated or unreliable {Q/2/6}	
ID_000465 {L2/318} ({A/2/54})	Defamation and the difficulties of law on the Internet email	No	Wright4¶93-98 {E/4/31}, Wright11 AxB §12 {CSW/2/44}	{Day4/p74} – {Day4/p89}		PM18¶1 {H/83/1}, PM18¶32-57 {H/83/10}, PM18¶63-72 {H/83/28}, PM45¶36 {H/241/18}, PM45¶49 {H/241/22}, PM45¶55 {H/241/23}, PM45¶64.a {H/241/24}, PM45¶66 {H/241/25}	Placks2§4 {I/6/7}		M&P: Manipulated {Q/4/4}	
ID_000504 {L3/230} ({A/2/56})	Non-Sparse Random Graphs	Yes	Wright1(List) {E/1/42}	{Day3/p47} - Day3/p49}, {Day8/p140} – {Day8/p142}	Wuille1¶29-32 {C1/1/7}	PM1¶34-35 {H/1/12}, PM1¶41 {H/1/18}, PM24¶8 {H/116/3}, PM24¶37 {H/116/13}, PM24¶41 {H/116/14}, PM28 {H/124/1}, PM33¶12 {H/138/4}, PM33¶15 {H/138/5}, PM34¶9-10 {H/139/3}, ,PM34¶16 {H/139/6}, PM34¶34 {H/139/9}, PM35¶8 {H/141/4}, PM40¶1-2 {H/156/1}, PM40¶32	Placks1¶4.01 {I/1/7}, 6.01 {I/1/11}, 6.09 {I/1/13}, 6.40 {I/1/17}		M&P: Manipulated {Q/2/6}	JHOp {Day1/p35}

Document Bundle Ref (Pleading)	Short document description	Reliance doc	Wright evidence	Wright XX Refs	Other witness evidence	Madden	Placks/Stroz	Madden XX	Joint report	Other Transcript Refs
						{H/156/13}, PM40¶42 {H/156/16}, PM43¶13 {H/219/5}				
ID_000525 {L2/148} ({A/2/58})	Bond Percolation in timecoin	Yes	Wright1(List) {E/1/43}, Wright4¶6.c.x {E/4/6}	{Day2/p106} – {Day2/p117}		PM1¶34-35 {H/1/12}, PM24¶8 {H/116/3}, PM24¶29 {H/116/10}, PM24¶34.c {H/116/12}, PM24¶37 {H/116/13}, PM24¶41 {H/116/14}, PM33 {H/138/1}, PM34¶9-10 {H/139/3}, PM34¶17 {H/139/6}, PM35¶8 {H/141/4}, PM43¶6 {H/219/3}, PM43.17 {H/237N/1}, PM43¶13-14 {H/219/5}, PM43¶17-35 {H/219/7}, PM43¶99.e.ii {H/219/34}, PM43¶91.c-91.d {H/219/35}, Madden3¶81 {G/5/33}	Placks1¶4.01 {I/1/7}, 6.01 {I/1/11}, 6.09 {I/1/13}, 6.38 {I/1/16}		M&P: Manipulated {Q/2/7}	
ID_000536 {L2/474} ({A/2/60})	Bitcoin White Paper PDF1 craigswright@acm.org	No	Wright11 AxB §13 {CSW/2/48}	{Day3/p160} – {Day3/p170}		PM3¶6 {H/20/2}, PM3¶10 {H/20/4}, PM3¶89-128 {H/20/27}, PM3¶130-133 {H/20/42}, PM3¶138 {H/20/45}, PM3¶142 {H/20/47}, PM3¶145 {H/20/47}, PM3¶146-148 {H/20/47}, PM3¶151-156 {H/20/49}, PM3¶160-162 {H/20/55}, PM3¶166-167 {H/20/56},PM3¶168-171 {H/20/57}, PM3¶233 {H/20/77}, PM3¶242 {H/20/79}, PM4¶15-16 {H/29/3}, PM4¶41-58 {H/29/12}, PM4¶60 {H/29/18}	Placks1¶7.22, Placks2§5 {I/6/8}, 6.02 {I/6/10}, 7.04-7.05 {I/6/11}		M&P: Manipulated {Q/4/4}	JHOp {Day1/p8}
ID_000537 {L5/28} ({A/2/62})	Bitcoin White Paper PDF2 craigswright@acm.org	No	Wright11 AxB ¶¶20.7-20.13 {CSW/2/65}	{Day3/p170} – {Day3/p172}		PM3¶6 {H/20/2}, PM3¶10 {H/20/4}, PM3¶129-145 {H/20/42}, PM4¶15-16 {H/29/3}, PM4¶59-63 {H/29/17}, PM43¶13-62 {H/238/4}	Placks2§6 {I/6/10}, 7.05 {I/6/11}		M&P: Manipulated {Q/4/4}	JHOp {Day1/p75}
ID_000538 {L5/16} ({A/2/65})	Bitcoin White Paper PDF3 craigswright@acm.org	No		{Day3/p172} – Day3/p176}, {Day8/p191} – {Day8/p192}		PM3¶6 {H/20/2}, PM3¶10 {H/20/4}, PM3¶146-167 {H/20/47}, PM4¶15-16 {H/29/3}, PM4¶59-63 {H/29/17}	Placks2§7 {I/6/11}		M&P: Manipulated {Q/4/4}	
ID_000549 {L3/288} ({A/2/67})	Maths.doc	Yes	Wright1(List) {E/1/42}	{Day3/p50} – {Day3/p55}		PM1¶14 {H/1/4}, PM1¶35 {H/1/13}, PM24¶8 {H/116/3}, PM24¶16 {H/116/5}, PM24¶37 {H/116/13}, PM24¶41 {H/116/14}, PM28¶14 {H/124/5}, PM34 {H/139/1}, PM35¶9-10 {H/141/5}, PM35¶12 {H/141/5}, PM43¶13 {H/219/5}	Placks1¶4.01 {I/1/7}, 6.01 {I/1/11}, 6.09 {I/1/13}, 6.12 {I/1/14}, 6.43 {I/1/17}		M&P: Manipulated {Q/2/7}	

ID_000550 {L3/237} ({A/2/69})	BitCoin: SEIR-C propagation models of block and transaction dissemination	Yes	Wright1(List) {E/1/42}, Wright11 AxB ¶14 {CSW/2/52}	{Day2/p132} – {Day2/p144},
				{Day8/p133} – {Day8/p140},
				{Day8/196} – {Day8/198}
					Wuille1¶24-25 {C1/1/6}
					Wuille1¶29-32 {C1/1/7}
					Wuille1¶50 {C1/1/12}
						Madden1¶14.a {G/1/8}, PM1 {H/1/1}, PM24¶3 {H/116/1}, PM24¶8 {H/116/3}, PM24¶16 {H/116/5}, PM24¶37 {H/116/13}, PM24¶41 {H/116/14}, PM26¶18 {H/121/5}, PM28¶9 {H/124/4}, PM28¶21 {H/124/7}, PM34¶9 {H/139/3}, PM34¶11 {H/139/5}, PM34¶20{H/139/7}, PM40¶1-2 {H/156/1}, PM40¶30 {H/156/12}, PM40¶32 {H/156/13}, PM40¶42	Placks1¶4.01 {I/1/7}, 6.01 {I/1/11}, 6.09 {I/1/13}, 6.32-6.33 {I/1/16}, 6.38 {I/1/16}, 6.40-6.41 {I/1/17}		M&P: Manipulated {Q/2/7}	

Document Bundle Ref (Pleading)	Short document description	Reliance doc	Wright evidence	Wright XX Refs	Other witness evidence	Madden	Placks/Stroz	Madden XX	Joint report	Other Transcript Refs
						{H/156/16}, Madden2¶35.b {G/3/13}, Madden2¶52 {G/3/22}, Madden2¶64 {G/3/24}, Madden2¶127 {G/3/43}, PM43.17 {H/237N/1}, PM43¶13 {H/219/6}, Madden3¶81 {G/5/33}, Madden4¶159.i {G/6/53}				
ID_000551 {L3/184} ({A/2/71})	The study of Complex networks	Yes	Wright1(List) {E/1/43}	{Day3/p32} – {Day3/p38}	Wuille1¶13-20 {C1/1/3}	PM24¶8 {H/116/3}, PM24¶16 {H/116/5}, PM24¶37 {H/116/13}, PM24¶41 {H/116/14}, PM34¶5 {H/139/2}, PM35 {H/141/1}, Madden2¶51 {G/3/20}, PM43¶13 {H/219/6}	Placks1¶4.01 {I/1/7}, 6.01 {I/1/11}, 6.09 {I/1/13}, 6.12 {I/1/13}, 6.21 {I/1/15}, 6.44-6.45 {I/1/18}		M&P: Manipulated or unreliable {Q/2/7}	
ID_000554 {L3/326} ({A/2/73})	Code2Flow source code flowchart	Yes	Wright1(List) {E/1/43}, Wright4¶45 {E/4/18}, Wright11 AxB §15 {CSW/2/55}	{Day4/p31} – {Day4/p37}		PM10 {H/63/1}, PM24¶41 {H/116/14}, Madden2¶91 {G/3/31}, PM43¶69-77 {H/219/28}, PM46¶166-176 {H/278/57}	Placks1¶4.01 {I/1/7}, 11.01-11.03 {I/1/43}, 11.06-11.08 {I/1/43}		M&P: Manipulated {Q/2/7}	
ID_000568 {L3/224} ({A/2/75})	BITCOIN Notes vs Commodity	Yes	Wright1(List) {E/1/42}	{Day3/p92} – {Day3/p94}		PM24¶8 {H/116/3}, PM24¶37 {H/116/13}, PM24¶41 {H/116/14}, PM28¶9 {H/124/4}, PM36 {H/143/1}, PM37¶17 {H/144/4}, Madden2¶53.c {G/3/22}, PM43¶13 {H/219/5}	Placks1¶4.01 {I/1/7}, 6.01 {I/1/11}, 6.09 {I/1/13}, 6.12 {I/1/13}		M&P: Manipulated {Q/2/7}	
ID_000569 {L3/264} ({A/2/77})	Bitcoin (law)	Yes	Wright1(List) {E/1/42}	{Day3/p94} – {Day3/p96}		PM1¶14 {H/1/4}, PM24¶8 {H/116/3}, PM24¶37 {H/116/13}, PM24¶41 {H/116/14}, PM37 {H/144/1}, PM39¶18.a {H/148/8}, PM43¶6 {H/219/3}, PM43¶13-14 {H/219/5}	Placks1¶4.01 {I/1/7}, 6.01 {I/1/11}, 6.09 {I/1/13}, 6.12 {I/1/13},6.25 {I/1/15}		M&P: Manipulated {Q/2/7}	
ID_000739 {L3/474} ({A/2/79})	bitcoin.exe	No	Wright1(List) {E/1/43}, Wright11 AxB §16 {CSW/2/56}	{Day4/p43} – {Day4/p53}, {Day4/p90} – {Day4/p96}		PM12¶1-4 {H/68/1}, PM12¶7-9 {H/68/2}, PM12¶11-13 {H/68/4}, PM12¶20.b {H/68/10}, PM12¶28-30 {H/68/14}, PM12¶38-39 {H/68/16}, PM12¶42-45 {H/68/17}, PM12¶48-51 {H/68/20}, Madden2¶17.c {G/3/9}	Placks2§8 {I/6/13}		M&P: Manipulated {Q/4/4}	JHOp {Day1/p48} – {Day1/p50}
ID_000848 {L4/188} ({A/2/81})	debug.log	No	Wright1(List) {E/1/43}	{Day4/p53} – {Day4/p60}		PM11¶1 {H/64/1}, PM11¶8-9 {H/64/2}, PM11¶12-13 {H/64/6}, PM11¶22-47 {H/64/12}, PM12¶14 {H/68/7}, PM12¶22 {H/68/10}	Placks2§9 {I/6/15}		M&P: Manipulated or unreliable {Q/4/4}	
ID_001317 {L8/441} ({A/2/83})	I cannot do the Satoshi bit anymore email	No				PM18¶1 {H/83/1}, PM18¶10 {H/83/3}, PM18¶92-94 {H/83/39}	Placks2§10 {I/6/16}		M&P: Manipulated {Q/4/4}	
ID_001318 {L8/446} ({A/2/85})	Defamation and the difficulties of law on the Internet email (2)	No	Wright4¶93-98 {E/4/31}	{Day4/p68} – {Day4/p73}	Wright closing in Kleiman {L17/336/134}	PM18¶1 {H/83/1}, PM18¶10 {H/83/3}, PM18¶32-57 {H/83/10}, PM18¶83-87 {H/86/36}, PM45¶55-61 {H/241/23}, PM45¶65-66 {H/241/24}	Placks2¶4.03 {I/6/7}, §11 {I/6/17}		M&P: Manipulated {Q/4/4}	JHOp {Day1/p71} – {Day1/p73}
ID_001379 {L1/79} ({A/2/87})	Project "Blacknet"	Yes	Wright11 AxB §17 {CSW/2/59}	{Day2/p56} – {Day2/p68}		PM8 {H/60/1}, PM9¶2 {H/62/1}, PM9¶131-132 {H/62/51}, PM9¶141 {H/62/53}, PM18¶3 {H/83/1}, PM8¶12-13 {H/83/3}, Madden2¶86-90 {G/3/29}, PM43¶62-68 {H/219/26}	Placks1¶4.01 {I/1/7}, 10.01-10.11 {I/1/40}, 10.13 {I/1/42}		M&P: Manipulated or unreliable {Q/2/7}	JHOp {Day1/p70}

Document Bundle Ref (Pleading)	Short document description	Reliance doc	Wright evidence	Wright XX Refs	Other witness evidence	Madden	Placks/Stroz	Madden XX	Joint report	Other Transcript Refs

ID_001386 {L9/218} ({A/2/89})	I think you are mad and this is risky email	No		{Day4/p119} – {Day4/p124}	Wright5¶68 [Tulip] {S1/1.13/22}
					Wright xx in Kleiman {L17/285/192}
						PM4¶15-16 {H/29/3}, PM4¶109-114 {H/29/34}, PM14¶5-18 {H/73/2}, PM14¶20 {H/73/8}, PM14¶23 {H/73/9}, PM14¶28-29 {H/73/11}, PM14¶34 {H/73/12}, PM4¶36-37 {H/73/13}, PM4¶39-40 {H/73/13}	Placks2§12 {I/6/18}		M&P: Manipulated {Q/4/4}	

ID_001421 {L9/214} ({A/2/91})	Purchase Invoice for Tulip Trading Limited	No		{Day4/p127} – {Day4/p129}	Wright xx in Kleiman {L17/285/215-220}	PM4¶15-16 {H/29/3}, PM4¶115-121 {H/29/37},PM4¶42-55 {H/73/14}, PM14¶70-71 {H/73/25} PM3¶73 {H/73/26}, PM48¶2 {H/304/2}	Placks2§13 {i/6/20}		M&P: Manipulated {Q/4/4}	
ID_001541 {L8/64} ({A/2/93})	We have now a company in the UK email	No				PM4¶15-16 {H/29/3}, PM4¶78-83 {H/29/24}, PM4¶86-87 {H/29/27}, PM18¶2 {H/83/1}, PM18¶101-109 {H/83/43}	Placks2§14 {I/6/21}		M&P: Manipulated {Q/4/4}	
ID_001546 {L8/338} ({A/2/95})	Thank you for being on board email	No	Wright11 AxB §18 {CSW/2/61}	{Day4/p60} – {Day4/p68}		PM21¶1-35 {H/104/1}, PM21¶48-49 {H/104/14}, PM21¶74 {H/104/20}, PM21¶76-93 {H/104/21}	Placks2§15 {i/6/22}		M&P: Unreliable {Q/4/5}	
ID_001919 {L7/386} ({A/2/97})	Tulip Trading Company and Trust memo	No				PM14¶98-102 {H/73/36}	Placks2§16 {I/6/23}		M&P: Manipulated or unreliable {Q/4/4}	
ID_001925 {L7/377} ({A/2/99})	Declaration of Trust relating to Tulip Trading Ltd	No		{Day4/p124} – {Day4/p129}		PM4¶15-16 {H/29/3}, PM4¶132-137 {H/29/44}, PM14¶108-147 {H/73/40}	Placks2§17 {I/6/24}		M&P: Manipulated {Q/4/4}	
ID_001930 {L7/357} ({A/2/101})	Application for Incorporation of Tulip Trading Ltd etc	No		{Day4/p129} – {Day4/p133}		PM4¶15-16 {H/29/3}, PM4¶132-137 {H/29/44}, PM14¶108-116 {H/73/40}, PM14¶148-174 {H/73/56}	Placks2§18 {I/6/25}		M&P: Manipulated {Q/4/4}	
ID_002586 {L9/441} ({A/2/103})	Michele Seven email	No		{Day4/p68} – {Day4/p68}		PM21¶1-5 {H/104/1}, PM21¶36-55 {H/104/10}, PM21¶74 {H/104/20}, PM21¶76-93 {H/104/21}	Placks2§19 {I/6/26}		M&P: Unreliable {Q/4/6}	
ID_003330 {L15/227} ({A/2/105})	Bitcoin White Paper – coffee-stained	Yes	Wright11 AxB ¶¶20.2-20.4 {CSW/2/64}	{Day4/p7} – {Day4/p9}		PM15 {H/74/1}, PM44 {H/238/27} Madden2¶10.b {G/3/7}, Madden2¶35.a {G/3/13}, Madden2¶82 {G/3/29}	Placks2§20 {I/6/27}		M&P: Manipulated or unreliable {Q/2/8}	

ID_003455 {L15/100} ({A/2/108})	NAB account details	No	Wright3 in BTC Core Claim {E1/4/1}
			Wright11¶171 fn112 {CSW/1/34},
			Wright11 AxB §19 {CSW/2/62}
				{Day2/p43} – {Day2/p44}		PM17 {H/78}	Placks2§21 {I/6/28}		M&P: Manipulated {Q/4/5}	JHOp {Day1/p51} – {Day1/p56}

ID_003702 {L15/442} ({A/2/110})	Northumbria University LLM Dissertation Proposal Payments Providers and Intermediaries as defined in the Law of the Internet LLM_ProposalA.doc (2)	Yes	Bridges1(list) {E/9/8},
			Wright11¶140-169 {CSW/1/27}
				{Day3/p67} – {Day3/p68}		PM3¶6-7 {H/20/2}, PM3¶11 {H/20/5}, PM25 {H/118/1}, PM43¶54-61 {H/219/23}, PM43.17 {H/237N/1}	Placks1¶4.01 {I/1/7}, 6.01 {I/1/11}, 6.05 {I/1/12}, 7.16 {I/1/21}		M&P: Manipulated {Q/2/8}	JHOp {Day1/p34}
										XXDB {Day11/p9} - Day11/p11}

ID_003732 {L5/27} ({A/2/111})	Bitcoin White Paper csw26@leicester.ac.uk	No				PM3¶6 {H/20/2}, PM3¶10 {H/20/5}, PM3¶75-88 {H/20/21}, PM3¶91.e {H/20/28}, PM3¶94 {H/20/29}, PM3¶98 {H/20/30}, PM3¶112-114 {H/20/35}, PM3¶128 {H/20/42}, PM3¶132 {H/20/43}, PM3¶151 {H/20/49}, PM3¶159	Placks2§22 {I/6/29}		M&P: Manipulated or unreliable {Q/4/5}	

Document Bundle Ref (Pleading)	Short document description	Reliance doc	Wright evidence	Wright XX Refs	Other witness evidence	Madden	Placks/Stroz	Madden XX	Joint report	Other Transcript Refs
						{H/20/55},PM3¶163 {H/20/56}, PM3¶166 {H/20/56},PM3¶172 {H/20/58}, PM3¶244 {H/20/79}, PM4¶15-16 {H/29/4}, PM4¶18-39 {H/29/4}, PM4¶44-47 {H/29/13}, PM43¶6 {H/219/3}, PM44¶1-7 {H/238/1}				
ID_004010 {L20/341} ({A/2/113})	Bitcoin White Paper – coffee-stained, rusty staples	Yes		{Day3/p176} – {Day3/p181}		PM3¶6 {H/20/2}, PM3¶10 {H/20/4}, PM3¶192-204 {H/20/63}	Placks1¶4.01 {I/1/7}, 7.16 {I/1/21}, 7.21 {I/1/22}, 7.24 {I/1/22}		M&P: Manipulated {Q/2/8}	
ID_004011 {L2/234} ({A/2/105})	Bitcoin White Paper – coffee-stained (2)	Yes	Wright11 AxB §20 {CSW/1/64}	{Day4/p9} – {Day4/p24}		PM3¶6 {H/20/2}, PM3¶10 {H/20/5}, PM3¶245 {H/20/80}, Madden2¶81-82 {G/3/28}, PM43¶8-62 {H/238/2}	Placks1¶4.01 {I/1/7}, 7.16 {I/1/21}, 7.21 {I/1/22}, 7.23 {I/1/22}		M&P: Manipulated or unreliable {Q/2/8}	SMXX{Day11/p90} – {Day11/p104}, {Day12/97} – {Day12/98}

ID_004013 {L2/159} ({A/2/114})	Handwritten BDO Minutes	Yes	Wright11 AxB §21 {CSW/1/66}	{Day3/p102} – {Day3/p114}	Wright xic in Kleiman {L17/327/84}
					Wright closing in Kleiman {L17/336/149}
					Stathakis & Lee {C/16/1}
						PM5 {H/31/1}, Madden2¶83-84 {G/3/29}	Placks1¶4.01 {I/1/7}, 8.01-8.13 {I/1/24}		M&P: Manipulated {Q/2/9}	

ID_004019 {L2/245} ({A/2/116})	Tominaka Nakamoto: Monumenta Nipponica	No	Wright11 AxB §22 {CSW/1/68}	{Day2/p16 } – {Day2/p25}		PM6¶1-12 {H/40/1}, PM6¶22-23 {H/40/13}, PM6¶26 {H/40/15}, PM6¶31-57 {H/40/21}	Placks2§23 {I/6/30}		M&P: Manipulated or unreliable {Q/4/5}	
ID_004077 {L5/150} ({A/2/118})	MYOB accounting screenshot 1	Yes	Wright11 AxB §23 {CSW/1/69}	{Day3/p114} – {Day3/p139}, {Day4/p3} – {Day4/p7}, {Day5/p42} – {Day5/p45}, {Day15/p10} – {Day15/p43}		PM7 {H/47}, PM42¶12-21 {H/209/3}	Placks1¶4.01 {I/1/7}, 9.01 {I/1/26}, 9.03 {I/1/24}, 9.06 {I/1/28}, 9.08 {I/2/29}, 9.13 {I/1/30}, 9.25-9.27 {I/1/32}		M&P: Manipulated {Q/2/9}	
ID_004078 {L5/471} ({A/2/118})	MYOB accounting screenshot 2	Yes	Wright11 AxB ¶23.8-23.15 {CSW/2/70}	{Day3/p114} – {Day3/p139}, {Day4/p3} – {Day4/p7}, {Day5/p42} – {Day5/p45}, {Day15/p10} – {Day15/p43}		PM7 {H/47}, PM42¶12-17 {H/209/3}	Placks1¶4.01 {I/1/7}, 9.01 {I/1/26}, 9.04 {I/1/27}, 9.13 {I/1/30}, 9.25 {I/1/32}, 9.28 {I/1/33}		M&P: Manipulated {Q/2/9}	
ID_004079 {L5/146} ({A/2/118})	MYOB accounting screenshot 3	Yes	Wright11 AxB ¶23.8-23.15 {CSW/2/70}	{Day3/p114} – {Day3/p139}, {Day4/p3} – {Day4/p7}, {Day5/p42} – {Day5/p45}, {Day15/p10} – {Day15/p43}		PM7 {H/47}, PM42¶12-17 {H/209/3}	Placks1¶4.01 {I/1/7}, 9.01 {I/1/26}, 9.05 {I/1/28}, 9.13 {I/1/30}, 9.24 {I/1/32}, 9.29 {I/1/33}		M&P: Manipulated {Q/2/9}	
ID_004515 {L7/213} ({A/2/120})	RDPlan – DeMorgan.doc email	No		{Day2/p103} – {Day2/p106}		PM9 {H/62/1}, PM43.17 {H/237N/1}	Placks2§24 {I/6/32}		M&P: Manipulated {Q/4/5}	

Document Bundle Ref (Pleading)	Short document description	Reliance doc	Wright evidence	Wright XX Refs	Other witness evidence	Madden	Placks/Stroz	Madden XX	Joint report	Other Transcript Refs
ID_004516 {L1/91} ({A/2/122})	Project "Spyder" document	No		{Day2/p98} – {Day2/p100}		PM9¶1 {H/62/1}, PM9¶5 {H/62/2}, PM9¶67-94 {H/62/19}, PM9¶131-132 {H/62/51}, PM9¶137-139 {H/62/52}, PM9¶141-143 {H/62/53}, PM43.17 {H/237N/1}	Placks2¶24.01 {I/6/32}, §25 {I/6/33}		M&P: Manipulated {Q/4/5}	
ID_004648 {PTR-F/5} ({A/16/14})	Section 4: Hash Chains: An Overview LaTeX file	Yes		{Day5/p112} – {Day5/p113}	Loretan {C/20/1}	Madden3¶31-35 {G/5/18}	LynchAx4 {J/22/3}		M&L: Manipulated {Q/6/4}	
ID_004682 {PTR-F/39} {L1/367} ({A/16/17})	A Competing Transaction or Block Model.doc	Yes		{Day5/p104} – {Day5/p106}	Wuille1¶29-32 {C1/1/7}	Madden3¶92-95 {G/5/37}	LynchAx4 {J/22/2}		M&L: Manipulated {Q/6/4}	
ID_004687 {PTR-F/44} ({A/16/14})	360° Security Summit LaTeX file	Yes		{Day5/p106} – {Day5/p112}	Macfarlane {C/19/1} Loretan {C/20/1}	Madden3¶28 {G/5/14}, Madden3¶31-35 {G/5/18}	LynchAx4 {J/22/2}		M&L: Manipulated {Q/6/4}	
ID_004695 {PTR-F/52} ({A/16/19})	The King's Wi-Fi: Leveraging Quorum Systems in the Byzantine Generals Problem for Enhanced Network Security	Yes	Wright11¶1137 fn460 {CSW/1/197}	{Day5/p76} – {Day5/p78}		Madden3¶87-91 {G/5/36}, PM46¶8-40{H/278/4}	LynchAx4 {J/22/1}		M&L: Manipulated {Q/6/4}	
ID_004697 {PTR-F/54} ({A/16/22})	Payments Providers and Intermediaries as defined in the Law of the Internet	Yes		{Day5/p78} – {Day5/p79}		Madden3¶87-91 {G/5/36}, Madden4¶101-105 {H/278/35}	LynchAx4 {J/22/2}		M&L: Manipulated {Q/6/4}	
ID_004712 {PTR-F/69} ({A/16/24})	C++ code	Yes	Wright11¶463 {CSW/1/87}, 465 {CSW/1/87}, 467 {CSW/1/88}, 468 {CSW/1/88}	{Day5/p113} – {Day5/p119}	Hinnant {C/18/1} Stroustrup {C/23/1}	#N/A	LynchAx4 {J/22/3}		M&L: Manipulated {Q/6/4}	XXHH {Day15/p29} – {Day15/p46}
ID_004713 {PTR-F/70} ({A/16/24})	C++ code	Yes	Wright11¶463 {CSW/1/87}, 465 {CSW/1/87}, 467 {CSW/1/88}	{Day5/p119} – {Day5/p120}	Hinnant {C/18/1} Stroustrup {C/23/1}	#N/A	LynchAx4 {J/22/3}		M&L: Manipulated {Q/6/4}	
ID_004715 {PTR-F/72} ({A/16/26})	An In-depth Analysis of Proof-of-Work Calculations in the Hashcoin White Paper: Exploring Alternative Strategies LaTeX file	Yes		{Day5/p79} – {Day5/p84}		PM46¶81-82 {H/278/18}, PM46¶87 {H/278/23}	LynchAx4 {J/22/1}		M&L: Manipulated {Q/6/4}	
ID_004716 {PTR-F/73} ({A/16/26})	section2 LaTeX file	Yes	Wright11¶314 fn154 {CSW/1/59}	{Day5/p84} – {Day5/p85}		Madden4¶134.b {G/6/42}, PM46¶86 {H/278/22}, PM46¶89 {H/278/23}	LynchAx4 {J/22/1}		M&L: Manipulated {Q/6/4}	
ID_004719 {PTR-F/76} ({A/16/26})	section4 LaTeX file	Yes	Wright11¶314 fn154 {CSW/1/59}	{Day5/p85} – {Day5/p86}		PM46¶86 {H/278/22}, PM46¶90 {H/278/24}	LynchAx4 {J/22/1}		M&L: Manipulated {Q/6/4}	
ID_004722 {PTR-F/79} ({A/16/29})	Predicates in Quorum Systems LaTeX file (LPA.tex)	Yes		{Day5/p86} – {Day5/p91}		PM46¶111-116 {H/278/38}, PM46¶119-120 {H/278/42}	LynchAx4 {J/22/2}		M&L: Manipulated {Q/6/4}	
ID_004723 {PTR-F/80} ({A/16/29})	Predicates in Quorum Systems LaTeX file (LP1.tex)			{Day5/p91} – {Day5/p93}		PM46¶117-120 {H/278/41}	LynchAx4 {J/22/2}		M&L: Manipulated {Q/6/4}	
ID_004729 {PTR-F/86}	Hash Based Shadowing handwritten note	Yes		{Day5/p94} – {Day5/p95}		PM46¶121-131 {H/278/43}	LynchAx4 {J/22/1}		M&L: Manipulated {Q/6/4}	

Document Bundle Ref (Pleading)	Short document description	Reliance doc	Wright evidence	Wright XX Refs	Other witness evidence	Madden	Placks/Stroz	Madden XX	Joint report	Other Transcript Refs
({A/16/31})										
ID_004732 {PTR-F/89} ({A/16/33})	Q.txt	Yes		{Day5/p95} – {Day5/p100}		PM46¶132-145 {H/278/45}	LynchAx4 {J/22/2}		M&L: Manipulated {Q/6/4}	
ID_004733 {PTR-F/90} ({A/16/35})	Internal Controls and Immutable Logging in Auditing Backend Operations of Messaging Systems	Yes	Wright11¶1146 fn466 {CSW/1/198}	{Day5/p100} – {Day5/p102}		Madden3¶87-91 {G/5/36}, PM4¶146-149 {H/278/52}	LynchAx4 {J/22/1}		M&L: Manipulated {Q/6/4}	
ID_004734 {PTR-F/91} ({A/16/33})	Secure and Trustworthy Voting in Distributed Networks: A Quorum-Based Approach with Hash Chains and Public Key Infrastructure	Yes	Wright11¶1146 fn466 {CSW/1/198}	{Day5/p95} – {Day5/p100}		Madden3¶87-91 {G/5/36}, PM46¶132-145 {H/278/45}	LynchAx4 {J/22/2}		M&L: Manipulated {Q/6/4}	
ID_004736 {PTR-F/93} ({A/16/37})	ESDT.tex	Yes	Wright11¶1032 fn426 {CSW/1/182}	{Day5/p102} – {Day5/p104}		Madden3¶49-76 {G/5/21}, Madden3¶123-124 {G/5/45}, Madden3¶133 {G/5/47}, PM46¶41-80 {H/278/10}	LynchAx4 {J/22/1}		M&L: Manipulated {Q/6/4}	
BDO Image ({A/16/10})	The BDO Drive Image (BDOPC.Raw)	Yes	Wright5 {E/20/1}, Wright12 {CSW/7/1}	{Day5/p23} – {Day5/p41}		Madden3¶96-165 {G/5/40}	Lynch¶65-89 {I/5/16}	{Day16/p83} – {Day16/p88}	M&L: Manipulated {Q/6/3} ¶6-9	
White Paper LaTeX Files ({A/16/4})	The file "main.tex" in Dr Wright's Overleaf "TC" directory	Yes	Wright6 {E/21/1}, Wright8 {E/23/1}	{Day5/p152} – {Day5/p154}		Rosendahl (G.7.1}	Lynch¶98-122 {I/5/27}		R&L: Not authentic {Q/5/1	
White Paper LaTeX Files ({A/16/4})	The file "E-Cash-main.tex" in Dr Wright's Overleaf "TC" directory	Yes	Wright6 {E/21/1}, Wright8 {E/23/1}			Rosendahl (G.7.1}	Lynch¶98-122 {I/5/27}		R&L: Not authentic {Q/5/1	
White Paper LaTeX Files generally				{Day5/p13} – {Day5/p19 }, {Day5/p155} – {Day5/p157}						
Email to Ontier {X/56/2}	18 February 2024 Email to Ontier RE MYOB	No	Wright15 {E/34/1}	{Day19/p7}- {Day19/p58}		Madden6 {G/11/1}		{Day19/p59} - {Day19/p93}		

Note: this schedule includes all of the forgeries in COPA's Re-Re-Re-Amended Particulars of Claim.

The 20 focussed forgeries identified at the PTR and the 20 further forgeries from Dr Wright's additional Reliance Documents are identified in red.

Appendix 3 – Dr Wright’s production of documents

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’ 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	Macs 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 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 Birds disclosure requests
8 November 2023	VOL012	393	Further hard drive documents
17 November 2023	VOL013	5	Birds 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)

Date	Name/ Volume Number	Number of Documents (where appropriate)	Summary of Contents
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
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