Made on behalf of Defendant in COPA Claim
Made on behalf of Claimants in the Coinbase Claim, the Kraken Claim and the BTC Core Claim
Fourth Witness Statement Dr Craig Steven Wright
Dated 23 October 2023
Exhibits CSW5 – CSW18

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

Claim No. IL-2021-000019
(the "**COPA Claim**")

BETWEEN:

CRYPTO OPEN PATENT ALLIANCE

Claimant

- and -

DR CRAIG STEVEN WRIGHT

Defendant

Claim No. IL-2022-000035
(the "**Coinbase Claim**")

BETWEEN:

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

Claimants

- and -

(1) COINBASE GLOBAL, INC.
(2) CB PAYMENTS, LTD
(3) COINBASE EUROPE LIMITED
(4) COINBASE, INC.

Defendants

Claim No. IL-2022-000036
(the "**Kraken Claim**")

BETWEEN:

(1) DR CRAIG STEVEN WRIGHT

(2) WRIGHT INTERNATIONAL INVESTMENTS LIMITED

Claimants

- and -

(1) PAYWARD, INC.
(2) PAYWARD LTD.
(3) PAYWARD VENTURES, INC

Defendants

Claim No. IL-2022-000069
(the "**BTC Core Claim**")

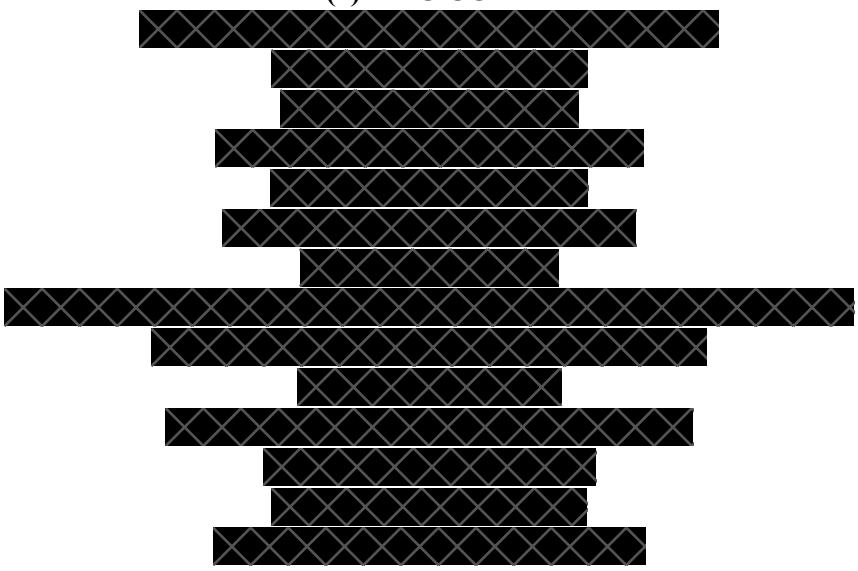
BETWEEN:

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

Claimants

- and –

(1) BTC CORE



(16) BLOCK, INC.
(17) SPIRAL BTC, INC.
(18) SQUAREUP EUROPE LTD
(19) BLOCKSTREAM CORPORATION INC.

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

Defendants

FOURTH WITNESS STATEMENT OF DR CRAIG STEVEN WRIGHT

I, CRAIG STEVEN WRIGHT, [redacted] state as follows:

Introduction

1. I refer to my first, second and third witness statements dated 28 July 2023, 9 October 2023 and 19 October 2023. I make this witness statement in response to requests 1 – 14, 15(b), 23 – 28, 34 – 36, 43 – 44, 51, 53 and 57 – 61 of the Combined Request for Further Information dated 23 June 2023 pursuant to the order of Mr Justice Mellor. I make this statement on my own behalf as Claimant and Defendant in the COPA Claim, Coinbase Claim, Kraken Claim and BTC Core Claim and am also authorised to make it on behalf of the other Claimants in the Coinbase Claim, the Kraken Claim and the BTC Core Claim.

2. To prepare this witness statement, I was sent the requests below and asked to consider them. I then prepared a draft statement, responding to each request. As before, I discussed this with my solicitors, who then amended the draft to reflect my further comments and sent it to me for review and amendments. This process was then repeated until the witness statement was complete.

3. I have been asked to confirm the following:

> "The purpose of this witness statement is to set out matters of fact of which I have personal knowledge. I understand that it is not my function to argue the case,

either generally or on particular points, or to take the court through the documents in the case. This witness statement sets out only my personal knowledge and recollection, in my own words. On points that I understand to be important in the case, I have stated honestly (a) how well I recall matters and (b) whether my memory has been refreshed by considering documents, if so how and when. I have not been asked or encouraged by anyone to include in this statement anything that is not my own account, to the best of my ability and recollection, of events I witnessed or matters of which I have personal knowledge."

I confirm this is correct.

Section A: Requests 1 to 6

4. On 25 September 2023, my then solicitors, Travers Smith LLP, wrote to the court explaining that I was "*willing to agree to identify all authentic drafts of the White Paper in [my] disclosure, specify the date on which each such document was created (to the best of [my recollection], and state whether [I] was aware of any of those documents having since been altered and, if so, in what respects.*" I have addressed this below.

5. At Exhibit CSW5 is a spreadsheet in which I set out those documents I have been able to identify as being drafts of the White Paper, specifying where I am able the date on which the document was created and whether I am aware of it having since being altered.

6. It is important to make the following observations about the requests asked and the responses in the spreadsheet:

    a. For the date of "creation", I have sought to record the date I wrote each draft to the best of my recollection and, when the exact date is not known, I have sought to provide a date range, where possible. However, as it has been over 15 years since I first started drafting the White Paper, it is difficult for me to offer dates for some of the drafts.

b. By “authenticity”, I understand the question being asked is whether the drafts were authored by me (whether under my name or the pseudonym Satoshi Nakamoto). I confirm that this is correct.

c. By “altered”, I understand the question to be whether the metadata or content of the draft has been altered or amended (including saving new versions or creating new documents):

i. The White Paper’s development involved a complex workflow utilising various software platforms, including LaTeX, OpenOffice and Microsoft Word. I also employed various LaTeX tools, including those by Apache, to uplift documents as ODT files. Moreover, all graphical images in the White Paper were produced using LaTeX code and then converted into DVI, PostScript, ODT and PDF formats. This multi-software approach naturally led to multiple versions, some of which may contain errors or inconsistencies.

ii. I did not apply a versioning system in relation to the White Paper. The lack of versioning makes it challenging to pinpoint which versions were being used at any particular time.

iii. Further, I have made (and do make) my research materials readily accessible to my staff members in and consultants to my various companies, including the drafts of the White Paper in the spreadsheet. This open accessibility fosters a collaborative environment and empowers team members with the necessary resources to contribute effectively.

iv. To facilitate this, I simply added files (and add files) to the relevant repository where research materials are organised and categorized, enabling team members and consultants to search and retrieve information effectively. This approach aims to strike a balance between accessibility and security.

v. No record is retained of whether the document has been accessed and, if so, who accessed the document and when, what modifications were made (if

any) or whether a new version or electronic document was created. In particular, there is no version control system to enable tracking of changes, revisions, and updates to research materials over time.

vi. Further, while metadata can provide supplementary information (such as the date of creation, modification, or the identity of the creator) it is not foolproof. Metadata is inherently volatile and is subject to change through a myriad of standard operations. It can be altered, corrupted, or may not even exist for particular files.

vii. In some instances, the documents have been printed and scanned or subject to other forms of reproduction.

viii. I am, therefore, unable to say whether the metadata or content of the drafts has been altered or amended (including saving new versions or creating new documents).

ix. For the documents on which I seek to rely, I have sought to explain who has had custody of that document since its creation in the chain of custody document served on 13 October 2023 (the "Chain of Custody Document"). This includes some of the drafts of the White Paper. The Chain of Custody Document therefore attempts to provide a historical context and timeline for those versions of the White Paper.

x. Each draft of the White Paper has its roots in the TimeCoin documents, examples of which are ID_000525, ID_003931 and ID_0004012. (ID_0004012 is a notepad consisting of 78 handwritten pages) has "Time coin" and "time chain" on the back cover (page 78).

7. As to whether the drafts of the White Paper were "shared with third parties", as explained above, I do not retain records of who has access to these documents. It is, therefore, not possible to provide details on which drafts were shared and, if so, the dates of such sharing or the recipients' identities.

8. I should note that my solicitors have written to the solicitors for the Crypto Open Patent Alliance (COPA) explaining that two additional drives have been identified, "Samsung T1 USB SSD" and "MyDigitalSSD OTG USB SSD". On the former is an image of a drive from when I worked for BDO, the accountancy and business advisory firm (the "**BDO Raw Image**"). I believe that this contains files up to 31 October 2007. I expect I will be supplementing the existing documents on which I rely to include documents from the BDO Raw Image. I believe that there is also an encrypted image on the drive "Samsung T1 USB SSD", the decryption keys for which I cannot find (the "**Encrypted Image**"). This image may also have relevant documents, but they are not accessible.

Section A: Requests 7 to 9

7. More particularly, please state whether the following documents, to which the Defendant referred in his evidence in the Kleinman Litigation trial, appear in his disclosure in these proceedings and, if so, please identify them in the disclosure: a) the handwritten first draft of the White Paper which he said he had written in about March 2008 (see Kleiman transcript, 95/8-9); b) the first typed version of the White Paper (of about 40 pages) which he claimed to have produced in April to May 2008 (see Kleiman transcript, 95,13-15); c) the second version (of about 20 pages) which he claimed to have produced after comments from others on the first typed version (see Kleiman transcript, 96/15-24); d) the third version (of about 10 pages) which he claimed to have produced after comments from others on the second version (see Kleiman transcript, 97/17-20); e) the various later drafts, which he claimed were subsequently produced (each of about 9-10 pages) (see Kleiman transcript, 97/22 to 98/4).

9. In the Kleiman Litigation, I made some generic references to the drafts of the White Paper. In doing so, I was not making a reference to a specific draft in disclosure. It is, therefore, not possible to address these requests.

10. As set out at paragraph 8 above, there are likely to be further relevant documents identified in the BDO Raw Image. The same may apply to any Encrypted Image.

8. For each document identified in response to request 7 above, please state whether it was shared with third parties and, if so, please state the time and method of sharing together with

the details of all such persons. This response need not be answered to the extent that the information has already been provided in response to request to request 6 above.

11. As explained above, I was making generic references to the drafts of the White Paper, not to specific drafts in disclosure. Therefore, it is not possible to explain which draft was shared and, if so, with who. In any event, as set out above, I do not retain records of who had access to some of the drafts.

9. For any documents identified in request 7 above which do not appear in the Defendant's disclosure, please explain what has happened to those documents and why they have not been disclosed.

12. Again, I was making generic references to the drafts of the White Paper and, therefore, it is not possible to explain which draft I was referring to. However, it is likely that certain drafts have been lost due to changes in storage solutions and company servers. As explained above, these may also be on any Encrypted Image.

Section A: Request 10

Please explain the steps the Defendant took to create the Bitcoin.org Website. If the Defendant's case is that he paid for this domain name, please indicate how he paid for it and which documents in the Defendant's disclosure evidence that purchase.

13. I recall buying the domain in August 2008, using Vistomail. It may be useful to explain the situation in relation to Vistomail. Vistomail was an anonymous email service provider, often associated with secure and private communications (for example, I used the email account Satoshi@Vistomail.com). It also operated a domain purchase and hosting service. Vistomail was subsequently discontinued. When this happened, I lost access to the email accounts Satoshi@Vistomail.com.

14. I should note that, yesterday (Sunday, 22 October 2023 at 09.22), I received an email at my email address "craig.wright@hotwirepe.com" (which is used to forward to my RCJBR domain) from "Michael Webber <michael@vistomail.com>" with the subject heading "Your VistoMail.com Account is Ready for Access". This is at Exhibit CSW6. This explains that my "VistoMail.com account is now ready for access. You can log in

using your credentials to enjoy the services and features provided by VistoMail. Your Account Details: · Username satoshi@vistomail.com · Password: [Your Password]. I have not sought to log-in to the account for the following reasons:

a. The email appears to be from Michael Webber. I understand that this is an alternative name for Michael Marquett, who hasn't been associated with Vistomail since 2014 or earlier.

b. In August 2023, I received an offer to buy the domain Vistomail.com from Velizar Sofranov at afternic for US$49 million. I did not take up the offer. As it is no longer available and WHOIS records that it was updated on 14 August 2023, it must have been sold to a third party. A copy of the email is at Exhibit CSW7 and the WHOIS record is at Exhibit CSW8.

c. The email domain in question is hosted on Gmail and has been set up independently. Extracts from Gmail are at Exhibit CSW9 which demonstrate this. As you will see, the recovery telephone number is a US number, ending in 82. The recovery email is bitcoin.org@gmail.com. From my recollection, this is an account that was set-up as a back-up in 2011 for Martti Malmi. For this reason, it is apparent that there is not a clear connection between the email and the Vistomail website. Rather, this raises suspicions that someone has carefully reconstructed the Satoshi email.

d. This leads me to conclude that someone is engaging in a phishing exercise, to try and get me to log-in to vistomail.com and take my password.

e. I should note that, given the above (and the possibility of a carefully reconstructed Satoshi email), I am concerned that a bad actor will use the satoshi@vistomail.com email address over the course of the next few months to say "Craig is not Satoshi". It's important to stress that any emails from this reconstructed address shouldn't be considered authentic Vistomail communications.

f. I should also note that satoshi@vistomail.com is also the recovery email for cites such as the Peer2peer Foundation and other organisations, meaning that there may be adverse postings here.

15. I should note that, while the concerns about phishing and impersonation above are real, the email from "Michael Webber <michael@vistomail.com>" was sent to the correct recovery address (namely, hotwirepe.com) for the satoshi@vistomail.com email. This is the correct recovery address, suggesting that the bad actor has access to some of the data behind Vistomail.com.

16. Returning to creating the Bitcoin.org Website, I do not recall how I purchased the domain name. I had various payment methods available to me then, including accounts with Liberty Reserve and overseas credit cards from companies I formerly operated. If I were to have used my Liberty Reserve account, I may have used LRD (Liberty Reserve Dollar). I believe that the financial records associated with this purchase were initially stored in MYOB accounting software (I was not the MYOB administrator), which have been submitted for forensic analysis. Given the digital nature of MYOB, it offers robust features for auditing and verification.

17. I recall employing a virtual private network (VPN) product for secure and encrypted access to this server, reinforcing the overall security framework. This was acquired from Anonymous Speech, a provider I had used since at least 2004. Initial purchases for these security services were made using my Westpac credit card. I believe that the statements corresponding to these early transactions may be on the BDO Raw Image.

18. I was also responsible for creating the initial content for the website and manually uploading it to the server. This meant that I had heightened control over the website's structure and content. This underscores the depth of my involvement in both the creation and the operational aspects of bitcoin.org. So far as I am aware, there is no initial content for the website in disclosure.

19. With regard to Vistomail, Simon Cohen, then a Managing Associate at Ontier LLP, accessed my Vistomail before it was discontinued. When he did, I understand that he saw records and communications pertaining to the purchase and operation of the

bitcoin.org domain and site. For the avoidance of doubt, my solicitors have asked me to emphasise that this is not a waiver of privilege.

20. I also exhibit videos at Exhibit CSW10 to CSW13, which show me accessing the following:

    a. CSW10: 20190607_130913.mp4: This shows the Satoshi@Vistomail.com account and its link to the PGP key (discussed at paragraph 104 onwards below).

    b. CSW11: 20190607_132440 1.mp4: This is a similar video to the above.

    c. CSW12: 20190607_133553.mp4: The video shows the Domain and hosting - Bitcoin.org.

    d. CSW13: 20190607_135057.mp4: This video shows the Satoshi@Vistomail.com email that people know and the link to my student account at CSU in Australia. Vistomail allows you to externally link accounts (or allowed) and I had integrated my personal email into Vistomail to simplify sending.

21. I should note that, if you look at the date in the top right of some of the videos, it says "Membership Until 2009/12/07". To be clear, this is when my subscription ended, but I continued the free version. It does not mean that the videos were taken in 2009.

22. The PGP key on the server was linked to the GMX account but was a Vistomail function.

23. These were taken on 7 June 2019 using a mobile phone. I do not recall which mobile phone I used or which laptop I was recording. I understand from my solicitors that these videos may not be in disclosure. If so, I do not understand why not. In particular, they were previously provided to at least Ontier and Travis Smith. I have been asked to emphasise that referring to this is not a waiver of privilege.

24. It may be useful to provide the following information:

    a. Vistomail was an anonymous email service provider, often associated with secure and private communications. While the specifics about its capabilities may vary based on the version and updates, the general process for importing external

emails into a secure, anonymous email service like Vistomail typically involves the use of standard email protocols like POP3 (Post Office Protocol 3) or IMAP (Internet Mail Access Protocol).

b. To import external emails, users would configure their Vistomail accounts to fetch emails from their other, external email accounts. The POP3 or IMAP server settings of the external email provider would need to be entered into Vistomail's account settings. This information typically includes the server address, port, and the type of encryption used (e.g., SSL/TLS). Upon successful configuration, Vistomail would connect to the external email servers and download messages into the Vistomail inbox or a designated folder, thus allowing users to access emails from multiple accounts in a single interface.

c. However, it is crucial to note that while importing emails from an external account into a secure email service might centralize your communications, it does not retroactively apply the security features of the secure email service to the imported emails. Messages sent to or from the external account would still be subject to the security measures, or lack thereof, of the external email provider.

d. The ability to import external emails serves as a functional convenience but is not a guarantee of increased security or privacy for those particular messages. Therefore, users keen on privacy and security should be discerning when importing external emails into any secure email service. However, I had linked these so my CSU student email was available.

e. In secure email platforms like Vistomail, it was possible to generate a PGP key pair that was associated with an external email address, even if that email address is not on the Vistomail server (e.g. the GMX address). To accomplish this, users would typically navigate to the PGP settings within their Vistomail account, found in the security or encryption section. Once there, the option to generate a new PGP key pair was provided. During this process, the system would prompt the user for an email address. At this point, an external email address (say, from a GMX account) could be entered. Following key generation parameters like

algorithm type and key length, and adding an optional passphrase for additional security, the key pair is then generated. The resulting public and private keys are stored on the Vistomail server but are associated with the external email address entered earlier.

f. It's important to note that while this process enables encrypted communication to and from the external email address, the actual level of security is contingent upon the management of the key pair. In particular, messages sent to the external email address can be encrypted by anyone who possesses the public key, but these encrypted messages can only be decrypted using the private key stored in the Vistomail account.

Section B: Requests 11-14

11. Please by reference to the documents in the Defendant's disclosure, which versions of the White Paper in that disclosure (if any) correspond to (a) the version referred to in paragraph 52; and (b) the version referred to in paragraph 53.

12. For each disclosure document identified in response to Request 11 above, please state the date of creation for that document. If the date of creation is not known with certainty, please if possible state the approximate date of creation or give the most precise date range possible for the period in which the document was created.

13. For each disclosure document identified in response to Request 11 above, please state whether it is the Defendant's case that that document is authentic.

14. For each disclosure document identified in response to Request 11 above, please state if that document has been altered in any way since it was first created in its full form. If it has been altered, please give full particulars of: (a) the nature of the alteration; (b) the time of the alteration; (c) who altered it; and (d) what was the purpose of altering it.

25. Before addressing these questions, it is imperative to clarify that the uploading of the versions of the White Paper to the Social Science Research Network (SSRN) in 2019 was not intended as proof or evidence that I was Satoshi Nakamoto. SSRN is devoted to the public display and distribution of scholarly research. I considered it important

that it published the final version of the White Paper from 2019 (the uploaded should not be misconstrued as an unaltered native document from 2008). I initially tried to upload under the name Satoshi Nakamoto, but the submission was rejected. I was told by SSRN that the author's real name needed to be used. For this reason, I uploaded it again but in my name.

26. Turning to the questions, I do not know what versions of the White Paper in disclosure (if any) correspond to the first version which I tried to upload and the second version which I uploaded to SSRN. As explained at paragraph 6, I did not apply a versioning system to the White Paper. The lack of versioning makes it challenging to pinpoint correspondences to the versions discussed above. I wish to emphasise that the absence of being able to identify the documents in disclosure should not be interpreted as an evasion of the query, but rather it is an inherent outcome of the document's unversioned nature.

27. For the avoidance of doubt, by "authenticity" I understand the question being asked is whether the versions were authored by me (whether under my name or the pseudonym Satoshi Nakamoto). I confirm that this is correct.

Section C: Request 15(b)

In relation to each of these five concepts [(i) digital currency systems (ii) audit technologies (iii) incentive systems (iv) peer networks and (v) digital signatures and key exchange systems], please state: … If documents were produced [relating to a concept], please identify them in the Defendant's disclosure or explain why they have not been disclosed.

28. At Exhibit CSW14 is a spreadsheet in which I set out those documents I have been able to identify as being documents relevant to the concepts on which the White Paper was based which I had been working on for many years. Where those documents are not in disclosure, there are at Exhibit CSW15. Where they are not in disclosure, this is because they are in the public domain.

Section F: Requests 23 – 28

23. Please explain when and how the Defendant came into possession of the hard drive containing these private keys.

29. To generate the private keys for all blocks mined (including blocks 1-11), I created an algorithm for key generation. The algorithm was contained in an encrypted file housed in a server image. The process itself was straightforward: the algorithm was run for the specific block and the key was generated. The key would then be transferred to a hard drive for storage. My last known location of the server image was on my QNAP NAS System.

30. The QNAP NAS System was taken by Alix Partners in 2019. I have been provided with the Disclosure Certificate which explains that Annex 1 of Section 2 of the Disclosure Review Document dated 7 March 2023 and this lists the servers as encrypted and, therefore, the documents have not been accessed.

31. The hard drive which contained the private keys which I used for the private demonstrations in 2016 was likely purchased by me from a retail store. Unfortunately, I do not recall when or where.

24. Please list which blocks' private keys (other than those for block 9) were contained on this hard drive.

32. As set out above, I did not indefinitely store individual private keys for blocks on a hard drive. Instead, I employed an algorithm capable of calculating these keys as and when needed. For the demonstrations, I employed the algorithm for the keys for blocks 1-11. Therefore, the hard drive did not contain a list of keys for specific blocks beyond this.

25. Please explain when the Defendant destroyed this hard drive.

27. Please explain how he destroyed it.

33. I destroyed the hard drive in around May 2016 but I do not recall the exact date. This was done at my former residence in Wimbledon. I threw the hard drive with enough force to shatter the glass platters in the hard drive. This destroyed the physical components of the drive rendering the data stored on it irretrievable.

26. Please explain why the Defendant destroyed this hard drive

34. Being autistic adds an extra layer of complexity to how I process and respond to emotional stimuli. When I felt deceived by Robert McGregor and others, it triggered a heightened emotional response that clouded my judgment. Autism often manifests in intense focus and a desire for consistency and trust, elements that I felt were compromised in this situation. This betrayal regarding the principles upon which I had invested so much intellectually and emotionally in creating Bitcoin led to a reactive decision. I impulsively destroyed the hard drive without fully contemplating the long-term consequences.

35. I had been looking forward to a comprehensive review of all my papers and the intricate work that went into creating Bitcoin. This was about showcasing the technical aspects and the philosophical underpinnings I hold dear. When I realised that the people around me were not acting in accordance with the trust and principles I valued, I was overwhelmed. My immediate response was to protect what I could control, leading to the destruction of the hard drive. This was not a calculated action but a reaction influenced heavily by my emotional state.

28. Who witnessed the Defendant destroying this hard drive, or did he undertake this act alone?

36. Given my emotionally charged state at the time, I don't recall if anyone witnessed me destroying the hard drive or if someone else was present.

Section H: Request 34

34 ... Please therefore identify by list (by reference to version numbers along with the string used to identify those versions in the filename): (a) all versions of the Bitcoin software that the Defendant alleges were created in the period 2007 to 2009 inclusive; and (b) all versions of the Bitcoin Source Code that the Defendant alleges to have created in the period 2007 to 2009 inclusive; and (c) all relevant dates of creation of each of those versions.

37. I created all versions of the Bitcoin software in the period between 2007 and its initial release in 2009. The Bitcoin source code was maintained using TortoiseSVN (which

assists programmers to manage different versions of source code) on a distributed depository.

38. In my setup, I utilised a dual-server architecture to maintain a consistent codebase across multiple locations. The primary Subversion repository was hosted on a web server in Malaysia, accessible through the domain svn.ridges-estate.com. This repository was linked to my email address, craigswright@acm.org. This provided a centralised access point, allowing me to manage my code regardless of where I was.

39. I also operated a secondary server in Melbourne, known as upload.ae, to mirror some of the directories. Upload.ae was linked to my Bigpond company account. I established a mirroring process between the Malaysian and Melbourne servers to ensure data consistency and availability. This offered a backup solution, mitigating the risks associated with having all the data hosted at a single location.

40. Unfortunately, I do not know what happened to the above servers. After 15 years, I expect that they have been decommissioned and destroyed/sold. I also do not have access to my Bigpond company account. craigswright@acm.org is a forwarding service, which does not host (and therefore retain) emails.

41. Utilising Anonymizer as my VPN service, I established a secure channel for remote access to both svn.ridges-estate.com in Malaysia and upload.ae in Melbourne. This VPN usage ensured that the data traffic between these servers and any other point of access was encrypted, effectively creating an extra layer of security to prevent unauthorised data interception or manipulation. Firewall rules were configured precisely to limit access to known IP addresses and specific ports, mitigating the risk of unauthorised access attempts. This was especially crucial given the sensitive nature of the code and data residing on these servers.

42. In addition to these measures, two-factor authentication provided an extra barrier against unauthorised access. This necessitated a password and a second verification step, such as a generated code sent to a secure device (RSA SecurID) to log into the servers.

43. The Bitcoin software and source code was moved to Sourceforge in October 2008. Although the TortoiseSVN is capable of tracking changes in versions of the source code, this information was lost during the transition to Sourceforge. For this reason, I do not have a list of all versions of the Bitcoin software/source code that were created in the period 2007 to 2009 or their dates.

44. After the release of the Bitcoin software, third parties became involved in coding the Bitcoin software on Sourceforge.

To the extent that versions of the Bitcoin Software and Source Code identified in response to request 34 above appear in the Defendant's disclosure, please specify each one by reference to its document production number. To the extent that they do not appear in the Defendant's disclosure, please specify why not.

45. I have been provided with the following documents from disclosure by my solicitors. These show maps of the source code:

    a. ID_000553

    b. ID_000554

    c. ID_000558

    d. ID_000559

    e. ID_000560

    f. ID_000561

    g. ID_000562

    h. ID_000563

    i. ID_000564

    j. ID_000565

46. I have been provided with the following documents from disclosure by my solicitors. These show the Bitcoin source code or software:

a. ID_000758

b. ID_000759

c. ID_000760

d. ID_000761

e. ID_000762

f. ID_000763

g. ID_000764

h. ID_000765

i. ID_000766

j. ID_000767

k. ID_000768

l. ID_000769

m. ID_000770

n. ID_000771

o. ID_000772

p. ID_000773

q. ID_000774

r. ID_000775

s. ID_000776

t. ID_000777

u. ID_000778

v. ID_000779

w. ID_000780

x. ID_000781

y. ID_000782

z. ID_000783

aa. ID_000784

bb. ID_000785

cc. ID_000786

dd. ID_000787

ee. ID_000788

ff. ID_000842

gg. ID_000843

hh. ID_000844

47. However, as I did not retain a list of all versions of the Bitcoin software I created in 2007 to 2009, I cannot say with any certainty when each of the documents in paragraphs 45 and 46 were created or what exactly each is.

48. For completeness, I should note that:

a. There are also two printouts of parts of the source code with handwritten annotations, which are part of my reliance documents:

i. ID_004014; and

ii. ID_004015

b. The BDO Raw Image and Encrypted Image may also contain versions of the Bitcoin source code which were created during this time.

Section I: Request 36

36 For each of the individuals to whom the Defendant in this paragraph claims to have sent a draft of the Bitcoin White Paper, and save to the extent that this request has been answered by the response to request 6 above, please:

(a) provide the name of each individual;

49. From my recollection, I provided drafts of the White Paper to at least the following individuals using my own name:

a. Danielle DeMorgan
b. Shane Patterson
c. Stefan Matthews
d. Dave Kleiman
e. Lynn Wright
f. Don Lynam
g. Max Lynam
h. Edward Archer
i. Shoaib Yousuf
j. Hector Mabborang
k. Neville Sinclair
l. Andrew Sommer
m. John Chesher
n. Mark Archibald
o. Gareth Williams
p. David Bridges
q. Steve Atkinson
r. Rana Paula
s. Nick Rishbeth
t. Robert Jenkins
u. Lloyd Peacock

50. From my recollection, I provided drafts of the White Paper (sometimes a copy / sometimes a link) to at least the following individuals using the Satoshi Nakamoto pseudonym:
    a. Wei Dai
    b. Adam Back
    c. Leslie Lamport
    d. David Chaum
    e. Stefan Brands
    f. Ronald L. Rivest
    g. Adi Shamir
    h. Leonard Adleman
    i. Peter Wayner
    j. Stuart Haber
    k. Douglas Jackson
    l. Barry Downey

51. I also sent a copy of the White Paper as Satoshi Nakamoto to Aura, T., Nikander, P., & Leiwo, J. who are authors of (2001). DOS-Resistant Authentication with Client Puzzles in B. Christianson, J. A. Malcolm, B. Crispo, & M. Roe (Eds.), Security Protocols (pp. 170–177). Springer found at https://doi.org/10.1007/3-540-44810-1_22.

52. Additionally, I provided drafts to representatives from ASX, RailCorp, News Ltd, Hoyts, CentreBet, Sporting Bet and QSCU. I also discussed the concepts with teaching staff from Charles Sturt University, Newcastle University and Northumbria University and members of the SANS Institute (but do not recall who).

(b) state the date(s) on which each individual was sent the draft(s) in question

(c) explain what means the Defendant used to send such draft(s) to each of these individuals

53. Given the amount of time that has elapsed, I cannot recall the specific dates that I sent drafts of the White Paper to each of the individuals above. Similarly, I cannot accurately

confirm the exact means by which I sent the White Paper to the individuals listed above. The means of communication could have included the use of various platforms, ranging from email to physical copies and possibly via secure file transfer protocols within corporate or academic settings.

(d) state whether the relevant draft(s) sent to the individual appear in the Defendant's disclosure and, if so, identify it/them by document production number(s)

(e) state whether any written communications sending or concerning the draft(s) appear in the Defendant's disclosure and, if so, identify it/them by document production number(s)

54. I produced various drafts of the White Paper but did not keep track of various versions (as explained at paragraph 6 above). This is complicated further by the documents undergoing various data migrations, changes in storage media and transfers following company acquisitions. Some of these drafts are in disclosure, but I cannot say with any certainty whether those drafts in disclosure were sent to third parties and, if so, to who and when.

55. I would like to emphasise that where I cannot provide the information requested above, this should not be interpreted as an unwillingness to comply but rather as a limitation imposed by the passage of time and the complex circumstances surrounding the storage and transmission of these documents.

Section L: Requests 43 & 44

43. Please identify the "email correspondence" referred to in the first sentence of paragraph 31C(1). For each such email, please state whether it appears in the Defendant's disclosure. If so, please identify it by document production number. If not, please explain why it does not appear in disclosure.

56. I do not have records of the email correspondence prior to June 2015 (namely, prior to the making of the series of agreements from June 2015 onwards, one of which was the EITC Agreement). This is because I have not had access to my DeMorgan emails since

2015 and my nCrypt emails since 2016. As a result, this email correspondence is not included in disclosure.

44. Please explain what documents are referred to in the second sentence of paragraph 31C(1) which the Defendant claims to have identified as relating to his authorship of the White Paper. For each such document, please state whether it appears in the Defendant's disclosure. If so, please identify it by document production number. If not, please explain why it does not appear in disclosure

57. In around 2014, I believe that Stefan Matthews may have told Rob McGregor that I was Satoshi Nakamoto. In 2015, Rob conducted a due diligence exercise of the intellectual property held by the DeMorgan group. This was in anticipation of him investing in the DeMorgan group and nCrypt, with a view to the investment being used to try and commercialise the intellectual property. As a result, he and his lawyers were given access to all of my research and development documents, which included drafts of the White Paper.

58. In paragraph 31(C)(1) of the Re-Re-Amended Defence, when I refer to me identifying certain documents relating to the authorship of the White Paper and indicating that I was the author of the White Paper, I am referring to this due diligence exercise. I do not have any record of the due diligence exercise and so I am unclear as to which specific documents were reviewed.

59. I expect that some of the documents which formed part of the due diligence exercise are included in disclosure. I have listed drafts of the White Paper in the spreadsheet at Exhibit CSW5. There may also be some of these documents on the BDO Raw Image. Some of the documents may also be on the QNAP NAS system, which Alix Partners have been unable to access (see paragraph 30 above).

Section N: Requests 51 & 53

51 As to the moving of exchange servers, please give full details of:(a) The date on which this took place. (b) The person(s) who undertook this moving of exchange servers. (c) What access remains to the original server and, if there is no access, why that is the case. (d) What was the reason for the move? (e) What technical process was utilised for moving exchange

servers, including the details of all software used. (f) What, if any, backups and precautions were taken during the transfer of this data from one exchange server to another; what backups, if any were made before the move; and what has happened to those backups if such existed.

60. Before addressing the request, it may be useful to explain the relevant companies and my role within them.

61. Since around 1991, I have had a number of businesses which I used for specific research projects, including Craig Wright R&D, Craig S Wright R&D, CSW R&D and CW R&D.

62. Ridges Estate Pty Ltd was a company that I founded around 2000. It was used to contract labour back to DeMorgan Information Security Systems Pty Ltd. It continued until around 2007, when it was closed. Before I closed this entity, I transferred the assets into the business Craig Wright R&D. This included all of the ongoing work and previous research that I had done until this period.

63. In around 2009, I started Information Defense Pty Ltd. In mid-2009, I also started another company, Integyrs Pty Ltd, which was to focus on cryptographic algorithm design and secure coding. Later in the year, I also recall starting another company John Keeble and others. This company was renamed Greyfog Pty Ltd, which was an IoT device company that was linked to the blockchain. There were other companies as well.

64. My then wife, Lynn Wright, started Cloudcroft Pty Ltd (I do not know when). The assets of Information Defense Pty Ltd was transferred to this when we separated. Lynn did not put a lot of effort into running it, and the business went into receivership. I purchased this from her on 30 December 2012 and transferred it into a company that my current wife, Ramona, and I founded in mid-2011. This company was called Panopticrypt Pty Ltd.

65. Hotwire Pre-Emptive Intelligence Pty Ltd was founded in September 2013. This was merged into what became the DeMorgan group under DeMorgan Ltd. There were over 17 companies in this group.

66. During my time at Ridges Estate Pty Ltd, Information Defense Pty Ltd, Panopticrypt Pty Ltd and the later DeMorgan Ltd group, I was technical CEO. This meant that, while I had oversight of the strategic direction of our technology infrastructure, I wasn't responsible for maintaining the IT systems, did not act as system administrator nor did I keep records of the company's IT developments. As a result, it is important to emphasise that my knowledge of the transfer from one exchange to the other is limited. I stepped down from this role in July 2015, after which my understanding of events is further limited.

67. In 2002, Ridges Estate Pty Ltd and CSW R&D were using Exchange 2000 which relied on Active Directory for user management. Exchange 2000 initiated the close coupling of the mail system with Active Directory, making Lightweight Directory Access Protocol (LDAP) an essential component for querying and updating the Directory. Microsoft Certificate Authority (CA) and Public Key Infrastructure (PKI) were used for security at this stage. Exchange 2000 ran on native X.500 protocols. These companies all shared the same exchange infrastructure.

68. From 2002 to 2007, Ridges Estate Pty Ltd migrated to Microsoft Exchange 2003 and later to 2007 (although, I do not recall exactly when).

69. Exchange 2003 brought improvements in mobile access and security features. Active Directory was enhanced for better group policy implementation and security features. The Microsoft Exchange Server 2003 Technical Reference Guide at Exhibit CSW16 (pp. 264 – 5) demonstrated how active directory domains and Internet domains are treated differently, and how this can lead to confusion. The same active directory domain can have multiple Internet domains attributed to it and these may change over time. As exchange migrated more towards pure Internet protocols (SMTP) this functionality varied. Exchange 2007 shifted towards 64-bit architecture and introduced PowerShell for task automation.

70. When upgrading to Exchange 2007, the businesses also integrated CentOS. The aim was to move towards integrating Linux-based email and messaging services with Microsoft. The objective was seamless interoperability between Linux and Windows-

based email systems. We wanted to use Linux's robustness, scalability, and cost-effectiveness by linking it with the existing Microsoft Exchange environment.

71. It may be useful to explain how the Linux and Windows-based email systems were integrated. The first step was to set up the Linux server to communicate with Exchange. We chose to work with CentOS, a Linux distribution known for its stability and enterprise readiness. The CentOS system was configured to run Postfix as the mail transfer agent and Dovecot for IMAP/POP3 services. These Linux-based services were then integrated with our Exchange server using connectors and protocol translation mechanisms.

72. A critical component was establishing a secure communication channel between the Linux and Windows servers. Transport Layer Security (TLS) was deployed to encrypt the email traffic between the Postfix on CentOS and Exchange. Active Directory's LDAP capabilities were used for centralised authentication, allowing a unified user database to be employed across both platforms. This was achieved using the open-source tool Samba to facilitate LDAP queries between Linux and Active Directory.

73. As part of the upgrade, the CentOS system was also configured to integrate with Microsoft's PKI for an added layer of security. The public and private key pairs generated by Microsoft CA were imported into the Linux system to authenticate and encrypt email communications.

74. Integrating calendaring and scheduling services was another crucial task. We opted for an open-source solution compatible with both systems, capable of synchronising with Exchange's calendar services. Microsoft Exchange APIs were utilised to ensure that messaging and collaboration features were fully functional across the Linux and Windows platforms.

75. The result was a hybrid email system that leveraged the best features of both Linux and Microsoft technologies. The process wasn't without its complexities, such as dealing with different mail storage formats and ensuring that all security features worked harmoniously across the two platforms. However, the integration was successful, yielding a cost-effective, highly scalable, and secure messaging environment.

76. In 2008, when Craig Wright R&D took over the assets of Ridges Estate Pty Ltd, Exchange 2007 was the base version for both. Active Directory transitioned to a 2008 version, which offered better auditing and more granular password policies. Subsequently, the intellectual property and computer servers at Craig Wright R&D were migrated into the new company, Information Defence Pty Ltd, when it was formed in January 2009.

77. From 2009 to 2011, CSW R&D group companies managed by Information Defense Pty Ltd and Integyrs Pty Ltd migrated to Microsoft Exchange 2010. This version came with Database Availability Groups (DAGs) for improved disaster recovery and Active Directory's 2008 R2 version introduced features like Recycle Bin and offline domain join. At this time, the domain structure changed from an SMTP Internet domain specified in the document by Microsoft listed previously to one of native active directory Internet domains.

78. Panopticrypt Pty Ltd was formed in June 2011. This corporation took over some of the research that was formally done in companies including Information Defense Pty Ltd and that had been migrated to Lynn's company, Cloudcroft Pty Ltd. This involved implementing Exchange 2010 at Panopticrypt Pty Ltd and migrating from the main information store for a select set of users when the companies were divided following the separation and later divorce. This exchange system was migrated later to 2013. Exchange 2013 offered a more simplified architecture merging client access and mailbox servers. The Active Directory created for Panopticrypt Pty Ltd and its subsidiary companies was migrated in 2012. This was integrated with Cloudcroft Pty Ltd after it was purchased back from Lynn in around December 2012. This new version brought features such as Dynamic Access Control and enhanced virtualisation support.

79. Later the companies that have migrated into the public company structure headed by DeMorgan Ltd transitioned to Exchange 2016. DeMorgan Ltd was a public company that headed a series of subsidiary companies. There were approximately 17 companies in the group. This version provided better data loss prevention and tighter integration with other Microsoft products. On the Active Directory front, the 2016 version brought

features like Just Enough Administration (JEA) and Just-In-Time Administration (JIT), focusing more on privilege security.

80. This migration process, in summary, required planning for hardware and software changes, especially for versions like Exchange 2007 and 2013, which changed architectural requirements. Data backup, pilot testing, and phased rollouts was crucial, given the complexity of configurations involving LDAP, CA and PKI. The transition from native X.500 protocols to standard Internet protocols required significant attention to data integrity and routing.

(b) The person(s) who undertook this moving of exchange servers

81. During this period, over 100 people were engaged as system administrators or consultants to handle the exchange server migrations. This includes in-house employees and external contractors with some operations managed by third party IT management firms. I do not, however, recall the names of each individual involved in this.

(c) What access remains to the original server, and if there is no access, why that is the case.

82. The servers for Ridges Estate Pty Ltd were decommissioned in around 2007/8. The business of Information Defense Pty Ltd was transferred to Cloudcroft Pty Ltd which was later sold. Information Defense Pty Ltd itself was placed into liquidation and closed. So far as I'm aware, the servers associated with Information Defense Pty Ltd remained with Lynn. I understand that AlixPartners' associate, KordaMentha, tried to image them. I've been shown by my solicitors the Disclosure Review Document and I believe that these servers are listed as follows: 4 x rack mounted servers: 1 x Dell PowerEdge 1650 (containing 2/2 retrievable hard drives); 1 x Dell PowerEdge 1650 (containing 4/6 retrievable hard drives); 1 x Dell PowerEdge 2500 (containing 6/8 retrievable hard drives); and 1 x Hewlett Packard Proliant (containing 2/2 retrievable hard drives).

83. The servers for Cloudcroft Pty Ltd and Panopticrypt Pty Ltd were decommissioned between 2012 and 2016. I do not know what happened to these servers.

84. All of the DeMorgan Ltd managed Australian companies closed in 2016. The servers were sold under the direction of Stefan Mathews and I do not know where they are. These systems were wiped before being sold. I do not know if the data on them was copied in full before being wiped. Some of the drive images were copied to the QNAP systems. These systems were supplied with the management account to AlixPartners in 2019. Please see paragraph 30 for further information.

(d) What was the reason for the move?

85. The rationale for moving the servers and undertaking frequent upgrades was guided by a policy of staying on the "bleeding edge" of technology. This typically meant migrating to the latest Microsoft and CentOS systems versions within six months of their respective releases. As a large group of companies, IT requirements were complex and demanding and therefore required periodic shifts in Active Directory domains and server upgrades. The driving force behind our server migrations and upgrades was to ensure we leveraged the latest features, security updates, and performance improvements that new software versions provided. This was about keeping our systems up-to-date, maintaining a competitive edge, and ensuring optimal security and performance for our operations.

(e) What technical process was utilised for moving exchange servers, including the details of all software used.

86. I cannot comment on the specific technical process utilised for moving the exchange servers and I expect that the precise details of the software and procedures used differ from one transition to another. At times, I have used graduate students that I taught in Charles Sturt University as administrative helpers.

87. My understanding is that the typical process started with a planning phase, assessing the compatibility of the new exchange version with the existing IT environment. A testing phase would follow this in a non-production environment. Once the test migrations were deemed successful, the actual migration would commence, generally during off-peak hours, to minimise business disruption.

88. The Active Directory would be updated in tandem with changes to user permissions, group policies, and organisational units as required. Security configurations like Microsoft CA and PKI services would also be reviewed and updated accordingly.

89. Standard tools for Exchange migrations would have included Microsoft's native migration features, Powershell for task automation and sometimes third party utilities for more specialised requirements.

(f) What, if any, backups and precautions were taken during the transfer of this data from one exchange server to another; what backups, if any, were made before the move; and what has happened to those backups if such existed.

90. I cannot recall the specific backups or precautions that were taken during the transfer from one exchange server to the other and what happened to these.

91. All activities, including server migrations, should have been conducted within the confines of stringent corporate and information security policies and processes. These policies were compliant with ISO 27001 standards, and our companies underwent external audits and were measured against COBIT 4.0.

92. If backups were created, they should have been saved to a secure location before any such move. In 2015, this would have been a QNAP server. As for the whereabouts of those backups, the QNAP server holding the system backups was taken by AlixPartners in 2019. I have described what happened to the QNAP servers at paragraph 30 above.

53. In light of the requests above, please explain how and why the Defendant has come to believe that the header is different, setting out in full detail who, or what sources of information, caused the Defendant to come to this belief.

93. I sent the email set out at paragraph 28 of the Re-Re-Amended Particulars of Claim to David Kleiman on 12 March 2008 using my wright_c@ridges-estate.com email address.

94. The wright_c@ridges-estate.com email address was configured within a Microsoft Exchange environment using an X.500 email store. X.500 is a suite of protocols that define a standard for directory services, primarily conceived to facilitate

communication within a network and support the exchange of information in a consistent manner. This environment was tightly integrated with Active Directory, a feature that allows for domain and identity management. The underlying domain structure was using a Windows domain of WDI.Local, ridges-estate.local and DeMorgan.CO. These windows domains were separate to the email domain and had migrated into an active directory structure. Each underlying active directory domain could hold multiple Internet domains. In this an Internet domain could be added or removed to the user's active directory profile without impacting their membership in the overall exchange and Windows domain structure.

95. The business migrated from the 'ridges-estate.com' domain to 'information-defense.com' domain on 31 December 2008 due to the planned migration to the new company that was being set up. While information-defense.com had not been registered at this point, it is important to note that the foundation of company structures was not as quick as it is today. I had planned setting up Information Defense Pty Ltd and information-defense.com as of the date when I received an offer of a redundancy package on 11 December 2008. This time, adjustments were made in Active Directory which could affect various system configurations, including email headers. During the transition from the 'ridges-estate.com' domain to the 'information-defense.com' domain the business underwent a process that included rebuilding accounts in the Microsoft Exchange server. This process would inherently result in changes to email headers, specifically the originating domain and potentially other metadata. However, no such rebuilding of accounts occurred for later domain shifts, such as to 'RCJBR' meaning the email headers would not undergo the same modifications.

96. This phenomenon could occur due to the interplay between X.500 identifiers and Active Directory's organisational unit (OU) structures. In a Microsoft Exchange environment, emails are often stored and referenced via their X.500 addresses, which are tied to an account's legacyExchangeDN attribute in Active Directory. When an organisation migrates from one domain to another or restructures its Active Directory, the OU structures and legacyExchangeDN attributes will likely change. In some cases, system administrators may manually update these attributes or be automatically

updated depending on the migration tools used. When this attribute changes, it affects the X.500 identifier associated with the user's mailbox.

97. In practical terms, an email sent before the migration from the 'ridges-estate.com' domain to 'information-defense.com' domain would have been associated with the original legacyExchangeDN attribute and, by extension, the original X.500 address i.e. the 'ridges-estate.com' domain. After the migration, even though it's the same user, the email in the Exchange repository might be updated to reflect the new legacyExchangeDN and the new X.500 address i.e. the 'information-defense.com' domain. This change would make it appear that the email is coming from a different domain, even though it is from the same user i.e. my account.

98. I have been provided to me by my solicitors document ID ID_001711, a copy of which is at Exhibit CSW17. This is an email to Stefan Matthews dated 9 July 2015 at (08.46), in which I forward an email from me to David Kleiman. This is referred to at paragraph 28 of the Re-Re-Amended Particulars of Claim. As can be seen, the header has again changed so that it shows the email to David to be from "Craig S Wright [mailto:craig@rcjbr.org]" to "craig@rcjbr.org". This is consistent with my account above, namely of the headers merging into new OU accounts. To be clear, the domain rcjbr.org did not exist in 2008, but was only introduced in 2011. I also note that "Craig S Wright [mailto:craig@rcjbr.org]" and "craig@rcjbr.org" are displayed differently. This suggests to me that they were separate email stores originally that have been merged.

Section P: Request 57

57. Please state whether the key referred to in the second sentence of paragraph 83(2) is the public key available in the following link
https://web.archive.org/web/20110228054007/bitcoin.org/satoshi_nakamoto.asc

99. I do not understand the request which is being made of me.

100. At Paragraph 61 of the Re-Re-Amended Particulars of Claim, COPA alleges that: "Wright has publicly asserted that he can prove he is Satoshi by reference to the

Genesis Block. Wright should therefore, amongst other things, be able to show: 61.1. That he has control over Satoshi's private key and the Genesis Block."

101. I've never asserted that I can prove that I used the Satoshi Nakamoto pseudonym by reference to the Genesis Block. It is also unclear what's meant by me having control over "Satoshi's private key" and "the Genesis Block". There is no such thing as the "Satoshi private key" and I do not understand how anyone could profess to have control over the "Genesis Block".

102. By way of explanation, the "Genesis Block" was created, not mined (mining refers to a process whereby blocks are verified, a process which follows the creation of the Genesis Block). The 50 Bitcoin associated with the "Genesis Block" was not designed to be withdrawn. As such, it has zero value. It follows that there never was a private key associated with the block. Expressed another way, it is a fact that the "Genesis Block" does not have (and never had) a private key. I explain this in more detail in my blog, an extract of which is at Exhibit CSW18

103. This is explained at paragraph 83 of the Re-Re-Amended Defence, which reads: "With regard to paragraphs 61 and 62 of the Particulars of Claim – (1) It is denied that Dr Wright has publicly asserted that he can prove that he used the pseudonym Satoshi Nakamoto by reference to the Genesis Block. It is further denied that anyone could have "control" over the Genesis Block."

104. The Defence goes on to explain that "(2) It is not clear from paragraph 61.1 what "private key" is referred to. There has been a public discussion of a key created in 2011 after Dr Wright "retired" his Satoshi Nakamoto persona. The key was created by a person or persons unknown." This is a reference to the PGP encryption key at https://web.archive.org/web/20110228054007/bitcoin.org/satoshi_nakamoto.asc. This was generated by Vistomail when I set-up the Sakura account in 2008. I subsequently shared this with a number of individuals, including Marti Malmi, so that they could send code updates to me. It was only published in 2011 by an unknown party (I suspect Marti Malmi), after I stopped the active use of the Satoshi Nakamoto pseudonym.

105. It may be helpful to explain the PGP key associated with Vistomail. It is essential to understand that the PGP key is not specific to any individual but to a server at Vistomail. Vistomail provided both domain services and original hosting for bitcoin.org. The PGP key in question was generated internally by Vistomail and used for domain and server management functions. I didn't create it; it is an integral component of the services provided by Vistomail, including its application to my Sakura account for domain and email management. Since this is a system-specific key, its primary role was securing various server operations, such as data encryption and user authentication. Therefore, its utility extended beyond individual use and is designed to safeguard the associated infrastructure.

106. A server PGP key is typically generated as a pair consisting of public and private keys. The public key is used for encryption and is distributed openly (an example of which is the PGP key at https://web.archive.org/web/20110228054007/bitcoin.org/satoshi_nakamoto.asc), while the private key is used for decryption and is kept secure.

59. When was the PGP key generated?

107. The PGP key linked to the Vistomail server and the Sakura account came into existence when the account transitioned to a paid subscription in 2008 (I expect around October 2008). The Vistomail service was shut down shortly after the Sakura account became inactive, around 2020. This inactivity occurred after my legal representatives from Ontier accessed the account, as referred to in paragraph 19 above.

60. Does the Defendant have the private PGP key corresponding to a public PGP key belonging to Satoshi in or before 2011?

108. This question is based on an incorrect premise. Vistomail offered an online PGP system where the service manages the system encryption keys. The private key was not removed from the Vistomail server because doing so would make the decryption of stored messages and ongoing encrypted communications impossible. In asymmetric cryptography systems like PGP, the private key is essential for decrypting messages

that have been encrypted with the corresponding public key. If Vistomail were to remove the private key, any previously encrypted messages would become permanently inaccessible, effectively causing data loss. Additionally, the absence of the private key would disrupt secure communication for users relying on that particular key pair for encryption and decryption. Therefore, the private key is an integral component that must remain on the server for the system to function as intended. The private key was 'lost' when Vistomail closed.

If so, why has the Defendant not signed a message using that key pair?

109. Again, this request is based on an incorrect premise. The private PGP key was for encryption and decryption, not signing (i.e. validating messages).

61. If the Defendant does not presently have any private PGP key corresponding to any public PGP key which belonged to Satoshi in or before 2011, did he have any such private key at any time in the past? If so, what has happened to cause him no longer to have the key?

110. First, it is important to emphasise that the key in question was linked explicitly to my Sakura account on the Vistomail email service, not Satoshi. Second, as explained above, I had the ability to use the server (which used the private PGP key) up until the Vistomail service was discontinued. I repeat my comments at paragraph 19 above in relation to solicitors from Ontier accessing the account and my videos.

Statement of Truth

I believe the facts stated in this witness statement are true. I understand that proceedings for contempt of court may be brought against anyone who makes, or causes to be made, a false statement in a document verified by a statement of truth without an honest belief in its truth.

Signed: DocuSigned by: EFCD3017AD2842B...

Name: Craig Wright

Dated: 23 October 2023

Certificate of Compliance

I hereby certify that:

1. I am the relevant legal representative within the meaning of Practice Direction 57AC.
2. I am satisfied that the purpose and proper content of trial witness statements, and proper practice in relation to their preparation, including the witness confirmation required by paragraph 4.1 of Practice Direction 57AC, have been discussed with and explained to Dr Craig Wright.
3. I believe this trial witness statement complies with Practice Direction 57AC and paragraphs 18.1 and 18.2 of Practice Direction 32, and that it has been prepared in accordance with the Statement of Best Practice contained in the Appendix to Practice Direction 57AC.

Signed: DocuSigned by: Antony Craggs D6B08A6229AD44C...

Name: Antony Craggs

Position: Partner

Dated: 23 October 2023