Made on behalf of the Claimant in the Coinbase Claim, Kraken Claim and BTC Core Claim
Made on behalf of Defendant in the COPA Claim
Fifth Witness Statement Dr Craig Steven Wright
Dated 1 December 2023
Exhibits CSW5

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**")

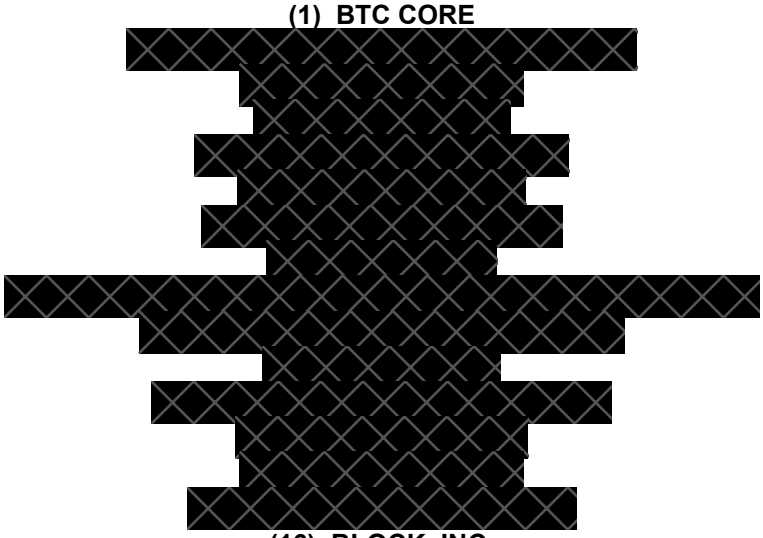
BETWEEN:

(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 GLOBAL INC.
(22) CB PAYMENTS, LTD
(23) COINBASE EUROPE LIMITED
(24) COINBASE INC.
(25) CRYPTO OPEN PATENT ALLIANCE
(26) SQUAREUP INTERNATIONAL LIMITED

Defendants

FIFTH WITNESS STATEMENT OF DR CRAIG STEVEN WRIGHT

I, **DR CRAIG STEVEN WRIGHT**, [redacted] **WILL SAY AS FOLLOWS**:

1. Unless otherwise stated, the facts and matters set out in this witness statement are within my own personal knowledge and recollection and I believe them to be true. Where the facts and matters are not within my own knowledge, they are based on the documents or other sources I mention below and are believed by me to be true, the best of my knowledge and belief. Nothing stated in this witness statement waives legal professional privilege over communications between myself and my current solicitors, Shoosmiths LLP ("**Shoosmiths**"), or between me and any of my former legal representatives.

2. There is now produced and shown to me a bundle marked "**CSW19-CSW**" to which I shall refer in this statement.

3. I make this witness statement in accordance with paragraph 8 of the Order of Mr Justice Mellor dated 31 October 2023, whereby I am required formally to attest in a witness statement the explanations provided by Shoosmiths in a letter dated 10 November 2023 ("**Shoosmiths' November Letter**") to Bird & Bird LLP ("**Bird & Bird**") concerning two hard drives discovered by me in my home office in September 2023, namely a Samsung T1 USB SSD with serial number A665403GAYNC52S (the "**Samsung Drive**") and a MyDigitalSSD OTG USB SSD with serial number 700001662137051115 (the "**MyDigital Drive**") [**CSW19**]. I also rely upon this witness statement in support of my application dated 1 December 2023 asking *inter alia* for an Order that I be permitted to rely upon certain documents that I have instructed my solicitors are from the Samsung Drive.

4. I confirm that Shoosmiths' November Letter to Bird & Bird is true and accurate, to the best of my knowledge and belief. I refer to the letter marked [**CSW19**]. To assist the Court, I provide certain further detail below of the Hard Drives and the circumstances in which I found them in September 2023.

Background

5. The Hard Drives contain various materials, as follows:

   5.1. The Samsung Drive contains approximately 1 terabyte of data. I believe that this drive was purchased in around 2015 or early 2016 as a replacement for an old backup drive; and

5.2. The MyDigital Drive contains approximately 500 megabytes of data. I do not recall when this drive was acquired, in what circumstances or for what period it was used. However, I believe that this drive has been in my possession for several years.

6. The Hard Drives predominately contain backups of forensic images of old drives and other material associated with files I had backed up from computers I was using at the time the back-ups were made. My practice is regularly to update my laptop and desktop systems and to make back-ups of the data held on those systems on separate hard drives. I am also in the practice of using several laptop and/or desktop systems simultaneously, each serving distinct functions within my comprehensive operational framework. I habitually use various operating systems on my computers, including but not limited to Red Hat Linux, Centos Linux and Windows. All or at least some of these operating systems will have been used to interact with the Hard Drives.

7. The Samsung Drive contains an image of a drive from when I worked at BDO, the accountancy and business advisory firm ("**the BDO Drive**"). I used this drive predominately to store data that I did not want to be corrupted or accessible. The BDO Drive was captured on or around 31 October 2007. It contains within it images from former systems that confirm that the BDO Drive pre-dates 31 October 2007, including, for example, a Sim card image from one of my mobile phones in 2006 and web caches of my web browsing history from 2006.

8. In addition to the BDO Drive, the Samsung Drive contains an image dating from 2009. I do not have the encryption password to access this image and have not been able to access the image since finding the Samsung Drive in a drawer in my home office in September 2023 (as explained further below).

9. Since I have owned the Hard Drives for a period of some years, I cannot recall exactly how and when they were accessed prior to my finding them in September 2023. I used both Drives from the time they were acquired until they were imaged by AlixPartners LLP ("**AlixPartners**") in February 2019, as explained below. In the course of using the Drives, I would have edited or amended documents contained on them. However, I did not edit or amend any documents in the BDO Drive after it was captured in October 2007. It is also the case that I did not edit or amend documents stored elsewhere on either of the Hard Drives after the Drives were imaged by AlixPartners.

10. I believed that the Hard Drives were amongst those made available to AlixPartners for forensic imaging when they collected materials from my home in February 2019 for the

purposes of disclosure. However, I am now aware that the Hard Drives were not forensically imaged by AlixPartners.

The disclosure process

11. In February 2019, my legal representatives in the United States, Rivero Mestre LP, and my then legal representatives in the United Kingdom, Ontier LLP ("**Ontier**"), conducted a document retention exercise in connection with proceedings brought against me in Florida by Ira Kleiman, in his capacity as Executor of the estate of David Kleiman ("**the Kleiman Proceedings**"). In the Kleiman Proceedings, I did not personally have access to the disclosure platform used in the proceedings and was therefore not in a position myself to monitor and verify precisely which documents were disclosed. My understanding, however, was that the disclosure requirements were very wide. As a result, I gave my legal representatives access to all documents and data in my possession and control and in the possession and control of my wife, Ramona Watts. This included documents, data and devices from ex-staff members which were sent to Ms Watts around June 2016 after the company DeMorgan had closed. Some of these were in a locked area in the basement and others were in Ms Watt's separate office in our home residence, [redacted] as part of her role as director and custodian of the Australian companies. Some documents were sent from company offices in Australia.

12. AlixPartners were engaged by Ontier as e-disclosure providers on my behalf. They arranged for all electronic storage devices (i.e. laptops, desktop computers, external hard drives and CDs etc) that were in my possession and control (including electronic storage devices that certain individuals at nChain Ltd had returned to me), or the possession and control of Ms Watts at our home in Cobham, to be imaged. These devices were mostly located in my home office and Ms Watts' home office (which are separate) which extends to more than 3000 square feet and contains over 20 laptop and desktop computers. This is not including larger server racks located in the basement and various other electronic storage devices which would have been throughout our home.

13. I recall AlixPartners attending our home during February 2019 to collect the requisite data and documents. This process took two days given the number of storage devices that needed to be collated and imaged. The task was a considerable one.

14. Throughout their visit, I was unable to monitor AlixPartners given that there were several personnel collecting data from various electronic devices in my office and elsewhere in my house simultaneously. However, for the avoidance of doubt, for the

entire duration of their visit I made all of my electronic storage devices within my home available to AlixPartners for forensic imaging.

15. I understand that the images taken by AlixPartners during this visit were then used by Ontier for the purposes of giving disclosure in the present proceedings. This is explained in my Disclosure Review Document in this action.

Discovery of the Hard Drives

16. On 2 September 2022, Mellor J made an Order directing (among other things) that I was to provide further information in these proceedings about the chain of custody in respect of the Reliance Documents (being documents on which I primarily rely in support of my contention that I am the author of the Bitcoin White Paper (the "**White Paper**")). In the course of preparing that chain of custody information, I became concerned as a result of privileged information provided to me by my then solicitors, Travers Smith LLP ("**Travers Smith**"), about the disclosure exercise carried out by AlixPartners that AlixPartners may not have collected and/or imaged everything as certain data may have been encrypted or otherwise not available. Until then, I had not been aware of any concerns about the comprehensiveness of the imaging process carried out by AlixPartners. For the avoidance of doubt, I do not waive privilege over communications between myself and my legal representatives concerning the disclosure exercises carried out in this action or in previous proceedings in which I have been involved.

17. Given my concerns, during the week commencing 11 September 2023 I began to search my home to check what drives and other devices had been imaged by AlixPartners. On around 14 September 2023, I was informed by Travers Smith that when AlixPartners collected material from my home in 2019, they could not image certain drives as they were encrypted, had no data or were damaged. I surmised from this that AlixPartners had access to the Hard Drives to image, had attempted to do so but (I assumed) had been unsuccessful.

18. On 15 September 2023, I was continuing to search my home for any drives that AlixPartners had imaged when I found the Hard Drives in a drawer with other hard drives that I understood had been imaged by AlixPartners. Some of those drives had AlixPartners stickers on them which I presumed meant they had in fact been imaged by AlixPartners. The Hard Drives did not have AlixPartners stickers on them; I therefore presumed they had not been imaged. The Samsung Drive had a bare section where the device information label should have been displayed; it was apparent to me that

something had been glued to the side of this drive but had fallen off. I later discovered a label that fitted the bare section on the outside of the Samsung Drive.

19. When I discovered the Hard Drives, I knew what they were, i.e. drives that I had used predominately to back up images of old drives and other material associated with files backed up from computers I was using at the time the back-ups were made, including the BDO Drive (as explained in paragraphs 6 to 7 above).

20. The Samsung Drive was architecturally designed and integrated with firmware and software layers to give the user an illusion of a singular partition despite having two partitions. When the drive was accessed under regular conditions (i.e. connecting it to a laptop or computer), only the primary public encrypted singular partition was visible and accessible to the user. However, upon utilising a specific password, the hidden encrypted second partition (including the BDO Drive) becomes accessible. The reason for this layered approach was because I had confidential client information on the BDO Drive that I did not want anyone to access without my authority.

21. If AlixPartners had imaged the Samsung Drive when live (i.e., when linked to an active system, such as my laptop), they would have been able to image the hidden encrypted partition (including the BDO Drive). However, if the Samsung Drive were unplugged from an active system when it was being imaged, it would have been transformed into a safeguarded system and AlixPartners would have not been able to see the hidden partition. This is evident from the difficulties KLD had accessing the Samsung Drive, described below.

22. After discovering the Hard Drives, I plugged them into my laptop to see if they were still working. I checked that they powered up and could be decrypted as this would be necessary if they were to be imaged. For the Samsung Drive, I plugged it into my laptop and ensured that the data diode software was available. This generates a pop-up on my computer asking if I want to unlock the drive. This confirmed for me that the drive was working. For the MyDigital Drive, I simply connected it to power up. I did not access the BDO Drive on the Samsung Drive or any files on either Hard Drive (see further on this, paragraphs 28 to 30 below).

23. Following my discovery of the Hard Drives, I notified Travers Smith and Zafar Ali KC (who was then engaged as a consultant by Christen Ager-Hanssen, the CEO of nChain UK Ltd at the time) of the Hard Drives' existence and my concerns that they had perhaps not been imaged by AlixPartners. I did not access the Hard Drives at this time (beyond checking that they were still working, as explained above).

24. On 20 September 2023, Travers Smith arranged for KLD Discovery, who have acted as my e-disclosure provider in these proceedings, to come to my home to take a full forensic image of both Hard Drives. I gave the Hard Drives to KLD Discovery and provided them with the passwords for the MyDigital Drive and the Samsung Drive. I stayed in the room whilst they carried out the imaging so as to ensure that they could successfully access the Drives and decrypt them as necessary. KLD Discovery attempted to connect the Samsung Drive to the KLD Discovery's forensic workstation in a 'read-only' state. The Samsung Drive would not operate with the read-only hardware system in place. This was therefore removed and the Samsung Drive was connected directly to the KLD Discovery's laptop with a software-based write blocker running. KLD Discovery were then able to access the outer partition and to run the Samsung decryption driver. This then closed the outer partition opening the intersection that could be imaged using FTK Imager forensic software. This limitation did not occur on the MyDigital Drive.

25. Using FTK Imager, KLD Discovery captured a physical forensic image of each of the Hard Drives in an 'E01' format onto a blank encrypted drive. FTK Imager creates a bit-for-bit duplicate image of the media. The forensic image is identical in every way to the original, including file slack and unallocated space or drive-free space. These images were verified whilst KLD Discovery was still at my home to ensure there was readable data. The hash generated by FTK Imager was also used to verify that the image hash and the drive hash matched after the image was created. KLD Discovery then returned the Hard Drives to me. They left my home and I believe returned to their London office with the captured forensic images. Shoosmiths has since taken custody of the Hard Drives and they remain in Shoosmiths' possession.

26. I understand that Travers Smith wrote to the Court (copying Bird & Bird) on 25 September 2023 to draw the Court's attention to the discovery of the Hard Drives [**CSW20**]. Travers Smith subsequently wrote to Bird & Bird again on 2 October 2023, setting out more details regarding the Hard Drives [**CSW21**].

27. Following my engagement of Shoosmiths as my solicitors in these proceedings, they provided further details about the Hard Drives and the circumstances in which they were found in September 2023, including in letters to Bird & Bird dated 11 October 2023 [**CSW22**and 10 November 2023 [**CSW19**].

Forensic examination of the Hard Drives

28. I understand that Stroz Friedberg Ltd ("**Stroz Friedberg**"), computer forensic experts engaged by Shoosmiths as consultants on my behalf, have examined the BDO Drive and produced a memorandum summarising a number of data points they have identified on the Samsung Drive. A copy of Stroz Friedberg's memorandum is at [**CSW23**]. I understand that the points identified by Stroz Friedberg will require further investigation by the parties' computer forensic experts.

29. In particular, Stroz Friedberg identify in their memorandum (i) metadata suggesting that the recycle bin on the Samsung Drive (which sits on the Samsung Drive outside the BDO Drive, which has its own recycle bin) was emptied in September 2023, (ii) the ordering of files added to the recycle bin and (iii) transactional log files within the BDO Drive with a created, modified and access date of 17 September 2023.

30. I believe that these matters may be explained by the software systems and processes that I habitually use. These include VMware, WinUndelete, Storage Sense, SAMBA shares and symbolic links. These may have caused the recycle bin on the Samsung Drive to have been automatically emptied when I plugged the Samsung Drive into my laptop to check that it was working (as explained above). They may also have altered the ordering of files in the recycle bin. It is also possible that one of these systems or processes was configured in such a way as automatically to open the BDO Drive when I checked that the Samsung Drive was working. However, I am sure that I did not myself do anything with either of the Hard Drives, other than to check that they were working, between the time I discovered them and the time they were imaged by KLD.

Conclusion

31. Although I made all of my electronic devices and hardware available to AlixPartners in 2019, it seems that they did not image the Hard Drives. I am unaware as to why this happened. I apologise to the Court for this oversight. However, I am aware of my continuing obligation of disclosure in these proceedings. I have therefore sought to ensure that relevant documents on the Hard Drives have been reviewed and disclosed for the purposes of these proceedings.

32. Given the significance of documents that were on the BDO Drive, I am applying to the Court for permission to rely upon certain documents from the BDO Drive in these proceedings. I appreciate that this will likely impact upon the timetable to trial of the Identity Issue. However, for the reasons set out in support of my application, I believe that the Identity Issue cannot fairly be determined without those documents being before the Court.

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: _____

Name: _____

Dated: _____

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
Fifth Witness Statement Dr Craig Steven Wright
Dated 01 December 2023
Exhibits CSW19

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**")
Claim No. IL-2022-000035
(the "**Coinbase Claim**")
Claim No. IL-2022-000036
(the "**Kraken Claim**")
Claim No. IL-2022-000069
(the "**BTC Core Claim**")

BETWEEN:

CRYPTO OPEN PATENT ALLIANCE

Claimant

- and -

DR CRAIG STEVEN WRIGHT

Defendant

EXHIBIT CSW19 TO
FIFTH WITNESS STATEMENT OF DR CRAIG STEVEN WRIGHT

SHOOSMITHS

FAO: Phil Sherrell
Bird & Bird LLP
12 New Fetter Lane
London
EC4A 1JP

No. 1 Bow Churchyard
London
EC4M 9DQ

DX 36 London

T +44 (0)370 086 3000
E: copavwright@shoosmiths.com

Sent by email only to:
B&B.CRYOP.0001@twobirds.com

Date 10 November 2023

SECOND LETTER

Your Ref PNQS/NIXL/WIDW/CRYOP.0001
Our Ref AC.HXF.MG.M-01078068

Dear Bird & Bird LLP

Claim No. IL-2021-000019 Crypto Open Patent Alliance v Dr Craig Wright
Claim No. IL-2022-000035 Dr Craig Wright & Another v. Coinbase Global, Inc & Others
Claim No. IL-2022-000036 Dr Craig Wright & Another v. Payward & Others
Claim No. IL-2022-000069 Dr Craig Wright & Another v. BTC Core & Others (Identity Issue only)

1. We refer to the Order of Mr Justice Mellor dated 31 October 2023 ("**the Order**") and your second letter dated 3 October 2023 ("**the Letter**"). In accordance with paragraph 8 of the Order, we respond to the Letter as follows. For the avoidance of doubt, our client does not waive privilege in relation to any of the matters referred to below and nothing in this letter is or should be taken to amount to such waiver.

What material the drives contain and why it was not disclosed earlier

2. The additional drives contain various materials being:

   2.1. The Samsung T1 USB SSD (serial number A665403GAYNC52S) which contains approximately 1 terabyte of data which our client believes was purchased in late 2015 or early 2016 as a replacement for an old backup drive; ("**the Samsung Drive**"); and

   2.2. MyDigitalSSD OTG USB SSD (serial number 700001662137051115) which contains approximately 500 megabytes of data ("**the MyDigitalSSD Drive**"). Our client does not recall when the MyDigitalSSD Drive was acquired or in what circumstances.

   (together "**the Additional Drives**")

3. It was our client's practice to regularly update his laptop or desktop system and makes back ups of the same on separate drives. Our client would also make use of several laptop or desktop system simultaneously, each serving distinct functions within his comprehensive operational framework.

4. Our client believes that the Additional Drives were amongst the hard drives and other data made available to AlixPartners for forensic imaging when they collected materials from our client's residence in 2019 for the purposes of the disclosure exercise in these proceedings. It now appears that the Additional Drives were not in fact forensically imaged by AlixPartners.

When our client discovered the existence of the drives and the material on them

5. This issue first came to our client's attention through the chain of custody exercise which our client was required to undertake in relation to the documents on which he relies in these proceedings. Our client's then instructed solicitors, Travers Smith LLP, provided him with a draft document which set out a guide for the chain of custody (this document was created for the purpose of litigation and therefore remains privilege and any reference to it does not constitute a waiver of privilege). This particular document contained a column in which it stated "*Contains encrypted Bitlocker partition*" and "*Bevel data. Not encrypted*" which caused our client concern. Our client reviewed further and found that there were further columns referring to "*Hardware failure*", "*Data encrypted*" and "*No data available*". From this, he concluded that certain data or drives may not have been collected or imaged because they were encrypted. As a result, during the course of the week commencing 11 September 2023, our client began to conduct a search of his residential property for the drives that AlixPartners had imaged.

6. On 14 September 2023, our client subsequently asked Travers Smith LLP where the information contained in the draft chain of custody guide had come from. Having enquired of AlixPartners, Travers Smith LLP informed our client that when AlixPartners collected material from our client in 2019, they could not image certain drives because they were encrypted, had no data or were damaged. Our client surmised from this that AlixPartners had access to the Additional Drives to image, had attempted to do so but our client can only assume were unsuccessful.

7. On 15 September 2023, our client continued his search of any drives that AlixPartners had imaged and identified the Additional Drives. The Additional Drives were in a drawer with other drives that our client understood were imaged by AlixPartners. Some of the other drives had AlixPartners stickers on them indicating an image was completed. The Additional Drives did not have AlixPartners stickers. The Samsung Drive had a bare section where the device information should have been displayed showed that something had been glued to the side of the drive. The drive label was missing such that the drive identification label had come off.

8. It is our client's position that the Additional Drives predominantly contain backups of forensic images of old drives and other material associated with files our client backed up from his computer. We understand there are two images on the Samsung Drive. The Samsung Drive specifically contains an image of a drive from when our client worked at BDO, the accountancy and business advisory firm ("**the BDO Drive**") and he used this drive to predominately hold images that he did not want to be corrupted or accessible. The BDO Drive was captured on or around 31 October 2007. The other image is from 2009. We understand that our client does not have the encryption password and has not been able to access the drive image from 2009.

When our client first informed any other person of the material, when our client first provided it to any other persons and when our client first provided it to legal representatives.

9. Our client notified Travers Smith LLP and Zafar Ali KC of the drives following identification of them. Our client did not access the drives at this time. On 20 September 2023, our client's current e-disclosure provider, KLD Discovery, attended our client's property and took a full forensic image of the Additional Drives. Further details on this process are set out below.

The circumstances in which he procured and used each drive, including the date on which it was purchased

10. Our client believes that the Samsung Drive was purchased in around late 2015 or early 2016.

11. Our client does not recall when the MyDigitalSSD Drive was acquired, in what circumstances, for what period it was used.

12. As mentioned above, it is our client's understanding that the Additional Drives were predominantly used as back-up drives.

Whether any of these hard drives in question are or are not the same hard drives as those referred to in any of the receipts for the purchase of equipment set out in the very-recently-disclosed documents ID_004637 to ID_004641, and if so which of them.

13. As stated in our letter dated 11 October 2023, the Additional Drives are not referred to in, and do not relate to, documents ID_004637 to ID_004641.

How frequently and at what times were the drives used since they were procured by Dr Wright

14. As already explained, our client believes that the Additional Drives were predominantly used as back-up drives. Apart from this, they were (our client believes) hardly used at all.

Which computers and operating systems have been used to interact with the hard drives and during which periods

15. Our client used various operating systems including Red Hat Linux, Centos Linux and Windows to interact with the Additional Drives. We are currently investigating whether information regarding the exact periods during which the Additional Drives were accessed, and by which computers they were so accessed, is available.

Whether the data contained has been manipulated or edited in any way and if so, in what way and by whom

16. As set out at paragraph 5a. of our letter dated 20 October 2023, documents contained on the Additional Drives may have been edited whilst in use. However, our client cannot recall which documents were edited and when. We understand your reference to data being "manipulated", to mean deliberately tampered with to obscure the true nature of the document. It is our client's position that he has not manipulated the documents contained on the Additional Drives.

When did Shoosmiths LLP first become aware of these additional drives and/or the material they contain

17. We first became aware of the Additional Drives upon being instructed. We have already provided material from the Additional Drives as part of our letter dated 8 November 2023.

Why this has only now been brought to Bird and Bird's attention

18. As set out above, this issue first came to our client's attention undertaking the chain of custody exercise within these proceedings in September 2023.

19. Our client discovered the Additional Drives on 15 September 2023 and thereafter made Travers Smith LLP and Zafar Ali KC aware of this. In three working days, KLD Discovery attended our client's property and took a full forensic image of the Additional Drives. On 25 September 2023, Travers Smith LLP wrote to the Court (copying in your firm) putting it on notice of the discovery of the Additional Drives. Travers Smith LLP subsequently wrote to your firm again setting out more details regarding the Additional Drives on 2 October 2023.

A detailed account of the circumstances in which the drives were inspected, and forensic images

20. KLD Discovery attended our client's home on the 20 September 2023. At 09:30 our client granted custody of the Additional Drives to KLD Discovery and provided the passwords for the MyDigitalSSD Drive and the Samsung Drive. The Samsung Drive was connected to KLD Discovery's forensic workstation in a 'read-only' state. The Samsung Drive would not operate with the read-only hardware system in place. As such, this was removed, and the drive was connected directly to the laptop with a software-based write blocker running. KLD Discovery were then able

to access the outer partition and to run the Samsung decryption driver. This then closed the outer partition opening the intersection that could be imaged using FDK. This limitation did not occur on the MyDigitalSSD device. Using the forensic software FTK Imager, KLD Discovery captured a physical forensic image of each of the Additional Drives in an 'E01' format onto a blank encrypted drive. FTK Imager creates a bit-for-bit duplicate image of the media. The forensic image is identical in every way to the original, including file slack and unallocated space or drive-free space. These images were verified whilst KLD Discovery was still at our client's home to ensure there was readable data. The hash generated by FTK Imager was also used to verify that the image hash and the drive hash matched after the image was created.

The Samsung Drive

21. It is standard practice when creating a forensic image of a USB device to connect the target media to a forensic workstation or drive duplicator in a "read-only" state; however, due to the built-in encryption that is present on the Samsung Drive, this wasn't an option. To unlock the data on the drive and make it available for forensic imaging it had to be connected to KLD Discovery's Windows computer in a "writable" state. A valid password was provided by our client to KLD Discovery to unlock the data stored on the Samsung Drive and allowed KLD Discovery to capture a readable forensic image. The drive runs as a "data diode". When the software in the initial partition is run and the password is provided, the internal drive partition is decrypted and available replacing the initial connected partition. This uses special Windows drivers that load from the software. A fault was identified with one of KLD Discovery's cable adaptors during the initial connection stage which they swapped out for another in their kit and that worked without issue.

The MyDigitalSSD Drive

22. When the MyDigitalSSD Drive was connected to KLD Discovery's forensic workstation, via write protection technology, a prompt to provide a BitLocker password was displayed onscreen suggesting that the data was encrypted. A valid password was provided by our client to KLD Discovery to unlock the data. It became apparent that the encryption process had previously been interpreted as an encryption progress bar was displayed. BitLocker is an encryption feature built into the Windows operating system that encrypts full volumes of drives. If BitLocker is interrupted during the encryption process then it would result in the volume not being fully encrypted. While BitLocker is encrypting a volume there is a progress bar along with a pause and cancel button, if the encryption processed is paused once the drive is reconnected to the machine it will continue to be in the pause state until the user clicks on resume. In this case, the MyDigitalSSD Drive continued to encrypt automatically suggesting the encryption process was interrupted without being paused.

23. As the MyDigitalSSD Drive was in a "read-only" state no changes would have been made to the drive whilst in KLD Discovery's possession. A forensic image was taken of the encrypted data and the BitLocker recovery key was exported to allow forensic tools to decrypt the data. A successful decryption of the data was confirmed. This is referred to as a physical image. As a precaution, in case there were any issues with the decryption process in KLD Discovery's forensic tools, a logical image (a copy of all data on a logical volume, including deleted files) was also captured.

24. At 14:02 both the Additional Drives were returned to our client and were left in his possession. At 15:35 KLD Discovery left our client's address and returned to KLD Discovery's London office with the captured forensic images. This firm has since taken custody of the Additional Drives and they remain in our possession.

25. After KLD had completed the imaging and left the premises, our client did a more comprehensive search of the drawer. He took everything out and checked the contents of the drawer and found a label that fit the missing end of the Samsung Drive.

Yours faithfully

Shoosmiths LLP

cc. Harcus Parker LLP; EIP LLP; Enyo Law LLP; Macfarlanes LLP

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
Fifth Witness Statement Dr Craig Steven Wright
Dated 01 December 2023
Exhibits CSW20

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**")
Claim No. IL-2022-000035
(the "**Coinbase Claim**")
Claim No. IL-2022-000036
(the "**Kraken Claim**")
Claim No. IL-2022-000069
(the "**BTC Core Claim**")

BETWEEN:

CRYPTO OPEN PATENT ALLIANCE

Claimant

- and -

DR CRAIG STEVEN WRIGHT

Defendant

EXHIBIT CSW20 TO
FIFTH WITNESS STATEMENT OF DR CRAIG STEVEN WRIGHT

Travers Smith LLP 10 Snow Hill, London, EC1A 2AL
T: +44 (0)20 7295 3000 | www.traverssmith.com

By email only

FAO: Mr Justice Mellor
c/o Ms Susan Woolley
HMCTS
Royal Courts of Justice
Rolls Buildings
Fetter Lane
London
EC4A 1NL

Our ref: JXL/TDK

Doc ID: 35544543

Direct line: +44 (0)20 7295 3744

Email: John.Lee @traverssmith.com

25 September 2023

Dear Ms Woolley

Crypto Open Patent Alliance v Dr Craig Steven Wright (Claim No. IL-2021-000019)

Please would you be kind enough to pass this message on to Mr Justice Mellor.

We have considered the transcript from the hearing on 22 September 2023 and the Judge's email of 21 September 2023.

The key point that emerges from the transcript from Dr Wright's perspective is that Mr Justice Mellor considers that it would be helpful for Dr Wright to provide certain further information. Dr Wright wishes to assist the Judge in that regard.

Having considered the clear view expressed by Mr Justice Mellor (p.1, line 20 to p.2, line 1), Dr Wright is willing to agree to identify all authentic drafts of the White Paper in Dr Wright's disclosure, specify the date on which each such document was created (to the best of his recollection), and state whether Dr Wright is aware of any of those documents having since been altered, and if so in what respects, provided that Dr Wright is given until 23 October 2023 to provide this information. Dr Wright understands that this would be *in lieu* of providing a response to the corresponding requests in the Claimant's Request for Further Information. Dr Wright hopes this indication is of assistance to the Judge.

At this stage, Dr Wright is not prepared to agree to provide equivalent information in respect of any further documents on the basis that such documents would not be the "key documents" (i.e., drafts of the White Paper) that the Judge had in mind at p.1 lines 21-22 of the transcript. However, if the Judge had other documents in mind, beyond those covered by Dr Wright's voluntary agreement as set out above, Dr Wright would want to understand what documents they were, in order to consider

the matter further. To that end, Dr Wright proposes that the judgment identifies any other "key documents" in respect of which the Judge would find further information helpful. Dr Wright will consider the judgment, following which the parties can seek to agree what (if any) further information should be provided. If the parties cannot reach agreement in that regard, the matter can conveniently come back before the court at the hearing that is likely to take place on 12th or 13th October 2023.

For completeness, it is worth adding that Dr Wright is not prepared to agree to provide equivalent information in relation to all of the Reliance Documents, or even "*all documents in extended disclosure*", which were categories of documents mentioned in the email from the Judge's clerk to COPA's clerks dated 21 September 2023 (15:51). To do so would involve going beyond what COPA has requested by way of its RFI.

Having now had the opportunity to review the transcript, Dr Wright is aware that COPA proposed an extension to the deadline for the expert evidence in digital currency technology until 14 days after further answers have been given to the questions under Section E of COPA's RFI. Dr Wright is prepared to agree to provide such further answers on the basis that (i) he is given until 23 October 2023 to do so and (ii) in line with COPA's proposal, the deadline for the expert evidence in digital currency technology shall fall 14 days later, i.e., on 6 November 2023. The following directions would then be convenient:

(a) Reply reports are dispensed with (because the experts will have the opportunity to make any points in reply by way of their joint statement); the experts meet on or before 24 November 2023 (i.e. the same date as the experts on forensic document analysis); and prepare a joint statement by 8 December 2023 (i.e. the same date as the experts on forensic document analysis); or

(b) Reply reports on 16 November 2023; the experts meet on or before 24 November 2023; and prepare a joint statement by 8 December 2023.

Dr Wright's voluntary agreement to provide the information set out above, on the terms set out above, is without prejudice to all of his rights and intended to be helpful to the court. If, however, COPA objects to this approach, or the agreement is otherwise not carried into effect, all of Dr Wright's rights are entirely reserved.

Turning briefly to a separate issue: Dr Wright raised in his skeleton argument a point about the timing of reply factual evidence (see paragraph 61). This was not addressed by the parties at the hearing, but it is hoped that the issue will be uncontroversial because (i) Dr Wright simply intends to preserve the structure of the CCMC Order (i.e. reply factual evidence falls two weeks after reply expert reports in forensic document analysis); and (ii) this structure has been upset by an inadvertent slip in the course of agreeing revised dates for those reply expert reports. Dr Wright will therefore be asking for this issue to be dealt with in the order following the Judge's judgment.

Dr Wright hopes that this email addresses the issues that the Judge wished to raise with the parties. If so, it may be that the hearing fixed for Tuesday morning does not need to go ahead. However, if a hearing would be of assistance to the court, Dr Wright is of course very happy to attend.

Finally, there is one further matter that Dr Wright wishes to raise at this stage in the interests of transparency. Dr Wright has recently discovered some additional documentation that has not been disclosed. A letter explaining the position will be sent to Bird and Bird within 7 days.

Yours faithfully

Travers Smith LLP

Travers Smith LLP

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
Fifth Witness Statement Dr Craig Steven Wright
Dated 01 December 2023
Exhibits CSW21

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**")
Claim No. IL-2022-000035
(the "**Coinbase Claim**")
Claim No. IL-2022-000036
(the "**Kraken Claim**")
Claim No. IL-2022-000069
(the "**BTC Core Claim**")

BETWEEN:

CRYPTO OPEN PATENT ALLIANCE

Claimant

- and -

DR CRAIG STEVEN WRIGHT

Defendant

EXHIBIT CSW21 TO
FIFTH WITNESS STATEMENT OF DR CRAIG STEVEN WRIGHT

Travers Smith LLP 10 Snow Hill, London, EC1A 2AL
T: +44 (0)20 7295 3000 | www.traverssmith.com

By email only

Bird & Bird LLP
12 New Fetter Lane
London
EC4A 1JP

Your ref:	PNQS/NIXL/WIDW/CRYOP.0001
Our ref:	JXL/AMZF/C07239-00002
Doc ID:	35621893
Direct line:	+44 (0)20 7295 3744
Email:	john.lee@traverssmith.com

2 October 2023

Dear Bird & Bird LLP

Crypto Open Patent Alliance v Dr Craig Steven Wright (Claim No. IL-2021-000019)

We refer to our letter to Mr Justice Mellor dated 25 September 2023.

In that letter, we mentioned that Dr Wright had recently discovered certain documentation, which has not yet been disclosed in these proceedings. We indicated that we would send, within seven days of that letter, a further letter to explain the position.

This letter sets out, for that purpose, a description of (i) the nature of the material, (ii) the identification of the hard drives and (iii) the likely timeframe for the review and disclosure of any disclosable material deriving from those devices.

The nature of the material

1. The material in question consists of two additional hard drives, containing roughly 1TB and 500GB of data (the "**Hard Drives**"). One of the Hard Drives is a "*Samsung T1 USB SSD*" with serial number A665403GAYNC52S, which contains approximately 1 terabyte of data. The other Hard Drive is a "*MyDigitalSSD OTG USB SSD*" with serial number 700001662137051115, which contains approximately 500 megabytes of data.

2. We have been informed by Dr Wright that the Hard Drives contain documents that are likely to be relevant to these proceedings, including (for example) notes Dr Wright wrote between 2005 and 2009.

The identification of the Hard Drives

3. As stated in previous correspondence, we have been liaising with Dr Wright in relation to the provision of further chain of custody information to your clients in relation to the Reliance Documents.

4. We are instructed that, in the course of conducting that exercise, it came to Dr Wright's attention that materials on certain devices (i.e. the Hard Drives) had not been harvested during the original disclosure exercise.

5. In view of Dr Wright's ongoing disclosure obligations, we arranged for a collection to be performed as soon as possible in order to identify whether any material from the Hard Drives was capable of being retrieved.

6. A member of the forensic data team at KL Discovery ("**KLD**"), Dr Wright's e-disclosure provider, attended Dr Wright's residence on 20 September 2023. Forensic images were then taken of the Hard Drives and taken to KLD for processing.

The likely timeframes and next steps

7. The data from those forensic images is still currently being processed by KLD. KLD has indicated that the processing of the data will likely be completed this week.

8. Following processing, a disclosure exercise will need to be undertaken over the data in the usual way (including the application of search terms and date ranges, a review of any responsive documents, and the preparation of any eventual disclosure). We are not currently in a position to estimate how long that exercise may take. As soon as search terms and date ranges have been run over the relevant data and the size of the review population is known, a further update on timings will be provided.

Yours faithfully

Travers Smith LLP

Travers Smith LLP

cc. Harcus Parker Limited, Macfarlanes LLP, Enyo Law, EIP

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
Fifth Witness Statement Dr Craig Steven Wright
Dated 01 December 2023
Exhibits CSW22

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**")
Claim No. IL-2022-000035
(the "**Coinbase Claim**")
Claim No. IL-2022-000036
(the "**Kraken Claim**")
Claim No. IL-2022-000069
(the "**BTC Core Claim**")

BETWEEN:

CRYPTO OPEN PATENT ALLIANCE

Claimant

- and -

DR CRAIG STEVEN WRIGHT

Defendant

EXHIBIT CSW22 TO
FIFTH WITNESS STATEMENT OF DR CRAIG STEVEN WRIGHT

SHOOSMITHS

No. 1 Bow Churchyard
London
EC4M 9DQ

DX 36 London

T +44 (0)370 086 3000
E: copavdrwright@shoosmiths.com

By Email Only (B&B.CRYOP.0001@twobirds.com)
FAO: Phil Sherrell
Bird & Bird LLP
12 New Fetter Lane
London
EC4A 1JP

Date 11 October 2023

Your Ref PNQS/NIXL/WIDW/CRYOP.0001
Our Ref AC.HXF.MG.M-01078068

Dear Bird & Bird LLP

Claim No. IL-2021-000019 Crypto Open Patent Alliance v Dr Craig Wright
Claim No. IL-2022-000035 Dr Craig Wright & Another v. Coinbase Global, Inc & Others
Claim No. IL-2022-000036 Dr Craig Wright & Another v. Payward & Others
Claim No. IL-2022-000069 Dr Craig Wright & Another v. BTC Core & Others (Identity Issue only)

We refer to your second letter of 3 October 2023 to Travers Smith LLP.

We have investigated the position with our client and are instructed as follows in relation to the two additional hard drives:

1. In 2019, our client's then legal representatives in the United States, Rivero Mestre LLP and Ontier LLP in the United Kingdom had conduct of a document retention exercise as part of the litigation in the United States between Ira Kleiman and our client (the "**Kleiman Claim**").

2. As part of this exercise, our client's legal representatives instructed AlixPartners LLP (or one of its associated entities) ("**AlixPartners**"). It arranged for the imaging of electronic storage devices in our client and his wife's control (for example, laptops, drives and CDs) at several locations including in the United Kingdom and Australia.

3. As part of the document retention exercise in the extant claim (IL-2021-000019), our client's then legal representatives in the United Kingdom relied on the aforementioned imaged devices. These formed the subject of disclosure and inspection.

4. Our client is obliged to provide information relating to the chain of custody of the documents which he relies on in the extant claim. During the course of this chain of custody exercise, approximately 6 weeks ago, he was provided by his solicitors with a copy of a draft document which set out a guide for the chain of custody. For the avoidance of doubt, this draft document was created for the purposes of the litigation and is, therefore, privileged. This document contained a column in which it was stated: "Contains encrypted Bitlocker partition" and "Bevel data. Not encrypted". This caused our client concern. The inference was that certain data or drives may not have been collected/imaged because they were encrypted, and that certain Bevel data may have been encrypted.

5. As a result, during the course of the week commencing 11 September 2023 our client started to conduct a search of his residential property, 21 Harebell Hill, Cobham, Surrey, KT11 2RS for drives imaged by AlixPartners.

6. On 14 September 2023, our client enquired of its then legal representatives, Travers Smith LLP, requesting further information on the draft document and where the information therein came from. In turn, Travers Smith LLP enquired of AlixPartners and subsequently explained that in 2019 AlixPartners could not image certain drives because they were encrypted or had no data available or were damaged.

7. On the 15 September 2023, our client intensified the search of his residential property. On the same day he identified two encrypted drives, "Samsung T1 USB SSD" and "MyDigitalSSD OTG USB SSD". These were in a drawer with other drives which had stickers on indicating that they had been imaged by AlixPartners. Following imaging, our client's disclosure provider explained that these drives have serial numbers A665403GAYNC52S and 70000166213705115 respectively. Our client considered that these may be drives which AlixPartners did not or could not image.

8. Our client physically recognised the drive "Samsung T1 USB SSD" as that which contained an image of a drive from when he worked for BDO, the accountancy and business advisory firm (the "**BDO Drive**"). He believes it was purchased in around late 2015 or early 2016 as a replacement for an old backup drive. In particular, he used it to hold images that he did not want to be corrupted or accessible.

9. In particular, he believes that the drive "Samsung T1 USB SSD" was architecturally designed and integrated with firmware and software layers to give the user an illusion of a singular partition despite having two partitions. He explains that this was achieved using advanced partition hiding techniques at the firmware level combined with specialised drivers at the operating system level. For example, such a system was feasible with encryption solutions like VeraCrypt, with a SSD relying on specialised proprietary drivers. When the drive was accessed under regular conditions, only the primary public encrypted partition was visible and accessible to the user. However, upon utilising a specific password, the hidden encrypted partition (including the BDO Drive) became accessible. This layered approach was adopted because the BDO Drive contains information confidential to his clients at BDO. He further explains that, if the drive "Samsung T1 USB SSD" were imaged by AlixPartners when live (namely linked to an active system such as our client's laptop), AlixPartners would have been able to image the hidden encrypted partition (including the BDO Drive). However, if AlixPartners were to have unplugged the drive when imaging it, it would have been transformed into a safeguarded system.

10. Our client believes the drive "MyDigitalSSD OTG USB SSD" as being one which he was using in 2018 which may (or may not) contain relevant document. In particular, he thinks that it may have documents from previous years (although these may have been retained and reviewed already from alternative sources). He does not recall when the drive was acquired or in what circumstances or for what period it was used or in relation to what.

11. Following the identification of the drives, our client did not access either drive. Rather, he notified Travers Smith LLP and Zafar Ali KC of the drives. On 20 September 2023, our client's disclosure provider KL Discovery attended our client's property above and took a full forensic image of the drives. Our client notes, however, that he gave his son access to some of the drives in approximately 2020 (to build his computer) after the 2019 document retention exercise was completed. He is unclear what use his son made of said drives.

12. On 25 September 2023, our client's then legal representatives notified the court of the discovery and, on 2 October 2023, your firm was provided with further details.

13. In the intervening period, KL Discovery has processed the imaged drives and explains that after de-duplication:

- "Samsung T1 USB SSD" contains approximately 89,600 documents;
- "MyDigitalSSD OTG USB SSD" contains approximately 181,400 documents.

14. Our client's disclosure provider has then applied the keyword searches from the disclosure review document (as updated) to these documents and the following have been identified as potentially relevant for review for relevance, privilege and confidentiality (see Annex 1):

    - "Samsung T1 USB SSD" contains approximately 41,853 documents;
    - "MyDigitalSSD OTG USB SSD" contains approximately 12,941 documents.

15. Our client considers a review of approximately 54,794 documents to be disproportionate. In particular, assuming one fee earner can review 800 documents a day, this will necessitate approximately 68 fee earner days. This is before any second review. Our client, therefore, proposes a narrower set of keyword searches (see Annex 2). When these are applied (instead of those at ¶14 above, the following have been identified as potentially relevant for review for relevance, privilege and confidentiality:

    - "Samsung T1 USB SSD" contains approximately 2,159 documents;
    - "MyDigitalSSD OTG USB SSD" contains approximately 4,143 documents.

16. Our client has also conducted his own preliminary review and found that there were approximately 100 documents which may be relevant.

Our client would like to emphasise the following:

17. For the document retention exercise conducted in 2019, he made available all of his electronic storage devices to AlixPartners for imaging;

18. Following the document retention exercise in 2019, he was assured by his then legal representatives, Ontier LLP, that AlixPartners had imaged all of the relevant drives and had all of the documents;

19. In the Kleiman Claim, our client was informed by Rivero Mestre LLP and/or Ontier LLP that they would submit everything that was relevant. Our client did not have access to a disclosure platform (such as Relativity) in the Kleiman Claim and so could not check what documents were disclosed.

20. In the Kleiman Claim, our client inquired about his main documents relevant to identity and whether they were disclosed (but was told that for the US case it was not about identity).

21. In the extant claim, with nearly a million documents for review in Relativity, it has been difficult for our client to cross-check what is and is not disclosed in the claim.

Addressing your remaining question, "Samsung T1 USB SSD" and "MyDigitalSSD OTG USB SSD" do not relate to documents ID_004637 to ID_004641.

We trust this addresses your client's questions.

It is incumbent on the parties to agree a reasonable and proportionate method for addressing the identification of these additional drives. To that end, our client proposes the following:

22. We are in the process of reviewing the documents which our client says are relevant (as described at ¶16 above). We will provide these documents to you as soon as possible. Upon receipt of these, our client invites your client's agreement within 7 days that it may rely on these additional

documents at trial, pursuant to CPR 57AD, ¶12.5. Absent agreement, our client will make an application to the court.

23. We invite your client's agreement to the keywords at ¶15 above within 7 days. Absent agreement, our client will again make an application seeking directions from the court.

Turning to your request for access to the forensic images, we do not consider this necessary or appropriate for the following reasons:

24. Disclosure of the forensic image is likely to result in inspection by your client of material which is not relevant to this litigation and which is private, privileged and/or confidential to our client. Further, Samsung T1 USB SSD may contain documents which are confidential to third parties and, in particular, our client's clients at BDO;

25. The forensic image is likely to necessitate both parties reviewing the documents for relevance, resulting in considerable duplication of cost and time;

26. Your allegation of "repeated 'incorrect' relevance marking", if correct, is not, of itself, a reason for wanting access to the forensic image.

27. There is no reason to conclude that our firm is unable to conduct the review for relevance;

28. We understand that forensic images were not ordered as part of the disclosure review document;

29. We understand that the disclosure of forensic images has been rehearsed between the parties, with your client not previously advancing any request;

30. We understand that your expert on electronic document authenticity has been able to produce a report absent the forensic images.

Turning to the allegations of Mr Ager-Hanssen as summarised in your letter, we are instructed as follows:

31. "Dr Wright provided hard drives of previously unseen material to colleagues at nChain…": Our client did not provide hard drives of previously unseen material to his colleagues at nChain. For completeness, following the hard drives above being imaged, he did review the hard drive and provide copies of certain documents to Mr Ager-Hanssen;

32. "… and that those hard drives contain evidence of internet searches by Dr Wright concerning methods of manipulating documents …": For the avoidance of doubt, the hard drives do not contain the internet searches to which Mr Ager-Hanssen refers. By means which are yet to be confirmed, we understand that Mr Ager-Hanssen obtained a record of our client's internet search history from his personal laptop. These were searches conducted by our client following service of your client's expert report on the authenticity of the electronic documents, to understand and test the allegations made therein.

We are in the process of obtaining copies of the search history materials to which Mr Ager-Hanssen refers and will revert shortly.

Yours faithfully

Shoosmiths LLP

Shoosmiths LLP

cc. Harcus Parker LLP; EIP LLP; Enyo Law LLP; Macfarlanes LLP

Annex 1 - Keywords

Keywords	RPs
"A purely peer-to-peer version of electronic cash"	01/08/2019 to 31/08/2019
"Abacus"	01/09/2012 to 30/09/2019
"Adam" AND "Back"	01/01/2001 to 30/04/2011
"Allan" OR "Granger"	01/01/2001 to 31/08/2019
"Allan" OR "Pedersen"	01/01/2001 to 30/04/2011 and 01/02/2016 to 30/11/2016
"Ash"	01/08/2007 to 30/04/2011
"AUS Industry"	01/01/2001 to 31/08/2019
"Avila" AND (timestamp* OR “time-stamp*”)	01/01/2001 to 31/08/2019
"Bagnoo" AND (*DSL OR FIBRE OR BROADBAND)	01/01/2001 to 31/08/2019
"Base58"	01/01/2001 to 31/08/2019
"Bayesian"	01/01/2001 to 30/04/2011
"BBC"	01/02/2016 to 30/11/2016
"Bear"	01/01/2001 to 30/04/2011
"Beneficiary"	01/09/2012 to 30/09/2019
"Benfords Law" OR "Benford's Law"	01/01/2001 to 30/04/2011
"beta w/7 tomorrow" OR “nosey”	01/01/2001 to 31/08/2019
"big reveal"	01/02/2016 TO 30/11/2016
"Bitcoin" w/5 "Trust"	01/09/2012 TO 30/09/2019
"Bitcoin" w/5 ("White Paper" OR "WhitePaper")	01/01/2001 to 31/08/2019
"Bitcoin: A Peer-to-Peer Electronic Cash System"	01/01/2001 to 31/08/2019
"Blacknet" OR "Project Blacknet"	01/01/2001 to 31/08/2019
"blind" AND "trust"	01/02/2016 TO 30/11/2016
"block 170" OR "##\#170" OR "block170"	01/01/2001 to 31/08/2019
"block 9" OR "##\#9" OR "block9"	01/01/2001 to 31/08/2019
"Blockchain" OR "blokchain" OR "blochain" OR "block-chain" OR "block chain"	01/01/2001 to 31/08/2019
"C++"	01/01/2001 to 30/04/2011
"Chancellor" w/4 "brink"	01/01/2001 to 31/08/2019
"Charles Sturt University" OR "Charles Sturt" OR "CSU"	01/01/2001 to 30/04/2011
"Chesher"	01/01/2001 to 31/08/2019
"Clear" w/2 "text"	01/01/2001 to 30/04/2011
"Copyright submission" OR "Copyright Registration"	01/04/2019 to 30/04/2019
"Costa Rica"	01/09/2012 TO 30/09/2019
"covad communications"	01/01/2001 to 31/08/2019
"CPU power"	01/01/2001 to 30/04/2011
"craig@rcjbr.org"	01/02/2016 TO 30/11/2016
"craigwright.net" OR "drcraigwright.net"	01/02/2016 TO 30/11/2016
"Cryddit"	01/01/2001 to 30/04/2011

"cryptographic proof"	01/02/2016 TO 30/11/2016 + to date
"cryptographic proof"	01/02/2016 TO 30/11/2016 + to date
"David Kleiman"	01/09/2012 TO 30/09/2019
"Dawn" OR "Song"	01/08/2007 – 30/04/2011
"Declairation"	01/01/2001 to 31/08/2019
"Deed of Assignment"	01/09/2012 TO 30/09/2019
"Deed of Trust"	01/09/2012 TO 30/09/2019
"DeMorgan"	01/01/2001 to 30/04/2011
"Design of a secure timestamping service with minimal trust requirements"	01/01/2001 to 31/08/2019
"DH Key"	01/01/2001 to 30/04/2011
"Diffculties"	01/01/2001 to 31/08/2019
"Diffe Hellman" OR "Diffe-Hellman" OR "DHKE" OR “Diffie Hellman” OR “Diffie-Hellman”	01/01/2001 to 30/04/2011
"Digicash"	01/01/2001 to 31/08/2019
"disk full"	01/08/2007 – 30/04/2011
"Distributed under the MIT/X11 software”	01/01/2001 to 31/08/2019
"DK"	01/01/2001 to 30/04/2011
"Dr Craig S Wright"	01/01/2019 – 31/12/2019
"Ecash" OR "E-cash"	01/01/2001 to 30/04/2011
"Economist"	01/02/2016 TO 30/11/2016
"EITC"	01/02/2016 TO 30/11/2016
"embargo"	01/02/2016 TO 30/11/2016
"exclusive" AND right*	01/02/2016 TO 30/11/2016
"extraordinary proof"	01/02/2016 TO 30/11/2016 + to date
"Feller" AND probability*	01/01/2001 to 31/08/2019
"Finney"	01/08/2007 – 30/04/2011 + 1/5/2011 to 21/07/2023
"First response"	01/02/2016 TO 30/11/2016
"Fraud detection"	01/01/2001 to 30/04/2011
"Gavin” OR “Andresen"	01/08/2007 – 30/04/2011 + 1/5/2011 to 21/07/2023
"GCC"	01/01/2001 to 31/08/2019
"Genesis Block"	30/04/2011 to proceedings
"Genesis"	01/01/2001 to 30/04/2011
"GIAC"	01/01/2001 to 30/04/2011
"GQ" OR "GQ Magazine"	01/02/2016 TO 30/11/2016
"Hack"	01/01/2001 TO 30/04/2011 AND 01/02/2016 TO 30/11/2016
"Hal"	01/01/2001 to 31/08/2019

"Harber" AND (timestamp* OR “time-stamp*”)	01/01/2001 to 31/08/2019
"Hashcash - a denial of service counter-measure"	01/01/2001 to 31/08/2019
"Hearn"	01/08/2007 – 30/04/2011 + 1/5/2011 to 21/07/2023

"How to time-stamp a digital document"	01/01/2001 to 31/08/2019
"IBC 064409"	01/01/2001 to 31/08/2019
"IBC 093344"	01/01/2001 to 31/08/2019
"IEEE Computer Society"	01/01/2001 to 31/08/2019
"Ignatius" OR "Pang"	01/01/2001 to 31/08/2019
"IKE SA"	01/01/2001 to 30/04/2011
"Immutable"	01/01/2019 – 31/12/2019
"Improving the efficiency and reliability of digital time-stamping"	01/01/2001 to 31/08/2019
"independently validated"	01/02/2016 TO 30/11/2016
"Integyrs"	01/08/2007 – 30/04/2011 and 01/02/2016 to 30/11/2016
"IPSec Encryption"	01/01/2001 to 30/04/2011
"IPSec SA"	01/01/2001 to 30/04/2011
"Jean-Paul" OR Sartre	01/01/2001 to 31/08/2019
"Journal of Cryptology"	01/01/2001 to 31/08/2019
"Judith" OR "Ryan" OR "Tramboo"	01/01/2001 to 31/08/2019
"Kleiman"	01/09/2012 TO 30/09/2019
"Kleiman" OR "Kleinman" OR "Klieman" OR "Klienman"	01/01/2001 to 30/04/2011
"Last" w/4 "out"	01/01/2001 to 30/04/2011 and 01/02/2016 to 30/11/2016
"Law"	01/01/2019 – 31/12/2019
"Liberty Reserve"	01/09/2012 TO 30/09/2019
"licence"	01/01/2001 to 31/08/2019
"Lisa" AND "Edwards"	01/01/2001 to 30/04/2011
"Ludwig" OR "Siegele"	01/01/2001 to 31/08/2019
"Lynn"	01/01/2001 to 30/04/2011 and 01/02/2016 to 30/11/2016
"Magnusson"	01/01/2001 to 30/04/2011 and 01/02/2016 to 30/11/2016
"Matonis"	01/01/2001 to 31/08/2019
"lynam" OR "maxlynam"	01/01/2001 to 31/08/2019
"Media Team"	01/02/2016 TO 30/11/2016
"Merkle"	01/01/2001 to 31/08/2019
"Merkle" AND (tree*OR key* OR crypt* OR protocol*OR IEEE*)	01/01/2001 to 31/08/2019
"Meta" OR "Metanet" OR "Meta net"	01/08/2007 – 30/04/2011
"Metzdowd.com" OR "Metzdowd"	01/01/2001 to 31/08/2019

"Milk Publicity"	01/02/2016 TO 30/11/2016
"MIT Licence"	01/01/2001 TO 31/08/2019
"move" OR "moving"	01/02/2016 TO 30/11/2016
"MSVC"	01/01/2001 TO 31/08/2019
"nChain"	01/02/2016 TO 30/11/2016 AND 01/01/2019 – 31/12/2019

"Neville" OR "Sinclair"	01/01/2001 TO 31/08/2019
"Nguyen"	01/01/2001 TO 31/08/2019
"Nick" OR "Nicholas" OR "Courtois"	01/01/2001 TO 31/08/2019
"Node"	01/01/2001 to 30/04/2011
"Nonreversible" OR "non-reversible"	01/01/2001 to 30/04/2011 and 01/02/2016 to 30/11/2016
"Northumbria University"	01/01/2001 to 30/04/2011
"online payment"	01/01/2001 to 30/04/2011
"overseas trust"	01/09/2012 TO 30/09/2019
"P2P Foundation"	01/01/2001 TO 31/08/2019
"P2P" OR "peer2peer" OR "peer 2 peer" OR "peer-2- peer" OR "peer to peer" OR "peer-to-peer" OR "PGP"	01/01/2001 TO 31/08/2019
"P2PK"	01/08/2007 – 30/04/2011
"P2PKH"	01/08/2007 – 30/04/2011
"Panopticrypt Pty Ltd"	01/09/2012 TO 30/09/2019
"Patch Tuesday"	01/01/2001 TO 31/08/2019
"Press Team"	01/02/2016 TO 30/11/2016
"proof of work"	01/01/2001 TO 31/08/2019
"Protocols for public key cryptosystems"	01/01/2001 TO 31/08/2019
"Quisquater" AND (timestamp* OR “time-stamp*”)	01/01/2001 TO 31/08/2019
"Rana Pala" OR "Ravinder" OR "Singh" OR "Pala"	01/01/2001 TO 31/08/2019
"Ray" OR "Dillinger"	01/01/2001 to 30/04/2011
"Rayner"	01/01/2001 to 30/04/2011
"Ridges"	01/01/2001 to 30/04/2011 and 01/02/2016 to 30/11/2016
"Macgregor" OR "Macgregor" OR "McGregor" OR rmacgregor*	01/01/2001 TO 31/08/2019
"root hash"	01/01/2001 TO 31/08/2019
"Rory" OR "Cellan-Jones"	01/01/2001 TO 31/08/2019
"SANS"	01/01/2001 to 30/04/2011
"Satoshi Nakamoto"	01/01/2001 to 30/04/2011 and 01/02/2016 to 30/11/2016
"Savannah Ltd"	01/09/2012 TO 30/09/2019
"Sebastian" OR "Stevens"	01/01/2001 TO 31/08/2019

"Secp256k1"	01/01/2001 TO 31/08/2019
"Secure names for bit-strings"	01/01/2001 TO 31/08/2019
"Secure"	01/01/2001 to 30/04/2011 and 01/02/2016 to 30/11/2016
"Sequences II: Methods in Communication, Security and Computer Science"	01/01/2001 TO 31/08/2019
"Services Agreement"	01/02/2016 TO 30/11/2016
"Settle"	01/09/2012 TO 30/09/2019
"Settlor"	01/09/2012 TO 30/09/2019
"Seycehlles" OR “Seychelles”	01/09/2012 TO 30/09/2019

"Shamir"	01/01/2001 TO 31/08/2019
"Shane" OR "Paterson"	01/01/2001 TO 31/08/2019
"Shoaib" OR "Yousuf"	01/01/2001 TO 31/08/2019
"Sidney" OR "Lim"	01/01/2001 TO 31/08/2019
"smart contract"	01/01/2019 – 31/12/2019
"SN"	01/01/2001 to 30/04/2011 and 01/02/2016 to 30/11/2016
"SourceForge"	01/01/2001 TO 31/08/2019
"Split key cryptographic process"	01/09/2012 TO 30/09/2019
"Stefan" OR "Matthews"	01/01/2001 TO 31/08/2019
"Sterling" AND "Group"	01/02/2016 TO 30/11/2016
"Stornetta" AND (timestamp* OR “time-stamp*”)	01/01/2001 TO 31/08/2019
"story" AND "life"	01/02/2016 TO 30/11/2016
"story" AND "Satoshi"	01/02/2016 TO 30/11/2016
"story" w/10 right*	01/02/2016 TO 30/11/2016
"Stuart" OR "McGurk"	01/02/2016 TO 30/11/2016
"submission"	01/01/2019 – 31/12/2019
"SysAdmin, Audit, Network, and Security" OR "SANS"	01/01/2001 to 30/04/2011
"Tanveer" OR "Zia"	01/01/2001 to 30/04/2011 and 01/02/2016 to 30/11/2016
"the Outside Organisation"	01/02/2016 TO 30/11/2016
"the Sartre message"	01/01/2001 TO 31/08/2019
"The Workshop Technologies"	01/02/2016 TO 30/11/2016
"thucuyen279@gmail.com"	01/02/2016 TO 30/11/2016
"Time Chain" OR "Timecoin" OR "Bytecoin" OR "Bytecash"	01/01/2001 TO 31/08/2019
"trusted central authority" OR "central authority"	01/01/2001 to 30/04/2011
"Trustee"	01/09/2012 TO 30/09/2019
"TTL"	01/09/2012 TO 30/09/2019
"Tulip Trading" OR "Tulip Trading Limited" OR "Tulip Trading Ltd"	01/09/2012 TO 30/09/2019

"Tulip Trust" OR "TulipTrust"	01/09/2012 TO 30/09/2019
"Tulip" w/5 Trust	01/09/2012 TO 30/09/2019
"TX0008708058"	01/04/2019 – 30/04/2019
"TXu002136996"	01/04/2019 – 30/04/2019
"University of Newcastle, Australia" OR "University of Newcastle"	01/01/2001 – 30/04/2011
"Upload.ae"	01/01/2001 TO 31/08/2019
"US Copyright Office" OR ("Copyright" w/2 "Office")	01/04/2019 – 30/04/2019
"Usenet"	01/01/2001 – 30/04/2011
"UT"	01/09/2012 TO 30/09/2019
"Uyen Ngyen"	01/01/2001 TO 31/08/2019
"Uyen"	01/09/2012 TO 30/11/2016

"verifiable cryptographic evidence"	01/02/2016 TO 30/11/2016
"version of me"	01/02/2016 TO 30/11/2016 + to date
"version of me"	01/02/2016 TO 30/11/2016 + to date
"Viveca"	01/01/2001 TO 31/08/2019
"W&K"	01/08/2007 TO 30/11/2016
"Wei Dai"	01/01/2001 TO 31/08/2019
"Whitepaper" OR "White Paper"	01/01/2001 TO 30/04/2011 AND 01/02/2016 TO 30/11/2016
"Workshop Technologies"	01/01/2001 TO 31/08/2019
"WORM"	01/01/2001 TO 30/04/2011 AND 01/02/2016 TO 30/11/2016
"Wright International Investments"	01/09/2012 TO 30/09/2019
"Wright International" OR "WII"	01/09/2012 TO 30/09/2019/4
"Yvonne" OR "Simeon"	01/09/2012 TO 30/09/2019
(ATO OR (Australia* AND "Tax* Office") OR ((Australia* w/6 investigation) AND tax*) OR (auscript w/100 tax)) AND 2009	01/01/2001 TO 31/08/2019
(ATO OR (Australia* AND "Tax* Office")) AND (2009 OR 2010)	01/01/2001 TO 31/08/2019
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND "white paper"	01/01/2001 TO 31/08/2019
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND ("compiler code" OR "Machine Language" OR M	01/01/2001 – 30/04/2011
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND (trademark* OR patent* OR copyright)	01/01/2001 – 30/04/2011
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND (trust OR trusts)	01/01/2001 TO 31/08/2019
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND “white- paper”	01/01/2001 TO 31/08/2019
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND agree*	01/01/2001 – 30/04/2011
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND bitcoin	01/01/2001 TO 31/08/2019
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND Bitcoin*	01/01/2001 TO 31/08/2019

(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND cash	01/01/2001 – 30/04/2011
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND code	01/01/2001 TO 31/08/2019
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND contract	01/01/2001 – 30/04/2011
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND corp*	01/01/2001 – 30/04/2011
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND Craig*	01/01/2001 – 30/04/2011
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND crypto*	01/01/2001 – 30/04/2011
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND draft	01/01/2001 TO 31/08/2019
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND electronic	01/01/2001 – 30/04/2011
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND exchange OR server OR "exchange server"	01/01/2001 TO 31/08/2019
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND gold	01/01/2001 – 30/04/2011
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND IP	01/01/2001 – 30/04/2011
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND key*	01/01/2001 TO 31/08/2019
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND LLC	01/01/2001 – 30/04/2011

(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND loan	01/01/2001 – 30/04/2011
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND mine*	01/01/2001 TO 31/08/2019
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND mining	01/01/2001 TO 31/08/2019
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND money	01/01/2001 – 30/04/2011
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND partner*	01/01/2001 – 30/04/2011
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND pay	01/01/2001 – 30/04/2011
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND peer	01/01/2001 – 30/04/2011
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND sale	01/01/2001 – 30/04/2011
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND sell	01/01/2001 – 30/04/2011
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND supercomputer	01/01/2001 – 30/04/2011
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND transfer*	01/01/2001 – 30/04/2011
(David OR Dave OR Davids OR Daves OR dave_kleiman OR davekleiman) AND venture*	01/01/2001 – 30/04/2011
("don" AND NOT "don't" AND NOT "don't" AND NOT "dont" AND NOT "don'ts" AND NOT "don'ts") OR "donlynam" OR "Lynam"	01/01/2001 TO 31/08/2019
(whitepaper OR paper OR "White Paper") AND draft*	01/01/2001 TO 31/08/2019
*@acm.org	01/08/2007 – 30/04/2011
*@floriculture.com.au	01/01/2001 TO 31/08/2019
*@gmx.com	01/01/2001 TO 31/08/2019
*@outside-org.co.uk	01/02/2016 TO 30/11/2016
*@theworkshop.com	01/02/2016 TO 30/11/2016

*@vistomail.com	01/01/2001 TO 31/08/2019
0.1	01/01/2001 TO 31/08/2019
*anonymousspeech.com	01/01/2001 TO 31/08/2019
*CSU.edu.au	01/01/2001 – 30/04/2011
*giac.org	01/01/2001 – 30/04/2011
*Information-defense.com	01/01/2001 TO 31/08/2019
mapAddresses.count	01/01/2001 TO 31/08/2019
*Newcastle.edu.au	01/01/2001 – 30/04/2011
*sans.edu	01/01/2001 – 30/04/2011
*sans.org	01/01/2001 – 30/04/2011
“craig@rcjbr.org”	01/08/2007 TO 30/11/2016
0x0000000000019d6689c085ae165-831e934ff763ae46a2a6c172b3f1b60a8ce26f	01/01/2001 TO 31/08/2019
1NSwywA5Dvuyw89sfs3oLPvLiDNGf48cPD	01/01/2001 TO 31/08/2019
Andreas OR Furche	01/01/2001 TO 31/08/2019
anon* OR annon*	01/01/2001 – 30/04/2011
Bayer AND (timestamp* OR time-stamp* OR Sequences OR Bit-string* OR Bitstring*)	01/01/2001 TO 31/08/2019
Bitcoin	01/01/2019 – 31/12/2019
Bitcoin OR bit-coin OR "bit coin"	01/08/2007 – 30/04/2011
Bitcoin.exe	01/01/2001 TO 31/08/2019

Bitcoin.org	01/01/2001 – 30/04/2011
bitcoin-0.1.1.rar	01/01/2001 TO 31/08/2019
Bitcointalk.org	01/01/2001 – 30/04/2011 + to end 31/12/2011
B-money	01/01/2001 TO 31/08/2019
Brooks	01/02/2016 TO 30/11/2016
Caley	01/02/2016 TO 30/11/2016
Calvin OR Ayre	01/01/2015 TO 30/11/2016
Chain*	01/01/2001 – 30/04/2011
Clear* w/4 system*	01/01/2001 – 30/04/2011
Cleartext*	01/01/2001 – 30/04/2011
Connie OR Merlino	01/08/2007 – 30/04/2011
Crypto*	01/01/2001 – 30/04/2011
Dav* w/3 (Klei* OR Klie*)	01/01/2001 TO 31/08/2019
David* OR Dave*	01/01/2001 – 30/04/2011
Digit* AND signat*	01/01/2001 – 30/04/2011
Digit* w/2 note*	01/01/2001 – 30/04/2011
Digit* w/4 signat*	01/01/2001 – 30/04/2011
Doubl* w/2 spen*	01/01/2001 TO 31/08/2019

Edwards	01/02/2016 TO 30/11/2016
Electr* AND cash	01/01/2001 – 30/04/2011
Electr* w/4 cash	01/01/2001 TO 30/04/2011 AND 01/02/2016 TO 30/11/2016
Electr* w/4 pay*	01/01/2001 TO 30/04/2011 AND 01/02/2016 TO 30/11/2016
electronic contract*	01/01/2001 – 30/04/2011
Finney	01/08/2007 TO 30/04/2011 + 1/5/2011 to 21/07/2023
Williams	01/01/2001 TO 31/08/2019
Gateway* w/2 Peer*	01/01/2001 TO 30/04/2011 AND 01/02/2016 TO 30/11/2016
Gavin OR Andresen	01/08/2007 TO 30/04/2011 + 1/5/2011 to 21/07/2023
Wrightson	01/01/2001 TO 31/08/2019
Harris	01/02/2016 TO 30/11/2016
Info* Defense OR Info* Defence	01/01/2001 TO 31/08/2019
Laimer	01/01/2001 TO 30/04/2011 AND 01/02/2016 TO 30/11/2016
Lasseter*	01/01/2001 TO 31/07/2007
Massias	01/01/2001 TO 31/08/2019
McLaughlin	01/01/2001 – 30/04/2011
Mine* OR mining	01/01/2001 TO 30/04/2011 AND 01/02/2016 TO 30/11/2016
Naka* OR Nako*	01/01/2001 TO 30/04/2011 AND 01/02/2016 TO 30/11/2016
nakamoto2	01/01/2001 TO 31/08/2019
Negotia* w/2 instrument*	01/01/2001 TO 30/04/2011 AND 01/02/2016 TO 30/11/2016

Poké* OR Poke* OR Poka*	01/01/2001 TO 30/04/2011 AND 01/02/2016 TO 30/11/2016
Priva* AND (anon* OR annon*)	01/01/2001 TO 30/04/2011 AND 01/02/2016 TO 30/11/2016
Privat* w/2 key*	01/01/2001 TO 30/04/2011 AND 01/02/2016 TO 30/11/2016
Publi* w/3 ledger*	01/01/2001 TO 31/08/2019
Public* w/2 key*	01/01/2001 TO 30/04/2011 AND 01/02/2016 TO 30/11/2016
Public* w/6 privat*	01/01/2001 TO 30/04/2011 AND 01/02/2016 TO 30/11/2016
Rees	01/01/2001 – 30/04/2011
s_nakamoto	01/01/2001 TO 31/08/2019
Sato* OR Sata*	01/01/2001 TO 30/04/2011 AND 01/02/2016 TO 30/11/2016
Satoshi AND reveal*	01/02/2016 TO 30/11/2016
Sava*	01/09/2012 TO 30/09/2019
Settle* w/4 system*	01/01/2001 TO 30/04/2011 AND 01/02/2016 TO 30/11/2016
SSRN	01/01/2001 TO 31/08/2019
SSRN-id*	01/08/2019 – 31/08/2019
Tatiana OR Itzel OR Saldana OR Escobar	01/02/2016 TO 30/11/2016
Traceable* OR untraceable*	01/01/2001 TO 30/04/2011 AND 01/02/2016 TO 30/11/2016
Zoren OR Illievich	01/01/2001 TO 31/08/2019

Annex 2 - Keywords

Keywords	RPs
Quorum	
King's Wi-Fi	
Timecoin	
hashchain	
hash chain	
Lamport	
Millicent	
epidemic models	
Micropayment	
e-cash	
Chaum	
Merkle tree	
Security proof	
distributed database	
cryptographic	
verifiability	
chronometer	
chain of rounds	
tikzpicture	
Electronic cash	
proof of work	
mining reward	
Digital cash	
ECDH	
Satoshi	

Nakamoto	
predicate	
game theory	
red Queen	
stochastic games	
Poisson	
digital tokens	
poker	
timestamp	
decentralised	
HMAC	
PKI	
public key	
CPU power	
double-spending	
reliability	
survivability	
nodes	
peer-to-peer	
Oracles	
cryptographic proof	
immutable	
ELECTRONIC CONTRACT	
Trusted Third Parties	
block transmission	
honest	
games	
pow	
latency	
Ecommerce	

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
Fifth Witness Statement Dr Craig Steven Wright
Dated 01 December 2023
Exhibits CSW23

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**")
Claim No. IL-2022-000035
(the "**Coinbase Claim**")
Claim No. IL-2022-000036
(the "**Kraken Claim**")
Claim No. IL-2022-000069
(the "**BTC Core Claim**")

BETWEEN:

CRYPTO OPEN PATENT ALLIANCE

Claimant

- and -

DR CRAIG STEVEN WRIGHT

Defendant

EXHIBIT CSW23 TO
FIFTH WITNESS STATEMENT OF DR CRAIG STEVEN WRIGHT

STROZ FRIEDBERG

MEMORANDUM

Date: 30 November 2023

To: Shoosmiths

From: Spencer Lynch on behalf of Stroz Friedberg

Re: Project Maol - Samsung Drive initial observations.

Recycle Bin

When a file is moved to the recycle bin, the file is renamed with a unique code that begins with $R. The “$R File” timestamps will be the files original timestamps that existed at the time it was deleted.

In addition, a $I file is created that records where the file was originally stored. The timestamps of the “$I file” will reflect when the file was deleted. The $R and $I file will have the same “code” to show they refer to each other.

When the Recycle bin is emptied, both the $R and $I files are deleted. The contents of deleted files remain recoverable until they are overwritten. If the $R file is overwritten we will not know what the file originally contained, and if the $I file is overwritten, we won’t know where it originally existed. Metadata (timestamps) are stored separately from the contents, so we might (and often do) have timestamps for files but would not know their content.

- The Recycle bin in the Samsung drive, contains metadata from September 2023, but all files within the Recycle Bin have been deleted. Therefore, the Recycle Bin must have been emptied in September 2023.

- These files cannot be opened from the Recycle bin directly.

- “$R391BYS.pdf” our forensic tools identified this $R file as being originally named ESDT.PDF
    - The “$R” file was deleted and has been overwritten – we cannot recover its contents. The $I file is still recoverable, so we know what the file was originally named: ESDT.PDF

Path	\$RECYCLE.BIN
Full path	\$RECYCLE.BIN\$R391BYS.pdf
Parent name	$RECYCLE.BIN
Size	130 KB (132,747)
Created	09/19/2017 10:15:50 +0
Modified	09/16/2023 13:54:06 +0
Accessed	09/19/2017 10:15:50 +0

Path	\$RECYCLE.BIN
Full path	\$RECYCLE.BIN\$I391BYS.pdf
Parent name	$RECYCLE.BIN
Size	78 B
Created	09/19/2017 10:17:02 +0
Modified	09/19/2017 10:17:04 +0
Accessed	09/19/2017 10:17:04 +0

- $RFH6M1E.rar and $IFH6M1E.rar
    - Both files are overwritten, so we do not know the original filename, or the content. We do have metadata for both $R (the original file) and $I (showing when deleted)

Path	\$RECYCLE.BIN
Full path	\$RECYCLE.BIN\$RFH6M1E.rar
Parent name	$RECYCLE.BIN
Size	20.6 GB (22,143,612,981)
Created	10/31/2017 18:48:21 +0
Modified	10/31/2017 18:47:56 +0
Accessed	10/31/2017 18:48:20 +0

Path	\$RECYCLE.BIN
Full path	\$RECYCLE.BIN\$IFH6M1E.rar
Parent name	$RECYCLE.BIN
Size	60 B
Created	10/31/2007 06:26:01 +0
Modified	10/31/2007 06:26:02 +0
Accessed	10/31/2007 06:26:02 +0

BDOPC.raw Image

- BDO Image File Metadata:

Full path	\BDOPC.raw
Parent name	\
Size	37.3 GB (39,999,504,384)
Created	10/31/2007 23:48:05 +0
Modified	10/31/2007 23:48:06 +0
Accessed	10/31/2007 23:48:06 +0

- The BDO image is similar to a forensic image – it is effectively a clone of an entire hard drive. That means with sophisticated tools, i.e. not built into Windows, it can be

opened and viewed just like a forensic image meaning we can identify what files it contains and the metadata of those files.

Contents of the BDO Image

- The BDO image contains ‘transactional’ log files with a created, modified, and access time of 17/09/2023. Transactional log files are log files which record certain modifications to data in a filesystem. They are a system file and not accessible or viewable to a normal PC user without forensic tools. We do not at this stage know what modifications were made.

Examples:

Path	\$Extend\$RmMetadata
Full path	\$Extend\$RmMetadata\$TxfLog
Parent name	$RmMetadata
Size	82.3 MB (4,152)
Created	09/17/2023 13:02:32 +0
Modified	10/19/2007 13:04:01 +0
Accessed	10/19/2007 13:04:01 +0

Full path	\$Extend\$RmMetadata\$TxfLog\$TxfLogContainer00000000000000000001
Parent name	$TxfLog
Size	10.0 MB (10,485,760)
Created	09/17/2023 13:02:33 +0
Modified	09/17/2023 13:03:26 +0
Accessed	09/17/2023 13:03:26 +0

Full path	\$Extend\$RmMetadata\$TxfLog\$TxfLogContainer00000000000000000001
Parent name	$TxfLog
Size	10.0 MB (10,485,760)
Created	10/31/2007 07:32:50 +0
Modified	10/31/2007 07:38:31 +0
Accessed	10/31/2007 07:38:31 +0

Full path	\$Extend\$RmMetadata\$TxfLog\$TxfLogContainer00000000000000000001
Parent name	$TxfLog
Size	10.0 MB (10,485,760)
Created	10/31/2007 16:59:51 +0
Modified	10/30/2007 10:44:18 +0
Accessed	10/30/2007 10:44:18 +0

Full path	\$Extend\$RmMetadata\$TxfLog\$TxfLogContainer00000000000000000001
Parent name	$TxfLog
Size	10.0 MB (10,485,760)
Created	10/19/2007 13:04:01 +0
Modified	10/19/2007 13:04:02 +0
Accessed	10/19/2007 13:04:02 +0