**Applicant/Claimant**
**CS Wright**
**1st**
**Exhibit CSW1**
**29 April 2021**

**CLAIM NO. BL-2021-000313**

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

**B E T W E E N:**

**TULIP TRADING LIMITED**
(a Seychelles company)

**Applicant/ Claimant**

**and**

**(1) BITCOIN ASSOCIATION FOR BSV**
(a Swiss verein)
**(2) WLADIMIR VAN DER LAAN**
**(3) JONAS SCHNELLI**
**(4) PIETER WUILLE**
**(5) MARCO FALKE**
**(6) SAMUEL DOBSON**
**(7) MICHAEL FORD**
**(8) CORY FIELDS**
**(9) GEORGE DOMBROWSKI**
**(10) MATTHEW CORALLO**
**(11) PETER TODD**
**(12) GREGORY MAXWELL**
**(13) ERIC LOMBROZO**
**(14) ROGER VER**
**(15) AMAURY SÉCHET**
**(16) JASON COX**

**Respondents/ Defendants**

---

**FIRST WITNESS STATEMENT OF DR CRAIG STEVEN WRIGHT**

---

I, **DR. CRAIG STEVEN WRIGHT** of 21 Harebell Hill, Cobham, KT11 2RS, state as follows:

1. I am one of the ultimate beneficial owners of the Applicant/Claimant, Tulip Trading Ltd ("**TTL**"). I am authorised to make this witness statement on TTL's behalf in support of its applications for: a) service out of the jurisdiction of the Claim Form, Particulars of Claim ("**PoC**") and other documents; and b) service by alternative methods ("**Application**").

2. This statement has been prepared following discussions with TTL's solicitors (who are also my solicitors) over the telephone and via video-conferencing facilities. In making this statement I do not intend, and shall not be deemed, to waive privilege in any respect.

3. The facts and matters set out in this statement are within my own knowledge unless otherwise stated, and I believe them to be true. Where I refer to information supplied by others, the source of the information is identified; facts and matters derived from other sources are true to the best of my knowledge and belief.

4. I have read the PoC and I confirm that the facts stated in it are true. I have also read the witness statement of Oliver James Cain ("**Cain 1**") and, to the extent facts and matters in that document are within my knowledge, I agree with them (although I would not have phrased some of the points in the same way). I have used defined terms used in both those documents.

5. There is now produced and shown to me a paginated bundle of true copy documents marked "CSW1". References in the form [**CSW1/XX**] are to pages in that exhibit.

*Structure of this witness statement*

6. This witness statement is divided into five sections, as follows:

   a. In Section A, I describe my qualifications, background and the creation of Bitcoin.

b. In section B, I describe the digital assets at issue.

c. In Section C, I explain that the private keys to the addresses holding the digital assets that were stolen during a hack of my personal computer, such that I have been deprived of control of those digital assets.

d. In Section D, I explain why the Developers can and should take the action proposed by TTL.

e. In Section E, I make disclosures which I am advised to make by way of full and frank disclosure.

**Section A: My qualifications, background and the creation of Bitcoin**

*My Qualifications*

7. I have eight Masters' degrees (soon to be nine) and two doctorates, including a PhD in computer science and economics from Charles Sturt University, Australia. I am currently studying for a further 21 degrees. I have received no fewer than 60 professional commendations or certifications.[1]

8. These various qualifications and achievements span a number of fields, from Networking Systems Administration to International Commercial Law. However, most relate to mathematics, economics or computer science – all fields in which I have been professionally involved.

[1] By way of example (three out of more than 60), I refer to the following: (1) I was a certified information systems security professional **[CSW1/1]** by the International Information Systems Security Certification Consortium ("**ISC**"); (2) I was certified by the ISC as an Information Systems Security Architecture Professional **[CSW1/2]**; and (3) between 2005 and 2009 I was certified by the Information Systems Audit and Control Association as an Information Systems Auditor **[CSW1/3]**.

*My background*

9. I am a citizen of Australia and Antigua and Barbuda, but since 2015 I have been permanently resident in the United Kingdom, where I live with my wife and two of our children. When eligible, I intend to obtain citizenship of the United Kingdom.

10. I have more than 25 years' experience in the fields of information technology, forensics and security and was previously a lecturer and researcher in computer science at Charles Sturt University. I have authored many articles, academic papers and books, and spoken publicly at conferences on IT, security, Bitcoin and other topics relating to digital currencies and blockchain technologies.

11. I have held senior executive positions with companies focused on digital currency, digital forensics, and IT security. Among my positions, I was between approximately 2009-2012 the vice president of the Centre for Strategic Cyberspace and Security Science with a focus on collaborating with government bodies in securing cyber systems. I also worked between approximately 1996-1997 on systems that protected the Australian Stock Exchange, and have trained Australian government and corporate departments in SCADA (security, cyber warfare, and cyber defence). In one of my early sector focuses, I helped design the architecture for the world's first online casino (Lasseter's Online in Australia, between approximately 2001-2006) and advised Centrebet on security and control systems.

12. I am presently the Chief Scientist of nChain Limited, a role I have had since around September/October 2015.

13. nChain Limited is the research and development arm of the nChain group of companies ("**nChain**"), which I helped establish in 2015. nChain develops blockchain technologies and aims to leverage global trade through blockchain-driven solutions, with the ultimate mission to provide the world, and most especially the business world, with a truly universal secure database. nChain has undertaken research and development for some of the largest global enterprises, as well as in its own right. In addition to creating proprietary products, nChain supports the BSV community by

creating open-source, royalty-free software tools that help to accelerate blockchain technology.

14. In effect, nChain is the vehicle through which I have developed my intellectual property ("**IP**") in blockchain technology since the end of 2015 (and into which I intend to create future IP). Presently, nChain holds 173 granted Patents worldwide, which all derive from my creations and I am therefore the inventor or co-inventor of all its Patents. My first Patent was granted in 2014 in my own name (following an initial application in October 2011).[2] It relates to the use of cryptography in operating a register and has been cited by (among others) Winklevoss LP, LLC in relation to its patents for stable value digital assets (I understand Winklevoss LP, LLC to be one of the corporate vehicles of billionaire BTC investors Cameron and Tyler Winklevoss).

*Creation of Bitcoin*

15. I am also, under the pseudonym "Satoshi Nakamoto", the creator of Bitcoin.

16. Specifically:

    a. Between 2007 and October 2008, I researched and then authored a White Paper entitled *"Bitcoin: A Peer-to-Peer Electronic Cash System"*, which, on 31 October 2008, I publicly released for the first time by uploading it onto the internet under the pseudonym 'Satoshi Nakamoto' (**"the White Paper"**).[3] My interest in digital currency arose from my work in digital security. The idea of electronic cash was not new, but Bitcoin (unlike previous forms of electronic cash) provided the security of the Blockchain to permanently record transactions and therefore protect against fraud.

[2] Wright, C and Wilson, J (2014) *Registry* (Australia Patent No. AU2013201602B2), Australia Patent Office, http://pericles.ipaustralia.gov.au/ols/auspat/applicationDetails.do?applicationNo=2013201602.

[3] This is an exhibit to Mr Cain's witness statement **[OJC1/1/1]**.

b. On 9 January 2009, acting under my pseudonym, I released the first version of the Bitcoin software, which I had also written.

c. I created Bitcoin in 2008 and, prior to its release, I consulted with a number of close friends and relatives, primarily in relation to the wording of parts of the White Paper (those people included Dave Kleiman and my uncle Don Lynam). Dave Kleiman died in April 2013 and the relationship between us is currently the subject of litigation in Florida, brought by Dave's estate ("**Florida Proceedings**"). A trial was set down in that case for June 2021, but it has been delayed (due to scheduling as a result of COVID-19) until probably the autumn of 2021. I deny almost all of the allegations made by Dave's estate and, given the impending trial, I will say little about them. For the avoidance of any doubt, Dave Kleiman had no interest or entitlement to the Bitcoin in the 12ib7 and 1Feex Addresses (which was purchased, not mined).

17. In or around April 2011, I handed over management of the Bitcoin code base (used in the Software), and the related access to and control of the Bitcoin source code repository, to a developer named Gavin Andresen, who took over management of the software maintenance from me. I did this because I had a lot of other things going on in my life at the time. I had created a protocol for Bitcoin that was not to be changed at its core and, as such, the primary task for Mr Andresen was to make sure the software was kept up to date (rather than make significant changes).

*Bitcoin after my involvement*

18. Following initial release of the software, other developers were also involved in the further development of Bitcoin. Some of these developers did not necessarily agree with my vision for Bitcoin (I refer to all the present developers, who are Defendants, as "**Developers**"). Among other things, some people saw potential value in Bitcoin's use for criminal activity and in particular the so-called "Dark Web" (which was not my original intention). Some of these developers are Defendants to this claim. I return to this point below.

19. In December 2015, two online magazines, Wired and Gizmodo, published articles naming me as the creator of Bitcoin. In May 2016, while I denied much of what had been written about me, I did confirm that the part of the stories about me being Satoshi were true.

20. Around this time, Mr Andresen also confirmed publicly that I was Satoshi; however, as a consequence of having done so, he was marginalised and locked out of the Bitcoin.org website, which was the website used for the development of Bitcoin, by the other developers (see further at paragraph [84] below). From that stage, neither Mr Andresen nor I could realistically contribute to the development of Bitcoin and a vicious campaign began against me to discredit me as being Satoshi Nakamoto.

21. I believe that many of the developers reacted in this way because they saw potential for the use of Bitcoin to enable criminal activity, including the use of the "Dark Web" in particular (a subset of the internet which is intentionally hidden and can only be accessed using special software, and is used by drug dealers and child pornographers among others).

22. When I wrote the White Paper, it did not contain any reference to the legal obligations incumbent on developers but that does not mean that there are none. It was outside the scope of the White Paper, which was only ever intended by me to be an outline of how Bitcoin worked.

23. For example, when I launched Bitcoin, I was working on the implementation of "alert" and "recovery" systems, which I hoped would allow for, among other things, the recognition of freezing orders. I had already referred in section 8 of the White Paper to a potential strategy whereby nodes identify "alerted" transactions . In 2010, I implemented the alert key, although I still had not fully determined how it would best work. However, there were problems with it principally because it did not link into individual nodes (at the time, unlike now, nodes were very small). Despite this, I am confident that this functionality could have been developed fully and implemented over time. Instead, it was disabled by the then-developers, and no further action has

been taken in respect of it or similar functionality introduced. I believe those developers took that position because such functionality does not fit with their "decentralised" view of Bitcoin (which is not decentralised at all). It also furthered their goal of Bitcoin sitting outside the law and governmental regulation, which is not what I wanted.

24. Only BSV is Bitcoin, as only it uses the original protocol. For the avoidance of doubt, BTC is not Bitcoin. It follows therefore that I support the First Defendant's stewardship of BSV, but there is no difference between my claim against the First Defendant, on the one hand, and the other 15 Defendants on the other hand. It is also only BSV which is effective for use as digital cash (rather than a store of value – sometimes referred to as "digital gold" – which BTC has become).

25. There are many people who have publicly stated that I am not Satoshi Nakamoto and did not create Bitcoin. Many of those same people have falsely accused me of being a "fraud" and of academic plagiarism, a matter I address in section E of this witness statement. Many of those people also aggressively attack me on Twitter and other social media forums, as I have already explained.

*The myth of decentralisation*

26. I do not accept that BTC is "decentralised" in any sense of the word.[4] In theory, the software code used on the network could be developed by anyone, but effecting changes to the software on an ongoing basis requires some form of structure (e.g. to ensure there are no software bugs, make necessary upgrades to the software and ensure a consistent approach for the direction of the network). This is why the operation of the Bitcoin blockchain (and the blockchain of other networks, i.e. BTC) is not decentralised. The developers control the software and therefore the network. This is not what the developers want the public to believe. Many developers also appear to work on the basis that "decentralisation" means being above the law or resistant to

[4] It is also wrong to say that Bitcoin has no "Issuer" since all the 21 million Bitcoin were issued by me (as Satoshi Nakamoto) when I created Bitcoin.

censorship. In particular, those developers refuse to acknowledge that they act effectively as a partnership (as I explain, next) and, because they are located in various countries around the world, they appear to think that they and BTC are above the law. This is not the case.

27. As I mentioned, it is my belief that the BTC developers (and the BTC Developers in this case) are essentially a partnership. They work in concert with one another to maintain the software and network, they have a common purpose and earn income from undertaking that common purpose. I would expect them to support each other and have a common position in most respects. I am also aware that these BTC developers deliberately keep aspects of their operation secret so as to further the myth of "decentralisation". The BTC website refers to various chat forums for "Development" (as referred to by Mr Cain), but I understand that much important business between the BTC Developers is discussed in a private chat forum called "Dragons Den", which is not publicly accessible.

28. It is well known that the Developers work together on BTC development with, and are funded by, organisations such as Blockstream Inc (which was founded by Gregory Maxwell and Peter Wuille, among others) and Chaincode Labs.[5] Some of the BTC Developers work full time on BTC and earn income by way of so-called "grants" or "sponsorship" from interested parties. I agree with Mr Cain's summary of the BTC Developers' involvement with BTC[6] and, for the reasons he states and the reasons above, I believe that each of the BTC Developers has considerable influence over the development of BTC and the BTC network.

29. Mr Ver's lawyers suggest that I am bringing this proceeding to intimidate developers and many of the developers say the same thing on Twitter. That is absolute nonsense. I am no more capable of intimidating developers than they are of me. Mr Cain rightly notes that Mr Ver is a multi-millionaire. I cannot speak to the circumstances of all the

[5] For example, I refer to the articles such as Lopp, J *Who Controls Bitcoin Core?* Article on blogg.lopp.net **[CSW1/4]** and van Id, J *Has Blockstream hijacked Bitcoin?* Article on www.medium.com **[CSW1/16]**.

[6] Cain 1, [54]-[57].

other developers, but I know that many of them have been involved in BTC for several years and I expect would have substantial resources with which to defend this claim.

30. Moreover, I believe funding will almost certainly exist for the Developers. By way of example, an organisation called the "Open Crypto Alliance" has been formed with the expressed purpose of fighting "patent pick pockets" and "patent trolls" (in other words parties who did not actually create the inventions they seek to patent). However, as far as I can tell, their main purpose is to fight nChain's patent applications (they do little to hide their true purpose, as I am the main feature of their website).[7] Furthermore, recently, a "complimentary" [sic] organisation[8] (in the words of the Open Crypto Alliance), the Crypto Open Patent Alliance, brought an action in the English Court against me to prevent me from claiming copyright in the Bitcoin Whitepaper which I authored (and has nothing to do with Patents). I expect this organisation would also fund any claim against me or defend a claim brought by me that relates to digital assets, Bitcoin, BTC or the Blockchain.

31. In this context, I simply do not believe that any of the Defendants would be "intimidated" by the prospect of litigation (regardless of whether that is my purpose – which it is not).

**Section B: TTL's digital assets**

*Introduction*

32. I was the victim of hacking on my home computer network, which occurred on or around 5 February 2020. I describe the hack in more detail in paragraphs [52] to [58] below. The hackers have not been identified.

33. Among the information taken during the hack are the private keys necessary to access approximately 111,000 unsplit Bitcoin recorded at two different addresses,

[7] Open Crypto Alliance website (*www.opencryptoalliance.org*) – Homepage (extract) **[CSW1/24]**.

[8] Open Crypto Alliance website (*www.opencryptoalliance.org*) - FAQs **[CSW1/25]**.

1FeexV6bAHb8ybZjqQMjJrcCrHGW9sb6uF (and the BCH equivalent of this address, 1FeexV6bAHb8ybZjqQMjJrcCrHGW9sb6uf, both together referred to as "**1Feex**") and 12ib7dApVFvg82TXKycWBNpN8kFyiAN1dr ("**12ib7**") (together, "**Addresses**"). The digital assets in the 1Feex and 12ib7 Addresses are owned by TTL. At the time of the hack the digital assets in these addresses were worth approximately £900m.

*TTL*

34. TTL is a limited liability company incorporated under the laws of the Republic of Seychelles. It is a holding company for the Bitcoin in the Addresses, which were purchased during the initial phase of Bitcoin (i.e. prior the airdrops). I also have significant other holdings in Bitcoin/digital assets (beneficially in most cases), well in excess off the amounts at issue in this claim, but those other holdings are not owned by TTL.

35. The ultimate beneficial owners of TTL are my wife, me and our children (two of whom live in England and one in Australia). The relevant trusts to which the shares in TTL are subject are governed by English law.

36. Because TTL is a holding company, it has no customers or bank account. It does not file accounts or tax returns. Its main asset is the Bitcoin in the Addresses, which I could control using the keys located on my computer at my home in Surrey (as I explain below). I therefore control the affairs of TTL in England.

*TTL's ownership of the digital assets in the Addresses*

37. The digital asset holdings in the Addresses pre-date the so-called "forks" that led to copies being made of the original Blockchain. It is a common misconception that "forks" in the Blockchain gave rise to the various copies.[9] "Forks" happen naturally

[9] For all Blockchains except for the original Blockchain (i.e. for what is now BSV), the Blockchain was created by copying the pre-existing Blockchain, but applying different software instructions thereafter (and, accordingly, save for BSV, references (if any) in this witness statement to "Bitcoin" should be read as a reference to "so-called Bitcoin" as the developers had no permission to copy the original Blockchain).

whereas what occurred to create BTC, BCH and BCH ABC was the result of deliberate changes by developers to the software used to support the network. A more accurate term is "airdrop" because copies of the existing Blockchain are copied and used with new software. The effect of this means that the holdings can be spent independently on each and all of the BTC, BCH, BCH ABC and BSV blockchains.

38. By around the date of this statement, the value of the digital assets in the two Addresses had increased to approximately £4.5 billion. The holdings are broken down as follows:[10]

| Holding | Value in BTC[11] | Value in BCH[12] | Value in BCH ABC[13] | Value in BSV[14] | Aggregate Total |
|---|---|---|---|---|---|
| 1Feex: 79,957 of each ("**1Feex**") | £3.16bn | £53.8m | £1.9m | £17.3m | £3.23bn |
| 12ib7: 31,000 of each ("**12ib7**") | £1.22bn | £20.9m | <£1m | £6.7m | £1.75bn |
| **Total** | **£4.38bn** | **£74.6m** | **£2.6m** | **£24m** | **£4.49bn** |

39. The 1Feex was originally purchased in February 2011. The purchase was funded by Liberty Reserve Dollars (a form of digital currency used at the time, which I had received for my work for online casinos), through an online Russian exchange, WMIRK. I approached the exchange and asked them how much Bitcoin I could buy

[10] Figures are rounded.

[11] Calculated using BTC:USD on 20 April 2020 - $55,225.37 and USD:GBP – 0.7155.

[12] Calculated using BCH:USD on 20 April 2020 - $940.47 and USD:GBP – 0.7155.

[13] Calculated using BCHA:USD on 20 April 2020 - $32.98 and USD:GBP – 0.7155.

[14] Calculated using BSV:USD on 20 April 2020 - $302.41 and USD:GBP – 0.7155.

with my Liberty Reserve Dollars (which I had been accumulating since 2005 and the exact amount of which I cannot recall), which is how the quantity was arrived at. I do not know from whom the exchange purchased the Bitcoin or what its procedures were for doing so. However, the Bitcoin was delivered on 1 March 2011, as the Blockchain record shows.[15] The purchase of the Bitcoin is evidenced by a contemporaneous purchase order (the "**Purchase Order**"), that was prepared by my then wife, Lynn (Wright).[16]

40. One of the reasons for my decision to buy the Bitcoin that was transferred to 1Feex and 12ib7 was because I had significant holdings of Liberty Reserve Dollars (as I have described above), which could only be spent in a limited number of places. Whilst Liberty Reserve Dollars may theoretically have been pegged to the US$, they were only as valuable as what they can be exchanged for.

41. As far as I recall, I instructed the exchange (WMIRK) by telephone to buy the Bitcoin using my Liberty Reserve Dollars, but, having done so, I left the rest of the transaction to Lynn.

42. As I have explained, the Bitcoin that was transferred to the Addresses was purchased and held on trust. It now belongs to TTL subject to the terms of a trust known as the Tulip Trust.

43. I am aware that there have been rumours and speculation that TTL does not own the 1Feex Address and some individuals have even asserted that they own the 1Feex Address.

---

[15] At **[CSW1/27]** is an extract of the Blockchain for the 1Feex Address. It shows all transactions in and out of the Addresses other than the "dust" payments I have referred to above. The payment into the 1Feex Address on 1 March 2011 is at **[CSW1/38-39]**.

[16] Exhibit **[OJC1/2/175]** to Cain 1.

44. In that regard:

a. It is alleged that the 1Feex coins were stolen in 2011 from a Japanese digital asset exchange called Mt Gox and even that I was responsible for such theft. This is not true. As I have explained, the 1Feex coins were purchased from a third party in exchange for Liberty Reserve dollars in late February 2011, and transferred into the 1Feex Address on 1 March 2011.[17] The well-publicised hack of Mt Gox took place later in June 2011. I had nothing to do with the hack or any other alleged earlier hacks. Mt Gox has been in liquidation since 2014 and neither the liquidator nor the Japanese police have contacted me regarding the coins in the 1Feex address despite the fact that TTL's ownership of the 1Feex Address has been public knowledge since 2018. I also made a public statement on this matter on 16 June 2020 where I referred to all the above matters.[18]

b. On 4 November 2020, I became aware that an individual from the USA by the name of Chadwick Austin wrote to U.S. District Judge Bloom (who is hearing the Florida Proceedings) to assert that he was the rightful owner of the 1Feex address. However, he has not pursued his claim and my solicitors have responded to it in detail.

c. Furthermore, as Mr Cain has described, my solicitors receive emails from time to time asserting claims to ownership by third parties but none appear credible (some seem nonsensical) and none have provided any evidence. I have nothing to add to Mr Cain's evidence in that respect.

45. I do not recall the reasons for the transactions in and out of the 12ib7 address or who the transactions were with.

---

[17] See footnote 15, above.

[18] Craig Wright Statement on the missing Mt. Gox Bitcoin (*https://coingeek.com/craig-wright-statement-on-the-missing-mt-gox-bitcoins/)* [**CWS1/40**].

46. The Addresses also contain other digital assets which have been gifted to TTL by various users over the years. These payments are referred to as "dust" payments, whereby small amounts of Bitcoin or other digital assets are transferred to an address. This is commonplace and is to be expected. Dust payments frequently are made to addresses, often because the paying party wants to track activity on the address and/or link that address to other addresses. Dust payments often are used as a preliminary step in seeking to perpetrate a phishing attack or even in order to ascertain whether the paying party can find information that will allow the paying party to blackmail the owner of the address in question.

*The private keys to TTL's digital assets were stored on my personal computer*

47. The private keys required to control and spend the Bitcoin and other digital assets in the Addresses were contained in encrypted wallet.dat files contained in a password protected RAR file stored on my computer at my home in Surrey. The password to the protected RAR file was contained in a digital password safe known as KeePass. The RAR file and KeePass were also stored in and synced with two cloud storage services, OneDrive and Google Cloud. I had not turned my mind to the fact that hackers might delete both copies effectively due to the syncing process (and, in any event, although the assets were worth around £1bn at the time of the hack, that was (and is) only a portion of my overall holding in digital assets). Furthermore and in any event, the private keys are just that: private keys. The loss of private keys does not mean that ownership is lost. The ownership of the digital assets remains with the owner even if the private keys are stolen and I believe that control over that property can be restored in the way that I am asking the court to do in this case.

48. I had not accessed the wallet.dat files for the Addresses for many years prior to the hack, and in consequence I cannot now be certain about the precise mechanism for opening the files. The assets in the Address are an investment (one of many investments held beneficially for myself and my family). I had no cause to access the files and had not done so (as I have said) for many years, but I could have done so if I had wanted to.

49. I do recall that there was an additional security measure in place to protect access to the wallet.dat files in that I had set up a scheme of algorithmic masking (a complex method of hiding original data with modified content generated by an algorithm) which protected the mechanism for opening the files. I stored notes in KeePass which were sufficient to remind me of the scheme of algorithmic masking used and the data that I needed to collect in order to pass through those schemes.

50. As and when I would have wanted to exercise control over the digital assets in the Addresses on behalf of TTL (for example by spending them), I would have done this on my computer at home in Surrey using the private keys and other information held on that computer.

**Section C: The hack of my computer and my loss of control over TTL's digital assets**

*The hack of my computer system*

51. At approximately 12.30pm on Saturday 8 February 2020, I accessed an Electrum Bitcoin Wallet (the "**Electrum Wallet**") of mine, which contained Bitcoin belonging to my wife and me, which was different to and separate from the digital assets in the 1Feex and 12ib7 Addresses. I did this to check that I had received a regular monthly payment in digital assets. Upon doing this, I observed that the expected payment had been received but I also noticed three further transactions, two of them substantial, which neither I nor my wife had actioned, in which all of the digital assets in the Electrum Wallet had been transferred out at 7:46 AM on 5 February 2020. [**CSW1/42**]

52. I knew at this point that my computer systems had been hacked – there was no other explanation as to why the Bitcoin in the Electrum Wallet could have been transferred. I was therefore very concerned by this and so I immediately investigated what had happened, what had been taken and what had not been taken.

53. I was unable to locate a record as to which files had been accessed and/or wiped during the hack as the system logs had been erased.

54. The transfers can only have been made using the seed phrase to the Electrum Wallet which was stored in Keepass. Other than the loss of the BSV in the Electrum Wallet, which had a value of approximately £1.1m at the time of the theft, I discovered that the following had been taken:

a. The RAR file containing the wallet.dat files for the 1Feex and 12ib7 Addresses and the KeePass data.

b. 0.333 BTC, with a value at the time of approximately £2,500, which was held on the FloatSV digital asset exchange. The BTC in this account was jointly held by my wife and me. A screen-print from the "Withdrawal History" of my account with the FloatSV exchange at **[CSW1/43]** shows the transfer of the BTC out of the wallet at 7.14 PM on 5 February 2020.

c. A large number of white papers (my best estimate is approximately 50) and associated research data related to my work in preparing valuable patent applications contained in 37GB of files that were wiped from my OneDrive and Google Cloud drives.

55. My documents were stored in OneDrive as well as the Google Cloud, but unfortunately as both OneDrive and the Google Cloud were synced with my computer, the data was lost in each location when it was deleted from one location.

56. The BSV stolen from my Electrum Wallet and the BTC stolen from the FloatSV exchange have been dissipated.

57. Following my discovery of the hack, I wiped the hard drives of my computers. This may appear odd to some people, but I did so because I did not know how the hackers obtained access to my computer. I have been the subject of cyber-attacks for many years. It was also critical to me to get my systems up and running without undue delay. My computer contained a great deal of confidential information (among other things). I wiped my hard drive to in order to ensure all malware and other threats were

removed from my network and it was simply not practicable to take a copy of any of these drives.

58. I believe that it is highly likely that the hackers retained copies of the large volume of data that they deleted from my systems during the hack rather than simply deleting the files. This is because (i) data taken during the hack was used to steal the digital assets in the Electrum Wallet and my FloatSV account, which indicates the intention was theft as well as destruction of data, and (ii) I believe that the hackers are highly likely to have known that my data included valuable information such that it would be unlikely that they would delete it without retaining a copy.

*TTL's and my loss of control over the digital assets*

59. The result of the deletion of my files is that TTL and I have lost the ability to control the digital assets in the Addresses. No-one else had access to the private keys and related data held on my personal computer. The theft meant that I have been deprived of the files containing the private keys and the information stored in KeePass which I needed in order to remind me of the scheme of algorithmic masking used and the data that I needed to collect in order to pass through those schemes and thereby be able to control the digital assets on behalf of TTL.

60. The digital assets in the Addresses have not been moved as at the date of this statement, as can be seen from the Blockchain records for 1Feex at **[CSW1/27]** and for 12ib7 at **[CSW1/44]**.[19] I believe that this must be for one or more of three reasons. First, because the hackers have not yet been able to access the private keys contained within the wallet.dat files because of the algorithmic masking in place. Secondly, it is not obvious from the description of the data contained in the KeePass application that it relates to the Addresses, so the hackers may not have realised what they have got, or which data relates to those addresses. Thirdly, it may be that the hackers have cracked the algorithmic masking but are waiting for attention to move away from me

[19] As explained above (footnote 15), these extracts show all transactions in and out of the Addresses other than the "dust" payments I have referred to above.

so that they can move the 1Feex and 12ib7 coins without arousing suspicion. It is now known publicly that TTL cannot access the digital assets in the Addresses and so the hackers may well feel confident in biding their time. Letters sent by my solicitors to certain Defendants, which referred to the hack and loss of control over the digital assets in the Addresses, were published on Twitter in June 2020.[20] I expect that, from that time, the hackers would have understood the underlying value of the data they had stolen.

61. In order to be able to transfer the digital assets out of the Addresses, the hackers would need to use specialised powerful computers to defeat the algorithmic masking in place. I estimated at the time of the hack that it would take between one and six months to defeat the masking, mainly depending upon the degree of sophistication of the computer systems available to the hackers. However, as the hackers may not yet have realised what the files contain or they have been trying to crack other files first, it is impossible to predict when they might be able to gain access to the wallet.dat files relating to the Addresses. As explained above, it may be that they already have the necessary access but are waiting to make the transfer.

*Police investigation and possible method of hacking*

62. I reported the hack to the Surrey Police as soon as I discovered the hack. I was provided with a crime reference number of 45200015992 by email ([**CSW1/67**]). Subsequently, on 8 April 2020, I was contacted by Ms Aisling Martin of the Cyber Crime Team of the South East Regional Organised Crime Unit, who informed me that they were responsible for investigating the crime.

63. The Police investigation is ongoing and, to date, the hackers' identity remains unknown. I am assisting the Police with their investigation.

[20] Arthur van Pelt Twitter at **[CSW1/65]** (Mr van Pelt is a pro-BTC commentator who makes regular posts opposed to me. He was not an addressee of the letter.).

64. Although I cannot be sure how the hacking occurred, I suspect that it was through (in combination, among other things) a wireless router which I found located in a discreet location in my home, and which does not belong to my family or me. I believe that it must have been planted there by the hackers, either when tradesmen were in our home or by breaking in. This is being considered by the Police and me in the context of the ongoing investigation.

**Section D: Developers can and should take the steps requested by TTL**

65. I have been asked to explain why it is possible for the Developers to take the steps requested by TTL.

66. Those who say it cannot be done say that Bitcoin and the other digital assets involved in these proceedings are "encrypted" in order to give the impression that they would not be able to restore the control over digital assets in this way. That is totally wrong. Whilst digital algorithms are used in order to generate public and private keys and enable the use of digital signatures to sign-off transactions, and users may use encryption as a method of securely storing their private keys, the Blockchain is not encrypted - nor are records of transactions in Bitcoin stored on the Blockchain. It is therefore wrong to describe Bitcoin, or any of the other networks, as encrypted, or as a cryptocurrency.

67. Therefore, it is wrong to say that Bitcoin or other digital assets can only be transferred using the private key to the digital assets which are the subject of this case. There is nothing to stop the developers from including a patch to the computer code which operates the network to enable control of the asset to be returned to the rightful owner. This could be as simple as creating a new address and transferring the Bitcoin or digital assets to that address.

68. It is not technically difficult to code such a patch. In fact, it is very easy. By way of comparison, I note that nChain is presently working on much more complex technology (by way of modification to the existing "Client software", i.e. the software used to support each network). This new software would enable an individual with a

court order confirming their ownership of digital assets to regain control of their digital assets. However, the new software is still under development and, when completed, would require a significant modification to the existing Client software. In contrast, the creation of a new address and transfer of the Bitcoin or digital assets to that address, as suggested in paragraph [67], requires very little effort by Developers.

**Section E: Full and Frank disclosure**

*Context*

69. In this section I set out factual matters that I understand may be relevant to my duty of full and disclosure, along with the matters set out by Mr Cain.

70. At the outset, I repeat that I am a controversial figure in the Bitcoin community. I promote BSV, because it is the only true Bitcoin. I also strongly oppose the way in which the BTC community (in particular) have taken certain concepts from the White Paper and manipulated their meaning. As I have set out above, they claim that BTC is "decentralised" in order to hide the true administrative structure behind BTC. Many (albeit I accept not all) of these people want to use BTC for illegitimate purposes and others are simply anarcho-capitalists who are seeking to avoid the rule of law and are against the role fulfilled by Government. Those people hate me with a passion and have an aggressive campaign against me labelling me a "liar" and a "fraud". They have trawled through my past to find as many examples as possible of perceived failures or inaccuracies on my part (or the part of my agents), and publicly shame me as a "faketoshi". From time to time, I have commenced defamation proceedings in relation to such allegations, which have not resulted in any findings that I am or am not Satoshi.

71. I admit that I sometimes use strong language and that I did, in an angry moment, suggest that I would bankrupt the developers through litigation. I suffer from Autism Spectrum disorder (also known as Asperger's Syndrome) as Mr Cain explains in his witness statement, which means that I sometimes communicate in a more aggressive manner than other people, especially in response to the developers whose positions I

strongly disagree with, and which are often intended to attack me. I still have very strong views about the Developers, especially the BTC Developers, for the reasons I have described, but my motivation in bringing the proceedings is not to attack the Developers personally. As I have already explained, even if I wanted to do that, I could not hope to succeed as they are part of a well-funded network. I regret making that statement as it has provided the Developers with another narrative to oppose me.

72. My detractors give as good as they get. There are numerous articles and internet posts every day about me being a "fraud" and a "liar" and these articles tend to reference one another and build upon the ever-growing assertion that I am fraudulently claiming to be Satoshi Nakamoto.

73. I have never forged documents. I have been asked to address various points alleged by the Australian Tax Office ("**ATO**") during their audits of certain Australian companies. I have done my best to respond to specific allegations made by the ATO (using their Reasons for Decision in respect of Denariuz Pte Ltd ("**Denariuz**") ("**Reasons Document**") as an example of their various allegations).[21] My responses are at paragraph [88] and following, below.

*Purchase Order*

74. There are certain discrepancies in the Purchase Order, which are referred to by Mr Cain. I do not specifically recall the creation of the Purchase Order. I believe that it was created by my former wife, Lynn, who administered our accounts at the time. I believe that because I found it in our accounting records, for which she was responsible. She is also shown as the author on the metadata. For the avoidance of doubt, I did not create this document.

75. I do not know for sure why the market price for Bitcoin is not the same as on the Purchase Order. I have already explained (paragraph [40] above) that the Bitcoin was purchased with Liberty Reserve Dollars, not US Dollars, and the value of Liberty

[21] Exhibit **[OJC1/3/485]** to Cain 1.

Reserve Dollars was substantially less than the equivalent amount in US Dollars. I believe that was likely to be the case, among other reasons because of the relatively low volume of Liberty Reserve Dollars that was traded at the time, since few people accepted the currency and because it was particularly difficult to spend large amounts of the currency. I believe that this was why the actual purchase price per Bitcoin in Liberty Reserve Dollars was substantially different from the US Dollar value listed in price indices at that time. Furthermore, prices at the time were volatile (and therefore not necessarily accurate at any particular time) and/or the figures might have been erroneous. I also doubt that the WMIRK exchange would require a Purchase Order in that particular form to effect a transaction like this. The document may have been sent separately by Lynn to the exchange, or indeed it may not have been sent at all (i.e. it might be a record of an order placed over the telephone).

*Accounting Records*

76. I have read Mr Cain's witness statement in relation to apparent inconsistencies in the accounting records relating to the Addresses. However, I see no inconsistency in the accounting records - the Craig Wright R&D Trust became the Tulip Trust and both TTL and Wright International Investments Ltd are companies whose shares are held within the Tulip Trust. The Bitcoin in the Addresses is now held by TTL as I have described above, and subject to the same trust, albeit my family members are now also beneficiaries.

*Lack of email records*

77. I have been asked why I do not have email records relating to the purchase of the Addresses. I cannot say for sure that email records ever existed for the purchase. If they did, I doubt they would have been retained as important documents (since 2011) among other reasons because: a) TTL has accounting records; and b) I had the private keys on my computer and backed up on two cloud-based servers. Furthermore, since 2011, I have moved several times, including from Australia to England, and have lost considerable amounts of electronic data in that time. I have also lost control of

electronic data belonging to various Australian companies from time to time. For example, Hotwire Pre-emptive Intelligence Pty Ltd was temporarily in receivership during 2013 and we were locked out of its premises. Although I regained control of the company, we lost access to its computer systems. Furthermore, I ceased to be a director of the various companies in 2015 and, eventually, many of those companies were put into administration or have otherwise been wound up (meaning I do not now have access to a full set of their electronic data).

*Statutory Declaration(s)*

78. I am aware of allegations concerning forgery of a Statutory Declaration, one of which was used as an exhibit by Dave's estate in the Florida Proceedings. I recall that I obtained a Statutory Declaration from my solicitor to prove ownership of Bitcoin in my control but I do not recall for what specific purpose (i.e. to whom it was intended to be provided). I would not have forged any of these documents.

79. The ATO alleged that, if the relevant addresses could be controlled by me from my mobile phone or my computer's wallet software, the private keys would have been required to input the addresses into the wallet software, so that the Statutory Declaration could not have been made at all. I presume the ATO meant to say that I could not have demonstrated control to Mr D'Emilio of all five Addresses at one time. I agree that private keys would be required to control (i.e. transfer) Bitcoin in the Addresses. This appears to be a pedantic point about the wording of the Statutory Declaration (i.e. whether I showed Mr D'Emilio each address separately or all at once). As I have said, I recall obtaining a Statutory Declaration to prove control of Bitcoin Addresses, but I cannot recall its precise purpose. However, I do recall showing Mr D'Emilio that I could control the Bitcoin in each address by entering the private keys one by one. I know this because I was careful to delete the private keys, as the keys were company property and I did not have authority to retain them on my phone. I also recall that the Statutory Declaration was made in 2013. By 2014, the digital assets in the Addresses and many other addresses were held outside Australia. It would not have been sensible or appropriate for me to demonstrate control over

those addresses at that time from within Australia, as doing so might have had tax consequences and I did not have permission to do that.

*Alleged fraudulent documents disclosed in the Florida Proceedings (and similar allegations)*

80. In the Florida Proceedings, as required under United States Federal Civil Procedure, I have produced over 226,000 documents. I understand that the Plaintiffs have challenged less than 1% of the documents produced. Many of the documents challenged come from electronic sources such as company servers to which others had access, many came from third parties and many came from electronic devices in the exclusive possession of the ATO since December 2015. I am unaware of how the ATO imaged or processed the materials on its electronic devices.

81. I address the ATO's allegations separately (paragraph [88] and below).

82. It is also alleged by Mr Ver's lawyers that I used hacking as a convenient excuse in that case to explain an apparently forged document. As I have explained, I have never forged documents and therefore, in the Florida Proceedings (referred to by Mr Ver's lawyers), I was speculating as to how the document was on my computer system. I am regularly subject to hacking attempts and I stand by the possibility that a forged document may have been put on my computer by a hacker or through other unauthorised access.

83. In this case, I am not alleging that any documents were put on my computer. Quite the opposite - they were stolen and/or deleted.

84. I also note the irony that I am being accused of "inventing" a hack. That is precisely what the then-BTC developers (including the Second, Fourth, Eleventh and Twelfth Defendants) did when they removed Gavin Andresen's site access right after he acknowledged me as Satoshi.[22]

[22] This is well documented. See for example the following articles: (1) Cush, A *Gavin Andresen: I Was Not Hacked, and I Believe Craig Wright Is Satoshi* (article on *www.gizmodo.com)* **[CSW1/70]**; (2) Das, A *Bitcoin*

85. Finally, as part of the Florida Proceedings, I was ordered to produce a list of Bitcoin addresses under my control. I did not personally collate this list. The list identified 16,405 mined Bitcoin addresses and disclosed them to the Court. Furthermore, the purpose of the list was not to assert ownership over all of those addresses. It was to comply with the Florida Court Order requiring disclosure.

86. For the purposes of the Florida Proceedings, Dave's estate has assumed I am Satoshi. The claim by his estate seeks an interest in other Bitcoin that I own, which (as I have described) is significant.

87. I say no more about the Florida Proceedings other than that I deny the allegations made by Dave's estate.

*ATO allegations*

88. I have been asked to respond to specific allegations made by the ATO in relation to companies associated with me in the period 2009-2015.

89. I do not have a strong recollection of the various tax audits, other than the few points I make below. I resigned as a director of the various companies in 2015 because I believed that the ATO had a vendetta against me and that was affecting the way that it was handling the audits. I tried to have as little to do with them as possible.

90. Initially, relations between the ATO and me were not so bad and I had been interested in openly discussing with them the taxation treatment of digital assets and electronic cash. In that context, in 2013 I had provided the ATO with a list of the various Bitcoin addresses under my control. It would have made no sense for me to have done that, if I did not control those addresses. That is because ownership of the addresses would have given rise to a significant capital gains tax liability upon realisation of any digital assets held in the addresses.

---

*Core Dev Gavin Andreson's GitHub Commit Access Removed* (article on *www.ccn.com)* **[CSW1/72]**; and (3) O'Connell, J *Andresen's Commit Access Hangs in Balance Following Wright Exit* (article on *www.bitcoinist.com)* **[CSW1/75]**.

91. I recall attending interviews with the ATO, but most of the documentary material was provided by company staff, internal and external accountants and the companies' lawyers. I was surprised to see various allegations referring to "Dr Wright" in the ATO Reasons Document for the simple reason that I had very little to do with the provision of documents to the ATO.

92. I was extremely surprised to see that Denariuz had apparently claimed a capital loss in relation to the value of an equitable interest in Bitcoin. My clear recollection is that the audits related to tax credits for Research & Development ("**R&D**") and had nothing to do with Bitcoin value. On further investigation, the accounts for Denariuz actually record a foreign currency loss.[23] It is not clear to me why the Reasons Document refers to a claim for capital losses for an equitable interest in Bitcoin. The analysis on this point on pages 56-57 of the Reasons Document do not refer to any taxpayer submissions.

93. I am clear about this particular point because the value of Bitcoin increased between July 2013 and June 2014 and it does not make sense to have claimed a capital loss.

94. The ATO alleged that I could have used the "message sign" function to show control of the Addresses. I chose not to do so (or to procure anyone else to do so) for tax reasons because, by the time that request was made to me, the assets in the Address (and other addresses) were outside Australia.

95. I was not responsible for the taxpayers' decisions not to challenge the ATO decisions because I was not a director by that time. In any event, the taxpayers were, in part as a result of the decisions, put into administration by the ATO. I understand that the ATO was keen to find grounds to take a derivative action against me for fraudulent conduct but had no grounds to, and did not, do so.

---

[23] Denariuz Pty Ltd Corporation Tax Return (year 2014) [**CSW1/78**] and Denariuz Pty Ltd – Profit & Loss (1 July 2013 to 30 June 2014) [**CSW1/91**]. The letter referred to in the ATO Reasons Document at paragraph [35] (footnote 25) also refers to the claim for foreign currency losses: Letter dated 1 April 2015 from Alan Ellis to ATO [**CSW1/121**].

96. Testament to the ATO's aggressive approach is the fact that they pressured AusIndustry (the Government entity with responsibility for administering the Industry Research and Development Act 1986 ("**IRDA**")) into retrospectively revoking the taxpayers' registration under IRDA, which would ordinarily give rise to an R&D credit for tax purposes. In other words, the ATO's conclusion in paragraph [6] of the Denariuz Reasons Document (i.e. that Denariuz was not registered under IRDA) is only true because the ATO requested AusIndustry to *de-certify* Denariuz's prior registration (as referred to in paragraphs [47] and [48] of the Reasons Document).

*Academic plagiarism*

97. I have been accused of plagiarising material, including for the purposes of my LLM dissertation and PhD thesis (at Northumbria and Charles Sturt universities respectively).[24] I believe that these accusations were generated primarily by an anonymous blogger using the pseudonym "Paintedfrog". The ideas and research in my degrees are my own and both universities investigated the allegations fully (Charles Sturt actually removed access to my thesis during its investigation) and then confirmed that they were not taking any further action.

98. I did not plagiarise other people's work when preparing these texts. Broadly speaking my response to the allegations are (among other things) (i) a number of the alleged examples of plagiarism concern common terms or common words, for which I say it is not necessary to credit other authors; (ii) a number of the alleged examples of plagiarism concern graphs and diagrams, which I say are commonly used and therefore that it is not necessary to credit other authors; (iii) in some cases I was asked by the academic institution to reduce the size of my thesis and that led to me omitting footnotes and references to other authors; and (iv) I was not trying to claim credit for basic and/or foundational concepts.

[24] *Craig Wright's LLM Dissertation is Full of Plagiarism* (article by "Painted Frog" on www.medium.com) [**CSW1/122**].

*Nodes would not cause a fork*

99. Mr Cain has described the so-called DAO hack,[25] which led to a fork in the Ethereum network.

100. Firstly, to be clear, nodes/miners do not control the network and there is no consensus mechanism in relation to the protocols that govern the various Blockchains (the "consensus mechanism" which is present relates to the selection of transactions). The developers set the rules and the miners have to comply with those rules – the miners are not involved in the creation of those rules. In other words, they normally follow the instructions of developers.

101. Accordingly, a fork is highly unlikely in relation to the networks at issue in the Claim. Nodes need to run the Client software, which needs to be regularly updated. The only way I foresee a fork occurring is if the group of developers split into effectively "compliant" and "non-compliant" groups (i.e. a group of developers runs software that does not contain the updated address details to give effect to any Court Order). While this is possible, I consider it unlikely, especially considering many Developers are located in countries such as the United States, New Zealand and Australia, which could be expected to follow similar principles as English law and/or in which recognition of an English Judgment may be possible.

*Summary*

102. As I have described: a) TTL is the owner of the Bitcoin and other digital assets in the Addresses; b) TTL lost control of that Bitcoin and other digital assets when the private keys were stolen during a hack of my computer in my home in Surrey; and c) prior to the hack, I controlled (or would have controlled) the Bitcoin in those Addresses from my home.

[25] Cain 1, [207].

**Statement of truth**

I believe that 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 .....

**DR. CRAIG STEVEN WRIGHT**

Date 29 APR 21