



**IN THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
MEDIA AND COMMUNICATIONS LIST
BETWEEN:**

CRAIG WRIGHT

Claimant

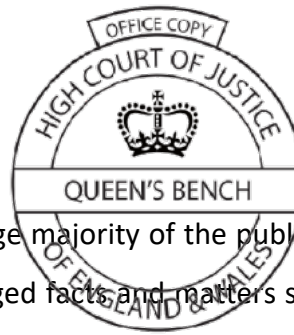
-and-

MAGNUS GRANATH

Defendant

REPLY

1. Save as specifically admitted below the Claimant joins issue with the Defendant on his Defence.
2. References in this Reply to paragraph numbers are to the Defence unless otherwise stated.
3. Paragraph 2 is denied.
4. As to the first sentence of paragraph 8(2): it is admitted that the Claimant, and others on his behalf have since 2016 (not 2015) made repeated public statements that the Claimant is Satoshi Nakamoto. As to the second and third sentences the Claimant's case is as set out below at 7.2.1 to 7.2.12. It is denied that the exercises "publicly failed" and accordingly, if and to the extent that there was a "widely held and expressed view" in the Bitcoin and cryptocurrency community that the Claimant's continuing claim to be Satoshi Nakamoto was "knowingly false", any such view was not based on fact.



5. As to paragraph 8(3), it is denied that a very large majority of the publishers of the words complained of knew the facts or alleged facts, and matters set out in paragraphs 8(2).

Serious Harm

6. Paragraph 9 is denied. The Claimant's case on serious harm is further particularised in the Particulars of Claim.
7. As to the matters relied on by the Defendant in sub-paragraphs 9(1)(a) to (g), the Claimant pleads as follows:

- 7.1. The first sentence of paragraph 9(1)(a) is admitted. The second sentence is denied and paragraphs 7.2.1 to 7.2.12 below are repeated. The third and fourth sentences are not admitted and the Defendant is put to strict proof of the same.

- 7.2. The first sentence of paragraph 9(1)(b) is denied, because it is denied that the Claimant made a "failed promise" to prove he was Satoshi Nakamoto by moving early bitcoin in May 2016. The Claimant's case on the May 2016 events referred to therein is as follows:

The media exposure

- 7.2.1. In November and early December 2015, the Claimant was approached by journalists from various international media outlets (including Wired and Gizmodo) who suggested that they were in possession of documentary evidence linking the Claimant with Satoshi Nakamoto and requesting the Claimant's comment or input.

- 7.2.2. Those approaches came as a complete and unwelcome shock to the Claimant and caused him considerable upset as he was unaware that information linking him to Satoshi Nakamoto had or might have been provided to the media.



- 7.2.3. The Claimant had sought advice from individuals, such as Robert MacGregor (the founder of nTrust and CEO of the same until 2018 when it was acquired by the nChain group of companies), concerning the approach by the media and was concerned that the media might release this information. The Claimant trusted the advice of Mr MacGregor who said that the media would not go to press with the information that they had.
- 7.2.4. However, on or around 8 December 2015 articles were published in Wired and Gizmodo announcing that the Claimant was likely to be Satoshi Nakamoto. On or around 11 December 2015, those articles were amended to state that those publications no longer believed the Claimant was Satoshi Nakamoto.

The demonstrations

- 7.2.5. In or around March 2016, the Claimant was told that he would need to take part in some form of practical demonstration in order to show that he had the private keys widely associated with Satoshi Nakamoto. This was the first time that the Claimant was made aware that the extent of the reveal would extend to use of private keys, and not just the evidence of his academic and professional qualifications and early drafts of the Bitcoin Whitepaper. The Claimant was very unhappy about participating in such a 'reveal' but was subject to considerable pressure to participate.
- 7.2.6. The Claimant never wanted to participate in any such demonstration, nor was it his idea to do so. The Claimant never wished to be exposed as Satoshi Nakamoto. Instead he was reacting to a situation which was not of his making, namely the very widespread speculation as to whether he was Satoshi Nakamoto following the Wired and Gizmodo articles. However, the Claimant



did not understand how to face public exposure.

7.2.7. The Claimant therefore very reluctantly agreed to provide private demonstrations to Gavin Andresen (a leading figure in the bitcoin community with whom the Claimant had corresponded regularly as Satoshi Nakamoto), Jon Matonis (a board member of the Bitcoin Foundation), Rory Cellan-Jones (the BBC's technology correspondent) and Ludwig Siegele (of The Economist).

7.2.8. The Claimant never intended those demonstrations to provide conclusive verification that he is Satoshi Nakamoto, and he never represented that the demonstrations would provide such verification. As the Claimant explained to Messrs Andresen, Matonis, Cellan-Jones and Siegele at the time of the demonstrations, use of the private keys cannot provide such verification; only in combination with materials such as original drafts of the Bitcoin White Paper and other evidence from the time of Bitcoin's creation, can the true identity of Satoshi Nakamoto be finally established. The demonstrations were as follows:

7.2.8.1. On 23 March 2016, the Claimant participated in a private demonstration of a key signing before Mr Matonis, using a message of Mr Matonis' choosing.

7.2.8.2. On 8 April 2016, the Claimant participated in a private demonstration of a key signing before Mr Andresen, using a message of Mr Andresen's' choosing. In order to be fully satisfied, Mr Andresen, having witnessed the Claimant complete the demonstration on his (i.e. the Claimant's) own computer, requested that a brand new, sealed laptop was purchased, used and that he himself install that software needed for the demonstration.



- 7.2.8.3. On the morning of 26 April 2016, the Claimant participated in demonstrations which took place (1) with Mr Cellan-Jones and (2) with Mr Siegele. For these demonstrations the Claimant signed messages, attaching the text of a speech by Jean-Paul Sartre with a private key from block #9 – a block believed to have been mined by Satoshi Nakamoto.
- 7.2.9. The Claimant only signed the messages privately as he was led to believe that the individuals involved would then validate his claim to be Satoshi Nakamoto by using the evidence he held concerning and not rely on the mere possession of keys. The Claimant was overly trusting and believed that if he did these private demonstrations, the individuals concerned would then act as responsible journalists and would follow up by exploring and reporting on the material and evidence the Claimant possessed, including the early drafts of the White Paper and the Claimant's academic credentials.
- 7.2.10. Messrs Andresen, Matonis, Cellan-Jones and Siegele applied the public key associated with the private key which the Claimant used and, by that method, verified that the Claimant had signed the messages with the correct private key. Had the Claimant used a different private key, those individuals would not have been able to verify the messages.
- 7.2.11. Messrs Andresen, Matonis, Cellan-Jones and Siegele were therefore able to confirm that the Claimant had signed those messages with that particular private key.
- 7.2.12. Following these demonstrations, on 2 May 2016, Mr Andresen and Mr Matonis publicly confirmed that the demonstrations were a success and that, in their opinion, the Claimant had proved to their



satisfaction that he was or was likely to be Satoshi Nakamoto.

- 7.3. In the premises, the second sentence of paragraph 9(1)(b) is admitted, save that it is denied, if it is so averred, that the Claimant ever agreed to participate in such an exercise. The third sentence is denied: the Claimant never agreed *“to send the Bitcoin back from that address”*. No admissions are made to the fourth sentence, save that it is denied that any such agreement included the Claimant. As to the fifth sentence: it is admitted that the Claimant did not send the Bitcoin back; it is denied that he promised he would do so. The Claimant did not promise to provide *“extraordinary proof”*.
- 7.4. The first sentence of paragraph 9(1)(c) is denied, the Claimant has not made the public acknowledgements described therein. It is admitted that the blog post referred to in the second sentence, (published on 5 May 2016 not 4 May 2016) (**“the 5 May 2016 blogpost”**), contained the words cited therein. However:
- 7.4.1. the Claimant did not personally compose or publish the 5 May 2016 blogpost. It was written and published by Mr MacGregor. Mr MacGregor controlled the website, www.drcraigwright.net (**“the Blog Website”**) on which the blog was hosted at that time. The website was owned by Mr MacGregor’s company, The Workshop Technologies Limited.
- 7.4.2. The Claimant has very limited recall of the events of and around 2-5 May 2016. Further and in any event, it is denied that the 5 May 2016 blogpost constituted the public acknowledgement pleaded. The Claimant will refer to the full context of the blogpost for its proper meaning and significance.



- 7.4.3. At the time the 5 May 2016 blogpost was published, the Claimant was in a state of despair and exhaustion, having not slept for days and having been subjected to sustained attacks on his qualifications and character. Further, the Claimant was consistently being manipulated and put under intense pressure by those around him, in particular by Mr MacGregor, to move bitcoin from the early blocks (something which the Claimant had and always has consistently stated he would not – and, in any event, could not (because he was not authorised to) – do). The Claimant was also told by those individuals that, if he did not move the bitcoins he would destroy the reputations of Gavin Andresen and Jon Matonis who had vouched for him following his demonstrations to them in April 2016. The pressure on the Claimant was so intense that, on 4 May 2016 the Claimant attempted to commit suicide and was admitted into hospital.
- 7.4.4. The extreme stress which the Claimant was under was exacerbated because it became clear to the Claimant at this time that Mr MacGregor was only interested in his own financial gain, without regard to the detrimental impact such ambition and conduct would inflict upon the Claimant.
- 7.4.5. The Claimant came to realise that Mr MacGregor thought that he could manipulate or otherwise force the Claimant into using one or more of the private keys to move bitcoin associated with the early blocks and that the media and crypto-currency world would fall into line behind him without question. Mr MacGregor did not appreciate how intellectual property is authenticated, nor did he care about the Claimant's repeatedly expressed desire to prove his identity as Satoshi Nakamoto by reference to and independent authentication of his past academic work, including early drafts of the Bitcoin Whitepaper.



- 7.5. Paragraph 9(1)(d) is not admitted, save that it is denied that the Claimant had made “failed promises” to prove he was Satoshi Nakamoto. To the extent that the Defendant is able to prove such “*continuous global publication within the Bitcoin and cryptocurrency sector in the mainstream media*” as alleged it is denied that such evidence is admissible on the issue of serious harm: *Dingle v Associated Newspapers Ltd* [1964] AC 371.
- 7.6. Paragraph 9(1)(e) is denied. Paragraphs 7.2.1 to 7.2.12 above are repeated.
- 7.7. As to paragraph 9(1)(f): it is denied that the words quoted (which are based on a tweet by Mr Ayre, not the Claimant) amount to the Claimant’s “*stated objective in bringing these proceedings*”. In any event it is denied that the Claimant’s desire for his reputation to be vindicated by a court finding is relevant to the issue of serious harm. As to the allegation that the Claimant has failed to “show the proof” paragraphs 7.2.1 to 7.2.12 above are repeated.
- 7.8. Paragraph 9(1)(g) is denied.
8. As to paragraph 9(2): the general assertion in the first sentence as to the way in which Twitter users “understand” Twitter is denied and is in any event irrelevant. The second sentence is denied and it is in any event denied that the Defendant is entitled to rely on any such previous “references” as alleged, because for the reasons already pleaded the Claimant had not “promised” to prove he was Satoshi and accordingly had not failed to do so.
9. Paragraph 9(3) is noted.
10. No admissions are made as to paragraph 9(4)(a) and the Defendant is put to strict proof of the same.
11. No admissions are made as to paragraph 9(4)(b) and the Defendant is put to strict



proof of the same.

12. The first sentence of paragraph 9(4)(c) is not admitted because the Claimant does not know the precise date on which the Defendant deleted the Tweet (save that the Defendant temporarily deactivated his Twitter account on or around 10 April 2019). The second sentence is denied insofar as the term "*well-known and generally understood point*" is intended to mean that the Tweet contained a well-known fact about the Claimant. Save as aforesaid paragraph 9(4)(c) is not admitted.
13. No admissions are made as to the first sentence of paragraph 9(4)(d) or the inference sought to be drawn in the second sentence.
14. Save that it is denied that the Tweet was "*simply repeating a well-known point*", no admissions are made to paragraph 9(4)(e).
15. Paragraphs 9(4)(f) and 9(4)(g) are noted. The Claimant's position is as set out in the Amended Particulars of Claim.
16. Paragraph 9(5) is irrelevant to this claim and should be struck out. The fact that the Claimant has brought additional claims against third parties is irrelevant to the assessment of harm caused by the Defendant's publication. In any event, it is denied that evidence of other claims (or purported claims), is admissible on the issue of serious harm. As to the proceedings referred to in the sub-paragraphs:
 - 16.1. Paragraph 9(5)(a): the claim against Peter McCormack relates to publications which post-date the publication in this claim.
 - 16.2. Paragraph 9(5)(b): no claim is being pursued against Mr Buterin, and in any event, the Github publication post-dates the publication in this claim.
 - 16.3. Paragraph 9(5)(c): no claim is being pursued against Mr Back, and in any event the Tweet referred to therein post-dates the publication in this claim.



16.4. Paragraph 9(5)(d): the claim against Mr Ver has been dismissed for want of jurisdiction. There are ongoing proceedings in Antigua against Mr Ver concerning the same subject matter.

17. Paragraph 9(6) is denied: paragraph 16 above is repeated.

18. As to paragraph 9(7) it is denied that there is any proper basis for the pleaded inference.

19. In the premises paragraph 9(8) is denied.

Alleged Abuse of Process

20. The first sentence of paragraph 10 is denied. As to the sub-paragraphs:

20.1. Paragraph 10(1) is denied. Paragraphs 6-19 above are repeated.

20.2. The first sentence of paragraph 10(2) is denied: the Claimant is bringing these proceedings to achieve vindication in respect of the Defendant's libel. It is denied that this litigation is being run by third parties for commercial gain.

20.3. The facts and matters in paragraph 10(2)(a) are irrelevant and should be struck out. Without prejudice to that contention:

20.3.1. The first and second sentences are admitted.

20.3.2. The third sentence is admitted save that it is denied that (i) Mr Ayre established Bitcoin SV or that Bitcoin SV was created with Mr Ayre's financial backing and (ii) Bitcoin SV, in November 2018, was "new". Bitcoin SV is the rebranded name which the Claimant gave to the original Bitcoin protocol in November 2018. It is averred



that, whereas Bitcoin SV is Bitcoin, other digital assets which refer to themselves as 'Bitcoin' (including Bitcoin Core, an asset which the Defendant is invested in) are not, but are improperly passing themselves off as, Bitcoin. (iii) Bitcoin is correctly described as a "cryptocurrency". Bitcoin does not use encryption and the records are published in clear text. It is further denied that Bitcoin SV is a "hard fork chain".

20.3.3. The fourth sentence is denied.

20.3.4. The fifth sentence is denied.

20.3.5. The sixth sentence is not admitted because the Claimant does not know the size of Mr Ayre's Bitcoin SV holdings.

20.3.6. The seventh sentence is denied: the Swiss company nChain Holdings (previously known as EITC Holdings Ltd, and then nCrypt Holdings Ltd), is an intellectual property holding company. It is the sister corporation of nChain Limited, an English registered company, formally known as nCrypt Limited, which was incorporated in October 2015 ("nChain"). nChain Holdings owns patent portfolios; it does not 'promote' any crypto or digital currency. The Claimant is the Chief Scientist of nChain, which is his employer (not nChain Holdings).

20.3.7. The eighth sentence is admitted.

20.3.8. The ninth sentence is not admitted because the term "closely linked" is insufficiently clear for the Claimant to plead to.

The EITC Agreement

20.4. As to paragraph 10(2)(b): whilst it is admitted that the EITC Agreement transferred rights associated with the Claimant's purported "story" to EITC and granted EITC the exclusive right to bring and control proceedings in



respect of the grant of those rights, it is denied that the EITC Agreement provides a proper basis for the pleaded inference. The EITC Agreement did not give EITC the right to initiate or control defamation proceedings which the Claimant may bring in respect of attacks on his reputation. It is specifically denied that:

20.4.1. the Claimant is merely a nominal claimant in these proceedings;
and

20.4.2. these proceedings were initiated, or are being controlled or funded by EITC (now called nChain Holdings) and/or Mr Ayre and/or other third parties. They were initiated by and are being controlled and funded by the Claimant.

20.5. Notwithstanding the foregoing, the Claimant puts the Defendant to strict proof regarding the relevance of the averment.

20.6. As to paragraphs 10(2)(c) and (d): it is denied that the Claimant brought these proceedings in order to 'trap' the Defendant as alleged or at all. It is denied that opinions expressed by Mr Ayre's tweets as referred to therein, (or whether or not they are "to like effect" to other opinions or observations, which is not admitted) are of any relevance to these proceedings.

20.7. As to paragraphs 10(2)(e) and 10(2)(f), it is admitted that the Claimant made the said statements, which have been selectively chosen by the Defendant. It is denied that the Claimant's statements related to early Bitcoin associated with Satoshi Nakamoto or the Claimant's access to or control over such early Bitcoin. The Claimant will rely on the whole of those articles and interviews and on the context of those statements for their full meaning. The Claimant is unable to plead to the unparticularised vague assertion that he "included very similar statements" in his book Satoshi's Vision.



20.8. Paragraph 10(2)(g) is denied.

20.9. Paragraph 10(2)(h) is denied. Paragraphs 20.4 and 20.5 above are repeated.

As to the sub-paragraphs:

20.9.1. 10(2)(h)(i) is admitted but the relevance of those matters is denied.

20.9.2. 10(2)(h)(ii): the relevance of the EITC Agreement is not understood, the parties terminated the EITC Agreement in May 2020.

20.9.3. 10(2)(h)(iii): it is denied that nChain has power of attorney to conduct this litigation (as opposed to litigation concerning intellectual property) on the Claimant's behalf.

20.9.4. 10(2)(h)(iv) and (v): paragraph 20.6 above is repeated.

Truth

21. Paragraph 11 is denied. As to the Particulars of Truth:

21.1. Paragraph 11(1) is admitted save that:

21.1.1. It is denied that bitcoin is the direct unit of account in all cases. Bitcoin is a token and, as such, it can represent a native information commodity that is traded on exchanges or via other methods including negotiable instruments, tokenised money and even access markers. It is denied that Bitcoin is properly described as a digital currency or cryptocurrency. As the Claimant's White Paper explains, Bitcoin acts as a form of digital cash and a micro-payment system. Ownership records are not stored on the Blockchain in any format and must be recorded by individuals as with physical cash. Bitcoin is not the unit of account but is an arbitrary designation representing 100 million of the individual



digital tokens that are used in the system.

21.1.2. It is denied that all bitcoin transactions are disclosed publicly and that ownership is public. Transactions are only partially disclosed publicly, and such transactions do not incorporate information about the identity of the parties. Without additional information the public are unable to attribute the parties to a valid transaction, and even those who mine bitcoin cannot validate the identity of those involved in a bitcoin transaction at all.

21.2. Paragraph 11(2) is admitted save that:

21.2.1. It is denied that *“Each published block has a unique cryptographic “hash” (that is, a digital fingerprint) that is derived from its contents and each block also contains a hash of the previous block”*. Each block of transactions will have a near infinite number of possible solutions any of which, if valid, will result in the individual noted having their verified candidate block accepted by other nodes. Nodes are devices or data points on the network and, typically, are computers. New transactions are broadcast to all nodes. Each node collects new transactions into a block. Each node works on finding a difficult proof-of-work for its block. When a node finds a proof-of-work, it broadcasts the block to all other nodes. Nodes accept the block only if all transactions in it are valid and not already spent. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash. The system limits the number of nodes to a maximum number of 2016.

21.2.2. Blocks are created within Bitcoin in order to set a chronological order of transactions. The secure hash function is used as an index that is published allowing individuals who exchange bitcoin tokens and transactions to validate that the information in a previous set



of transactions that have been included in prior blocks were validated at an earlier time. This allows general users of the system not to have to download the entire Blockchain and to only require users of the system to keep the series of hash indexes that are referred to as “block headers”.

21.3. It is denied that a “*proof of work*” is a mathematical challenge which necessarily has a known probabilistic number of computations must be applied in order to solve it. The proof of work computation is not a means to cryptographically secure the Blockchain but, rather, is a game theoretic signaling device that allows law enforcement agencies and governments to determine the existence of significant entities that control the registration of transactions on the Blockchain, allowing them to take action against individuals and companies transferring Bitcoin.

21.4. It is denied that the history of the blockchain has not been subject to significant interference or alteration. Forks or “*orphans*” are common within the blockchain, being part of the nature of bitcoin, and as such have led to changes in the history of the blockchain.

21.5. It is denied that it is “computationally expensive to replace a block and becomes exponentially more difficult to do so the further back in the chain you go.” The Bitcoin protocol uses what is known as a difficulty adjustment algorithm. The difficulty of solving the first eight years of Bitcoin’s protocol is less than the difficulty of solving a single year going forward. Such a process is not exponential in difficulty.

22. Paragraph 11(3) is denied. Bitcoin nodes or miners act as a distributed or mutualised settlement and clearing house. The rules to bitcoin were set immutably; an alteration to the protocol such as been done with software forks, including Bitcoin Core (“**BTC**”), create an airdrop coin. No authority needs to manage bitcoin as nodes follow a set protocol. Nodes can enforce rules but do not create them. It is further denied that:



22.1. the verification process known as mining is *performed by specialized hardware made for this specific purpose*". The White Paper specifies that the users of the network use a process called simplified payment verification (or "**SPV**"). The users do not need to verify transactions and do not act as miners. The number of miners on the Bitcoin network is severely limited with less than 100 entities acting either as corporations or for their own interest or as "mining pools" that act as nodes coordinating groups of contracted parties.

22.2. Bitcoin miners "*receive rewards for their mining activities in the form of newly created bitcoin*". The entire issue of just under 21 million Bitcoin units were created when the Claimant launched Bitcoin in January 2009. Bitcoin nodes are paid in transaction fees and a diminishing subsidy. This payment is not through the creation of new bitcoin but through the distribution of Bitcoin that were created in January 2009.

23. Paragraph 11(4) is admitted save that:

23.1. It is denied that wallets hold "digital credentials". A wallet is a software methodology for holding keys. There are many varieties of wallet.

23.2. Signing a bitcoin transaction is one of the many ways of transferring entries in the ledger including hash puzzles and complex transaction templates but it does not denote ownership.

23.3. Bitcoin was designed to update a new key every single time that key was used to sign a digital transaction. Keys are designed to be used once. Although this practice is no longer followed, this is how Bitcoin maintains security and privacy.

23.4. It is not required that keys must only be known by an individual owner who created the Bitcoin wallet. For example, in the case of cloud wallets, the keys may be managed by a third party acting in a fiduciary capacity. Bitcoin



exchanges can allow multiple entities to control their keys under corporate arrangements. The possession or control of a bitcoin is separate to the ownership of property rights on Bitcoin. A Bitcoin wallet is only one method used for controlling the bitcoin tokens. It is possible to send raw transactions and alternative methodologies can exist outside of wallets for sending and receiving bitcoin. A Bitcoin wallet is merely the simplest format of storing keys and tokens.

23.5. Paragraph 11(5) is admitted save that paragraph 21.1.2 above is repeated *mutatis mutandis*, and it is denied that “*bitcoin funds are registered to cryptographically generated Bitcoin addresses*”. Transactions can be sent to public keys rather than addresses and other formats may be created that do not involve either public keys or addresses for the sending of Bitcoin.

Satoshi Nakamoto

24. Paragraph 11(6) is admitted save that it is denied that the SN Paper was published on 31 October 2008. A draft of the SN Paper was uploaded on 31 October 2008 and distributed publicly. The final version was only published in 2019. In respect of the genesis of the SN Paper:

24.1. In 2004, the Claimant began working at accountancy and business company BDO Kendalls (a member of the BDO Global partnership) in Sydney, Australia. Whilst there, he worked on various projects, including distributed systems and peer-to-peer networks. Around this time the Claimant worked on a project in his spare time that would eventually become Bitcoin.

24.2. In working on this project, the Claimant wished to be able to create value on a platform which is otherwise free. He wished to move the internet away from an insecure non-commercial model to a secure commercial model. The Claimant believed, and still believes, that this is impossible to achieve without a method of allowing micropayments to occur at a granular level, as small as 1/1000 of a cent. Bitcoin was developed specifically to allow



micropayments to occur.

- 24.3. The term 'Bitcoin' was not coined until 2008. It was chosen as a name because each one is a coin in bit format. Prior to this, it had been characterised by the Claimant as another micropayment system adjunct to the internet. It differed from well-known payment systems such as Paypal or Visa as it offered micropayments at a much more granular level. The Claimant considered various possible names for this micropayment system before he settled on 'Bitcoin'; early candidates included "Time Coin", "Byte Coin" and "Byte Cash".
- 24.4. In 2008 the Claimant had been completing his masters in law ("**LLM**") at the University of Northumbria at Newcastle, alongside his masters in statistics, for which he was studying at the University of Newcastle, Australia. His LLM thesis was submitted in February 2008 and concerned internet intermediaries, reflecting the Claimant's original vision for Bitcoin. The Claimant included passages from his LLM thesis proposal (which he initially submitted in August 2007 and later re-submitted in November 2007) in the Bitcoin White Paper. The Claimant was awarded his LLM in May 2008.
- 24.5. In March 2008 the Claimant requested input from Wing Commander (ret) Don Lynam, David Kleiman and others into a paper relating to the project. In May 2008, the Claimant released the first version of the White Paper, edited by Mr Lynam and Mr Kleiman, under the name Satoshi Nakamoto.
- 24.6. On 31 October 2008, the Claimant, as Satoshi Nakamoto, announced the payment project on the forums, cryptographic lists, a community money group and peer-to-peer forums. This led to Hal Finney and a number of other third parties offering the Claimant assistance. At this point the code was still in development.
- 24.7. The Claimant chose the name Satoshi Nakamoto as he worried about the success of the White Paper if released in his own name: in the past he had received abuse from critics for highlighting the dangers of the free internet.



He had used the pseudonym since mid-2008 as he has a long-held interest in and affinity with Japanese history and culture. The name 'Satoshi Nakamoto' is a combination of two Japanese names which are significant or otherwise have meaning to the Claimant: 'Satoshi' signifies wise or intelligent history – a concept which fits in with the Claimant's vision for the blockchain as an immutable public ledger; it is also the Japanese name for the protagonist in Pokémon as well as the name of the Claimant's favourite character from Ron Chernow's history of the J.P. Morgan banking dynasty "*The House of Morgan: An American Banking Dynasty and the Rise of Modern Finance*"; 'Nakamoto' is a homage to the 18th century Japanese philosopher Tominaga Nakamoto.

25. As to paragraph 11(7):

25.1. The first and second sentences are admitted and it is averred that the Claimant was the individual who created the genesis block (block #0) and mined the first block (block #1). The first block was mined on 9 January 2009. Between 3 and 9 January 2009, the Bitcoin code crashed repeatedly, and the Claimant spent that time identifying and correcting these issues; that is the reason why there were six days between the date that the Claimant created the Genesis block and the date that the first bitcoin was mined.

25.2. The third sentence is denied: there were several Alpha and Beta versions of the software which the Claimant worked on prior to 9 January 2009. The version of the Bitcoin executable file and associated code which the Claimant released on 9 January 2009 (v.0.1.1 Alpha) was the first version the Claimant released to the public at large. At this time, David Kleiman, Ray Dillinger and Hal Finney reviewed some of the code of this software.

25.3. The fourth and fifth sentences are admitted.

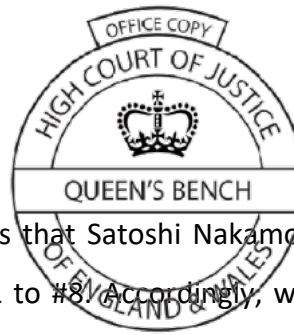
25.4. The sixth sentence is admitted save that Hal Finney was a software



developer not a computer scientist.

25.5. The seventh sentence is admitted.

26. Paragraph 11(8) is admitted. From mid-2010 onwards the Claimant began to retire the Satoshi Nakamoto pseudonym. The Claimant's last communication as Satoshi Nakamoto was an email to Mike Hearn on 23 April 2011. The Claimant completed the New South Wales Bar course in or around June 2013. In January 2013, the Claimant enrolled in the Practical Legal Training Program Course at The College of Law in New South Wales, Australia. Following this the Claimant began teaching as an academic lawyer at Charles Sturt University. Until this point he did not describe himself as a lawyer, in the sense of being an individual with a formal legal qualification. The Claimant does not have a licence to practise law in any jurisdiction, although he is an Ordinary Member of The Society of Legal Scholars, which he joined in January 2019.
27. Paragraph 11(9) is denied. This is a mischaracterisation of the nature of Bitcoin. It is not possible to identify the address as suggested in the Defence: at the time addresses, as now understood, were not used and Bitcoin relied on an exchange of public keys between individuals through a process known as "IP-to-IP exchange" (IP standing for "Internet Protocol"). Addresses as are most commonly used now would later be introduced into the system. The concept of an address was designed only for limited use when individuals were not online. It was originally noted on the Bitcoin.org website in 2009 that the proposed address format would be used if individuals could not be contacted and that this would reduce the privacy of a transaction.
28. As to paragraph 11(10):
- 28.1. It is admitted that if a person had transferred bitcoin mined in blocks #1 to #8 by using the appropriate private key, that would suggest that that person controlled the key and could, therefore, suggest that that person owned the key without any extrinsic evidence to the contrary.



- 28.2. There is no available evidence that proves that Satoshi Nakamoto – the Claimant – mined the bitcoin in blocks #1 to #8. Accordingly, whilst it is admitted that use of a private key associated with any of those blocks could potentially prove control of such key, it is denied that such evidence could prove that the person using the key is Satoshi Nakamoto.
- 28.3. A person can obtain access to and use a private key without being either its creator or its owner; in other words, a person other than Satoshi Nakamoto may be able to obtain and use the private key that has been publicly associated with Satoshi Nakamoto.
29. As to paragraph 11(11), paragraph 28 above is repeated. The fact a person had cryptographically signed a message with a private key from block #9 would provide strong evidence that that person possessed or controlled the key, but would not be compelling evidence that the person was in fact Satoshi Nakamoto.
30. As to paragraph 11(12), paragraphs 28-29 above are repeated. It would be technically straightforward for the person who held the keys to perform either of the exercises described in paragraphs 11(10) and 11(11) of the Defence; but performance of those exercises would not provide compelling evidence that the person performing the exercises was Satoshi Nakamoto.
31. Paragraph 11(13) is admitted.
32. Paragraph 11(14) is wholly irrelevant and should be struck out. Without prejudice to this contention the summary of the ATO audit (not investigation) in this paragraph is admitted. However, it was not the Claimant personally who was the subject of the audit and the Claimant was not in fact the controlling mind of Coin Exch.
33. Paragraph 11(15) is admitted save that:
- 33.1. it is denied that the Claimant entered personally into an agreement with nTrust in late June 2015. In late June 2015 a Heads of Terms agreement was made between the Claimant, DeMorgan Limited and Calay Holdings, Inc.



(t/a The Sterling Group) (“**the nCrypt Agreement**”) relating to acquisition of IP for a company that would become nCrypt.

33.2. Insofar as it is suggested, it is denied that Mr Ayre and/or Mr MacGregor were signatories to that agreement.

34. Paragraph 11(16) is admitted save that it is denied that EITC was at any material time connected to nTrust or that the consideration for the EITC Agreement was payment of any tax or other liabilities. The Claimant will refer to the full terms of the EITC Agreement for its context and meaning.

35. Save that it is admitted that pursuant to the nCrypt Agreement the Claimant agreed that the products and IP rights accruing in connection with his research would be held by nCrypt, paragraph 11(17) is denied:

35.1. the Claimant was not aware of any plan to sell or license products and IP which had arisen from the Claimant’s research as works of Satoshi Nakamoto.

35.2. Save as follows, the Claimant was not made aware of any plan, whether pursuant to any nCrypt Agreement or otherwise, for a big ‘Satoshi reveal’, i.e. an unmasking of the Claimant as Satoshi Nakamoto, as alleged or at all. The Claimant had no wish ever to be revealed publicly as Satoshi. However, following publication of the articles in Wired and Gizmodo in December 2015, which linked the Claimant with Satoshi Nakamoto, the Claimant was reluctantly persuaded to extend the scope of the sale of his life story to include his story as Satoshi Nakamoto and the associated details relating to the creation of bitcoin. He was prepared to do this in order to address misconceptions that had been published about him in the wake of the Wired and Gizmodo articles.

35.3. As pleaded above, in or around March 2016, the Claimant was informed that he would need to take part in some form of practical demonstration.



Paragraph 7.25 above is repeated.

35.4. Accordingly, and up to March 2016 there was, as far as the Claimant was aware, no intention to sell a 'Satoshi package' as alleged or at all. The Claimant is a high functioning sufferer of Asperger's Syndrome (now referred to as Autism Spectrum Disorder). One of the manifestations of the condition is an excess of trust placed in third parties. As a result of his condition, the Claimant placed excessive trust in individuals – including Mr MacGregor – who sought to take advantage of the Claimant and exploit him and his creation of Bitcoin for their own purposes.

36. As to paragraph 11(18):

36.1. The first sentence is admitted save that it is denied that the Claimant was aware of an 'SN Project' to 'unmask' him as described.

36.2. As to the second sentence of paragraph 11(18), it is admitted that Andrew O'Hagan's involvement commenced in late 2015. However, Mr O'Hagan was not 'brought in' as part of any 'reveal'. Mr O'Hagan wished to research and document the creation and promotion of nChain Limited with the Claimant and his patents, including Bitcoin, at the heart of the story. The Claimant was content to speak to Mr O'Hagan and provide him with assistance. Mr O'Hagan's ambition was to research the story with reference to a variety of materials, including documentary materials which may link the Claimant to the creation of Bitcoin, including the Claimant's academic body of work and the early drafts of the Bitcoin Whitepaper. Mr O'Hagan spent considerable time on the story, and, during the course of his research, decided that he would as part of the story report upon the public revelation of the Claimant as Satoshi Nakamoto, including the demonstrations using private keys.

36.3. The third sentence is admitted.

37. As to paragraph 11(19):



37.1. The first sentence is admitted. Paragraphs 7.2.1 and 7.2.2 above are repeated.

37.2. The second sentence is admitted.

37.3. As to the third sentence, it is denied that the Claimant provided, or otherwise authorised the provision of, information to Wired and Gizmodo prior to publication of the articles on 8 December 2015. To the best of the Claimant's knowledge, none of the individuals or entities he was communicating with at that time provided any information to Wired or Gizmodo. The appearance of those articles came as a shock to the Claimant, and caused him considerable upset.

37.4. As pleaded above, the Claimant had sought advice from individuals: paragraph 7.2.3 above is repeated.

38. As to paragraphs 11(20) and 11(21):

38.1. It is admitted that the Claimant agreed to give a limited number of private demonstrations to evidence that he possessed a private key associated with one of the early blocks widely assumed to be held by Satoshi Nakamoto. As pleaded above, the Claimant had never wanted to participate in any such demonstration but felt under considerable pressure to respond to the speculation and publicity following the publication of the Wired and Gizmodo articles Paragraphs 7.2.6 and 7.2.7 above are repeated

38.2. It is denied that the Claimant intended those demonstrations to provide "conclusive verification" that he is Satoshi Nakamoto, or that he ever represented that the demonstrations would provide such verification. Paragraph 7.2.8 above is repeated.

38.3. The Claimant trusted the assurances made by Mr MacGregor that the media would wish to publish the evidence that the Claimant wanted to present to the world concerning the fact is Satoshi, particularly his original authorship documentation and academic credentials.



38.4. As pleaded above between late March and late April 2016, the Claimant carried out private demonstrations before Messrs Andersen, Matonis and Cellan-Jones, and Siegele. Paragraphs 7.2.8.1 to 7.2.8.3 above are repeated.

38.5. Paragraphs 7.2.9 to 7.2.12 above are repeated.

38.6. The demonstrations to the BBC and Economist were conducted in back-to-back 90 minutes sessions on the morning of 26 April 2016. The Claimant's interview with GQ magazine took place that afternoon.

38.7. The Claimant does not know all of the information which was provided to media organisations, so cannot plead to the last sentence of paragraph 11(20).

38.8. Subsequently, in early May 2016, the Claimant destroyed the hard drive which contained the private keys which he had used in the above demonstrations. As the Claimant no longer has those keys, he is, and at all times since he destroyed the hard drive has been, unable to replicate the demonstrations. The keys had been provided to him by a blind trust in which the Satoshi keys had previously vested on condition that they be used only for the purpose of the private demonstrations, and only if he destroyed them thereafter. Accordingly, the Claimant no longer has access to those keys.

38.9. As to the last sentence of paragraph 11(21), it is admitted that the Claimant did inform Mr Cellan-Jones that he was about to demonstrate the signing of a message with the public key which was associated with the first transaction ever done on Bitcoin. It is denied that the Claimant informed Mr Cellan-Jones that he would thereby (i.e. through use of the key) demonstrate that he was Satoshi Nakamoto. The video of the Claimant's interview with Mr Cellan-Jones was heavily edited down from over 1 hour to 4 minutes and fifty seconds. The published recording of that interview is misleading and does not accurately reflect the Claimant's responses to Mr



Cellan-Jones' question.

39. As to paragraph 11(22) it is admitted that the Claimant was meant to carry out a further private demonstration in front of a journalist from GQ Magazine but it is denied that that demonstration took place. It is admitted that the journalist, Stuart McGurk, was accompanied by Dr Nicolas Courtois of University College London; no admission is made as to Dr Courtois' expertise in cryptography. While it is admitted that the Claimant did make the statements quoted in that paragraph, the statements have been selectively chosen by the Defendant and the Claimant will rely on the entirety of the published recording of the interview for context. It is denied that the Claimant reacted furiously to, or was defensive in respect of, Dr Courtois' question regarding the traceability of early bitcoin. It is further denied that the Claimant's quoted statements ("*If you don't like it, fuck off! Fuck off!*" and "*It's none of your business!*") were said in response to that question. The published version of the GQ session is a heavily edited 8-minute recording which does not reflect the entirety of the hour and a half session. It is denied that the Claimant breached the EITC Agreement or that the inference pleaded by the Defendant can reasonably be drawn.
40. Paragraph 11(23) is admitted, save that:
- 40.1. In relation to the Claimant's 'claims to be Satoshi', his production of evidence, and his demonstrated 'proof', paragraphs 28-30 above are repeated.
- 40.2. As to whether there was a 'SN Project', paragraphs 35-35.4 above are repeated.
41. As to paragraph 11(24):
- 41.1. The first sentence is admitted. The 2 May 2016 post ("**the 2 May Post**") was published on to the Blog Website by Robert MacGregor of The Workshop Technologies Ltd, which owned and controlled the Blog Website. At that



time the Claimant did not have access to or control over what went on the Blog Website; this was done by Mr MacGregor and/or his company. The 2 May Post was an edited version of a document written by the Claimant; the Claimant did not approve the edits before the 2 May Post was uploaded to the Blog Website.

41.2. It is denied that the Claimant "*clearly intended*" to corroborate the media reports of his "*proof*" by publishing the 2 May Post; or that by publishing the 2 May Post the Claimant purported to demonstrate his control over Satoshi Nakamoto's private key. In the 2 May Post, the Claimant did not purport to cryptographically sign the Sartre message. The 2 May Post did not provide or purport to provide any proof that the Claimant was Satoshi Nakamoto. Nowhere in the 2 May Post did the Claimant state that that was the purpose of the post.

42. Paragraph 11(25) is admitted save that it is denied that the 2 May Post was intended to corroborate or justify any attempts at a "proof." Paragraphs 41.1 - 41.2 and 28-30 above are repeated. As to the last sentence of paragraph 11(25), it is denied that the Claimant deleted the 2 May Post. On 5 May 2016, the Claimant was in hospital. The Claimant does not know if the 2 May Post was deleted and, if it was deleted, by whom; however, the 2 May Post is live on the Claimant's current blog, hosted at www.craigwright.net.

43. As to paragraphs 11(26) and 11(27):

43.1. It is admitted that on 2 May 2016 and thereafter many commentators condemned the Claimant for having perpetrated what was described as a 'scam' and for having provided 'fake proof' that he is Satoshi Nakamoto. Those commentators had comprehensively misunderstood the 2 May blog post.

43.2. Whether or not third parties 'condemned' the Claimant is irrelevant to the issue of whether the allegation published by the Defendant was true.



Further it is denied that such condemnation was universal or was so widespread as to make it likely, let alone inevitable, that readers of the Claimant's Twitter feed several years later would have known of the alleged 'fakery'. The claim of "fakery" was made primarily by people with vested interests in discrediting the Claimant. Furthermore, there were many people who both privately and publicly supported the Claimant, and continued to believe that he is Satoshi Nakamoto, notwithstanding the publicity surrounding the 2 May Post.

43.3. The Claimant and Mr Kaminsky had a long history of rivalry with each other that pre-dates the launch of Bitcoin in 2009. Mr Kaminsky died in April 2021.

44. As to paragraph 11(28):

44.1. Save that it is admitted that the Claimant met Dr Courtois on 26 April 2016, no admissions are made to the first sentence because the Claimant does not know whether the alleged email referred to therein was sent as alleged.

44.2. The second sentence is admitted.

45. Paragraph 11(29) is denied.

46. As to paragraph 11(30):

46.1. It is admitted that a blog post was posted onto the Blog Website on 3 May 2016 and included the text pleaded ("**the 3 May Post**").

46.2. The Claimant did not write that blog post or plan to place it on his blog. He was shown it briefly before it was posted, he believes by Mr MacGregor. By this stage the Claimant was extremely upset by the events of recent days, in particular the media furore surrounding his claims to be Satoshi Nakamoto. He was therefore not in a fit state to make an informed decision



as to whether the 3 May Post should be put on the site, or what that post should say. He had not slept in four days and was in a state of mental collapse. Paragraphs 7.4.3-7.4.4 above are repeated. Events had by that stage been taken entirely out of his hands. There was no obligation under the EITC Agreement for the Claimant to make such a blog post.

46.3. Further and in any event, it is denied that the implication of the 3 May Post was that the Claimant's first proof had not proven he was Satoshi Nakamoto.

47. As to paragraph 11(31):

47.1. The Claimant had no involvement in the arrangements alleged to have been made. Nor was there any obligation under the EITC Agreement to agree to a final session. On 3 and 4 May 2016, the Claimant retreated into himself and was barely functioning; he was not checking or reading his emails but instead relied on his wife to relay emails to and from the outside world. Notwithstanding his fragile mental state, he was getting frequent phone calls from individuals around him like Robert MacGregor, pressing him to move bitcoin from an early block and to sign multiple messages using the private keys from the early blocks.

47.2. The Claimant played no part in any arrangements with the BBC, or any arrangement for Messrs Matonis, Andresen and Cellan-Jones to send bitcoin to a public address; neither was he involved in any arrangement to send bitcoin back from that address. If any such arrangement was made it was without the Claimant's involvement or consent.

47.3. The Claimant does not know, and cannot plead to, the last sentence of paragraph 11(31).

48. As to paragraph 11(32):

48.1. As to the first sentence, paragraphs 41.1-41.2 above are repeated. The



Claimant never promised to provide 'extraordinary proof'. It is admitted that the Claimant did not send the bitcoin back; he never promised he would do so, and was in any event not in a position to do so given his emotional state and his destruction of the keys.

48.2. The second sentence is admitted.

48.3. As to the third sentence, it is denied that the Claimant explained that he was 'not strong enough' to send the bitcoin back. He did not compose the 5 May blogpost. It was written and published by Mr MacGregor. The Claimant has no recollection of telling Mr O'Hagan that he feared he could be arrested under UK anti-terrorism legislation.

48.4. As to the fourth sentence, paragraphs 41.1-41.2 above are repeated. The Sartre message was not signed with Satoshi's private key.

49. As to the first sentence of paragraph 11(33) it is admitted that the Claimant (as part of a pleading in the McCormack case), explained that he had destroyed a hard drive containing the relevant private keys in early May 2016. As to i) of the second sentence, it is denied that the Claimant promised to provide "extraordinary proof", paragraphs 28-30, 46.1-46.3 and 48.1 above are repeated; (ii) of that sentence is denied.

50. Paragraph 11(34) is denied, and it is further denied that the inference therein can reasonably be drawn.

The Florida Proceedings

51. Paragraph 11(36) is admitted save that it is denied that the Claimant claimed or admitted that he and Mr Kleiman ever created or mined bitcoin together. The Claimant has been consistent in his assertion that he alone created Bitcoin but that others commented on his Draft White Paper (including Mr Kleiman) and helped with coding. No bitcoin purportedly owned by Mr Kleiman were ever placed into any trust of which the Claimant was the trustee, settlor or beneficiary.



The exact date on which the mined bitcoin will be accessible is not certain. It is denied that the Claimant made any claim that such access would be granted on 1 January 2020; rather, he did testify that he expected to receive encryption key slices to decrypt an encrypted file containing information necessary to produce a list of the bitcoin that he mined (on behalf of his company) from 2009 through August 2010 sometime in January 2020, but could not be certain that that information would in fact arrive.

52. Paragraph 11(37) is admitted save that:

52.1. It is denied that the list of the public keys will evidence the ownership of the bitcoin in issue. Paragraphs 23.2 and 28.1-28.3 above are repeated. The Claimant has not claimed to own any of the bitcoin in dispute in those proceedings. Rather, he has asserted that organisations and companies that he was associated with own the rights to these bitcoin.

52.2. It is denied that the Claimant stated that he is unable to provide the list of his public addresses due to such information being held in a Tulip Trust; rather, the public address information is contained in an encrypted file, the encryption key to which having been split up using a Shamir Secret Sharing Scheme, and the necessary keys to decrypt that file were planned to be sent to him in January 2020.

52.3. It is denied that the Claimant stated that the missing "slice" of the Shamir Secret Sharing Scheme to be provided in January 2020 would be delivered to him by a "bonded courier".

52.4. It is denied that the Claimant's position as regards his ability to produce the list of public addresses for the mined Bitcoin as well as the existence of the Tulip Trust has changed. The Claimant has continually maintained the position set out in paragraph 51 above.

52.5. As to the third sentence, it is admitted that the Claimant initially objected to the production of all of the public addresses on various grounds, all of



which emanated from the fact that, aside from the first seventy blocks (which the Claimant produced upon the Plaintiffs' request), he did not have possession or control of those addresses. As to the rest of that sentence, no admission is made and the Claimant will refer to and rely on the full context of the Florida proceedings in respect of which his sworn testimony was made.

53. Paragraph 11(38) is admitted save that:

53.1. The judgment of Magistrate Judge Reinhart was overturned by District Judge Bloom in the judgment of 10 January 2020.

53.2. For the purpose of context, the Claimant will rely on the entirety of Magistrate Judge Reinhart's judgment of 27 August 2019, not just the extracts referred to in 11(38)(a)-(g) that are provided without context and are therefore misleading.

53.3. Further and in any event, it is denied that the assessment and findings of Magistrate Judge Reinhart, which are not binding in these proceedings, are (a) correct or (b) relevant to the issues in this case.

54. As to paragraph 11(39) the Claimant will rely on the entirety of that judgment for context. In any event, the findings of the Florida court in those proceedings are not binding in these proceedings, nor are they (a) correct or (b) relevant to the issues in this case.

55. Paragraph 11(40) is denied. In particular:

55.1. As to the first sentence, paragraph 52.3 above is repeated.

55.2. It is denied that private keys are required to mine bitcoin.

55.3. It is denied that the Claimant ever promised that he would transfer the early bitcoin either at all or by using the associated private keys.



55.4. It is denied that the Claimant personally made any promise to provide “extraordinary proof”.

55.5. It is denied that the Claimant would reasonably have been expected to rely on the explanation that he does not have control over his private keys. In respect of the references to “extraordinary proof” and the averment that the failure to sign the Sartre message was a mistake paragraphs 41.1-41.2 and 47.1-47.3 above are respectively repeated.

55.6. The last sentence is denied. The issues that have arisen in the Florida proceedings regarding the Claimant’s and his former companies’ bitcoin holdings relate to matters of disclosure and production of documents. In those proceedings, the Plaintiffs have not sought, nor has the Florida court ordered, the disclosure or production of any private keys.

56. As to paragraph 11(41), the first sentence is admitted. In January 2020, the trustee of the Tulip Trust received information from a third party. That information included a list of Bitcoin public keys, from which the Claimant was able to produce the list of public addresses which he had been ordered by the Florida court to produce and he did so. The second sentence is admitted.

57. Paragraph 11(42) is denied save that it is admitted that the Claimant acknowledged that he mined the first 70 blocks. The Claimant is unable to plead to a list which is not properly particularised.

Locations

58. Paragraph 11(43) is denied. The Defendant has not indicated the posts to which he refers, however the Claimant used a feature whereby posts could be written in advance and uploaded automatically at a time predetermined by the Claimant and/or, from 2010 onwards, persons with access to his blog.



59. As to paragraph 11(44): the first sentence is not admitted because the Claimant (i.e. Satoshi Nakamoto) does not know what ISPs he was using in January 2009, but it is in any event denied that identifying an ISP identifies the location of the user. Accordingly it is denied that the ISP details “located” Satoshi Nakamoto in the California area during that period. The remainder of that paragraph is admitted save that the Claimant cannot recall whether he was in Australia for the entirety of January 2009.

Further Instances

60. As to paragraph 11(45), when interviewed by GQ in June 2017 the Claimant was asked about “early” bitcoin transactions and he replied that, other than sending bitcoin to Hal Finney and Zooko, he had not moved them. He was not there referring to the moving of bitcoin to Mike Hearn, which took place in April 2009, some 3-4 months after the moving to Hal Finney and Zooko and therefore, as far as the Claimant was concerned, was not an “early” bitcoin transaction. It is accordingly denied that what the Claimant said to GQ indicates (whether strongly or at all) that the Claimant is not Satoshi Nakamoto.
61. As to paragraph 11(46):
- 61.1. It is denied that the Claimant tweeted that he had submitted a research paper to the Australian government in 2001. He had submitted a research grant application.
- 61.2. It is denied that the Claimant claimed that the 2001 application had the same abstract as the Bitcoin Whitepaper.
- 61.3. It is admitted that the Claimant, acting under his Satoshi Nakamoto pseudonym, shared a draft of the Bitcoin Whitepaper in August 2008 with an individual, although not publicly.
- 61.4. It is denied that the Claimant’s Project “Blacknet” paper matched the final Satoshi Nakamoto Paper.



61.5. It is denied that the Project “Blacknet” paper was a backdated attempt by the Claimant intended to make it look as if he was the author of the Satoshi Nakamoto Paper and thereby Satoshi Nakamoto.

61.6. As to the final sentence of paragraph 11(46), it is admitted that on or around 15 February 2019, the Claimant informed the US Commodity Futures Trading Commission that, as was the case, he had previously registered a project named “Blacknet” with the Australian Federal Government’s Department of Innovation. No admissions are made to the remainder of that sentence because the Freedom of Information request referred to therein has not been sufficiently identified.

61.7. Paragraph 11(46) is otherwise denied.

62. Paragraph 11(47) is denied. The Claimant has no intention to monetise the connection between himself and Satoshi Nakamoto. His intention is to: 1) clear Bitcoin’s name; 2) disassociate it from anarchists, criminals and terrorists; and 3) by so doing, enable governments and regulators to understand the potential for Bitcoin to operate as the Claimant intended – within and under the law. As to Mr Ayre’s connection with nChain paragraph 20.3 above is repeated.

63. Paragraph 11(48) is admitted save that:

63.1. It is denied that the Claimant’s work in connection with this technology and these patents has been funded in part or full and/or otherwise supported by Mr Ayre. Mr Ayre is not and has never been an angel investor or other funder of the Claimant’s technologies, patents or research.

63.2. It is denied that the Claimant continues to maintain his claim to be Satoshi Nakamoto in part or at all to inflate the value of the intellectual property associated with the patents. Paragraph 62 above is repeated.

63.3. It is not admitted that the patents would be more interesting to potential



investors if filed by “the man behind Satoshi”.

64. As to paragraph 11(49):

64.1. It is admitted that the Claimant and Mr Ayre have sought to promote Bitcoin SV. It is denied that the Claimant has been aggressive in his promotional activity.

64.2. It is denied that Bitcoin SV is a ‘new’ product. It is the legacy Bitcoin, as the Claimant intended it to be when he invented Bitcoin.

64.3. It is admitted that the Claimant has continued to assert that he is Satoshi Nakamoto. This does add credibility to Bitcoin SV.

64.4. Paragraphs 20.3, 20.4 and 20.9 above are repeated.

64.5. The last two sentences are admitted; the decision, by Binance, to delist Bitcoin SV is directly connected with the actions of the Defendant.

65. As to paragraph 11(50):

65.1. the first sentence is admitted.

65.2. As to the second sentence it is admitted that a Financial Times article contained the quoted words cited therein, but it is denied that the Claimant authorised that quote.

65.3. As to the third sentence it is admitted that the United States Copyright Office issued the press release cited therein, but as the Claimant had not authorised any quote to the effect that he had obtained “government agency recognition”, its relevance is denied.

65.4. No admissions are made as to the final sentence because the Claimant does not know how many other registrations have been made.



Other matters

66. Paragraph 11(51) is denied. Further, the matters pleaded in paragraphs 52 to 55 are irrelevant to the question of whether the Claimant fraudulently claimed to be Satoshi.
67. Paragraph 11(52) is admitted insofar as it is an accurate summary of the 2004 judgment.
68. Paragraph 11(53) is denied. As to the sub-paragraphs:
- 68.1. The Claimant is unable to admit or deny whether the blog post referred to in the first sentence of 11(53)(a) was posted on the GSE Compliance blog as alleged, but it is denied that, if it was so published, he wrote or published it. The remainder of that paragraph is denied. If any such amendments were made, they were not made by the Claimant.
- 68.2. Save that it is admitted that in or around December 2015, the Claimant deleted posts from the GSE Compliance blog, paragraph 11(53)(b) is denied.
- 68.3. Paragraph 11(54) is admitted but the relevance of the investigation into DeMorgan Limited, or the position of Clayton UTZ to these proceedings is denied. The Claimant resigned as a director of DeMorgan Limited on 9 July 2015.
- 68.4. The first sentence of paragraph 11(55) is admitted save that it is denied that the Claimant controlled C01N Pty Limited ("**C01N**") at all material times. He was not the sole Director and ceased his directorship on 9 July 2015. The remainder of that paragraph is admitted insofar as the ATO Report included those findings.

Publication on a matter of public interest

69. Paragraph 12 is denied.



70. As to paragraph 12(1) it is denied that the publications complained of were on a matter of public interest. The words complained of were no more than a gravely defamatory slur against the Claimant.
71. As to paragraph 12(2) paragraphs 5, 7.5 and 48.1 above are repeated.
72. Paragraph 12(3) is too vague to be pleaded to: the Claimant does not know what the Defendant and his Twitter followers used Twitter to discuss.
73. As to paragraph 12(4) to 12(5), the Claimant is unable to plead to the state of mind or knowledge of the Defendant or his Twitter followers.
74. As to paragraph 12(6): the Claimant is unable to plead to the state of mind or knowledge of the Defendant or his Twitter followers, but it is in any event denied that the Defendant is entitled to rely on any matters which post-date the original publication.
75. Paragraph 12(7) is denied and in any event, in respect of the alleged “bullying and apparently strategic public threat of legal proceedings for libel” it is denied that the Defendant is entitled to rely on any matters or alleged matters which post-date the original publication.
76. Paragraph 12(8) is admitted insofar as the Defendant did not approach the Claimant for comment. The Claimant is unable to plead to the reason why the Defendant did not approach him because he does not know. The Defendant cannot plead to the vague reference to “context” in the final sentence.
77. In the premises paragraph 12(9) is denied.

ADAM WOLANSKI QC

VICTORIA JOLLIFFE



STATEMENT OF TRUTH

I believe that the facts stated in this Reply 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.

Full name: Craig Steven Wright

Signed:

Date:

23 June 2021