IN THE HIGH COURT OF JUSTICE

QUEEN'S BENCH DIVISION

MEDIA AND COMMUNICATIONS LIST

B E T W E E N:

CRAIG WRIGHT

Claimant

- and -

PETER MCCORMACK

Defendant

REPLY TO DEFENCE

---

1. Save as specifically admitted below the Claimant joins issue with the Defendant on its Defence.

2. References in this Reply to paragraph numbers are to the Defence unless otherwise stated.

Parties

3. In respect of Paragraph 2:

   3.1. As to paragraph 2.1 it is denied that the Claimant claimed in 2015 to have a PhD in computer science from Charles Sturt University, Australia. He had submitted his thesis at this time for his Doctorate in philosophy of computer science, which was conferred on 7 April 2017.

3.2.As to paragraph 2.3:

3.2.1. The Claimant and his young family immigrated to England from Australia in late 2015, bringing with them all their belongings, and have lived here ever since.

3.2.2.The Claimant has rented properties in London continually since this date.

3.2.3.Since late 2015 the Claimant has carried out work as Chief Scientist at nChain, based in London at nChain's head office. nChain is a company formerly called nCrypt which is incorporated in this jurisdiction.

3.2.4.The Claimant pays local and national taxes in this jurisdiction, including income tax.

3.2.5.The Claimant is undertaking postgraduate study in this jurisdiction.

3.2.6.The Claimant intends to remain resident in this jurisdiction and will apply for naturalization once he becomes eligible, namely, after October 2020 when he satisfies the minimum criteria of five years' residence.

3.3.Paragraph 2.4 is irrelevant, prejudicial and falls to be struck out. For the avoidance of doubt, it is denied that the Claimant left Australia due to a raid on his home and office by the Australian Tax Office. No charges have ever been brought by the Australian Tax Office against the Claimant or his companies as a result of the raid.

4. The facts and matters in paragraph 3 are irrelevant and the paragraph falls to be struck out. Without prejudice to this contention, the matters set out therein are admitted, save that it is denied that Mr Ayre established Bitcoin SV.

The publications complained of

5. Whilst it is admitted and averred that the Defendant, as pleaded in paragraph 6.4, deleted the Tweets complained of, no admissions are made as to the date on which the Defendant deleted those Tweets and the circumstances in which the tweets were deleted. It is noted and averred that the Defendant deleted the Tweets complained of at least a month after the Particulars of Claim were issued and served on the Defendant. Deletion of tweets results in deletion of associated metrics, including as to the extent of publication and the identity of readers of the tweets. By destroying this information the Defendant was in flagrant breach of his duty to retain and preserve materials relevant to these proceedings.

Meaning

6. In respect of the facts and matters pleaded in paragraphs 7.1 to 7.4 the Defendant's case in response is set out in paragraphs 5 above and 10.1.1-10.1.5 below.

7. Further and in any event it is denied that the reasonable reader of the words complained of would have been aware of the facts and matters pleaded in paragraph 7.3 of the Defence; and accordingly it is denied that such a reader would have understood the words to bear the meaning pleaded in paragraph 21 of the Defence.

Serious Harm

8. Paragraph 18 is denied. The Claimant's case on serious harm is further particularised in the Amended Particulars of Claim.

9. As to paragraphs 18.2 to 18.3:

9.1. Paragraph 18.2 is not admitted and the Defendant is put to strict proof of the same. Paragraph 5 above is repeated in respect of the Defendant's breach of the duty to retain and preserve data.

9.2. Paragraph 18.3 is admitted save that:

9.2.1. it is not admitted that Tweets are readily retweeted or liked without any or much regard being paid to the content.

9.2.2. It is denied that the allegations were not serious in nature. As to the Defendant's denial that the words complained of have been published "*extraordinarily widely*", the Defendant has deleted data relevant to this contention. Paragraph 5 above is repeated in respect of the Defendant's failure to comply with his duty to retain and preserve data relating to the words complained of.

10. As to paragraphs 19.1 to 19.7:

10.1. Paragraph 19.1 is not admitted:

10.1.1. it is denied that a very large majority of the publishees of the words complained of knew:

10.1.1.1. the facts and matters set out in paragraphs 7.3 to 7.4 of the Defence.

10.1.1.2. the alleged 'failed promises' by the Claimant to prove he was Satoshi.

10.1.2. Further, the consequence of the decision by the Defendant to delete the tweets complained of (and associated metrics) during these proceedings is that, in so far as there is any evidential dispute as to the identity and/or number of and/or knowledge of publishees, inferences must be drawn adverse to the Defendant's case.

10.1.3.It is admitted and averred that the publishees of the words complained of would have known that the Claimant had claimed to be Satoshi Nakamoto.

10.1.4.The reference to the Claimant's "*global public reputation*" as evidence of lack of serious harm caused by the publications complained of is an impermissible plea of general bad reputation and is bad in law. It is in any event denied that the Claimant had the 'global public reputation' as pleaded.

10.1.5.The reference to "*mass statements published worldwide*" as evidence of lack of serious harm caused by the publications complained of is inadmissible as offending the rule in *Dingle v Associated Newspapers Ltd* [1964] AC 371;

10.2.Paragraph 19.2 is irrelevant and falls to be struck out. Without prejudice to this contention:

10.2.1.It is denied that the Claimant has publicly acknowledged that he failed to provide promised 'proof'.

10.2.2.It is denied that the Claimant has publicly acknowledged that he would be regarded generally as being guilty of deception.

10.2.3.The Claimant did not personally compose or publish the blog post on 4 May 2016. As more fully explained in paragraph 10.2.4-10.2.5 immediately below, the Claimant has very limited recall of the events of and around 4 May 2016. Further and in any event it is denied that this post constituted the public acknowledgement pleaded. The Claimant will refer to the full context of the blogpost for its proper meaning and significance.

10.2.4.At the time the 4 May blogpost was posted, 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 Robert 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 – 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 (see paragraphs 35.3-35.7 and 35.9 below). The pressure on the Claimant was so intense that, after this post was uploaded, the Claimant attempted to commit suicide and was admitted into hospital.

10.2.5. 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. The Claimant came to realise that Mr MacGregor thought that he could manipulate or otherwise force the Claimant into using one or more of his 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.

10.3. As to paragraph 19.3:

10.3.1. It is admitted that the immediate context of the publications complained of was tweets by Mr Ayre.

10.3.2. It is denied that Mr Ayre's tweets made the matters in paragraphs 19.1 and 19.2 of the Defence 'apparent'. Mr Ayre's tweets did no more than describe how that it had been alleged that the Claimant had made fraudulent claims to

be Satoshi Nakamoto; that those claims were false; and that the Claimant was planning to bring legal action in respect of those claims.

10.3.3. It is denied that readers could see for themselves from Mr Ayre's tweets what both sides of any dispute were saying.

10.4. Paragraph 19.4 is denied. As to the Claimant's alleged promises to prove to be Satoshi Nakamoto, paragraphs 41.1 and 45.1 below are repeated. It is denied that the Claimant's objective in bringing these proceedings is that alleged. As to the Claimant 'showing the proof', paragraphs 24.1-26 and 37.1-37.3 below are repeated.

10.5. Paragraph 19.5 is denied. Readers of the words complained of would not have regarded the words as trivial or as no more than references to the Claimant's alleged failure to prove he was Satoshi Nakamoto; nor would readers have regarded the words as 'commentary' or 'verbal banter'.

10.6. Paragraph 19.6 is legal argument and the Claimant accordingly does not plead thereto.

10.7. Paragraph 19.7 is denied.

Abuse of Process

11. As to paragraph 20, it is denied that the claim in an abuse of process. The Claimant is bringing these proceedings to bring an end to the Defendant's campaign of vilification against him and to achieve vindication in respect of the Defendant's libels. Further:

11.1. It is denied that the Claimant has brought these proceedings in order to 'trap' the Defendant as alleged or at all.

11.2. It is denied that the Claimant has brought these proceedings as part of a tactical or public relations game as alleged or at all. Further and in any event Bitcoin SV node software was launched in November 2018 to ensure that the original legacy Bitcoin as created by the Claimant continues, and these proceedings were issued several months later, in May 2019.

11.3. It is denied that the claim is an infringement of the Defendant's Article 10 rights under the ECHR or an unjust waste of the Defendant's costs and time. The Claimant will refer in this regard to the fact that in the words complained of the Defendant issued the Claimant with an invitation to sue him for libel for publishing those words.

Truth

12. It is denied that the words complained of bore the meaning alleged in paragraph 21. As to paragraph 21.1, readers of the words would not have known the facts and matters in paragraphs 7.3 to 7.4 of the Defence.

13. For the reasons as set out below, paragraphs 21 and 22 are denied.

14. Paragraph 21.2 is denied.

15. Paragraph 22.1 is admitted save that:

15.1. 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.

15.2. It is denied that all bitcoin transactions are disclosed publicly. 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 validate a complete transaction, and even those who mine bitcoin can only partially validate the identity of those involved in a bitcoin transaction.

16. Paragraph 22.2 is admitted save that:

16.1. It is denied that a "*proof of work*" is a mathematical challenge which necessarily has a known number of computations must be applied in order to solve it.

16.2. 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.

17. Paragraph 22.3 is denied. Bitcoin nodes or miners act as a distributed or mutualised settlement and clearing house. The rules to bitcoin was set immutably an alteration to the protocol such as been done with 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.

18. Paragraph 22.4 is admitted save that:

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

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

18.3. 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.

19. Paragraph 22.5 is admitted save that paragraph 15.2 above is repeated *mutatis mutandis*.

20. Paragraph 22.6 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 this year. In respect of the genesis of the SN Paper:

20.1. 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.

20.2. 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.

20.3. 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".

20.4. 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 submitted in November 2007) in the Bitcoin White Paper. The Claimant was awarded his LLM in May 2008.

20.5. 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.

20.6. In March 2008 the Claimant requested input from David Kleiman into a paper relating to the project. In May 2008, the Claimant released the first version of the White Paper, edited by Mr Kleiman, under the name Satoshi Nakamoto.

20.7. 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.

21. As to paragraph 22.7:

21.1. It is denied that the Genesis Block was mined. It was created by the Claimant on 3 January 2009 without being mined.

21.2.It is denied that the first version of bitcoin software was released on 8 January 2009. The first version of the bitcoin software was released in November 2008. At this time, David Kleiman, Ray Dillinger and Hal Finney reviewed the code of this software. It was then updated and re-released in December 2008 and again in January 2009. The bitcoin executable file and associated code were released on 9 January 2009. 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.

21.3.Save the above, paragraph 22.7 is admitted.

22. Paragraph 22.8 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 and then completed his solicitor training at the College of Law in Australia. Following this the Claimant began teaching as an academic lawyer at Charles Stuart 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.

23. Paragraph 22.9 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 this time there were no addresses as now understood, and as would later be introduced into the blockchain; instead, transactions were conducted via Paid Public Keys.

24. As to paragraph 22.10:

24.1. 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.

24.2. 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 or ownership of such key, it is denied that such evidence could prove that the person using the key is Satoshi Nakamoto.

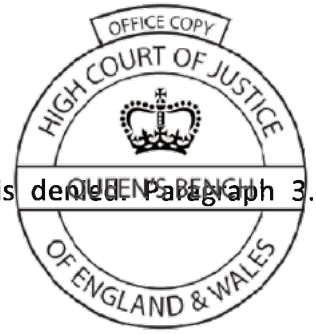
24.3. A person can obtain access to and use a private key without being either its creator or its owner; in other words, a person other than Satoshi Nakamoto may be able to obtain and use the private key that has been publicly associated with Satoshi Nakamoto.

25. As to paragraph 22.11, paragraph 24 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.

26. As to paragraph 22.12, paragraphs 24 and 25 above are repeated. It would be technically straightforward for the person who held the keys to perform either of the exercises described in paragraphs 22.10 and 22.11 of the Defence; but performance of those exercises would not provide compelling evidence that the person performing the exercises was Satoshi Nakamoto.

27. As to paragraph 22.13:

27.1. The first and second sentences of paragraph 22.13 are admitted.



27.2. The third sentence of paragraph 22.13 is denied. Paragraph 3.1 above is repeated.

28. Paragraph 22.14 is wholly irrelevant and falls to be struck out. Without prejudice to this contention:

28.1. It is denied that the ATO investigated the Claimant's business affairs.

28.2. It is denied that the Claimant was the controlling mind of Coin-Exch in June 2015.

28.3. The Claimant resigned as a director of Coin-Exch Pty Ltd in 2015 and does not know what the liabilities if any penalty was imposed on Coin-Exch Pty Ltd. He therefore, cannot plead to the second and third sentences.

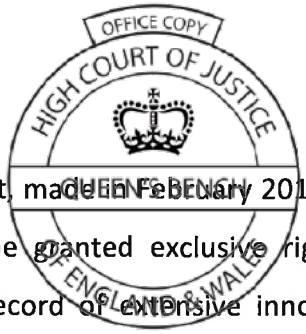
29. Paragraph 22.15 is admitted save that it is denied that:

29.1. 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.

29.2. Insofar as it is suggested Calvin Ayre was a signatory to that agreement this is denied.

30. Paragraph 22.16 is denied. In fact:

30.1. The nCrypt Agreement was made to set up a new company, nCrypt Group Holdings Ltd, to sign over intellectual and property rights owned by the Claimant, the Claimant's companies and other individuals to nCrypt and to pay off debt accrued by the Claimant's companies.



30.2. There was a subsequent related agreement, made in February 2016, by which another company, EITC Holdings, would be granted exclusive rights to the Claimant's life story, and specifically his record of extensive innovation and creativity. This included but was not confined to his work as Satoshi Nakamoto.

31. 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 22.17 is denied:

31.1. 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.

31.2. Save as follows, the Claimant was not made aware of any plan, whether pursuant to any nTrust 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.

31.3. In or around March 2016, the Claimant was informed 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 the 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.

32. 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.

33. The first sentence of paragraph 22.18 is admitted. As to the second sentence of paragraph 22.18, 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.

34. In respect of paragraph 22.19:

    34.1. The first sentence is admitted. 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. Those approaches came as a complete and unwelcome shock to the Claimant and caused him considerable upset as he was wholly unaware that information linking him to Satoshi Nakamoto had or might have been provided to the media.

    34.2. The second sentence is admitted.

    34.3. As to the third sentence, it is denied that the Claimant provided, or otherwise authorised the provision of, 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.

35. As to paragraphs 22.20 and 22.21:

35.1. 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.

35.2. 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, in combination with negative speculation and publicity which cast doubt on his qualifications and credentials.

35.3. Following the publication of the Wired and Gizmodo articles, the Claimant felt under considerable pressure to respond to such speculation and publicity. He 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).

35.4. 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. As the Claimant explained to Messrs Andreson, 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.

35.5.Between late March and late April 2016 the Claimant carried out private demonstrations before Messrs Andresen, Matonis and Cellan-Jones, and Siegele. During the demonstrations to Messrs Andresen and Matonis the Claimant signed messages of their choosing. In order to be fully satisfied, Mr Andresen requested that a brand new, sealed laptop was used and that he himself installed that software needed for the demonstration. For the demonstrations to the BBC and Economist 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.

35.6.Messrs Andreson, 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.

35.7.Messrs Andreson, Matonis, Cellan-Jones and Siegele were therefore able to confirm that the Claimant had signed those messages with that particular private key.

35.8.There was no "second day" in which the process was filmed. The demonstrations to the BBC and Economist were conducted in back-to-back 90 minutes sessions on the morning of 27 April 2016. The Claimant's interview with GQ magazine took place that afternoon.

35.9.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.

35.10.The Claimant does not know what information was provided to media organisations, so cannot plead to the last sentence of paragraph 22.20.

35.11. 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.

36. Paragraph 22.22 is admitted, save that:

36.1. In relation to the Claimant's 'claims to be Satoshi', his production of evidence, and his demonstrated 'proof', paragraphs 24-26 above are repeated.

36.2. The Claimant does not know whether Calvin Ayre issued the tweet referred to in the third sentence and cannot plead thereto.

36.3. As to whether there was a 'SN Project', paragraphs 31-32 above are repeated.

37. As to paragraph 22.23:

37.1. The first sentence is admitted. The 2 May post was published on the Claimant's blog by Robert MacGregor of The Workshop Technologies Ltd, which company owned and controlled the website on which the Claimant's blog was hosted. At that time the Claimant did not have access to or control over what went on the blog; this was done by Mr MacGregor and/or his company.

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

Satoshi Nakamoto. Nowhere in the blog post did the Claimant state that that was the purpose of the post.

37.3. Instead, the Claimant published the blog as a riposte, in particular to those who were taunting him for supposedly not providing cryptographic proof that he is Satoshi Nakamoto. He did this because he was profoundly unhappy at the attention that was being focused on him and the supposed revelation that he is Satoshi Nakamoto. Jean-Paul Sartre had turned down the Nobel Prize as he knew that his life would change beyond recognition if he were forever known as a Nobel Prize winner.

38. Paragraph 22.24 is admitted save that it is denied that the blog post was intended to corroborate or justify any attempts at a "proof."

39. As to paragraphs 22.25 and 22.26:

39.1. 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.

39.2. 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 2016 blog post.

40. As to paragraph 22.27:

40.1. It is admitted that a blog post was posted on the Claimant's blog on 3 May 2016 and included the text pleaded.

40.2. 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 blog 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 10.2.4-10.2.5 above are repeated. Events had by that stage been taken entirely out of his hands.

40.3. Further and in any event, it is denied that the implication of the blog post was that the Claimant's first proof had not proven he was Satoshi Nakamoto.

41. As to paragraph 22.28:

41.1.The Claimant had no involvement in the arrangements alleged to have been made. 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.

41.2.The Claimant played no part in, and was unaware of, any arrangements with the BBC, or any arrangement for Messrs Matonis, Andreson 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 (which the Claimant does not know, and therefore does not admit) it was without the Claimant's involvement or consent.

41.3. The Claimant does not know, and cannot plead to, the last sentence of paragraph 22.28.

42. As to paragraph 22.29:

42.1. As to the first sentence, paragraphs 40.1-40.3 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 key.

42.2. The second sentence is admitted.

42.3. 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 4 May blogpost. It was written and published by Mr MacGregor.

42.4. As to the fourth sentence, paragraphs 37.1-37.3 above are repeated. The Sartre message was signed with Satoshi's private key.

43. Paragraph 22.30 is denied.

44. Paragraph 22.32 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 and helped with coding, including Mr Kleiman. No bitcoin owned by Mr Kleiman were ever placed into any trust which the Claimant was the trustee, settlor or beneficiary to his knowledge. The exact date on which the Claimant will be able to access the trust in which he mined bitcoin is not certain and it is denied that the Claimant made any claim that he will have access on 1 January 2020; however, he did testify that he expects to receive encryption key slices to decrypt an encrypted file containing information necessary to produce a list of the bitcoin that he

mined from 2009 through August 2010 sometime in January 2020, but cannot be certain that information will in fact arrive.

45. Paragraph 22.33 is admitted save that:

45.1.it is not admitted that the list of his public keys will evidence his ownership of the bitcoin in issue. Paragraphs 18.2 and 24.1-24.3 above is repeated.

45.2.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.

46. Paragraph 22.34 is admitted save that:

46.1.It is denied that the Claimant personally made any promise to provide "extraordinary proof".

46.2.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 37.1-37.3 and 40.1-40.3 above are respectively repeated.

47. Paragraph 22.35 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.

48. Paragraph 22.36 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.

49. Paragraph 22.37 is denied and the Defendant is put to strict proof. The Claimant was never in California in January 2009.

50. As to paragraph 22.38, 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.

51. As to paragraph 22.39:

    51.1. 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.

    51.2. It is denied that the Claimant claimed that the 2001 application had the same abstract as the Bitcoin Whitepaper.

    51.3. It is admitted that Sastoshi Nakamoto shared a draft of the Bitcoin Whitepaper in August 2008 to a select group of individuals, although not publicly.

    51.4. It is denied that the Claimant's Project "Blacknet" paper matched the final Satoshi Nakamoto Paper.

    51.5. Para 22.39 is otherwise denied. In particular 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.

52. Paragraph 22.40 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. Mr Ayre has no connection with nChain other than being a supporter of the Claimant, although it is admitted that Mr Ayre owns a quantity of Bitcoin SV.

53. Paragraph 22.41 is admitted save that:

53.1. 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.

53.2. 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.

53.3. It is not admitted that the patents would be more interesting to potential investors if filed by "the man behind Satoshi".

54. As to paragraph 22.42:

54.1. 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.

54.2. 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.

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

Public Interest

55. As to paragraph 24, it is denied that the publications complained of were on a matter of public interest. The words complained of were gravely defamatory slurs against the Claimant as part of a broader campaign against the Claimant, undertaken with the clear aim of damaging the Claimant's reputation.

56. As to paragraph 25, it is denied that the Defendant was, in any way, operating in a journalistic capacity in publishing the words complained of. No comment was sought from the Claimant, none of the publications complained of contain the Claimant's side of the story and the tone of the publications is highly polemical as opposed to factual. The Claimant notes that despite this averral, in paragraph 19.5 of the Defence the Defendant seeks to compare the publications complained of as "*verbal banter*" as opposed to "*edited news copy*".

57. As to paragraph 26 paragraph 10.1.2 to 10.1.5 above are repeated.

58. As to paragraphs 27 to 36, the Claimant cannot positively plead to the Defendant's state of mind in making the publications complained of. The Claimant denies that the Defendant's purported belief that the publication of the words complained of was in the public interest was reasonable in nature. In this regard the Claimant repeats paragraphs 15 to 54 above.

Remedies

59. As to paragraph 38:

59.1. The Defendant's averment that particularisation of which European States are relied upon in order to claim for damage suffered throughout the EU is bad in law.

59.2.As to the Defendant's averment concerning the Claimant's links to the jurisdiction paragraphs 3.2.1-3.2.6 above are repeated.

59.3.The final sentence of paragraph 38 is noted.

ADAM WOLANSKI QC

ALED MACLEAN-JONES

LILY WALKER-PARR

Statement of Truth

The Claimant believes that the facts set out in this Reply to Defence are true.

Signed:

Name: DR CRAIG WRIGHT

Date: 11 October 2019

Served on 11th day of October 2019 by SCA Ontier LLP (solicitors for the Claimant)