

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

**Claim No. BL-2021-000313**

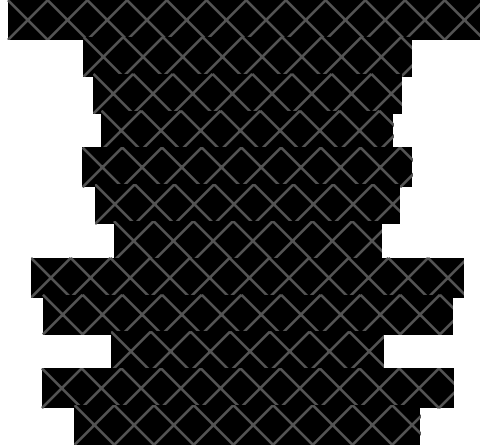
**BETWEEN:**

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

**Claimant**

**-and-**

**(1) BITCOIN ASSOCIATION FOR BSV (a Swiss verein)**



**(14) ROGER VER**  
**(15) AMAURY SÉCHET**  
**(16) JASON COX**

**Defendants**

---

**REPLY TO DEFENCE**  
**OF THE SECOND TO TWELFTH DEFENDANTS**

---

**A: INTRODUCTION**

1. In this Reply, TTL adopts the same definitions as in the Amended Particulars of Claim (“**APoC**”). Where any abbreviations or headings in the Defence of the Second to Twelfth Defendants (“**2<sup>nd</sup> to 12<sup>th</sup> Defendants**” and the “**D2-D12 Defence**”) are adopted, this is for convenience only and no admissions are made thereby. TTL will rely on all documents referred to in this Reply for their full terms and effect.
2. References to paragraph numbers are to paragraphs in the D2-D12 Defence unless otherwise stated.

3. Save where expressly admitted or not admitted herein, all allegations in the D2-D12 Defence are denied.
4. The D2-D12 Defence is highly repetitious and, where pleas are repeated by reference to another paragraph in the D2-D12 Defence, TTL should be taken as repeating its plea in respect of the paragraph in the D2-D12 Defence to which cross-reference is made, even if that is not expressly stated.
5. While this Reply necessarily focuses on the control that the 2<sup>nd</sup> to 12<sup>th</sup> Defendants have of the BTC Network, it remains TTL's position that the Thirteenth Defendant ("**13<sup>th</sup> Defendant**") also controls the BTC Network in the same way as, and together with, the 2<sup>nd</sup> to 12<sup>th</sup> Defendants, and this Reply should be read accordingly. The 13<sup>th</sup> Defendant has not served a Defence or otherwise engaged with the proceedings.
6. Paragraph 1 is denied.

**B1: THE DEVELOPMENT AND OPERATION OF THE NETWORKS**

7. As to paragraph 4:
  - 7.1. It is admitted that the BTC Network enables one party to pay to another party BTC tokens online without the need for a trusted third-party financial intermediary to process those electronic payments.
  - 7.2. It is admitted that the term 'Bitcoin' is sometimes used as a reference to the system that facilitates transactions of BTC tokens, but no other admissions are thereby made.
  - 7.3. The definition used by the 2<sup>nd</sup> to 12<sup>th</sup> Defendants is noted.
  - 7.4. References to Bitcoin tokens in the APoC and in this Reply are to so-called Bitcoin tokens in the form of BTC tokens, BCH tokens and ABC tokens, as well as to BSV tokens, which are the original and the only true Bitcoin tokens. This is done for convenience only. Paragraph 14(a) of the APoC is repeated.
8. As to paragraph 5:
  - 8.1. The pseudonymous Satoshi Nakamoto ("**Satoshi**") created the original and only true Bitcoin system – namely the original and only true Bitcoin protocol (a protocol being a set of rules and specifications that govern the network) ("**Bitcoin**

**Protocol**”) governing the original and only true Bitcoin blockchain (“**Bitcoin Blockchain**”).

- 8.2. The BSV Network (rather than the BTC Network) is the Network that is operated using the Bitcoin Protocol on the Bitcoin Blockchain, and it is therefore the original and only true Bitcoin Network. Paragraphs 14 to 17 of the APoC are repeated.
- 8.3. Dr Wright is Satoshi. No admissions are made as to D2-D12’s knowledge of the same.
- 8.4. The identity of Satoshi is not an issue that needs to be determined in this claim and the relevance of paragraph 5 is not explained and is in any event denied.
- 8.5. It is denied that the BTC Network was “*created by*” Satoshi, because (i) the blockchain utilised by the BTC Network (“**BTC Blockchain**”) is an unauthorised copy of the Bitcoin Blockchain, and (ii) it operates using software that implements a protocol (“**BTC Protocol**”) that has been amended from the Bitcoin Protocol that is still used on the BSV Network.
9. As to the paper entitled ‘*Bitcoin: A Peer-to-Peer Electronic Cash System*’ (“**Bitcoin White Paper**”) referred to in paragraph 6 and the sub-paragraphs that follow, the relevance of the same to the relief sought in the Claim is denied. The BTC Network is not operated consistently with the Bitcoin White Paper. The remainder of this Reply is without prejudice to that denial of relevance.
10. As to the first sentence of paragraph 6 and sub-paragraphs 6.1 and 6.2, it is denied that the Bitcoin White Paper was ever released under the MIT Licence. In any event, the Bitcoin White Paper is not software, so the MIT Licence cannot apply to it.
11. As to sub-paragraph 6.3:
  - 11.1. Save that the definition of ‘Bitcoin System’ used by the 2<sup>nd</sup> to 12<sup>th</sup> Defendants is denied, for the reasons stated at paragraph 15 of this Reply, the first sentence is admitted.
  - 11.2. As to the second sentence, the only “*consensus mechanism*” involving nodes described in the Bitcoin White Paper relates to their validation of transactions and acceptance of a new block on the blockchain.

- 11.3. It is denied that the Bitcoin White Paper described this “*consensus mechanism*” as ‘decentralised’. While nodes may work individually, and no central body is required to oversee the validation process, the apt description of the consensual validation process is ‘distributed’ not ‘decentralised’. This is because nodes simply follow the protocol of the Network in question, which protocol is set by the developer or developers in control of the particular Network at that time (“**Developers**”).
- 11.4. The third sentence is admitted.
12. As to sub-paragraph 6.4, while the definition of ‘nodes’ used by the 2<sup>nd</sup> to 12<sup>th</sup> Defendants is noted, it is denied that it is appropriate, and the definition is therefore not adopted:
- 12.1. Each Network comprises a collection of nodes (as properly described in sub-paragraph 12.2 and 12.3 of this Reply) which each run software implementing the protocol of the Network in question, the development of which protocol is controlled by the Developer(s) of that Network. The Developers also control the development of the base software for the Network that implements the protocol (“**Software**”). In order to be able to participate in a particular Network, the users and nodes are required to run the Software (or other software that implements the protocol, and which mirrors the core features of the Software). There are two primary classes of Software in the Networks: (i) the full version required for mining used by nodes (properly so called) (“**Node Software**”); and (ii) a lightweight version used by non-nodes (users), which cannot be used for mining, but instead allows users to verify any relevant transactions through Simplified Payment Verification (“**Client Software**”). The Node Software enables the nodes, by consensus, to validate transactions on that Network’s blockchain.
- 12.2. It is denied that the definition of ‘nodes’ given in sub-paragraph 6.4 accurately reflects the description of nodes given in either sub-paragraph 6.3 or the Bitcoin White Paper, in particular sections 5 and 8 (the relevance of the Bitcoin White Paper to the relief sought being denied in any event, as explained above).
- 12.3. Section 5 of the Bitcoin White Paper makes it clear that a node is a computer (in practice, it is generally a pool of computers acting in concert) that engages in proof-of-work (a process often referred to as ‘mining’) and, having done so,

extends the blockchain of the Network in question. When TTL refers to a ‘node’ that is what it means by the term.

- 12.4. It is denied that any “*computer running the relevant software that connects to other nodes running that same piece of software*” is a node; some computers on the Networks, (to the extent relevant, described as ‘users’ in section 8 of the Bitcoin White Paper), run the Client Software and do not undertake mining or validate transactions for themselves – and they are not nodes properly so-called.
- 12.5. Save as aforesaid, sub-paragraph 6.4 is denied.
13. As to sub-paragraph 6.5:
  - 13.1. Sub-paragraph 11.3 of this Reply is repeated; the consensual validation process undertaken by nodes is distributed not decentralised.
  - 13.2. It is noted that the only aspect of the Networks’ operation that the 2<sup>nd</sup> to 12<sup>th</sup> Defendants claim to be ‘decentralised’ is the consensual process of validating transactions undertaken by nodes; they rightly do not claim that the process of amending the protocol that must be implemented by any Software that wishes to operate on that Network or amending the Software itself is decentralised.
14. As to paragraph 7:
  - 14.1. It is denied that the software referred to therein should be defined as the ‘Original BTC Software’; the only Software to implement the Bitcoin Protocol is used on the BSV Network (“**Bitcoin Software**”).
  - 14.2. The paragraph is otherwise admitted.
15. As to paragraph 8, it is denied that the 2<sup>nd</sup> to 12<sup>th</sup> Defendants’ defined term of “Bitcoin System” is accurate because it is premised on the false contention that the BTC Network is the original and a true Network; the BSV Network is the original and only true Network. In that regard, paragraphs 15 to 17 of the APoC are repeated. Further:
  - 15.1. The composition of the BTC Network is as stated at sub-paragraph 12.1 of this Reply. Insofar as the constitution of the “Bitcoin System” (intending to refer to BTC) as defined by the 2<sup>nd</sup> to 12<sup>th</sup> Defendants differs from that description, it is denied.

- 15.2. As to sub-paragraph 8.1, the BTC Network comprises a network of nodes that each operate Node Software that implements the BTC Protocol (which BTC Protocol is updated by the 2<sup>nd</sup> to 12<sup>th</sup> Defendants from time to time) (“**BTC Node Software**”). The BTC Node Software enables those nodes to mine the BTC Network by competing to extend the BTC Blockchain.
- 15.3. As to sub-paragraph 8.2, it is admitted that the BTC Blockchain operates in the way stated.
- 15.4. As to sub-paragraph 8.3.1, the software released by Satoshi on 8 January 2009 was the Bitcoin Software. The paragraph is otherwise admitted.
- 15.5. As to sub-paragraph 8.3.2:
  - 15.5.1. It is denied that a “*community of contributors*” dictates the relevant development of the Software used on any of the Networks. The development of the protocol is controlled by the Developers; and the Software has to follow (in the sense that it has to implement) the protocol of that Network. It follows that the Developers also control the Software. Nodes have to run the Node Software (or other software that implements the protocol, and which mirrors the core features of the Node Software) if they wish to participate in the Network.
  - 15.5.2. While any person can *propose* changes to the protocol or the Software of each Network, changes to that protocol or the Software will be effected only when approved by the Developer(s) in control of the Network in question. This is, for example, analogous to a person proposing a change to Microsoft's products and software.
  - 15.5.3. Effecting changes to any protocol on the Networks, or to the Software, on an ongoing basis cannot be done without some individual or individuals having control over the process (for example, to ensure that no bugs arise, to make necessary upgrades and to ensure a consistent approach to its development).
  - 15.5.4. In any case, as a matter of fact, the 2<sup>nd</sup> to 12<sup>th</sup> Defendants have ultimate control over the BTC Protocol that is implemented by the BTC Network's Software (“**BTC Software**”), and over the BTC Software

itself (and any other software used has to implement the protocol and mirror the core features of the BTC Software).

15.5.5. Insofar as relevant, which is denied, the 2<sup>nd</sup> to 12<sup>th</sup> Defendants are required to prove that the most popular BTC Software implementing the BTC Protocol is called Bitcoin Core.

15.6. As to sub-paragraph 8.3.3, it is irrelevant that various versions of software can be used by nodes on the BTC Network, because each version that allows nodes to mine the BTC Network implements the BTC Protocol that is determined and controlled by the 2<sup>nd</sup> to 12<sup>th</sup> Defendants and has to be consistent with the core features of the BTC Software controlled by the Developers. In that regard, for example:

15.6.1. Libbitcoin (<https://libbitcoin.info/>) is a version of the BTC Software which implements the BTC Protocol, as amended from time to time, and has the front-end removed (including the Graphics User Interface) in order to make it faster.

15.6.2. btcd (<https://github.com/btcsuite/btcd>) is another version of the BTC Software which implements the BTC Protocol, as amended from time to time, and has the wallet feature removed.

16. As to sub-paragraph 8.4:

16.1. It is admitted that nodes validate transactions in accordance with a set of rules.

16.2. These rules are part of the protocol of each Network, which protocol is controlled by the Developer(s) of the Network in question and implemented by each Network's Software.

16.3. If nodes wish to mine a Network, they have to accept the protocol of that Network.

16.4. The 2<sup>nd</sup> to 12<sup>th</sup> Defendants are understood to use 'Consensus Rules' as a misleading term for the BTC Protocol. This term is misleading because it implies that nodes have some say in the formulation of the BTC Protocol, when it is in fact the 2<sup>nd</sup> to 12<sup>th</sup> Defendants who control its development, with the nodes simply implementing the protocol made available to them.

17. Save that the mechanism for validating transactions is not decentralised - it is set by the Developers in control of each Network by way of the protocol – and that the reference to

‘Consensus Rule’ should be replaced by ‘the relevant protocol’, sub-paragraph 8.5 is admitted.

18. Paragraph 9 is denied:

18.1. The 2<sup>nd</sup> to 12<sup>th</sup> Defendants control the development of the BTC Protocol. Any BTC Node Software that allows nodes to mine the BTC Network must implement the BTC Protocol, as updated by the 2<sup>nd</sup> to 12<sup>th</sup> Defendants from time to time. Moreover, the Developers control the BTC Software and any other software that may be used on the BTC Network has to be compatible with the core features of the BTC Software (and the BTC Protocol).

18.2. Sub-paragraphs 15.5.1 to 15.5.4 of this Reply are repeated.

19. Sub-paragraph 9.1 is denied: whether or not the 2<sup>nd</sup> to 12<sup>th</sup> Defendants *in fact* control the BTC Protocol and BTC Software cannot be determined by what Satoshi “*envisaged*”.

20. Sub-paragraphs 9.2 and 9.3 are denied:

20.1. While each person operating a node is *theoretically* free to decide whether to continue to run any particular software, run alternative software, or cease operating as a node altogether, *in reality*, persons operating nodes are not free so to act, because they are highly unlikely to do anything that would prevent them from mining, as they are running large commercial enterprises and their conduct is governed by commercial (not ideological) imperatives, including a need to continue operating and making profits (and to recoup, and have the benefit of, the sunk costs of their investment).

20.2. If nodes wish to continue mining the Network in question, they can only run software that implements the protocol of that Network and that contains the core features of the Software, each of which has been approved by the Developers in control of the Network. Sub-paragraphs 15.5 and 18.1 of this Reply are repeated.

20.3. If the Developer(s) in control of a Network agree to update the protocol (and/or the Software) of that Network and a node chooses to run software that does not implement that updated protocol (or is not consistent with the core features of the updated Software) then within a short period of time following the update the node will cease to be able to mine that Network.



- 20.4. If nodes did choose to leave the Network, they would simply be replaced by new mining companies given the vast profits to be made from mining.
- 20.5. An airdrop (or so-called “hard fork”) only occurs where: (i) there is a dispute between the Developer(s) in control of a Network as to the characteristics of the protocol of that Network or as to how the protocol of that Network should develop; (ii) some of those Developer(s) then produce a new, alternative protocol and Software which copies the blockchain of the existing Network and implements that new protocol; and (iii) some nodes implement that alternative protocol through the alternative Software.
- 20.6. Where the Developers in control of a Network all support one particular protocol, as would be the case if all the Developers complied with the order sought by TTL, there cannot be an airdrop (or a ‘hard fork’ as the 2<sup>nd</sup> to 12<sup>th</sup> Defendants have erroneously called such an occurrence).
21. As to paragraph 10, it is admitted that Satoshi released the Bitcoin Software implementing the Bitcoin Protocol under the terms of the MIT Licence.
22. As to sub-paragraphs 10.1 to 10.3, it is admitted that they contain an (incomplete) quotation from the MIT Licence.
23. As to sub-paragraph 11.1:
  - 23.1. While it is admitted that BTC Software is, and has been at all material times, ‘open source’ in the sense that it is freely available to the general public to use, modify and distribute, it is denied that any software can be successfully used by nodes on the BTC Network unless that software implements the BTC Protocol, as amended by the 2<sup>nd</sup> to 12<sup>th</sup> Defendants from time to time, and is sufficiently compatible with the core features of the BTC Software, as also controlled by them.
  - 23.2. It is admitted that the BTC Software is non-proprietary in the sense that it is widely licensed in the public domain and the copyright notice contained in the terms of the MIT Licence pursuant to which it is released makes clear that it can be used provided the copyright notice is included. However, it is denied that this means that it is free from control by anyone; for any version of the BTC Software to permit nodes to mine the BTC Network, it must implement the BTC Protocol, the development of which protocol is controlled by the 2<sup>nd</sup> to 12<sup>th</sup> Defendants,

and the core features of the BTC Software are controlled by the 2<sup>nd</sup> to 12<sup>th</sup> Defendants.

24. As to sub-paragraph 11.2, it is admitted that anyone is able to *propose* changes to the BTC Software, but it is denied that contributors have any control over whether their proposed changes are implemented – that control lies with the 2<sup>nd</sup> to 12<sup>th</sup> Defendants.
25. As to sub-paragraph 11.3, it is denied that in practice contributors are able to create (and successfully implement) software that is incompatible with the BTC Protocol and BTC Software, for the reasons set out herein.
26. As to sub-paragraph 11.4, it is admitted that there are individuals who propose changes to the BTC Protocol who are not the Developers in control of the BTC Network, but for the reasons already set out, their relevance is denied. The second sentence is denied.
27. As to paragraph 12, it is denied that there was a “*community*” of contributors or that Satoshi ceased to have any role in developing Bitcoin tokens in 2011.
28. Paragraph 13 and sub-paragraphs 13.1 and 13.2 are admitted. However, the Bitcoin Blockchain and the blockchains utilised by the other Networks (“**Other Networks**”) are not encrypted, nor are records of transactions in Bitcoin stored on the relevant blockchain. It is therefore wrong to describe the BSV Network, or any of the other Networks, as encrypted, or Bitcoin as a cryptocurrency. There is no encryption in Bitcoin.
29. As to sub-paragraph 13.3:
  - 29.1. It is denied that transfers of Bitcoin tokens can only be effected by using a private key:
    - 29.1.1. The scripting language utilised in Bitcoin allows for the creation of a set of conditions under which the coins can be spent other than by way of digital signatures. One such example is a hash puzzle transaction, whereby coins are locked in such a way that whoever can produce a data piece that, when hashed, matches a specific hash value, can spend them. This type of transaction does not require a digital signature for validation.
    - 29.1.2. The Developers of a Network could create a patch to the Software of that Network which could allow a user (such as TTL) to access its Bitcoin tokens.

- 29.1.3. The Developers could broadcast a transaction involving the transfer of tokens to a newly assigned address or locking script, controlled by the owner.
- 29.2. It is denied that possession of the private key associated with a public address is required for ownership of the Bitcoin tokens at that public address; as the Fourteenth Defendant agrees (at sub-paragraphs 33.2 and 36.5 of his Defence), there is no necessary connection between knowledge of a private key and ownership of the Bitcoin tokens registered to the public address associated with that private key.
30. Save that the term “cryptocurrency” is an inapposite term for Bitcoin for the reasons set out in paragraph 28 of this Reply, sub-paragraph 13.4 is admitted.
31. As to paragraph 14, this is admitted. As set out in paragraph 10 of the APoC, the validation, verification and announcement process is virtually instantaneous.
32. As to paragraph 15:
- 32.1. The first sentence is admitted.
- 32.2. The second sentence is denied: any node that is properly so called undertakes mining, otherwise it is not a node. Sub-paragraphs 12.2 to 12.4 of this Reply are repeated.
33. As to paragraph 16:
- 33.1. It is denied that ‘non-mining nodes’ exist or that users (which the 2<sup>nd</sup> to 12<sup>th</sup> Defendants appear erroneously to call ‘non-mining nodes’) on any of the Networks can validate transactions for themselves (or “*conduct a validation process*” as alleged at sub-paragraph 16.5).
- 33.2. Further, as to sub-paragraph 16.6, users of any particular Network, who typically use the Client Software, only add copies of the block *headers* of validated blocks to the copies they keep of the blockchain of the Network in question; they do not necessarily download the full blocks containing a list of all transactions constituting that blockchain.
- 33.3. As to sub-paragraph 16.7, nodes on any Network always seek to add blocks to and keep copies of the longest, honest (that is, one which has followed the relevant protocol) proof-of-work chain of that Network, and users on any

Network always keep copies of the longest, honest proof-of-work chain of that Network (albeit generally only the block headers) for verification purposes.

34. As to paragraph 17:
  - 34.1. It is admitted that nodes are only able to mine a Network if they use Node Software that implements that particular Network's protocol. Paragraphs 15.5 and 16 of this Reply are repeated.
  - 34.2. It is further admitted that non-node users wishing to verify transactions by reference to the validation activities of nodes on a Network can use Client Software implementing the protocol of the Network in question.
  - 34.3. As explained at paragraphs 20.5 and 20.6 of this Reply and paragraph 14(c) of the APoC, the 2<sup>nd</sup> to 12<sup>th</sup> Defendants are using the term 'hard fork' to mean what is properly termed an 'airdrop', and as explained at paragraph 16 of this Reply, they are confusing what they term 'Consensus Rules' with the protocol of the Network in question, which protocol is implemented by that Network's Software.

**B2: ALLEGED 'FORKS'**

35. As to paragraph 18, sub-paragraphs 15.5 and 15.6 and paragraphs 18 and 20 of this Reply are repeated.
36. As to paragraph 19:
  - 36.1. It is the 2<sup>nd</sup> to 12<sup>th</sup> Defendants who determine whether to authorise any proposed modifications to the BTC Protocol or to the core features of the BTC Software so as to bring them into effect.
  - 36.2. Modifications to any version of the BTC Software that do not modify the BTC Protocol implemented by the software do not cause an airdrop and are irrelevant for the purposes of this claim. TTL pleads to the remainder of paragraph 19 on that basis.
  - 36.3. The 2<sup>nd</sup> to 12<sup>th</sup> Defendants conspicuously fail to particularise or explain the "*different procedure*" said to govern changes to the 'Consensus Rules', namely the BTC Protocol, anywhere in the D2-D12 Defence.
37. Sub-paragraphs 19.1 and 19.2 are admitted.

38. Sub-paragraphs 19.3 and 19.4 are required to be proved, save that it is denied that operators of nodes are in reality free to decide whether to run updated Software. Nodes who wish to continue to mine BTC are required to run BTC Node Software (controlled by the 2<sup>nd</sup> to 12<sup>th</sup> Defendants) or software compatible with the same, either of which must necessarily implement the BTC Protocol, as controlled and updated from time to time by the 2<sup>nd</sup> to 12<sup>th</sup> Defendants.
39. As to paragraph 20 and its sub-paragraphs:
  - 39.1. So-called ‘soft forks’ are irrelevant to the claim.
  - 39.2. The 2<sup>nd</sup> to 12<sup>th</sup> Defendants describe a situation where the Developers in control of a particular Network update that Network’s protocol and any node that wishes to continue consistently being able to mine the Network in question must implement that updated protocol (through appropriate Node Software containing core features controlled by the 2<sup>nd</sup> to 12<sup>th</sup> Defendants).
  - 39.3. In the situation described the Developers of the Network do not disagree about the development of that Network’s protocol, such that some promote a rival protocol that creates a new network.
40. As to paragraph 21 and its sub-paragraphs, the process by which a new network is created is properly described as an airdrop and involves the Developers of a Network disagreeing on how the Network’s protocol should be developed and promoting two different protocols. Paragraphs 20.5 and 20.6 of this Reply are repeated.
41. Paragraph 22 is inadequately particularised and therefore cannot be pleaded to. So-called ‘soft forks’ are irrelevant to the claim.
42. Paragraph 23 is inadequately particularised and therefore cannot be pleaded to.
43. As to paragraphs 24 to 24.4:
  - 43.1. Paragraph 15 of the APoC is repeated.
  - 43.2. It is denied that the airdrop that took place on 1 August 2017 was caused because some Developers did not wish to increase the size of the blocks that could be mined on the network; most of the Developers agreed that the overall block size should be increased, and their disagreement was over *how* to achieve that. The Developers who ultimately continued to control the development of the Bitcoin Protocol wished to use the existing Bitcoin Protocol, so as to maintain the

traceability of transactions, whereas the other Developers who split off wished to make amendments to the Bitcoin Protocol – and those dissenting Developers ultimately produced the BTC Protocol.

- 43.3. Some of the nodes that mined the original and only true Bitcoin network (now the BSV Network) started using Node Software that implemented the new BTC Protocol, and they therefore started mining BTC tokens on the BTC Blockchain as part of the new BTC Network.
- 43.4. Prior to 1 August 2017, the original and only true Bitcoin network was referred to as “XBT” or “BTC”. Following the airdrop on 1 August 2017, it adopted the BCH ticker, and the new network took over the BTC ticker.
44. As to sub-paragraph 24.5, paragraph 15(c) of the APoC is repeated. It is admitted that the airdrop led to the market value of the original and only true Bitcoin tokens prior to the airdrop being spread between those pre-existing tokens and the new tokens.
45. As to paragraph 25:
  - 45.1. Paragraphs 16 and 17 of the APoC are repeated.
  - 45.2. As to sub-paragraph 25.1:
    - 45.2.1. It is admitted that Dr Wright established nChain.
    - 45.2.2. It is denied that Bitcoin Satoshi Vision made any amendment to the Bitcoin Protocol, or that BSV Software started running only in 2018.
  - 45.3. As to sub-paragraphs 25.2 to 25.4:
    - 45.3.1. Subparagraph 25.2 is denied.
    - 45.3.2. On 15 November 2018, some of the Developers then in control of the original and only true Bitcoin Network, made available Software that implemented a new amended protocol and copied the Bitcoin Blockchain. This is the BCH Software referred to in paragraphs 25.3 and 25.4. It was the adoption of this new BCH Software that caused an airdrop and created a new network.
    - 45.3.3. Following the airdrop, the original and only true Bitcoin network adopted the ‘BSV’ ticker (BSV Network), and the new network which

used a protocol that diverged from the Bitcoin Protocol adopted the ‘BCH’ ticker: BCH Network.

45.4. As to sub-paragraph 25.5:

45.4.1. It is admitted that the airdrop on 15 November 2018 led to holders of what had become known as BSV tokens on the BSV Network becoming holders additionally of an equivalent amount of new tokens on the new BCH Network, and to the market value of the original tokens being spread between the original BSV tokens and the new BCH tokens.

45.4.2. Paragraph 25.5 appears to be mistaken as it contains the values for BTC tokens (not BCH tokens).

45.5. As to sub-paragraph 25.6, it is denied that BSV is “*rarely used in the cryptocurrency community*” (whatever that is supposed to mean). Approximately 95% of all transactions globally conducted on blockchain networks today are conducted on the BSV Network. It is admitted that the value of one BTC token is presently greater than the value of one BSV token but the relevance of the same is denied.

**C: APoC PART I - PARTIES**

46. Paragraph 26 is noted. However, the approach adopted by the 2<sup>nd</sup> to 12<sup>th</sup> Defendants is grossly disproportionate, unnecessary, and contrary to the overriding objective. TTL’s rights are reserved in relation thereto.

47. As to sub-paragraph 27.1, paragraphs 7 and 8 of this Reply are repeated.

48. Sub-paragraphs 28.4 – 28.4.5 are of no relevance to the claim and TTL does not plead to them.

49. As to sub-paragraph 28.4.6:

49.1. It is denied that Dr Wright has given deliberately false evidence as to matters concerning his scientific standing. The only example pleaded of such alleged conduct is at paragraph 54.9.6 of the D2-D12 Defence, which is responded to below.

49.2. The inference it is alleged should be drawn from the alleged conduct is, like the alleged conduct, denied.

50. Sub-paragraph 28.5 is of no relevance to the claim and TTL does not plead to it.
51. Sub-paragraph 29.1 is of no relevance to the claim and TTL does not plead to it.

**D: ALLEGED ‘CASE’ AS TO ABUSE OF PROCESS**

52. Paragraph 30 is denied and is in any event irrelevant.
  - 52.1. If, as alleged (incorrectly), it were to be correct to find that Dr Wright and TTL do not and never did have any interest of any kind in the Bitcoin in the Addresses, then the Claim would fail.
  - 52.2. On the other hand, in circumstances where (as is in fact the case) the Court concludes TTL is the owner of the Bitcoin in the Addresses, the premise of paragraph 30 would therefore be incorrect and there would be no basis for alleging an abuse of process.
  - 52.3. The allegation of abuse of process is therefore misconceived and irrelevant.

**E: APoC PART II – BITCOIN**

53. As to paragraph 31.2:
  - 53.1. This is a matter that the 2<sup>nd</sup> to 12<sup>th</sup> Defendants are able to admit or deny, and accordingly they are taken as admitting that Bitcoin tokens are property capable of being owned.
  - 53.2. Moreover, paragraph 31.2 is inconsistent with paragraph 13.3, which accepts that there is “ownership” of Bitcoin tokens, consistent only with Bitcoin tokens being property that is capable of being owned.
54. As to sub-paragraph 32.1, save for the admission therein, the relevance is denied. Without prejudice to the foregoing, whether Bitcoin tokens held by third-party exchanges are owned by the exchange in question or by the customer depends (at least in part) on the terms under which they are held and whether or not the exchange moves deposited Bitcoin tokens into a central unsegregated pool and then credits the customer’s account with the deposit amount against which the customer is permitted to draw.
55. As to sub-paragraph 33.2:
  - 55.1. It is admitted that transactions involving Bitcoin can take place ‘off-chain’, and that the Bitcoin Lightning Network facilitates such transactions.



- 55.2. The relevance of these facts is not explained and is denied.
56. As to the first sentence of sub-paragraph 35.3, sub-paragraphs 15.5.1 to 15.5.3 and 15.6 of this Reply are repeated.
57. As to sub-paragraph 36.1, save for the admission therein, which is noted:
- 57.1. Paragraphs 12 and 33 of this Reply is repeated.
- 57.2. As to paragraph 36.1(ii), paragraph 11 of the APoC is repeated. The Networks automatically release Bitcoin tokens to miners as payment for each block they mine and miners are also automatically paid a transaction fee (in Bitcoin) for each transaction by the persons spending Bitcoin tokens. To the extent it is inconsistent with the foregoing, paragraph 36.1(ii) is denied.
58. As to sub-paragraph 37.1:
- 58.1. The purported reason given for the denial in the first sentence does not follow from the matters asserted in the second sentence.
- 58.2. As to the second sentence, while the number of nodes controlling the hash power varies with time, the number of nodes and the hash power they control is always information that is publicly available.
59. As to sub-paragraph 38.4.1, this is admitted. The reference to the 1Feex Address with a lowercase 'F' was included in error. It in fact has an upper case 'F' as with all of the 1Feex Addresses.
60. Sub-paragraphs 39.2.1 and 39.2.2 are denied for the reasons set out above (in the paragraphs which answer the paragraphs relied upon by the 2<sup>nd</sup> to 12<sup>th</sup> Defendants).
61. As to sub-paragraph 41.2, paragraph 45 of this Reply is repeated.
62. As to sub-paragraph 44.1, save for the admission therein, it is embarrassing for its want of particularity and cannot be pleaded to.
63. As to sub-paragraph 44.2:
- 63.1. It is accepted that it is the mining/validation process that prevents double-spending and not the use of private keys.
- 63.2. The second sentence is argumentative and inappropriate for a pleading.

- 63.3. There is no “*decentralized setting*” insofar as this unparticularised term can be understood.
64. As to sub-paragraphs 45.1:
- 64.1. Sub-paragraph 29.2 of this Reply is repeated.
- 64.2. The second sentence is therefore denied.
- 64.3. To the extent that it is alleged, it is denied that the Other Networks currently operate consistently with the Bitcoin Protocol invented by Satoshi.
- 64.4. In any event, Satoshi’s alleged statement is insufficiently particularised and cannot be pleaded to.
65. As to sub-paragraph 46.1:
- 65.1. The words in brackets are argumentative and inappropriate for a pleading (and irrelevant).
66. As to sub-paragraph 46.1.1:
- 66.1. This is denied and paragraph 21 of the APoC and paragraph 29 of this Reply are repeated.
- 66.2. The 2<sup>nd</sup> to 12<sup>th</sup> Defendants have failed to particularise the alleged “*foundational principles of the Bitcoin System*” or explain why it is said they can be identified as such.
67. As to sub-paragraph 46.1.2:
- 67.1. If certain owners of Bitcoin have a desire or expectation of complete anonymity, which is not admitted, that is misplaced.
- 67.2. It is denied that the identities of persons who own Bitcoin tokens are never disclosed or that their anonymity is guaranteed, because such persons (i) will need to declare such ownership to the relevant tax authorities for tax purposes if they sell their Bitcoin tokens for profit, (ii) are often required to divulge their identities as part of money laundering checks, (iii) are required by many exchanges and hosting wallets to verify their identities; and (iv) will often reveal their identities to their counterparties to any given transaction.

- 67.3. Insofar as relevant, the Bitcoin White Paper, at section 10, proposes that public keys be anonymous in order to achieve a degree of privacy similar to, but not greater than, that enjoyed by users of traditional banking. The term ‘anonymous’ in the Bitcoin White Paper does not imply that users are fully anonymous. Instead, it indicates that user identity is separate from the Bitcoin Blockchain (see the diagram at section 10 of the Bitcoin White Paper).
68. As to sub-paragraph 46.2, the responses to paragraphs 9 and 46.1 of the D2-D12 Defence are repeated. The first sentence of paragraph 46.2 is therefore denied (except for the admission therein).
69. The second sentence of sub-paragraph 46.3 is denied for the reasons set out in paragraphs 18 to 20 of this Reply. In addition, the reference to the “*so-called*” legitimate owner is not understood.
70. Except for the admission therein, paragraph 47 is embarrassing for its want of particularity and cannot be pleaded to pending its proper particularisation.
71. The first sentence of paragraph 48 is denied. The second sentence of paragraph 48 is argumentative and inappropriate in a pleading.
72. As to sub-paragraph 49.1, sub-paragraphs 15.5.1 to 15.5.3 and 15.6 and paragraphs 18 to 20 and 24 to 26 of this Reply are repeated. It is noted that paragraph 49.1.1 relies on paragraph 11 of the D2-D12 Defence, which itself contains a bare assertion, without proper particulars, as to the role of the 2<sup>nd</sup> to 12<sup>th</sup> Defendants. The third sentence is denied (in the sense that users are required to use software that is compatible with the core features of the BTC Software and which, in any event, implements the BTC Protocol). Sub-paragraph 49.1.2 is therefore denied, and sub-paragraph 49.1.3 is irrelevant.
73. Sub-paragraph 49.2.3 is denied: the admission at sub-paragraph 49.2 confirms that the 2<sup>nd</sup> to 12<sup>th</sup> Defendants all have a financial interest in the continued operation of the BTC Network.
74. As to sub-paragraph 49.2.4, the 2<sup>nd</sup> to 12<sup>th</sup> Defendants are named as Defendants to the claim because they are in control of the BTC Network; general contributors who *propose* (but cannot *authorise*) changes to the BTC Protocol are not in control of the BTC Network and do not owe TTL the alleged duties. No admissions are, however, made as to the payments such individuals receive.

75. The first sentence of sub-paragraph 50.1 is internally contradictory and in any event denied. The Developers control the Networks.
76. As to sub-paragraph 50.3:
  - 76.1. Sub-paragraphs 15.5.1 to 15.5.3 and 15.6 and paragraphs 18 to 20 and 24 to 26 of this Reply are repeated.
  - 76.2. As to sub-paragraphs 50.3.1 – 50.3.5, the Defendants identified are still in control of the BTC Network even if they do not publicise their control.
77. Sub-paragraph 52.1 is admitted.
78. As to sub-paragraph 52.2, the 2<sup>nd</sup> to 12<sup>th</sup> Defendants are the final arbiters of any changes to the BTC Software and as to whether to change the BTC Protocol. Other repositories may contain versions of software that is consistent with the core features of the BTC Software, and which also implements the BTC Protocol, both of which are controlled by the BTC Developers. The following paragraphs, which respond to specific pleas in relation to each of the 2<sup>nd</sup> to 12<sup>th</sup> Defendants, is subject to the foregoing.
79. Sub-paragraph 52.3 is denied. Anyone who can control the BTC GitHub can control the BTC Protocol. Paragraph 20 of this Reply is repeated.
80. As to sub-paragraph 52.4.1:
  - 80.1. The Second Defendant had control of the BTC Network at all material times and remains in control of the BTC Network even if he does not publicise his control.
  - 80.2. On the Second Defendant's own case, he had the relevant credentials at the time TTL first requested his assistance in regaining access to his Bitcoin in the Addresses in June 2020 and at the time TTL served its letter before action in respect of this claim in February 2021, and he gave up his access credentials after this Claim was served on him on 15 June 2021.
81. As to sub-paragraph 52.4.2:
  - 81.1. The Third Defendant had control of the BTC Network at all material times and remains in control of the BTC Network even if he does not publicise his control.
  - 81.2. On the Third Defendant's own case, he had the relevant credentials at the time TTL first requested his assistance in regaining access to his Bitcoin in the Addresses in June 2020 and at the time TTL served its letter before action in

respect of this claim in February 2021, and he gave up his access credentials after this Claim was served on him on 20 August 2021.

82. As to sub-paragraph 52.4.3, the Fourth Defendant's admission that he still has the relevant credentials is noted: he had control of the BTC Network at all material times and is in control of the BTC Network.
83. As to sub-paragraph 52.4.4:
  - 83.1. The Fifth Defendant had control of the BTC Network at all material times and remains in control of the BTC Network even if he does not publicise his control.
  - 83.2. On the Fifth Defendant's own case, he had the relevant credentials at the time TTL served its letter before action in respect of this claim in February 2021, and he gave up his access credentials after this Claim was served on him on 6 July 2021.
84. As to sub-paragraph 52.4.5, the Sixth Defendant had control of the BTC Network at all material times and remains in control of the BTC Network even if he does not publicise his control.
85. As to sub-paragraph 52.4.6, the Seventh Defendant's admission that he still has the relevant credentials is noted: he had control of the BTC Network at all material times and remains in control of the BTC Network.
86. As to sub-paragraph 52.4.7, the Twelfth Defendant had control of the BTC Network at all material times and remains in control of the BTC Network even if he does not publicise his control.
87. As to sub-paragraph 52.5, the Eighth, Ninth, Tenth and Eleventh Defendants had control of the BTC Network at all material times and remain in control of the BTC Network.
88. As to sub-paragraph 53.2.4, paragraphs 15.5 and 20 of this Reply is repeated.
89. As to sub-paragraph 53.2.6, second sentence, it is admitted, but its relevance is not explained, and is denied.
90. As to sub-paragraph 53.2.7, the 2<sup>nd</sup> to 12<sup>th</sup> Defendants have control over the BTC Network through their control of the BTC Protocol and/or the BTC Software. Paragraphs 15.5 and 20 of this Reply are repeated. The level of influence that Satoshi had in comparison to the 2<sup>nd</sup> to 12<sup>th</sup> Defendants is irrelevant to the issues in dispute.

91. As to sub-paragraph 53.3.1:

91.1. The second sentence is misconceived. If Developers consider it unclear that a person owns the Bitcoin tokens claimed, they could require that person to obtain a court order as to ownership.

91.2. The third sentence is denied. Paragraphs 15.5 and 20 of this Reply are repeated.

**F: TTL'S OWNERSHIP**

92. Paragraph 54 is denied. TTL is the owner of the Bitcoin tokens in the Addresses. None of the allegations made in the sub-paragraphs of paragraph 54, individually or together (even were they to be correct), are sufficient to support an inference that none of TTL, any entity related to Dr Wright or Dr Wright owns or has ever owned the Bitcoin tokens in the Addresses. The remainder is without prejudice to the foregoing.

93. As to sub-paragraph 54.1:

93.1. This is denied in respect of the 1Feex Address. The purchase order relied upon by TTL in respect of the Bitcoin in the 1Feex Address ("**Purchase Order**") is genuine.

93.2. It is admitted that there is no contemporaneous record of the *purchase* of the Bitcoin in the 12ib7 Address.

94. As to sub-paragraph 54.2:

94.1. It is denied that the Purchase Order is a forgery.

94.2. Dr Wright instructed an online Russian exchange called WMIRK.com ("**WMIRK**") by telephone to buy the Bitcoin tokens that were transferred to the 1Feex Address, but he did not create the Purchase Order.

94.3. Dr Wright believes that his then wife, Lynn (Wright) ("**Lynn**"), created the Purchase Order, because the document's metadata indicates as much, and it was Lynn who dealt with the administrative side of the purchase.

94.4. TTL does not know whether the Purchase Order was required by WMIRK, whether it was even sent to WMIRK, or whether it was simply created as a written internal record of the order that was placed by telephone.

95. Sub-paragraph 54.2.1 is denied. Any similarity between the Purchase Order and a template released in 2015 is coincidental or, it is inferred, the result of the template being based on a format already used for purchase orders.
96. As to sub-paragraph 54.2.2, it is admitted that there is a typographical error in the Purchase Order relating to the mining fee.
97. As to sub-paragraph 54.2.3, it is admitted that 80,000 rather than 79,956 Bitcoin tokens was stated in the Purchase Order. TTL is not aware of whether this was a typographical error or used by way of rounding.
98. As to sub-paragraph 54.2.4, it is admitted that the 1Feex Address is mistyped in the Purchase Order. This was, it is assumed, a typographical error by Lynn.
99. As to sub-paragraph 54.2.5:
  - 99.1. It is admitted that Liberty Reserve dollars and Bitcoin tokens were both pegged approximately 1:1 with the US\$ at the date of the Purchase Order on 27 February 2011.
  - 99.2. However, the true value of Liberty Reserve Dollars was much lower because they could not be exchanged for assets of such value in US\$ as they could only be exchanged legitimately in a very limited number of places (there was no real market at that time).
100. As to sub-paragraph 54.3:
  - 100.1. The bald assertion that the 1Feex Address “*contains Bitcoin stolen from Mt Gox (a digital asset exchange which collapsed in 2014) in a hack that occurred in March 2011*” is denied, save that it is admitted that Mt Gox was a digital asset exchange that collapsed in 2014.
  - 100.2. The 2<sup>nd</sup> to 12<sup>th</sup> Defendants have inappropriately failed to plead any facts or matters in support of their bald assertions in that regard. Such assertions are liable to be struck out. TTL reserves its right to plead further to these allegations if they are properly particularised.
  - 100.3. The Bitcoin tokens registered to the 1Feex Address were not stolen from the Mt Gox exchange; they were transferred into the 1Feex Address on 1 March 2011, more than three months before the well-publicised Mt Gox hack took place in June 2011.

101. As to sub-paragraph 54.4:

101.1. The first two sentences are admitted.

101.2. In respect of the last sentence, Dr Wright did not use the 'message sign' function to prove to the ATO that he controlled the Bitcoin tokens in the Addresses when asked to do so, because, if he had done so, he would have contradicted his stated tax position that those assets were being managed outside Australia.

102. As to sub-paragraph 54.5:

102.1. It is liable to be struck out because in relying on Dr Wright's decision not to challenge formally the finding of the ATO regarding his ownership of the Bitcoin tokens in the Addresses in order to found an inference that neither he nor TTL owns the Bitcoin tokens in the Addresses, the 2<sup>nd</sup> to 12<sup>th</sup> Defendants are impliedly and necessarily relying on the findings of the ATO as evidence of their correctness, which is impermissible in these proceedings.

102.2. Findings made in other judicial or quasi-judicial proceedings between different parties are not admissible in English civil court proceedings as evidence of the correctness of those findings, and it is therefore an abuse of the court's process to plead in a defence in reliance (including implied reliance) upon such findings as evidence of their correctness.

102.3. TTL reserves its right to plead further to paragraph 54.5 in the event it is not struck out.

103. As to sub-paragraph 54.6:

103.1. The first sentence is admitted.

103.2. As to the second sentence, the list was emailed to Dr Wright by an anonymous third-party and was provided by him to the court pursuant to discovery rules with no warranty as to its accuracy. In any event, the list concerned Dr Wright's ownership not TTL's ownership.

104. Sub-paragraph 54.7 is admitted.

105. As to sub-paragraph 54.8, this is admitted.



106. As to sub-paragraph 54.9 and the sweeping statement regarding Dr Wright's general credibility contained in the first sentence, it is denied that Dr Wright has ever fabricated documents or provided deliberately false evidence.
107. As to sub-paragraphs 54.9.1 to 54.9.4, 54.9.6 and 54.9.7:
  - 107.1. These sub-paragraphs purportedly raise issues of fact to be determined at trial which are of no, or no sufficiently direct, relevance to the issues to be determined in the Claim.
  - 107.2. That being the case, and pending clarification from the 2<sup>nd</sup> to 12<sup>th</sup> Defendants as to (i) why such matters should properly form part of the trial of the Claim, and (ii) how, if at all, the 2<sup>nd</sup> to 12<sup>th</sup> Defendants intend to prove them, TTL's position is that they are not properly issues in the Claim.
  - 107.3. TTL reserves its right to apply to strike out these sub-paragraphs and/or to plead further to them as appropriate.
108. As to sub-paragraph 54.9.5, this is a repeat of paragraph 54.2, and the allegation therein is responded to at paragraphs 94 to 99 of this Reply.
109. Sub-paragraph 56.2 is denied. The sale of the Bitcoin tokens in the 1Feex Address was one of WMIRK's first transactions in Bitcoin tokens, and it did not undertake many, if any, other such transactions at that time.
110. As to the second sentence of sub-paragraph 60.2, sub-paragraph 29.2 of this Reply is repeated.

**G: THEFT OF THE TTL PRIVATE KEYS**

111. As to sub-paragraph 61.2, paragraphs 92 to 108 of this Reply are repeated
112. It is denied that any of the matters referenced in paragraph 62.3 is sufficient to support the inference alleged, which inference is in any event incorrect because there was a hack as set out in the APoC. The remainder is without prejudice to the foregoing.
113. As to sub-paragraph 62.3.1:
  - 113.1. It is admitted that the Bitcoin in the Addresses has not been moved since 2011.
  - 113.2. It is likely that the Bitcoin in the Addresses has not moved since the Hack because the Hackers:

- (i) have not yet been able to access the TTL Private Keys contained with the wiped wallet.dat files because of the complex algorithmic masking in place to protect them,
- (ii) may not have realised what they have, or which data relates to the Addresses, because it was not obvious from the description of the data contained in the KeePass application which stored the wallet.dat files that it related to the Addresses, and/or
- (iii) have cracked the algorithmic masking but are waiting for the attention that has been focused on the Addresses during the past three years to reduce before they seek to move the Bitcoin in the Addresses, so that they have a better chance of doing so without it being traced or their being identified.

114. As to sub-paragraph 62.3.2, its premise and the inference relied upon is denied:

114.1. The Hackers not only accessed and deleted but *wiped* the TTL Private Keys and the Keys Access Material, which means that they could not have been recovered or retrieved, either from the hard drives themselves, or the cloud-based back-ups.

114.2. Following the discovery of the Hack, Dr Wright himself wiped *only* the hard drives of two *other* computers connected to his home network. He did so in order to secure them, because he did not know whether the Hackers had hidden malware or other threats on them, and he did not wish the Hackers to obtain access to the confidential information that remained on those hard drives.

115. Sub-paragraph 62.3.3 is admitted. There would have been no purpose in contacting Microsoft or Google, because the TTL Private Keys and the Keys Access Material were *wiped*, not deleted, by the Hackers and wiped data cannot be recovered.

116. Sub-paragraph 62.3.4 is admitted. There is nothing surprising or suspicious about Dr Wright contacting the police the day after the Hack.

117. As to sub-paragraph 64.2, this is a repeat of sub-paragraph 62.3.4, the response to which is repeated.

**H: FIDUCIARY DUTIES AND BREACH OF FIDUCIARY DUTY**

118. As to sub-paragraph 67.1 (save for the denial in the first sentence), it is denied that the terms of the MIT Licence, properly construed, exclude liability for the breaches of fiduciary duty claimed. TTL's loss does not arise as a result of, from, out of, or in

connection with its use of the Bitcoin Software; it arises as a result of the 2<sup>nd</sup> to 12<sup>th</sup> Defendants' refusal to comply with their duties to restore TTL's control of its BTC tokens in the Addresses. The MIT Licence is therefore irrelevant to the claim. Further:

- 118.1. TTL is not subject to the terms of the MIT Licence in circumstances where TTL itself did not download or otherwise accept the Bitcoin Software.
  - 118.2. In any event, the purported exclusion of liability contained in the MIT Licence has no legal effect against TTL pursuant to either (i) Part 2 of the Consumer Rights Act 2015, because the terms of the MIT Licence are (a) unfair, and (b) insufficiently transparent as to the liability said to be excluded, or (ii) sections 3 and 11 of the Unfair Contract Terms Act 1977.
119. Furthermore, the MIT Licence cannot be read as excluding liability for breach of fiduciary duty in the absence of clear and unambiguous words to that effect.
120. As to sub-paragraph 67.2.2.
- 120.1. Paragraphs 70 to 74 of this Reply are repeated.
  - 120.2. The second sentence is denied. The Developers do have complete power over the system in which the digital assets are held.
121. As to sub-paragraph 67.2.3:
- 121.1. Sub-paragraph 29.1 and paragraph 67 of this Reply are repeated. Therefore, save for the admissions therein, sub-paragraph 67.2.3 is denied.
  - 121.2. It is denied that it is an absolute requirement of any of the Networks that private keys be used to transfer Bitcoin tokens. Paragraph 29.1 of this Reply is repeated.
  - 121.3. Further, it is denied that average reasonable users of the Networks would be aware of the precise design or unparticularised "*foundational principles*" of the Networks, or have any expectation as to how the Software operating each of the Networks would be developed, other than that those developing it would not act capriciously or unreasonably and, would vindicate owner's property rights and prefer the interests of owners of Bitcoin tokens over the interests of fraudsters.
  - 121.4. It is denied that the changes that TTL requests be made are contrary to the principles set out in the Bitcoin White Paper (the relevance of which to the relief

sought in the Claim is denied, as explained at paragraph 9 above) or to the design or any unparticularised “*foundational principles*” of the BTC Network.

122. As to sub-paragraph 67.2.4:

122.1. TTL has entrusted its BTC tokens to the 2<sup>nd</sup> to 12<sup>th</sup> Defendants by reason of their *role* controlling the development and operation of the BTC Network.

122.2. It is reasonable for users of the BTC Software to expect that those in control of its development (through their control of the BTC Protocol which it implements) would not act capriciously or unreasonably and would prefer the interests of owners of BTC tokens over the interests of fraudsters.

122.3. It is denied that the expectations of those generally “*in the cryptocurrency community*”, which term is unparticularised and unexplained, are relevant.

123. As to the second sentence of sub-paragraph 67.3.1, sub-paragraphs 15.5.1 to 15.5.3 and paragraphs 18 and 20 of this Reply are repeated.

124. As to the second and third sentences of sub-paragraph 67.4, sub-paragraph 29.1 and paragraphs 67, 121 and 122 of this Reply are repeated.

125. As to second and third sentences of sub-paragraph 67.5, paragraphs 18, 20, 121 and 122 of this Reply are repeated.

126. As to sub-paragraph 67.6, paragraphs 70 to 74 of this Reply are repeated.

127. Sub-paragraph 69.2.1 is admitted, but the amendments required can be made, and would very likely be adopted by nodes on the Networks for the reasons set out in paragraph 20 of this Reply.

128. As to sub-paragraph 69.2.2:

128.1. It is denied that TTL or Dr Wright (unlike the 2<sup>nd</sup> to 12<sup>th</sup> Defendants) is in a position to approve changes to the BTC Protocol or BTC Software; it is not therefore open to TTL (including through Dr Wright) to secure for itself the relief it seeks in its claim.

128.2. It is denied that nodes would need to be “*persuaded*” to adopt the updated BTC Software (or any updated BTC Protocol). Paragraphs 18 and 20 of this Reply are repeated.

- 128.3. It is denied that a “*hard fork*” would result from the 2<sup>nd</sup> to 12<sup>th</sup> Defendants making the amendments sought for all the reasons set out above, and because if none of the 2<sup>nd</sup> to 12<sup>th</sup> Defendant act in contempt of the court order then there is no possibility of an airdrop.
129. Sub-paragraph 69.2.3 is therefore denied.
130. As to sub-paragraph 69.3 (save for the admission and the denial therein), paragraphs 18 to 20 and 121 of this Reply are repeated.
131. As to sub-paragraph 69.4:
- 131.1. The defrauded owner of Bitcoin tokens would only have effective recourse against the fraudsters who stole his private keys if those fraudsters could be identified (and even then, such recourse might not be effective for innumerable reasons common to fraud litigation or otherwise, including difficulties with enforcement and bankruptcy or insolvency).
- 131.2. The final sentence is denied. Paragraphs 29.1 and 127 to 129 of this Reply are repeated.
132. As to sub-paragraph 69.5, it is denied that the Developers’ conduct is inconsistent with the existence of fiduciary duties.
133. As to paragraph 70, it is noted that the 2<sup>nd</sup> to 12<sup>th</sup> Defendants have failed to plead to a number of facts therein based on the (incorrect and itself inappropriately argumentative) first sentence (and similar statements in the sub-paragraphs to paragraph 70).
134. As to paragraph 71, second sentence, paragraphs 127 to 132 of this Reply (in response to paragraph 69) are repeated.
135. As to sub-paragraphs 71.1 to 71.3, the unexplained and unparticularised assertions that the orders sought are too widely framed (or are inappropriate on account of their scope, to the extent this is intended to be different), imprecise, unclear, or disproportionate are denied. The precise formulation of the relief to be granted is in any event a matter for trial.
136. The second and third sentences of paragraph 72 are denied:
- 136.1. TTL’s primary case is that the 2<sup>nd</sup> to 12<sup>th</sup> Defendants all became subject to the fiduciary duties pleaded in respect of it and all other owners of Bitcoin tokens on

the BTC Network as soon as the 2<sup>nd</sup> to 12<sup>th</sup> Defendants voluntarily undertook their roles controlling the BTC Network; further, that they breached those duties when they failed to respond to TTL's request for assistance in regaining access to its Bitcoin tokens in the Addresses either by offering assistance or offering assistance conditional upon TTL first obtaining a declaration as to its ownership of the Bitcoin tokens in the Addresses – and that analysis is not changed by reason of TTL seeking a declaration as to ownership of the Bitcoin in the Addresses.

136.2. TTL's alternative case is that the 2<sup>nd</sup> to 12<sup>th</sup> Defendants will be in breach of duty at such time as TTL obtains a declaration that it is the owner of the Bitcoin tokens in the Addresses on the BTC Network.

136.3. The confused statement that the 2<sup>nd</sup> to 12<sup>th</sup> Defendants will be subject to fiduciary duties only once injunctive relief is granted, which relief is dependent upon the existence and breach of those same fiduciary duties is denied.

136.4. As to the final sub-clause, it is denied that this is relevant, but in any event is denied for the reasons set out herein.

137. The second sentence of paragraph 73.3, and the second sentence of paragraph 74, are therefore denied.

**I: DUTY OF CARE AND BREACH OF DUTY**

138. As to paragraph 75.1:

138.1. As to the first sentence, this is denied. The Defendants voluntarily assumed responsibility to TTL by reason of voluntarily assuming roles that put them in control of the Networks, which control is pleaded in the APoC and above.

138.2. As to the second sentence, paragraph 118 of this Reply is repeated *mutatis mutandis* in respect of the claimed duty of care in tort.

139. As to the second sentence of sub-paragraph 75.4, paragraphs 29.1 and 122 of this Reply are repeated.

140. As to sub-paragraph 75.5.1, the special relationship between the Developers and owners of Bitcoin tokens on the Networks arises as a result of the role undertaken by the Developers, as set out herein and in the APoC, and the fiduciary duties the Developers consequently owe owners of Bitcoin tokens, as also set out herein and in the APoC.

- 141. Sub-paragraph 75.5.2 is denied. The class of persons to whom the 2<sup>nd</sup> to 12<sup>th</sup> Defendants potentially owe the claimed fiduciary duties is all the owners of BTC tokens, and that class is clearly defined, necessarily limited by the number of BTC tokens in existence, and knowable (even in circumstances where a court declaration is required to confirm that a person is a true owner).
- 142. As to sub-paragraph 75.5.3, (a) does not prevent the imposition of the claimed duty; (b) is embarrassing for its lack of particularity, its relevance is denied, and in any event is denied as a matter of fact; (c) is not admitted (the term “*cryptocurrency community*” being unparticularised in any event) but, regardless, is irrelevant to whether the claimed duty should be imposed, (d) is embarrassing for its lack of particularity, but in any event is denied; and (e) is denied for the reasons set out above, and in any event it is denied that the same would preclude the imposition of the duty.

JOHN WARDELL KC  
BOBBY FRIEDMAN  
SRI CARMICHAEL

**Statement of truth**

I believe the facts stated in this Reply are true. I understand that proceeding 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. I am authorised to sign this statement of truth on behalf of the Claimant.

Signed: .....  .....  
EFCD3017AD2842B...

Name: Dr Craig Steven Wright  
For and on behalf of Equator Consultants AG, a director of Tulip Trading Limited

Date: .....  
31 July 2023