IN THE HIGH COURT OF JUSTICE   **Claim No. BL-2021-000313**
BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES
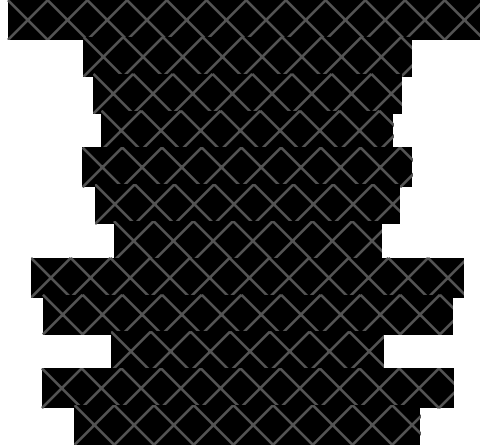**BUSINESS LIST (ChD)**
BETWEEN:

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 FIFTEENTH AND SIXTEENTH DEFENDANTS

---

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 Fifteenth and Sixteenth Defendants ("**15th & 16th Defendants**" and the "**D15-D16 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 D15-D16 Defence, unless otherwise stated.

3.   Save where expressly admitted or not admitted, all allegations in the D15-D16 Defence are denied.

4.	The D15-D16 Defence is highly repetitious and, where pleas are repeated by reference to another paragraph in the D15-D16 Defence, TTL should be taken as repeating its plea in respect of the paragraph in the D15-D16 Defence to which cross-reference is made, even if that is not expressly stated.

5.	On numerous occasions throughout the D15-D16 Defence, the 15th & 16th Defendants improperly plead to statements made in witness statements served in support of TTL's application to serve its Claim out of the jurisdiction and in response to the jurisdiction challenges then brought against TTL. Such conduct is contrary to the purpose of a defence, which is for a defendant to admit, not admit or deny facts and matters pleaded in a Particulars of Claim, and to plead any alternative facts and matters upon which he positively relies in support of his defence. The purpose of a defence is <u>not</u> to deny facts and matters that are not pleaded. To the extent that TTL pleads to these improper statements in the D15-D16 Defence, it is without prejudice to the foregoing.

**A1:	15th & 16th DEFENDANTS' SUMMARY OF THEIR DEFENCE**

6.	Paragraph 1 and the second sentence of paragraph 2 are denied. Further, it is denied that the term 'cryptocurrency' is an appropriate description of Bitcoin and the remainder of this Reply should be read accordingly.

7.	As to paragraph 3:

7.1.	It is denied that the Claim is brought against the wrong defendants. The relief in question is sought against the Defendants. It is denied that TTL is required to join to the Claim the small number of individuals who have alleged ownership of the Bitcoin tokens in the 1Feex Address; such assertions lack any credible supporting evidence (indeed, they are made by obvious time-wasters or cranks) and those individuals have chosen not to pursue their claims.

7.2.	The second sentence is admitted, although its relevance is denied.

7.3.	The inclusion of the fourth sentence is also inappropriate in a statement of case, and it does not positively aver any relevant fact. The tweet, while admitted, is irrelevant.

7.4.	As to the final sentence:

7.4.1.	TTL has brought its Claim in order to obtain the relief it seeks.

7.4.2. The relevance of the allegation regarding TTL's motivation for bringing its Claim is in any event denied.

7.4.3. The unparticularised allegation that Dr Wright is "closely associated" with the blockchain utilised by the BSV Network (the "**BSV Blockchain**") is embarrassing and so cannot be pleaded to.

7.4.4. Dr Wright supports and promotes the BSV Network because it is the only Network to use 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 (the "**Bitcoin Blockchain**"), and he is the Chief Scientist of nChain Limited, a company conducting blockchain research and development that supports the BSV Network by creating, amongst others, open-source, royalty-free software tools to help accelerate blockchain technology.

8. As to paragraph 4:

8.1. As to the first sentence:

8.1.1. It is admitted that TTL's position is that the Defendants owe the fiduciary duties contended for to all owners of Bitcoin on the Networks, including itself.

8.1.2. The 15th & 16th Defendants have failed to particularise "*the underlying rules of the system*" which they allege the contended for fiduciary duty requires them to change, such that TTL cannot plead to that allegation.

8.2. As to the second sentence:

8.2.1. The 15th & 16th Defendants fail to explain or particularise their assertion that TTL is asking the Defendants to act as "*worldwide guarantors and bailiffs to the entire cryptocurrency system*". TTL's case is that the Defendants owe fiduciary duties to owners of Bitcoin on the Networks to assist them in regaining control of their Bitcoin if they lose such control because their private keys are misappropriated by third parties.

8.2.2. It is denied that the fiduciary relationship contended for arises out of the (unparticularised) "*rules*" of the Bitcoin networks; the Defendants are

fiduciaries by reason of their voluntary assumption of their roles controlling the development of the protocol and of the software that are used to operate each the Networks.

8.2.3. The developer, or developers, in control of a particular Network ("**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, and references to Software should be understood accordingly). 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.

8.3. Accordingly, the final sentence is misconceived and denied. In any event, (in accordance with the Court of Appeal's judgment on the jurisdiction challenges in this Claim) it is denied that the fiduciary duties contended for are "*inconceivable*". It is further denied that the "*rules*" (whatever they may be) of the Networks preclude the actions which TTL contends that the Defendants ought to take.

9. Paragraph 5 is also confused and misconceived. More particularly:

9.1. As to the first sentence, it is admitted that the ABC Network was created after the Hack and after TTL became the owner of the Bitcoin in the Addresses, but the relevance of this timeline is denied.

9.2. As to the second sentence, upon the creation of the ABC Network, (i) TTL became the owner of ABC tokens in the Addresses on the ABC Network, which ABC tokens it was unable to access or control as a result of the Hack that had already occurred, and (ii) the 15th & 16th Defendants voluntarily assumed their roles controlling the protocol and Software of the ABC Network ("**ABC Protocol**" and "**ABC Software**"), and by doing so became subject to the fiduciary

duties; the 15th & 16th Defendants became subject to the fiduciary duties contended for as a result of their voluntary assumption of their <u>roles</u> and not as a result of the creation of the ABC Network *per se.*

9.3. In the premises, the last sentence (which consists of inappropriate argument) is denied.

10. Paragraph 6 is denied.

10.1. The first sentence is denied. The 15th & 16th Defendants control the ABC Protocol and the development of, and updates to, the ABC Software.

10.2. As to the second sentence:

10.2.1. The 15th & 16th Defendants control the development of the Software for the ABC Network, i.e. the ABC Software. The only software that can be, and is, successfully run on the ABC Network is the ABC Software, which implements the ABC Protocol (which originates from the Bitcoin Protocol that is still used on the BSV Network, but which was amended by the 15th & 16th Defendants and is updated by them from time to time), or other software that implements the ABC Protocol (as updated from time to time), and which mirrors the core features of the ABC Software.

10.2.2. Following any material update to the ABC Software, nodes will, within a short period of time, be unable to mine the ABC Network using older versions of the ABC Software, or software that incorporates or mirrors older versions of the ABC Software.

10.2.3. While anyone can *propose* changes to the ABC Software, changes will be effected only once they are approved by the 15th & 16th Defendants. This is, for example, analogous to a person proposing a change to Microsoft's products and software. As explained above, any software operating on the ABC Network must implement the ABC Protocol, which is also controlled by the 15th & 16th Defendants.

10.2.4. Effecting changes to any protocol or software on an ongoing basis cannot be done without some individual or individuals having control over its content (for example, to ensure that no bugs arise, to make necessary upgrades and to ensure a consistent approach to its development).

5

10.2.5. While each person operating a node is *theoretically* free to decide whether or not to run the ABC Software (being the software controlled by the 15th & 16th Defendants or software mirroring the core features of such software, and implementing the ABC Protocol), *in reality*, persons operating nodes on the ABC Network are not free so to act, because they are highly unlikely to do anything that would prevent them from mining the ABC Network, 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).

10.2.6. 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.

10.2.7. 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.

10.2.8. Further, if nodes did choose to leave the ABC Network, they would simply be replaced by new mining companies given the vast profits to be made from mining.

10.3. In the premises, the third to fifth sentences are denied.

11. As to paragraph 7:

11.1. Paragraph 7.1of this Reply is repeated.

11.2. The Court cannot proceed on the basis that it will make an erroneous determination as to whether TTL is the owner of the Bitcoin in the Addresses.

11.3. As such, any person making a rival claim to the Bitcoin in the Addresses that had been declared by the Court to belong to TTL would be a fraudulent claimant.

11.4. Accordingly, there is no proper (nor pleaded) basis for the 15th & 16th Defendants' assertion that they are at "*considerable risk of worldwide civil and criminal actions*" from competing claimants, as this assertion relies on either (i) the improper premise that, if the Court declares TTL to be the owner of the Bitcoin in the Addresses, that declaration will be wrong, or (ii) the unrealistic premise that necessarily fraudulent "*competing claimants*" will expend time and money bringing actions against the 15th & 16th Defendants in respect of the ABC tokens in the Addresses following the Court's (correct) declaration regarding TTL's ownership of those ABC tokens and the Court's order against the 15th & 16th Defendants, having not previously sought to join themselves to the Claim, even though it has attracted substantial global attention.

11.5. To the extent that there is any real risk of the 15th & 16th Defendants incurring costs or expenses as a result of facing such fraudulent claims, that risk does not prevent them owing fiduciary duties as a result of the control they exercise over the ABC Network.

12. Paragraph 8 has no proper purpose and is liable to be struck out. It is inconsistent with the Court of Appeal's decision that the English courts have jurisdiction to hear the Claim, and, further, the 15th & 16th Defendants submitted to the jurisdiction of the English courts following the Court of Appeal's decision, and such submission is irrevocable. In any case, paragraph 8 is embarrassing:

12.1. The 15th & 16th Defendants assert that they have "*national and/or constitutional rights*" and their "*own national legal protections*", with which they allege the claim conflicts – but they fail to identify any such rights or protections.

12.2. The 15th & 16th Defendants also purport to "*expressly reserve any and all rights*" they have in respect of the alleged "*improper overreach*" of the English courts – but they fail to identify any such rights, and their reservation is empty rhetoric.

A2: PRELIMINARY

13. As to paragraph 11.2:

13.1. Paragraph 10.2of this Reply is repeated.

13.2. TTL uses the following terminology: the ABC Network operates using the ABC Software, as updated from time to time (or, as explained above, software that

incorporates or mirrors the core features of the ABC Software, as updated from time to time), which software (i) implements the ABC Protocol and (ii) enables nodes to validate transactions of ABC tokens that take place on the ABC blockchain (**"ABC Blockchain"**) and accept a new block on the ABC Blockchain.

B: **PARTIES**

14. As to paragraph 13:

    14.1. The unparticularised allegation that Dr Wright is "*closely associated*" with the First Defendant is embarrassing, and so cannot be pleaded to.

    14.2. Paragraph 7.4.4 of this Reply is repeated.

    14.3. TTL brought its Claim against the First Defendant in order to obtain the relief it seeks against it.

15. As to paragraph 14, the first two sentences are admitted.

C: **BITCOIN**

C1: **The Bitcoin White Paper**

16. As to paragraph 16:

    16.1. Dr Wright is the pseudonymous Satoshi Nakamoto – although the identity of Satoshi Nakamoto is not an issue that needs to be determined in this Claim.

    16.2. It is admitted that the paper entitled '*Bitcoin: A Peer-to-Peer Electronic Cash System*' ("**Bitcoin White Paper**") was published on 31 October 2008.

    16.3. The extract from the Bitcoin White Paper is accurately stated (absent the added emphasis).

    16.4. The relevance of the Bitcoin White Paper to the relief sought in the Claim is denied. The ABC Network is not operated consistently with the Bitcoin White Paper. The remainder of this Reply is without prejudice to the foregoing.

17. Save that blocks are linked through hashes, not cryptography, paragraph 17 is admitted.

18. As to paragraph 18.1, it is admitted that the 15th & 16th Defendants have lifted phrases from section 1 of the Bitcoin White Paper, but quoted them out of context so as to misrepresent what is stated:

18.1. Section 1 does <u>not</u> state that the electronic payment system proposed in the Bitcoin White Paper enables ""*completely non-reversible transactions" without the possibility of mediation of disputes*". Instead, section 1 states that "*Completely non-reversible transactions are not really possible [in the fiat money system], since financial institutions cannot avoid mediating disputes*".

18.2. Insofar as it is alleged, it is admitted that the Bitcoin White Paper envisaged that Bitcoin transactions would be "*non-reversible*" in the sense that, once recorded on the Bitcoin Blockchain ledger, that record cannot be deleted or altered. That is of no relevance to the relief sought in the Claim.

18.3. Further, while section 1 notes that mediating disputes increases transaction costs, it in fact says nothing about whether or not mediation of disputes is possible in the proposed system.

19. As to paragraph 18.2:

19.1. Points (a) and (c) are admitted.

19.2. As to point (b), insofar as the 15th & 16th Defendants intend their statement "*requires the use of a private key held only by the owner*" to mean that section 2 states that (i) a private key <u>must</u> be used to transfer Bitcoin tokens, and (ii) a private key can only ever be held by the owner of the Bitcoin tokens associated with that private key, it is denied that section 2 states either of those things.

19.3. Further, 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 14th Defendant agrees (at 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.

20. As to sub-paragraph 18.3, the first two sentences are admitted. The last sentence is admitted as a general rule, but its relevance to the Claim and the relief sought is denied. Paragraph 18.2 above is repeated.

21. Paragraphs 18.4 and 18.5 are admitted.

22. As to paragraph 18.6:

22.1. The 15th & 16th Defendants misrepresent the Bitcoin White Paper. While it is admitted that section 10 includes the quoted words, those words are <u>not</u> used to support a proposal for "*anonymity of ownership*".

22.2. Instead, section 10 proposes that public keys be anonymous in order to achieve a "*level of privacy*" in respect of transactions that is similar to, but not greater than, the level of privacy 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).

23. As to paragraph 19:

23.1. The 15th & 16th Defendants again misrepresent the Bitcoin White Paper: it does not identify any "*fundamental principles*" or similar, let alone any principles which are "*immutable*". In any event, it is denied that, even if the Bitcoin White Paper did contain "*immutable principles*" or "*fundamental principles*", that would be relevant to the relief sought in the Claim or would preclude the existence of the duties contended for.

23.2. It is admitted that the Bitcoin White Paper does not state that the code developed to give effect to its proposals cannot, or should not, be amended from time to time; indeed, it is inevitable that any software used on an ongoing basis will need to be updated from time to time in order to ensure that no bugs arise within it and it is upgraded as necessary, as the technology interacting with it develops.

C2: **Bitcoin as a digital asset and the blockchain**

24. As to paragraph 20, the first sentence is admitted. The original Bitcoin Blockchain is the blockchain utilised by the BSV Network.

25. Paragraphs 20.1 and 20.2 are admitted. The blockchains of the Networks are all distributed (not decentralised).

26. As to paragraph 20.3:

26.1. As to the first and second sentences, it is admitted that Bitcoin tokens are intangible assets, and can be transferred. It is denied that an owner of Bitcoin tokens cannot 'access' them. The first sentence also is inconsistent with the averment in the second sentence of paragraph 43.8.

26.2. The third sentence is denied:

26.2.1. Paragraphs 19.2 and 23.1 of this Reply are repeated.

26.2.2. It is denied that transfers of Bitcoin tokens can only be effected by using a private key:

26.2.2.1. As referred to in paragraph 58.3 of this Reply, some transactions such as a hash puzzle transaction, do not require a digital signature for validation.

26.2.2.2. 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.

26.2.2.3. The Developers could broadcast a transaction involving the transfer of tokens to a newly assigned address, or locking script, controlled by the owner.

26.3. As to the last sentence, it is denied. It is also misleading because there is a maximum supply of 21 million Bitcoin that can be issued.

27. As to paragraph 20.4:

27.1. As to the first and second sentences:

27.1.1. It is admitted that transfers to and from public addresses on the blockchain of each of the Networks are publicly visible on the relevant blockchain.

27.1.2. It is denied that the identities of those taking part in such transactions are always unknown and anonymous, 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 sometimes reveal their identities to their counterparties to any given transaction.

27.2. As to the last sentence:

27.2.1. Paragraphs 22 and 23 of this Reply are repeated.

27.2.2. The alleged "*well-publicised examples of threats and attacks on people known to control cryptocurrency*" are unparticularised, embarrassing and cannot be pleaded to, but in any event are irrelevant.

28. Paragraph 21 is admitted, on the basis that by "*coin*" the 15th & 16th Defendants mean Bitcoin tokens.

29. As to paragraph 22:

29.1. As to the first sentence, references to 'Bitcoin' and '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.

29.2. As to the last sentence, paragraph 23.1 of this Reply is repeated.

30. As to paragraph 23:

30.1. It is admitted that a person purchasing Bitcoin tokens purchases the ability to control a chain of digital signatures.

30.2. Paragraph 26.2.2 of this Reply is repeated: a private key is not required to transfer Bitcoin tokens.

30.3. Paragraph 23 of this Reply is repeated and paragraph 23(b) is therefore denied.

31. As to paragraph 23.1:

31.1. The Networks operate without the need for financial institutions serving as trusted third parties to process electronic payments. However, as explained at paragraph 10.2.4 of this Reply, it is necessary for some individual(s) to have control over the protocol and the content of the Software which govern the operation of each Network.

31.2. Owners of Bitcoin tokens on the Networks therefore entrust their Bitcoin tokens to those individuals by reason of those individuals' role controlling the development and operation of the Networks, and in doing so they trust those individuals not to prefer the interests of fraudsters, or thieves, or their own interests over those of owners of Bitcoin tokens when determining how the Network should operate.

32.　As to paragraph 23.2, paragraph 26.2 is repeated.

33.　As to paragraphs 23.3 and 23.4, paragraphs 18.1 to 18.3 are repeated.

34.　As to paragraph 23.5, paragraph 27.1.2 is repeated.

35.　As to paragraph 24, paragraph 23 of this Reply is repeated.

36.　As to paragraph 25.2, the issues therein are irrelevant to the Claim. 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.

37.　As to the last sentence of paragraph 25.3, this is not admitted.

38.　As to paragraph 25.4, it is admitted that the blockchains of the Networks do not record off-chain transactions.

39.　As to paragraph 25.5, paragraph 9 of the APoC does not refer to "*anonymity of ownership*"; it simply states that the identity of those who transfer Bitcoin tokens on the blockchains of the Networks is not disclosed publicly or recorded on those blockchains. Paragraph 27.1.2 is repeated.

C3:　Role of nodes/miners

40.　As to paragraph 26:

　　40.1.　A node is a computer (or, generally, a pool of computers acting in concert) running the (freely-available) Software of a particular Network, as updated from time to time (or software that incorporates or mirrors the core features of that Software), which engages in proof-of-work (a process often referred to as 'mining') and, having done so, extends the blockchain of the Network in question.

　　40.2.　It is denied that *any* computer running the Software is a node; some computers or devices on the Networks run Client Software and do not undertake mining or validate transactions for themselves, and they are not nodes properly so called.

　　40.3.　Nodes tend to be large commercial enterprises controlled by companies, not single computers run by private individuals.

41. Paragraph 27 is inaccurate: all nodes properly so called *validate* transactions (the proof-of-work process called mining), but other users of the Networks may *verify* transactions by reference to the *validation* activities of nodes.

42. As to paragraph 28, the implication that 'non-mining nodes' exist is denied, and is inconsistent with the averment at paragraph 18.4 as to the activities of nodes. Save that mining does not require solving the hash equation for each *transfer,* but rather for each *block*, the description of the activities of nodes is admitted.

43. As to paragraph 29, it is admitted that a node operates on a Network using the Node Software of the Network in question, or software that incorporates or mirrors the core features of that Node Software and implements that Network's protocol.

44. As to paragraph 29.1:

    44.1. The statements in paragraph 10.2 of this Reply are repeated and apply *mutatis mutandis* to the other Networks.

    44.2. The first sentence is admitted.

    44.3. As to the second sentence, so-called soft forks are irrelevant to the Claim.

    44.4. As to the last sentence, paragraph 10.2.1 of this Reply is repeated. The software needs to incorporate or mirror the core features of the Software.

45. As to paragraph 29.2:

    45.1. As to the first two sentences, paragraphs 10.2 of this Reply are repeated.

    45.2. 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.

    45.3. It is denied that a "*hard fork*" would result from the 15th & 16th Defendants making the amendments sought for all the reasons set out above, and because, if neither of them acts in contempt of the court order, then there is no possibility of an airdrop.

46.   As to paragraph 30, paragraph 10.2 of this Reply is repeated.

47.   As to paragraph 31:

    47.1.   Paragraphs 10.2 and 45 of this Reply are repeated.

    47.2.   It is admitted that following an airdrop, the blockchains of the original network and the new network are identical up until the time of the airdrop, but from the time of the airdrop they extend independently and thus diverge, such that transactions that take place after the time of the airdrop on the original blockchain and on the new blockchain are distinct from one another.

48.   As to paragraph 32, this is irrelevant because no "*hard fork*" would occur.

49.   As to paragraph 33:

    49.1.   As to the first sentence, it is admitted that the Software used to run the Networks is open-source and publicly accessible, in the sense that it is freely available to the general public to use, modify and distribute.

    49.2.   As to the second sentence:

        49.2.1.   It is admitted that (Node) Software can be (and is) downloaded by nodes.

        49.2.2.   It is admitted that Software can be downloaded by anyone who wishes to inspect it or use it.

        49.2.3.   However, it is denied that anyone can change the Software so that it does not contain the core features and still be able to engage with the Network in question.

        49.2.4.   Paragraph 10.2 of this Reply is repeated.

    49.3.   As to the last sentence:

        49.3.1.   Nodes choose to download the Node Software of the Network in question that they know contains the amendments and updates approved by the Developers of that Network (or software that they know incorporates or mirrors the Node Software of the Network in question, as updated from time to time). Otherwise, the nodes in question would not be able to act as nodes.

49.3.2. The 15th & 16th Defendants' reference to a "*static*" version of software is misleading, and it is properly understood to be a reference to Software, as updated by the Developers in control of the Network in question from time to time.

50. As to paragraphs 33.1 and 33.2, paragraph 10.2 of this Reply is repeated.

51. Paragraph 34 is admitted, but any proposed change must be approved by the 15th & 16th Defendants. Paragraphs 10.2 of this Reply is repeated.

52. As to paragraph 35, following an airdrop, nodes wishing to participate on the new network will need to use the Node Software of that new network, which implements the new protocol of the new network and copies the blockchain of the old network.

53. As to paragraph 36.1, this is irrelevant for the reasons given in paragraph 45.3 above. Without prejudice to the foregoing:

53.1. The first sentence is denied. "*Material amendments*" to Software will not cause an airdrop where they are agreed upon by all of the Developers of the Network. Paragraph 45.3 is repeated.

53.2. As to the second and third sentences:

53.2.1. The only relevant airdrops that have taken place are those identified in paragraphs 15 to 17 of the APoC.

53.2.2. It is admitted that new networks other than the BTC Network, the BCH Network and the ABC Network have been created by way of airdrops since the inception of the original Bitcoin network (now called the BSV Network), and that none of these other networks took off. It is denied that that was because an insufficient number of nodes downloaded the new Node Software developed to run those other new networks.

53.2.3. It is further denied that airdrops creating new networks ever occur "*as a result of error or failed experiment*"; they are only ever deliberate and occur as a result of a dispute between the Developers in control of a particular Network.

54. As to paragraph 36.2, it is embarrassing and cannot be pleaded to. TTL responds to the Fourteenth Defendant's Defence in its Reply to the same.

55. As to paragraph 37:

   55.1. As to the first two sentences, it is admitted that the Software used on each of the Networks is made available under the terms of the MIT Licence and that the MIT Licence is a commonly used open source licence.

   55.2. As to the third sentence, the 15th & 16th Defendants have failed to explain how they allege that TTL "*impliedly*" accepted the MIT Licence when it acquired the Bitcoin in the Addresses, and the allegation is denied.

   55.3. It is admitted that the terms of the MIT Licence are accurately stated.

56. As to paragraph 38.1:

   56.1. The second sentence is denied: the Defendants control the Networks by determining the protocol and what Software implementing that protocol is available for nodes to use. Furthermore, nodes do not act in consensus with other nodes in deciding which Networks they choose to mine; they invest significant amounts of resources in direct competition with each other to be the first to solve the hash equation for each block in order to obtain mining rewards.

   56.2. As to the third sentence, this is denied, and paragraphs 10.2 and 45 of this Reply are repeated.

   56.3. As to the fourth sentence, the 15th & 16th Defendants are in control of the ABC Software and the ABC Network.

   56.4. As to the penultimate sentence:

      56.4.1. Whether or not the 15th & 16th Defendants *in fact* control the ABC Software cannot be determined by the content of the Bitcoin White Paper.

      56.4.2. In any case, references to the original Bitcoin network being a "*peer-to-peer*" network which would operate "*without the need for a trusted third party*" are references to there being no need for a "*trusted third party to process electronic payments*" [emphasis added], i.e., to the absence of a financial intermediary between payor and payee, such as a bank, not to the absence of individuals in control of software development.

   56.5. The final sentence is denied. Paragraphs 40 to 42 of this Reply are repeated.

57.   As to paragraph 39:

57.1.   As to the third and fourth sentences, paragraphs 40 to 42 of this Reply are repeated: all nodes engage in mining. It is denied that there are nodes behind firewalls that cannot be known. Every node, properly so called, with any significant amount of investment in the ABC Network is known. There are fewer than ten nodes engaged in mining the ABC Network, with one main node.

57.2.   As to the last sentence, this is unexplained and denied. Paragraph 10.2 of this Reply is repeated.

C4:   Addresses on the blockchain

58.   As to paragraph 40.2:

58.1.   It is denied that TTL's description of UTXOs at paragraph 13 of its APoC is misleading (that allegation not being particularised) and the relevance of the sub-paragraphs of paragraphs 40.2 is denied. The remainder is without prejudice to the foregoing.

58.2.   Sub-paragraph (a) is admitted.

58.3.   Sub-paragraph (b) is denied. Each UTXO has a spend script. This *may* use, but does not *require*, a digital signature. A script can be created without a digital signature algorithm. 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.

58.4.   Sub-paragraph (c) is denied. A UTXO is spent when a node accepts, validates and adds it to a block.

58.5.   Sub-paragraph (d) is admitted.

58.6.   Sub-paragraph (e) is denied. A UTXO cannot be spent twice. Where a UTXO is spent, the recipient of the tokens from that transaction holds a new UTXO.

58.7.   Sub-paragraph (f) is denied on the basis that it is incomplete. UTXOs can also be transferred directly IP-address-to-IP-address, without the use of addresses.

59.   As to paragraph 40.3, it is admitted that an uppercase 'F' is required (and the statement to the contrary was an error).

C5: **The existence of multiple blockchains**

60. As to paragraph 41, this is embarrassing. To the extent it can be understood, paragraphs 10.2, 45.2 and 53.2 of this Reply are repeated.

61. As to paragraph 42 and paragraph 43.2, paragraphs 15 to 17 of the APoC are repeated. While it is admitted that the only significant airdrops took place on 1 August 2017, 15 November 2018 and 15 November 2020 and that the ABC Network and ABC Blockchain were created by way of an airdrop of the blockchain of the BCH Network ("**BCH Blockchain**") on 15 November 2020, it is denied that the first two airdrops created the Networks (and blockchains) alleged; they created, respectively, what is now known as the BTC Network, and what is now known as the BCH Network, each time as a result of an airdrop of the original Bitcoin Blockchain (what is now known as the BSV Blockchain).

62. As to paragraph 43.4, it is admitted that Software used to create a new Bitcoin network by way of an airdrop of an existing Bitcoin network implements a new protocol that is incompatible with the protocol of the pre-existing Bitcoin network. Otherwise, the final sentence of paragraph 43.4 is denied.

63. As to paragraphs 43.6 and 43.7, it is denied that the then-BCH Blockchain (being the BSV Blockchain) did not apply the same protocol as before; it retained the Bitcoin Protocol. The block size limit is not, and never was, part of the Bitcoin Protocol.

64. As to paragraph 43.8:

    64.1. It is obvious that TTL used the word 'hold' to denote ownership.

    64.2. The second sentence is admitted on the understanding that when the 15th & 16th Defendants refer to a 'hard fork' they are referring to an airdrop.

    64.3. As to (a):

        64.3.1. The relevance of the first sentence is denied, given that English law applies to the Claim, and it is liable to be struck out. Further, as the 15th & 16th Defendants are in a position to admit or deny sub-paragraph 15(c) of the APoC, by their non-admission they are taken as admitting the same.

64.3.2. As to the remainder of the sub-paragraph, Bitcoin tokens are property: the Court of Appeal stated as much (albeit obiter) in its judgment in this case.

65. As to paragraph 43.10:

65.1. Paragraphs 15 and 16 of the APoC are repeated.

65.2. Developers control the protocol and the Software that implements it, for the reasons set out above.

65.3. While nodes operate the Node Software of the Bitcoin network in question, nodes can and will only operate whatever Node Software is made available by the Developers of the network in question (or other software compatible with the core features of the same).

66. As to the second sentence of paragraph 43.11, this is repetitive and the matters set out above are repeated.

67. As to paragraph 43.12, the 15th & 16th Defendants are in a position to admit or deny whether there was a disagreement between the 15th Defendant and the 14th Defendant. They are therefore taken, by their non-admission, as admitting the same.

C6: The ABC Blockchain

68. As to paragraph 44, it is admitted that the ABC Network and ABC Blockchain came into existence following an airdrop of the BCH Network and BCH Blockchain on 15 November 2020.

69. As to paragraph 45, paragraphs 10.2 of this Reply are repeated.

70. As to paragraph 45.1, this is not admitted.

71. As to paragraph 45.2, it is not admitted. Regardless, any software run by nodes mining the ABC Network must be compatible with the core features of the ABC Software and must implement the ABC Protocol, both of which the 15th & 16th Defendants control.

72. As to paragraph 45.3:

72.1. Although the term "*consensus rules*" is not explained and therefore not understood, it is admitted that software versions that incorporate or mirror the core features of the ABC Software (as updated from time to time) can be used by nodes wishing to mine the ABC Network.

72.2. The second sentence is not admitted.

73. As to paragraph 46, it is denied that the ABC Software is not subject to a hierarchical approval process and that amendments can be made by anyone registered as a 'reviewer'; the 15th & 16th Defendants control the ABC Software as set out herein. Sub-paragraphs 46.4 and 46.6 are thereby denied. Without prejudice to that denial, the details set out in sub-paragraphs 46.1 to 46.3 and 46.5 are not admitted.

74. As to paragraph 47, it is denied that there has ever been or is presently any Developer other than the 15th & 16th Defendants in control of the ABC Software.

75. As to paragraph 48, paragraphs 10.2, 45 and 49.3 of this Reply are repeated.

C7: Private keys

76. As to paragraph 50:

76.1. Paragraphs 23, 26.2, 30 and 35 of this Reply are repeated.

76.2. It is denied that owners of ABC tokens "*necessarily accept*" any "*system rules*" (by which it is assumed the 15th & 16th Defendants are referring to the "*fundamental rules*" they allege at paragraph 23 of the D15-D16 Defence) when they purchase their tokens.

76.3. Further, 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. Paragraph 58.3 of this Reply is repeated.

77. As to paragraph 51:

77.1. As to the second and third sentences, paragraph 26.1 is repeated.

77.2. The fourth sentence is admitted.

77.3. As to the fifth sentence:

77.3.1. It is denied ownership is anonymous: paragraphs 22 and 27.1.2 of this Reply are repeated.

77.3.2. It is denied that transfers can only be effected with the use of the private key: paragraphs 23, 26.2, 30 and 35 of this Reply are repeated.

77.3.3. The 15th & 16th Defendants fail to state what they contend the phrase "*not your keys, not your coins*" means, and TTL reserves its right to

plead to any particulars ultimately provided. It is not admitted that the phrase "*not your keys, not your coins*" is well known.

77.4. The penultimate sentence is denied: an owner of Bitcoin tokens who has lost access to his private key remains the owner of those Bitcoin tokens, with proprietary rights in the same.

78. As to paragraph 52, it is denied that the "*risks*" identified are real or that they prevent or are relevant to the imposition of the duties claimed, which duties arise by reason of the roles voluntarily undertaken by the Defendants in respect of their control of the Networks. In respect of the alleged risks:

78.1. In terms of (a), "*transfers to non-owners*", and (b), "*fraud by transferors in off-chain transfers*", these are both versions of the 15th & 16th Defendants' misconceived "*rival claimants*" argument, and paragraph 11 of this Reply is repeated *mutatis mutandis*.

78.2. In terms of (c), "*fraud by those said to have control over the system and ability to transfer*", which is understood to mean the risk of fraud by the Developers in control of the Networks, this argument is again misconceived: the Defendants, as the Developers in control of the Networks, *already* have the ability to develop the Software in the manner sought in the Claim (and the ability, more generally, to misappropriate Bitcoin tokens if they wish) – a factor which supports the contention that they owe fiduciary duties to owners of Bitcoin tokens.

79. As to paragraph 53.1, the first sentence is denied. Paragraphs 77 and 78 of this Reply are repeated.

80. Paragraph 53.2 is denied, save that it is admitted that owners of Bitcoin tokens can be located anywhere in the world. Paragraphs 22, 23 and 27.1 of this Reply are repeated.

81. Paragraph 53.3 is repetitious. Paragraphs 10.2, 23, 30, 35, 45, 49.3 and 76 are repeated.

82. As to paragraph 53.4:

82.1. As to the first sentence, TTL has specified in its Claim what it requires the updated Software to do.

82.2. As to the second sentence, it is denied that TTL (unlike the 15th & 16th Defendants) is in a position to approve changes to the ABC Software; it is not

therefore open to TTL to secure for itself the relief it seeks in its Claim. Paragraph 10.2 of this Reply is repeated.

    82.3.   The third sentence is therefore admitted. Any such attempt would have been pointless.

    82.4.   The last sentence is denied: it is not for TTL to write the update to the ABC Software controlled by the 15th & 16th Defendants; it is for them to undertake that task.

83.   As to paragraph 55.4, paragraph 76 of this Reply is repeated.

C8:   **The role of Developers**

84.   As to paragraph 58.1, paragraphs 10.2 and 72 of this Reply are repeated.

85.   As to paragraph 58.2, it is clear that TTL was referring to testing the Software. Paragraph 10.2.4 of this Reply is repeated.

86.   As to paragraph 58.3, paragraphs 10.2.5 to 10.2.6 of this Reply are repeated.

87.   Paragraphs 59.1 and 59.2 are repetitious. Paragraphs 10.2 and 73 are repeated.

88.   The second and third sentences of paragraph 60 are denied for the reasons set out above. As to paragraph 60.1:

    88.1.   It is admitted that Satoshi Nakamoto made the amendment to the Software of the original Bitcoin network.

    88.2.   It is denied that this amendment is properly termed a 'soft fork', because the previous version of the Software immediately became incompatible with the original Bitcoin network, such that any nodes who wished to keep mining the original Bitcoin network had to switch to the amended Software. It was therefore inevitable that the vast majority of nodes downloaded the updated Software, for the reasons set out at paragraph 10.2.5 of this Reply.

89.   As to paragraph 60.2:

    89.1.   The second sentence is denied for all the reasons set out in the APoC and this Reply.

    89.2.   As to the third sentence:

        89.2.1.   Paragraph 16.4 above is repeated.

89.2.2. It is admitted that all transactions are recorded on the blockchain of the Network in question.

89.2.3. Paragraphs 18, 22, 23, 31.1, 35 and 56.4 are repeated.

89.3. As to the fourth sentence, this is misconceived. The 15th & 16th Defendants could, if there was any genuine doubt in relation to ownership, require a claimed owner to obtain a court declaration as to its ownership, upon which they could then properly rely. For the reasons set out above, the 15th & 16th Defendants can reverse the effect of a fraud.

89.4. The remainder of the paragraph is repetitious and is denied for the reasons already given in this Reply.

90. As to paragraph 60.3, the second and third sentences are denied. Paragraphs 26.1 and 26.2.2 are repeated.

D: **TTL'S OWNERSHIP OF THE BITCOIN IN THE ADDRESSES**

91. As to paragraph 61.1, TTL owns the Bitcoin tokens in the Addresses. The second sentence is therefore denied (and the reservation of rights is misplaced and appears to be included for the improper and misguided purpose of attempting to intimidate Dr Wright). The third sentence constitutes impermissible argument, but in any event the First Witness Statement of Mr Cain in support of TTL's application to serve out of the jurisdiction does not identify any matters that are necessarily inconsistent with TTL's ownership as claimed.

92. As to paragraph 62:

92.1. Accounting documentation shows that entities related to Dr Wright recorded the Bitcoin tokens in the Addresses from 2011 in respect of the 1Feex Address, and from 2013 in respect of the 12ib7 Address. TTL's case is not that TTL itself was the owner since February 2011. It is admitted that TTL did not exist in February 2011.

92.2. It is denied that WMIRK.com did not deal in Bitcoin tokens at the end of February 2011 when the Bitcoin in the 1Feex Address was purchased from the exchange.

92.3. It is denied that the purchase order relied upon by TTL in respect of the Bitcoin in the 1Feex Address ("**Purchase Order**") is a forgery.

24

92.4. The bald assertion that the Bitcoin tokens in the 1Feex Address "*are understood to have been stolen from the Mt Gox exchange*" is denied. The 15th & 16th Defendants have, inappropriately, failed to plead any facts or matters in support of their bald assertion in that regard, and their assertion is liable to be struck out.

92.5. 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.

93. As to paragraph 64.3:

93.1. It is denied that subparagraph 32(b) of the APoC inaccurately characterises the nature of an airdrop. New Software that implements a new protocol so that nodes using it will mine a new network necessarily embeds within itself the data comprising the existing blockchain of the original Bitcoin Blockchain, prior to the airdrop: it is therefore correct to describe an airdrop as involving the copying of the existing blockchain.

93.2. On that basis, the remainder of the paragraph is admitted.

94. As to paragraph 65, it is denied that anonymity is a "*key principle*" underpinning the Networks. Paragraphs 22, 23, 27.1.2 and 35 are repeated.

E: THE HACK

95. As to the fourth and fifth sentences of paragraph 67, the propositions therein, and the alleged inferences, are denied. In addition to the matters set out at paragraph 111 below, such that the MIT Licence is irrelevant for those reasons:

95.1. The mere fact of storing of private keys in an MIT-licensed wallet would not mean that the MIT Licence was accepted in respect of the ABC Network. That is all the more so because the storage took place (and ended) prior to the airdrop creating the ABC Network.

95.2. In any event, Networks other than the BTC Network (and its derivatives) are compatible with wallet.dat files. Other wallets were not created under an MIT licence. Therefore, the plea in paragraph 67 does not follow.

96. As to paragraph 68.1, the inference alleged is denied.

97. As to paragraph 68.1(b):

    97.1. 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.

    97.2. 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.

    97.3. There would have been no purpose in attempting to restore the wiped TTL Private Keys and the Keys Access Material from One Drive and/or Google Cloud, because such data was *wiped*, not deleted, and wiped data cannot be recovered.

98. As to paragraph 68.1(c), privilege applies. TTL does not plead thereto. In any event, the pleading in paragraph 68.1(c) is a non-sequitur.

99. As to paragraph 69.1, it is denied that TTL has fabricated Dr Wright's discovery of the Hack.

100. Paragraph 69.2 is denied; paragraph 97 of this Reply is repeated.

101. As to paragraph 69.3, it is denied that Dr Wright made a false police report regarding the Hack. The second sentence is irrelevant.

102. As to paragraph 69.4, paragraph 97.3 of this Reply is repeated.

F: **FIDUCIARY DUTIES**

103. As to paragraph 72.1:

    103.1. It is admitted that the 15th & 16th Defendants have never communicated with TTL prior to these proceedings, but the relevance of that fact is denied.

    103.2. It is further denied that the 15th & 16th Defendants have no relationship with TTL whatsoever: they are TTL's fiduciaries, and control the ABC Network on which TTL holds tokens.

104. It is not admitted that the 15th & 16th Defendants are not remunerated for their role as the Developers for the ABC Network and they are put to strict proof regarding the same. As to paragraph 72.2, TTL is willing to pay the 15th & 16th Defendants for their reasonable

time and expenses incurred in procuring the creation and introduction of the amendments TTL seeks, insofar as they can evidence that time and those expenses.

105. As to paragraph 72.3, paragraph 9 above is repeated. The final sentence does not follow from the preceding sentences of paragraph 72.3 and is in any event denied.

106. Paragraph 72.4 is repetitious and is denied for the reasons set out above in this Reply.

107. As to paragraph 72.5, the characterisation of fiduciary duties (which constitutes impermissible legal submission) is denied. The Claim requests that the 15th & 16th Defendants use the control that they have over the ABC Network and ABC Protocol in a specific way, so as to assist TTL to deal with its ABC tokens.

108. As to paragraph 72.6, it is denied: as set out above, it is denied that "*an inability to effect a transfer without a private key is a fundamental system rule*" or that this would negate the existence of the fiduciary alleged even if it were.

109. As to paragraph 72.7:

109.1. The fiduciary duties contended for do not "*arise as an incidence of the rules by which the system operates*" (whatever that means); they are imposed on the 15th & 16th Defendants by reason of their voluntary assumption of their roles.

109.2. The existence of the 'rules' identified are denied: paragraphs 18, 19, 20, 22 and 23 of this Reply are repeated.

109.3. In the premises, the last sentence is misconceived and denied.

110. As to paragraph 72.8:

110.1. As to the first sentence, the Defendants owe the fiduciary duties claimed to all owners of Bitcoin tokens on the relevant Networks.

110.2. As to the second sentence, all the various reasons why it is alleged the software changes sought would cause detriment to other owners of Bitcoin tokens are denied, and it is denied that the Defendants owe owners conflicting fiduciary duties, though, if there was such a conflict, there would be implied consent to the same.

110.2.1. As to reason (i), paragraphs 23, 35 and 76 of this Reply are repeated.

110.2.2. As to reason (ii), the 15th & 16th Defendants' bare assertion that allowing an owner of Bitcoin tokens to regain control of those tokens after

27

temporarily losing access to them would depreciate the value of other owners' Bitcoin tokens is denied. It is further, and in any event, denied that other owners of Bitcoin tokens could reasonably expect to benefit from another owner falling victim to a fraud, such that the reversal of any such benefit cannot properly be said to cause detriment.

110.2.3. As to reason (iii), paragraphs 19, 26.2.2 and 76 of this Reply are repeated.

110.2.4. As to reason (iv), owners do not have, and cannot reasonably expect, anonymity: paragraphs 22, 23, 27.1.2 and 35 of this Reply are repeated.

110.2.5. As to reason (v), paragraph 18 of this Reply is repeated.

111. As to paragraph 72.9:

111.1. Paragraphs 55 and 95 are repeated.

111.2. It is denied that the terms of the MIT Licence, properly construed, exclude liability for the breaches of fiduciary duty and tortious duty of care claimed. TTL's loss does not arise as a result of, from, out of, or in connection with, its use of the ABC Software; it arises as a result of the 15th & 16th Defendants' refusal to comply with their duties to restore TTL's control of its ABC tokens in the Addresses. The MIT Licence is therefore irrelevant to the Claim. Further:

111.2.1. TTL is not subject to the terms of the MIT Licence in circumstances where TTL itself did not download or otherwise accept the ABC Software.

111.2.2. 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 2, 3 and 11 of the Unfair Contract Terms Act 1977.

111.2.3. 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.

112. As to paragraph 72.10:

112.1. The first sentence is admitted, but its relevance is not explained and is denied.

112.2. The relevance of off-chain transfers of ownership is not explained and is denied.

113. As to paragraph 72.11, whether or not Developers are a fluctuating class of individuals and entities is irrelevant to the question of whether fiduciary duties are owed by the Defendants.

114. As to paragraph 72.12:

114.1. The location of the Defendants is irrelevant to the question of whether they owe fiduciary duties to TTL.

114.2. One of the reasons that the English courts concluded that they have jurisdiction to hear TTL's Claim (and why TTL was granted permission to serve the Claim out of the jurisdiction) was because of the strength of TTL's argument that it is resident in England; the same argument will not be available to "*all users of the Bitcoin system worldwide*".

114.3. The remainder of the paragraph is abusive in circumstances where the 15th & 16th Defendants lost their jurisdiction challenge and the "*Defendants' own national and/or constitutional rights*" are not particularised. It is liable to be struck out.

115. As to paragraph 72.13:

115.1. This paragraph contains submissions regarding general propositions of law in respect of fiduciary duties that should be contained in a skeleton argument, not a statement of case.

115.2. Without prejudice to that contention, it is denied that either the claimed fiduciary duties, or the claim that those duties require the Defendants to take the positive steps sought, are contrary to authority.

115.3. In the premises, the reference to 'pure omission' is misconceived.

115.4. As to sub-paragraph (a), the phrase "*police, judiciary and bailiffs*" is misconceived and unhelpful rhetoric. The sub-paragraph is in any event denied, to the extent it can be understood. The Defendants were obliged to commit at the time TTL informed them it had lost control of its Bitcoin in the Addresses to assist TTL to regain that control once it had established its ownership of the Bitcoin in the Addresses, by court declaration if the Defendants considered its ownership to

be unclear. That does not render the 15th & 16th Defendants "*police, judiciary and bailiffs*".

115.5. As to sub-paragraph (b):

115.5.1. The updates to the Software sought are relatively straightforward.

115.5.2. The reference to the Defendants acting as "*bailiff*" by controlling the development of the Software governing the Networks, which they do on a day-to-day basis, makes the alleged analogy no clearer.

115.5.3. The relevance of the last sentence is not understood. TTL is not claiming that the Defendants owe fiduciary duties by reason of a court order; they owe fiduciary duties by reason of the role they have voluntarily undertaken.

115.6. As to sub-paragraph (c), even if it were correct, it would be irrelevant. However, the Software modification outlined at paragraph 26.2.2.3 above is a one-off modification that would then allow any owner with a court order declaring their ownership to regain access to their Bitcoin tokens.

116. As to paragraph 72.14, it is denied that it would be impossible for the Defendants to comply with the fiduciary duties claimed.

116.1. Sub-paragraphs (a) to (c) are denied for the reasons set out above.

116.2. Further, as to sub-paragraph (c), it is denied that the court order sought by this Claim needs to prescribe what updates the Defendants must write in respect of the Software governing the Networks; it need only set out what outcome the updated Software is to achieve.

116.3. As to sub-paragraph (d):

116.3.1. The updated Software would be adopted by the nodes and would not cause an airdrop (or so-called 'hard fork') for the reasons set out above.

116.3.2. In circumstances where the 15th & 16th Defendants, like all the other Defendants, would be required to comply with a court order or face contempt proceedings, it is denied that their reputation would be tarnished. In any regard, the relevance of the same is denied.

116.4. Sub-paragraph (e) is denied:

116.4.1. TTL is the true owner of the Bitcoin in the Addresses, and the current controller of the TTL Private Keys is/are fraudsters who, unlike TTL, do not have any proprietary interest in the Bitcoin in the Addresses.

116.4.2. Paragraph 11 of this Reply is repeated.

117. As to paragraph 72.15:

117.1. The first sentence is denied: TTL's losses arise as a result of the Defendants' refusal to comply with their fiduciary duties.

117.2. The second and third sentences are admitted, although their relevance is denied.

117.3. As to the remainder, the law imposes the fiduciary duties claimed.

118. As to paragraph 72.16:

118.1. The first sentence is denied: the class of persons to whom the 15th & 16th Defendants owe the claimed fiduciary duties is all the owners of ABC tokens, and that class is clearly defined, necessarily limited by the number of ABC tokens in existence, and knowable (even in circumstances where a court declaration is required to confirm that a person is a true owner).

118.2. The second, third and fourth sentences are admitted, but their relevance is denied.

118.3. The penultimate sentence is a repeat of the first sentence, and is denied.

118.4. The last sentence is denied in the premises (wherever the quote is from, which is not explained).

119. Paragraph 72.17 is misconceived:

119.1. The first sentence is admitted, but its relevance is denied.

119.2. The second sentence does not follow from the first and is denied. Paragraph 11 of this Reply is repeated.

120. Paragraph 72.18 is again a (misconceived) submission and has no place in a pleading. Without prejudice to that contention, there is no requirement for duties to be "*an incremental extension*" of any established fiduciary relationship.

121. As to paragraph 72.19:

121.1. As to the first sentence, it is admitted that owners of Bitcoin tokens have the ability to secure and back up their private keys, but it is denied that they could ever take steps to guard fully against theft or loss of their private keys.

121.2. As to the second and third sentences, the claim that TTL could insure against loss is wholly unparticularised and the 15th & 16th Defendants are required to prove it alongside their claim that they cannot, or cannot adequately, insure themselves.

122. Paragraph 72.20 is denied. Paragraphs 18, 19, 20, 22, 23 and 76 of this Reply are repeated.

123. As to paragraph 73, the preceding paragraph of this Reply is repeated.

124. As to paragraph 74.2, paragraphs 26.2.2, 35, 76 and 121.1 of this Reply are repeated.

125. As to paragraph 74.3, paragraphs 26.2.2, 35 and 76 of this Reply are repeated.

126. As to paragraph 74.4, the second sentence mischaraterises paragraph 44.d. of the APoC; the manipulation referred to therein is in relation to a wrongful transfer by fraudsters.

127. Paragraph 74.5 is denied for all the reasons already stated.

128. Paragraph 75 is denied. The precise formulation of the relief to be granted is a matter for trial, and paragraph 116.2 of this Reply is repeated.

129. Paragraph 77.2 is denied. The preceding paragraph is repeated.

130. As to paragraph 77.3:

130.1. As to the first sentence, paragraphs 26.2.2, 35 and 76 of this Reply are repeated.

130.2. In the premises, the second sentence is denied.

130.3. The final sentence is admitted but its relevance is denied. TTL wishes to have the ability to transfer its Bitcoin in the Addresses, but it is not required to commit to making such a transfer.

131. As to paragraph 77.4, insofar as it is alleged, it is denied that the 15th & 16th Defendants would escape liability for breaching their fiduciary duties to TTL by reason of their wrongly determining that TTL was not the owner of the ABC tokens in the Addresses (or by refusing to follow a Court order determining the same).

132. As to paragraph 77.5, it is denied that the nodes operating on the ABC Blockchain would refuse to download updated ABC Software made available by the 15th & 16th Defendants, for the reasons set out above.

133. As to paragraph 78.3:

    133.1. As to the first sentence, it is admitted that the declaration TTL seeks would not be *in rem*, but the significance of that is denied.

    133.2. As to the second sentence, those who have purported to assert rival claims are obvious cranks or time-wasters, and there is no serious contrary claim to ownership (consistently with the fact that TTL is in fact the owner), such that such (fraudulent) cranks and time-wasters are not proper defendants to the Claim (such individuals nonetheless being free to apply to be joined to the proceedings, were they to wish to do so).

    133.3. As to the third sentence, the order sought would be conclusive as to ownership between the parties, and any concern about it not being *in rem* is denied. Paragraph 11 of this Reply is repeated.

    133.4. As to the fourth sentence, the 15th & 16th Defendants do not escape the imposition of fiduciary duties by reason of their misplaced concern about 'rival claimants', if that is what is being alleged.

134. Paragraph 79.1 is denied for the reasons set out above.

135. Paragraph 79.2 is misconceived and is denied. TTL's loss is the value of the Bitcoin in the Addresses; paragraph 130.3 of this Reply is repeated, and the last sentence is irrelevant to the question of whether the Defendants are liable. It also proceeds on the false premise that the value of the Bitcoin is necessarily to be measured by reference to a single transaction to a single buyer of all of TTL's Bitcoin.

136. As to paragraph 79.3:

    136.1. The first sentence is denied. Those matters are irrelevant to whether the Defendants are liable and, in any event, TTL's conduct has been reasonable in all the circumstances.

    136.2. The second sentence is denied because it is based on a premise that TTL's conduct was unreasonable, which is denied, but is in any case irrelevant.

137. Paragraph 79.4 is denied for the reasons set out above.

138. Paragraph 79.5 is denied. In any event, a fiduciary is not required to be paid in order to be liable.

139. As to paragraph 80:

    139.1. The matters raised on the second, third and fourth sentences are repetitive and have been addressed above.

    139.2. As to the penultimate sentence, the bailiff analogy is inapt and denied.

    139.3. The final sentence is nonsensical and is denied. The Defendants are parties to the Claim and the 15th & 16th Defendants have failed to explain their bare and inappropriate assertion that they are being denied their right to a fair trial.

G: TORTIOUS DUTY OF CARE

140. Paragraph 81.1 is denied. In any regard, the duty of care alleged is a permissible extension of the *Quincecare* duty.

141. Paragraph 81.2 is denied. For the reasons set out in the APoC and above, the 15th & 16th Defendants voluntarily assumed responsibility to TTL by reason of voluntarily assuming roles that put them in control of the ABC Network, and it would be fair, just and reasonable to impose the duty of care claimed.

142. Paragraph 81.3 is denied for all the reasons set out above and in the APoC.

143. As to paragraph 81.5, the special relationship between the 15th & 16th Defendants and TTL arises as a result of the role undertaken by the 15th & 16th Defendants, as set out herein and in the APoC, and the fiduciary duties the 15th & 16th Defendants consequently owe TTL (and other owners of Bitcoin tokens), as also set out herein and in the APoC.

144. As to paragraph 81.6, this is irrelevant rhetoric and denied.

145. Paragraph 82 is denied. Paragraph 128 of this Reply is repeated.

146. Paragraphs 83.1 to 83.3 repeat earlier paragraphs of the D15-D16 Defence and TTL's response to those paragraphs stated herein is similarly repeated.

147. As to paragraph 83.4, it is the 15th & 16th Defendants who control the ABC Software and ABC Network. The final sentence is embarrassing and so cannot be pleaded to.

148. Paragraph 83.5 repeats claims made elsewhere in the D15-D16 Defence, and is denied for the reasons stated above.

149. Paragraph 83.6 is denied:

149.1. Points (a) and (b) are not relevant to the question of whether the 15th & 16th Defendants owe fiduciary duties. In any event, the amendments in question would be straightforward.

149.2. Points (c), (e), (f) and (g) are denied for the reasons set out above.

149.3. As to point (d):

149.3.1. The points pleaded therein, which are pleaded earlier in the D15-D16 Defence are denied for the reasons stated above.

149.3.2. The allegations regarding Dr Wright's conduct in respect of the Australian Tax Office and "*online articles and other research*" are all inadequately particularised and cannot be pleaded to. TTL reserves its right to plead to them if they are properly stated.

149.3.3. As to the allegations regarding unparticularised judicial and quasi-judicial findings against Dr Wright, they are liable to be struck out because: (i) findings made in other, previous judicial or quasi-judicial proceedings between different parties are not admissible in English civil proceedings as evidence of the correctness of those findings; and (ii) it is therefore an abuse of the court's process to plead in a Defence reliance upon judicial or quasi-judicial findings made in other proceedings as evidence of their correctness.

150. Paragraph 83.7 is denied for all the reasons set out in the APoC and herein. There is an obvious risk of imminent harm, as the Hackers could move the Bitcoin in the Addresses at any moment.

151. Paragraph 83.8 is denied for all the reasons set out in the APoC and herein. TTL has acted reasonably in all the circumstances and has not been contributorily negligent.

I: **RELIEF**

152. Paragraph 84 is denied for all the reasons set out in the APoC and herein. Paragraph 84.2 is liable to be struck out for the reasons set out above. Further, the declaration as to ownership would serve a useful purpose:

152.1. The declaration would further the aims of justice.

152.2. The issue of ownership is plainly in dispute between the parties and will be determined following argument between the parties.

152.3. If relevant, it would be fair, just and equitable for the Court to make a declaration as to TTL's ownership of the ABC tokens in the Addresses.

152.4. It is denied that the existence of any realistic rival claims to ownership of the Bitcoin in the Addresses would be relevant to the utility, fairness, justness or equitability of the declaration.

152.5. Regardless, there are no realistic rival claims and so the point does not arise.

152.6. Moreover, any such realistic rival claimants would be entitled to seek to be joined to the proceedings.

153. The relevance of paragraph 85 is denied. It is liable to be struck out.

<div align="right">

JOHN WARDELL KC

BOBBY FRIEDMAN

SRI CARMICHAEL

</div>

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: .... *Craig S Wright* ....

Name: Dr Craig Steven Wright

For and on behalf of Equator Consultants AG, a director of Tulip Trading Limited

31 July 2023
Date: …………………………………………………………….

For and on behalf of Equator Consultants AG, a director of Tulip Trading Limited