Claim No: BL-2021-000313

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

BETWEEN:

TULIP TRADING LIMITED

Claimant

and

(1) BITCOIN ASSOCIATION FOR BSV (A SWISS VEREIN)
(2) [redacted]
(3) [redacted]
(4) [redacted]
(5) [redacted]
(6) [redacted]
(7) [redacted]
(8) [redacted]
(9) [redacted]
(10) [redacted]
(11) [redacted]
(12) [redacted]
(13) [redacted]
(14) [redacted]
(15) [redacted]
(16) [redacted]

Defendants

DEFENCE OF THE SECOND TO TWELFTH DEFENDANTS

A. INTRODUCTION

1. This is a fraudulent claim. TTL does not own the digital assets it claims to own in these proceedings and has never owned them. As particularised at paragraph 30 below, TTL has made a deliberately false claim to ownership of those assets and has commenced these proceedings knowing that it has no claim in respect of those assets. The claim is accordingly an abuse of the Court's process.

2. In this Defence:

   2.1. All paragraph references are to the Amended Particulars of Claim dated 13 February 2023 ('**APoC**') save where otherwise stated.

   2.2. Save to the extent that the definitions in the APoC (and in particular at paragraphs 2 and 4 thereof) are consistent with the definitions set out in Part B below, those definitions are not adopted.

   2.3. Where any headings or defined terms used in the APoC are adopted, no admissions are thereby made.

   2.4. Any averment as to, or summary of, the contents or effect of a document is without prejudice to the full terms of the document in question, on which the Second to the Twelfth Defendants ('**the Enyo Defendants**') reserve the right to rely at trial.

3. There are a number of passages in the APoC containing what would appear to be submissions of law as to the characterisation of the Bitcoin System (as defined below), supposed analogies with conventional assets, or what public policy requires. These are not proper pleas and the Enyo Defendants generally do not plead to them.

B. THE BITCOIN SYSTEM AND DEFINITIONS USED IN THE DEFENCE

(1) <u>The origin and development of Bitcoin</u>

4. '**Bitcoin**' (with ticker '**BTC**') is a cryptocurrency that enables payments to be made online by one party to another without the need for a trusted third party as intermediary. The term 'Bitcoin' is sometimes used as a reference to the system that facilitates transactions of BTC, but all references to 'Bitcoin' in this Defence are references to the cryptocurrency with ticker BTC.

5. As pleaded at paragraphs 6-8 below, Bitcoin was created by Satoshi Nakamoto ('**Satoshi**'), which is a pseudonym for a person or group of persons whose identity is unknown.

6. On 31 October 2008, a paper titled '*Bitcoin: A Peer-to-Peer Electronic Cash System*' (the '**White Paper**') was released under the name Satoshi to a mailing list known as the '*metzdowd cryptography*' mailing list. As to this:

    6.1. The White Paper was also hosted on SourceForge from December 2008 under the MIT Licence (an open source software licence the terms of which are pleaded at paragraph 10 below).

    6.2. An updated version of the White Paper was posted on SourceForge on 24 March 2009, also under the MIT Licence.

    6.3. The White Paper stated that the Bitcoin System (as defined at paragraph 8 below) was intended to be an electronic payment system based on cryptographic proof that would enable any two willing parties to transact directly with each other without the need for a trusted third party (such as a bank) as intermediary. This was to be achieved by the use of a peer-to-peer network consisting of computer 'nodes' that would (using the necessary software) verify transactions by applying a decentralised consensus mechanism. Verified transactions were to be recorded in a public ledger known as a blockchain.

    6.4. All references in this Defence to '**nodes**' are to nodes in the sense defined in paragraph 6.3 above, namely a computer running the relevant software that connects to other nodes running that same piece of software. This collection of nodes connected to other nodes constitutes the Bitcoin network.

    6.5. All references in this Defence to **'decentralised**' are to the concept of 'decentralised consensus' referred to in paragraph 6.3 above, namely a method of reaching agreement as to which version of Bitcoin's history is the active version without the need for or interference of any trusted third party such as a bank.

7. Satoshi released software implementing the concepts referred to in the White Paper on 8 January 2009 (the '**Original BTC Software**').

8. The system that enables transactions in Bitcoin (i.e. BTC) will be referred to in this Defence as the '**Bitcoin System**'. The Bitcoin System consists of the following components:

   8.1. A peer-to-peer network of nodes, referred to in this Defence as the '**BTC Network**'.

   8.2. A blockchain (the '**BTC Blockchain**') which is created by nodes participating in the BTC Network. The BTC Blockchain consists of blocks which record verified transactions. Each block is identified by a cryptographic hash and contains the hash of the previous block. The sequence of hashes linking each block to the previous block creates a chain going back to the first block, which first block is referred to in this Defence as the '**Genesis Block**'.

   8.3. Software used by each node. As to this:

      8.3.1. The Original BTC Software released by Satoshi on 8 January 2009 included the source code, the executable program and the Genesis Block.

      8.3.2. As pleaded at paragraph 11 below, the Original BTC Software has subsequently been developed by a community of contributors. The most popular node software used by nodes in the BTC Network stems from this development and is generally known as '**Bitcoin Core**'.

      8.3.3. Bitcoin Core is not the only software that can be (or is) used by nodes in the BTC Network. Other compatible software include btcd, libbitcoin, Bitcoin Knots and bitcore.

   8.4. A set of rules to determine the validity of transactions and blocks, referred to in this Defence as the '**Consensus Rules**'.

8.5. A mechanism for reaching decentralised consensus on the valid blockchain which, as pleaded at paragraph 16.7 below, will be the chain with the most accumulated proof-of-work among those valid under the Consensus Rules.

9. No individual or group of persons has or has had responsibility for the Bitcoin System or the power to consent to, or withhold consent for, improvements or changes to the software used by other participants' nodes in the BTC Network. In particular:

9.1. The existence of such a power would be inconsistent with the Bitcoin System envisaged by Satoshi because it would make the holder of that power a trusted third party.

9.2. It is not conceptually possible for such a power to exist because nodes in the Bitcoin System are not obliged to use Bitcoin Core or any particular node software. It is for Bitcoin participants to decide which node software (and which version of it) to use.

9.3. If modifications made to a particular node software are thought by Bitcoin participants to be unsuitable, those Bitcoin participants are not obliged to continue to use it and would in practice switch to another node software.

10. The terms of the MIT Licence under which the Original BTC Software was released by Satoshi included the following:

10.1. The software was released 'as is' and without warranty of any kind.

10.2. Neither the author of the software nor copyright holders was to be liable for '*any claim, damages or other liability, whether in an action of contract, tort or otherwise, arising from, out of or in connection with the software or the use or other dealings in the software*.'

10.3. Any person obtaining a copy of the software had permission to deal in it without restriction, including (without limitation) the rights to use, copy, modify, merge, publish and distribute it.

11. As a result of the fact that the Original BTC Software was released under the MIT Licence:

11.1. The Original BTC Software is and has at all material times been open source and non-proprietary.

11.2. Contributors who choose to use it are able to propose changes to improve the software and resolve flaws.

11.3. They are also able to create new software using the source code for the Original BTC Software as a basis and encourage others to use that software in preference to the Original BTC Software.

11.4. A community of contributors emerged from mid or late 2009. Save that its output is governed by the MIT Licence, this community has no formal organisation, management or structure.

12. In or around early 2011, Satoshi withdrew from the community of contributors (or developers as they are also known) and from any role in developing the Bitcoin System.

(2) <u>The operation of the Bitcoin System</u>

13. Bitcoin transactions generally use public key cryptography to create key pairs that allow users to transfer Bitcoin. As to this:

13.1. Each user's key pair consists of a private key and a public key.

13.2. A Bitcoin address, which is derived from the public key, is public. It represents the address into which its owner can receive funds or out of which its owner can send funds.

13.3. The private key is required for the user to spend, withdraw, transfer or carry out any other transaction in respect of the digital assets at the public address to which it relates. It is the possession of the private key that constitutes ownership of the Bitcoin at the public address to which the private key relates.

13.4. Owners of cryptocurrencies, such as Bitcoin, commonly store their private keys in a 'wallet', which can be a hardware device or a software application.

14. New transactions in Bitcoin, when they occur, are added to a temporary pool of unconfirmed transactions maintained by each node participating in the BTC Network. Until a transaction is confirmed, it is not added to the BTC Blockchain.

15. The mechanism that allows transactions to be confirmed is known as mining. Only mining nodes are referred to as miners; and not all nodes are mining nodes.

16. The process of mining involves the following steps:

    16.1. The first step is the addition of unconfirmed transactions into a new candidate block.

    16.2. Miners then compete to solve a cryptographic hash problem. A valid solution to the equation is known as the 'proof of work'.

    16.3. The first miner to find a solution (i.e. the proof of work) broadcasts its block to the BTC Network.

    16.4. The Consensus Rules allow that first miner to award itself up to a predetermined amount of Bitcoin in the new block in addition to any transaction fees.

    16.5. Each node (whether a mining node or a non-mining node) that receives the new block conducts a validation process by reference to the Consensus Rules to verify whether the new block is valid. As a result, only valid blocks are recorded on the BTC Blockchain and invalid blocks are rejected.

    16.6. If and when the new block is validated in this way, each node (whether a mining node or a non-mining node) adds it to its own copy of the BTC Blockchain.

    16.7. Although blocks can arrive at different nodes at different times, each node always selects (and each mining node always attempts to extend) the chain of blocks that represents the most proof of work, i.e. the greatest cumulative work chain. This ensures that the BTC Network will converge to a consistent state (i.e. agreeing on one BTC Blockchain).

17. It is the software used by the miners that determines the Consensus Rules applied to the blocks that they mine. As further particularised below, if all Bitcoin users in a network do not use the same Consensus Rules, a 'hard fork' can result, giving rise to a new cryptocurrency. This is undesirable and regarded by the cryptocurrency community as undesirable for the reasons pleaded at paragraph 21.4 below.

(3) The meaning and cause of hard and soft forks

18. No one developer or group of developers can require users to use Bitcoin Core or any modified version of Bitcoin Core or any Bitcoin software. As to this, paragraph 9 above is repeated.

19. The modification of Bitcoin Core is itself governed by a process that is dependent on consensus. The procedure is as follows (save in respect of proposed changes to the Consensus Rules, which are governed by a different procedure):

    19.1. Anyone has the ability to propose a software modification by creating what is known as a '**pull request**', which is a proposed change to the code or documentation in the relevant source code repository (such as GitHub).

    19.2. The pull request can be reviewed by anyone who wishes to do so. This involves a review of both the nature of the modification (i.e. the concept) and its proposed execution (i.e. the code).

    19.3. Maintainers of the relevant repository in which Bitcoin Core is stored then decide, based on comments from reviewers, whether there is general agreement (i.e. consensus) to merge the pull request into Bitcoin Core. The role of maintainers is particularised more fully at paragraph 52 below.

    19.4. From time to time, new versions of Bitcoin Core are released which incorporate all pull requests that have been merged into Bitcoin Core since the previous release. But it is for operators of nodes running the previous (or still previous) version of Bitcoin Core to decide whether to install the updated software. They have no obligation to do so and are free to use prior versions of Bitcoin Core or other node software altogether, such as libbitcoin, as to which paragraph 8.3.3 above is repeated.

20. A 'soft fork' occurs when Consensus Rules are changed to make them more restrictive. As to this:

    20.1. The effect of making the Consensus Rules more restrictive is that a block validated under the new rules would necessarily also be valid under the old rules. This means that a node that does not implement the modified Consensus

Rules is nonetheless able to process blocks created under those rules because they are by definition valid under the old rules, which are less restrictive.

20.2. Such a change to the Consensus Rules is known as a backwards compatible change or a soft fork.

20.3. Blocks created under the old Consensus Rules will not necessarily be valid under the new, more restrictive, Consensus Rules.

21. By contrast, a 'hard fork' occurs where a change to the Consensus Rules makes them less restrictive such that some blocks which would have been invalid under the previous Consensus Rules would now be regarded as valid. As to this:

21.1. A node that does not implement that change will be unable to process blocks created under the new Consensus Rules if they are invalid under the old Consensus Rules. Such a change to the Consensus Rules is known as a change that is backwards incompatible.

21.2. If the change is unanimously adopted by nodes in the BTC Network, a chain split will not occur because all new blocks will be created and validated by reference to the new rules.

21.3. If the change is not adopted or rejected unanimously (i.e. by every single Bitcoin participant) and its behaviour is triggered, a chain split will occur as follows:

21.3.1. Upon the mining of blocks which are invalid under the old Consensus Rules but valid under the new Consensus Rules, the BTC Network will split.

21.3.2. The split will occur because nodes running software based on the previous Consensus Rules will disconnect from nodes running software based on the new Consensus Rules. As a result, there will be two networks of nodes, each consisting of nodes running software based on distinct sets of Consensus Rules (the previous Consensus Rules or the new Consensus Rules, as the case may be).

21.3.3. The mining power will correspondingly split, with mining nodes mining blocks based on the respective Consensus Rules that they are following. Each of the resulting networks accepting distinct blocks due to incompatible Consensus Rules would constitute distinct currencies.

21.4. A hard fork is undesirable (and regarded by the cryptocurrency community as undesirable) for various reasons which include the following:

21.4.1. A hard fork affects the value of the original cryptocurrency (which would be split between the original and the forked cryptocurrency).

21.4.2. It would give rise to significant costs to users of the existing network.

21.4.3. The existence of multiple blockchains operating in a similar manner can result in users not running node software to transact on the wrong blockchain, causing substantial losses.

21.4.4. A hard fork can have, and usually has, adverse tax implications because the asset created by the hard fork is treated in some jurisdictions as income.

21.4.5. The existence of a new related chain can (and has in the past) exposed bugs in node software causing outages and requiring additional fixes.

(4) <u>History of hard and soft forks</u>

22. Since the Bitcoin System was created in 2009, there have been a number of soft forks.

23. There have also been some hard forks and corresponding chain splits, including (but not limited to) the following.

24. On 1 August 2017, a new implementation of Bitcoin Core, known as the '**BCH Software**' or the '**BCH ABC Software**', was deployed. As to this:

24.1. The main purpose of the change was to increase the blocksize limit from 1MB to 8MB.

24.2. This arose from a disagreement within the community as to the blocksize limits in the Consensus Rules. The participants in favour of increasing the blocksize

introduced the BCH Software in order to provide nodes with an option to use a distinct blockchain with a different and incompatible set of Consensus Rules.

24.3. The deployment of the BCH Software resulted in a hard fork because it was based on backward incompatible Consensus Rules.

24.4. The hard fork gave rise to a new system (the '**BCH System**') which included a new network (the '**BCH Network**'), a new blockchain (the '**BCH Blockchain**') and a new cryptocurrency, 'Bitcoin Cash' with ticker 'BCH' ('**BCH**').

24.5. Owners of BTC at the time of the August 2017 hard fork became owners of an equivalent amount in BCH in addition to the BTC they already owned. But, when a chain split occurs, the market value of the original asset tends to be split between the original and forked asset and that is what happened when the August 2017 hard fork occurred.

25. On 15 November 2018, two further hard forks occurred in respect of the BCH System. As to these:

25.1. On 16 August 2018, nChain, a company established by Dr Wright, announced alternative software for the BCH System called Bitcoin Satoshi Vision (the '**BSV Software**'). Among other changes, the BSV Software provided for the blocksize limit to increase from 32MB to 128MB.

25.2. The use of the BSV Software resulted in a hard fork from the BCH System, giving rise to a new system (the '**BSV System**') which included a new network (the '**BSV Network**'), new blockchain (the '**BSV Blockchain**') and new cryptocurrency, 'Bitcoin Satoshi Vision' with ticker 'BSV' ('**BSV**').

25.3. At the same time, a new version of the BCH ABC Software was released, which provided for certain backwards incompatible changes relating to the transaction order and Opcodes (Opcodes are computer instructions which can be included in transactions to specify programmatic rules which constrain how funds can subsequently be spent).

25.4. The new version of the Bitcoin ABC Software was adopted by a majority of mining and non-mining nodes in the BCH Network. It was accepted within the

cryptocurrency community that this should continue to be referred to as the BCH System, which included the BCH Network, the BCH Blockchain and the cryptocurrency referred to as BCH above.

25.5. Owners of BCH at the time of the two hard forks pleaded above became owners of the equivalent amount of BSV in addition to the amount of BCH they already owned. Paragraph 21.4.1 above is repeated. The value of the forked BSV token was a small fraction of the original BCH token: on 15 November 2018, 1BTC was worth US$5,775.82 (high) and US$5,358.38 (low) whereas 1BSV was worth US$179.51 (high) and US$70.97 (low).

25.6. BSV today has very little value compared to BTC and is rarely used in the cryptocurrency community. As at 26 April 2023, 1 BTC is worth US$28,850.51 and 1 BSV is worth US$34.45 (BTC was therefore more than 800 times as valuable as BSV as at the aforesaid date).

C. PART I OF THE AMENDED PARTICULARS OF CLAIM

26. As to paragraph 1, the Enyo Defendants hereby give notice under CPR 32.19 that they require the authenticity of every document disclosed to them or relied upon by TTL to be proved at trial.

27. Paragraph 2 contains defined terms that are both tendentious and at odds with how they are used in the cryptocurrency community. In particular:

27.1. The digital asset class referred to in paragraph 2 as '*so-called Bitcoin Core ('BTC')*' is in fact BTC, commonly known as Bitcoin, as pleaded at paragraph 5 above. Bitcoin Core is a software, not a digital asset class (i.e. a cryptocurrency), as to which paragraph 8.3.2 above is repeated.

27.2. The tendentious use of the phrase 'so-called' in paragraph 2 is not adopted.

27.3. It is admitted that the four digital asset classes referred to in paragraph 2 are digital asset classes. For the avoidance of doubt:

27.3.1. What paragraph 2 (wrongly) describes as 'so-called Bitcoin Core' is referred to in this Defence as BTC.

27.3.2. What paragraph 2 (wrongly) describes as 'so-called Bitcoin Cash' is referred to in this Defence as BCH.

27.3.3. What paragraph 2 (wrongly) describes as 'so-called Bitcoin Cash ABC' is referred to in this Defence as ABC.

28. As to paragraph 3:

28.1. The first sentence is not admitted.

28.2. The second sentence is not admitted, save that the words '*including those particularised below*' are denied. It is averred, for the reasons pleaded at paragraph 53 below, that TTL is not, and has never been, the legal (or, if alleged, beneficial) owner of the digital assets in the Addresses.

28.3. The third sentence is not admitted.

28.4. The fourth sentence is not admitted, save that it is denied that Dr Wright is a renowned computer scientist. In particular:

28.4.1. Dr Wright does not have a computer science degree.

28.4.2. Dr Wright does not have the ability to code C++ (alternatively, does not have anything beyond the ability of a beginner).

28.4.3. Dr Wright failed his Theory of Computation course in his Information Systems Security programme at Charles Sturt University. The Theory of Computation course was the only true computer science course in the curriculum.

28.4.4. Dr Wright does not have a significant publication history or impact factor in computer science journals.

28.4.5. Dr Wright's claims to renown are heavily disputed in the cryptocurrency and scientific communities.

28.4.6. Dr Wright has in other proceedings given deliberately false evidence as to matters concerning his scientific standing, such as invitations to academic conferences and the supposed acceptance of academic papers

following peer review. As to this, paragraph 54.9.6 below is repeated. It is to be inferred that he is not a renowned computer scientist because such a person would not give (or need to give) false evidence about their standing in the scientific community.

28.5. The fifth sentence is denied. Dr Wright is not Satoshi and did not create the Bitcoin System. In particular:

28.5.1. Dr Wright's claim that he is Satoshi has been discredited in the cryptocurrency community.

28.5.2. Dr Wright has displayed ignorance of obvious matters concerning the Bitcoin System of which the inventor of the system (i.e. the real Satoshi, whoever that is) would not be ignorant. As examples of this, and without prejudice to the generality of the foregoing, paragraphs 44.2 and 46.1 below are repeated.

28.5.3. If Dr Wright were Satoshi, it would be easy for him to attempt to prove that, for example by:

28.5.3.1. releasing the original document of the White Paper that Satoshi published in 2008 or the pre-release builds of bitcoin.exe.

28.5.3.2. using the relevant private key to sign a message on the Genesis Block (or any of the public addresses known to be controlled by Satoshi).

28.5.3.3. releasing the original private correspondence between Satoshi and other members of the community.

28.5.3.4. signing a message with Satoshi's well known PGP key.

28.5.4. Dr Wright has not done so because (it is to be inferred) he is not Satoshi.

29. As to paragraph 4:

29.1. The first two sentences are admitted. As to this:

29.1.1. The Bitcoin Association was founded by Calvin Ayre, who is also a member of its executive committee.

29.1.2. The President of the Bitcoin Association is Jimmy Nguyen, who is a long time collaborator of Dr Wright and was previously the CEO of nChain, of which Dr Wright is founder and Chief Science Officer.

29.1.3. BSV is developed by staff of nChain rather than by staff of the Bitcoin Association.

29.1.4. Dr Wright is closely associated with Mr Ayre, who has funded many of Dr Wright's projects and litigation in which Dr Wright is involved.

29.1.5. Mr Ayre is the publisher of CoinGeek, which is supportive of and closely associated with BSV.

29.1.6. Mr Ayre owns a stake in TAAL, which is the largest BSV block producer.

29.1.7. Mr Nguyen has previously acknowledged that the Bitcoin Association is funded by Mr Ayre.

29.1.8. In the premises, it is to be inferred that the Bitcoin Association is controlled by Dr Wright and funded by Mr Ayre.

29.2. As to the third sentence:

29.2.1. It is denied that there are '*controllers*' or '*operators*' of the BTC Network. Paragraphs 9-11 above are repeated.

29.2.2. It is admitted that the Enyo Defendants are, or were previously, developers of the BTC Network in the sense that they made contributions to the BTC Network as members of the voluntary community of contributors referred to at paragraph 11.4 above. The role of the Enyo Defendants in the BTC Network is pleaded in more detail in paragraphs 49-53 below.

29.2.3. Save as aforesaid, the third sentence is denied.

29.3. The Enyo Defendants do not plead to the fourth sentence and fifth sentences, which do not concern them.

29.4. The sixth and seventh sentences are noted. The eighth sentence is not a proper plea, containing as it does the reservation of a right that TTL does not have and which should not be pleaded even if it did.

D. DEFENDANTS' CASE AS TO ABUSE OF PROCESS

30. It is averred that this claim is an abuse of process because it has been brought by TTL fraudulently in the knowledge that it has no claim. As to this:

30.1. As pleaded at paragraph 54 below, Dr Wright and TTL do not have and have never had an interest of any kind in the digital assets in the Addresses.

30.2. Dr Wright and TTL must, necessarily, have known this and did know it.

30.3. In the premises, this claim is an abuse of process because Dr Wright and TTL have known at all material times that TTL has no claim.

E. PART II OF THE APOC

(1) Bitcoin as a digital asset

31. Paragraph 5 is admitted, save that:

31.1. it is averred that the term 'Bitcoin' is used in the cryptocurrency community as a reference to BTC. All references below to Bitcoin (and in admissions, non-admissions or denials of allegations in the APoC that use the term Bitcoin) are to BTC save where otherwise specified;

31.2. it is not admitted that Bitcoin is property capable of being owned as a matter of English law.

32. As to paragraph 6:

32.1. The first sentence is admitted, save that it is averred that Bitcoin held as an asset on third party exchanges is owned by the exchange in question, which in turn owes a separate obligation to the customer.

32.2. The second sentence is admitted.

(2) <u>The blockchain</u>

33. Paragraph 7 is admitted, save that:

33.1. The vague reference to '*the reasons explained further below*' is not understood and no admissions are made in respect of it.

33.2. The implicit allegation that it is not possible to undertake transactions involving Bitcoin without recording them on the blockchain is denied. Such transactions are possible and the Bitcoin Lightning system is an example of it.

34. Paragraphs 8 and 9 are admitted, save that:

34.1. The second sentence of paragraph 8 is not admitted, as to which paragraph 3 above is repeated.

34.2. Paragraph 33.2 above is repeated.

(3) <u>The role of nodes/miners</u>

35. As to paragraph 10:

35.1. The implicit allegation in each of the first, third, fifth and sixth sentences that all nodes are miners is denied, as to which paragraph 16 above is repeated. Save as aforesaid, each of those sentences is admitted.

35.2. The second, fourth and seventh sentences are admitted.

35.3. There is no person or group of persons who '*controls the network*'. The eighth sentence is accordingly denied, save that it is admitted that miners do not control the network.

36. As to paragraph 11:

36.1. The first sentence is admitted, save that: (i) the first sentence of paragraph 35.1 above is repeated *mutatis mutandis*; and (ii) there is a 'payment' to miners only in the sense that coins are issued to them by the Bitcoin System itself (rather than by any individual, group or entity).

36.2. The second sentence is not admitted. Paragraph 3 above is repeated.

36.3. The third and fourth sentences are admitted, save that it is denied, if alleged, that the transaction fee is proportionate to the amount of Bitcoin transferred (it is not necessarily proportionate either to the amount or to the size of the transaction).

37. As to paragraph 12:

37.1. The first sentence is denied. Both the number of nodes and the number of nodes that control the hash power vary with time and are incapable of precise estimation.

37.2. The second sentence is not admitted.

(4) <u>Addresses on the blockchain</u>

38. As to paragraph 13:

38.1. The first sentence is admitted, save that the supposed analogy with a bank account number is not admitted, as to which paragraph 3 above is repeated.

38.2. The third sentence is admitted, save that the supposed analogy with a bundle of cash is not admitted, as to which paragraph 3 above is repeated.

38.3. The fourth sentence is admitted.

38.4. As to the second and fifth sentences:

38.4.1. The 1Feex address with the lowercase 'f' at the end does not and cannot exist. It is an invalid address because addresses contain a built-in checksum such that only certain combinations are valid and the address with the lowercase 'f' at the end is not such a combination.

38.4.2. Save as aforesaid, it is admitted that the two addresses referred to exist, but it is denied (for the reasons set out at paragraph 54 below) that they are owned by TTL.

(5) <u>The existence of multiple blockchains</u>

39. As to paragraph 14:

39.1. The first three sentences are admitted.

39.2. Paragraphs 14(a) and 14(c) are denied. In particular:

39.2.1. It is denied that what is now BSV is the 'original Network'. The original Network is BTC. Paragraphs 4-7 and 25 above are repeated.

39.2.2. The blockchain for the BCH, BSV and ABC networks were not created by copying the blockchain of any pre-existing network but as a result of a hard fork as pleaded at paragraph 23 above.

39.3. Paragraph 14(b) is denied save that it is admitted that, at the time of the occurrence of the hard forks, the blockchain for the old network and the new network will be the same.

40. As to paragraph 15:

40.1. The first sentence is admitted.

40.2. The second sentence and sub-paragraphs 15(a)-15(c) are denied save insofar as they are consistent with the matters pleaded at paragraph 24 above.

41. As to paragraph 16:

41.1. The first sentence is admitted.

41.2. Paragraph 16(a) is denied. In particular:

41.2.1. The first sentence is denied. BSV was a fork of BCH as pleaded at paragraph 25.2 above.

41.2.2. The second sentence is denied. The BSV Software contained backward incompatible changes which resulted in the hard fork pleaded at paragraph 25.3 above.

41.2.3. The third sentence is admitted but it is denied that the developers used the same protocols and instructions as they had prior to the occurrence of the hard fork.

41.3. Paragraph 16(b) is denied save as insofar as it is consistent with the matters pleaded at paragraph 25 above.

42. Paragraph 17 is admitted, save that what occurred was a hard fork, not an airdrop.

(6) <u>Lack of encryption and the use of private keys</u>

43. Paragraph 18 is admitted.

44. As to paragraph 19:

44.1. Save that private keys are not necessarily generated by a digital algorithm, the first sentence is admitted.

44.2. It is denied that the use of private keys prevents double counting. As the inventor of Bitcoin would know, the feature of the Bitcoin system which allows double spends to be prevented in the decentralized setting is proof of work. Save as aforesaid, the second sentence is admitted.

45. As to paragraph 20:

45.1. The first sentence is denied. It is inherent in the nature and design of the Bitcoin System that the holder of a private key is the owner of the digital asset with which that private key is associated, as Satoshi expressly said in February 2009.

45.2. The second sentence is admitted but it is denied that it follows from this that someone other than the holder of the private key can be the owner of the digital asset.

45.3. The third sentence constitutes an impermissible argument or submission, as to which paragraph 3 above is repeated.

46. As to paragraph 21:

46.1. The first sentence is denied. The reasons why a private key is required to transfer Bitcoin include the following (of which it is averred the inventor of Bitcoin, Satoshi, would be aware):

46.1.1. It is inherent in the design of the Bitcoin System that a user's private keys are required to undertake a transaction. It would be inconsistent with the foundational principles of the Bitcoin System to permit access to coins without the private key, as to which paragraph 67.2.3 below is repeated.

46.1.2. Many users of the Bitcoin System have a desire and expectation of anonymity, which is consistent only with a system in which private keys are required to undertake a transaction.

46.2. It is admitted that developers can write the software referred to in the second and third sentences but to do so would be (i) contrary to the basic principles of the Bitcoin System, and (ii) of no utility. As to (i), paragraph 46.1 above is repeated. As to (ii), developers, as pleaded at paragraph 9 above, have no power to compel nodes to use such software and it is inevitable (alternatively, likely) that they will not use such software since to do so would be contrary to the basic principles of the Bitcoin System. Save as aforesaid, the second sentence is denied.

46.3. The fourth sentence is denied. Even if the developers were to write the software referred to in the second and third sentences, the so-called legitimate owner would not be able to access the Bitcoin except on the new network formed by nodes that agreed to use that software, which (as pleaded above) they would not.

47. Save that storing private keys without adequate security is risky and would be regarded as such by the cryptocurrency community, paragraph 22 is admitted.

48. Paragraph 23 is embarrassing. It belongs (if anywhere) in a written opening for trial, not in a pleading.

(7) The role of the Developers

49. As to paragraph 24:

49.1. The first sentence is denied. In particular:

49.1.1. The so-called 'Developers' are no more than members of a voluntary community of contributors as pleaded at paragraph 11 above. Any use of the word 'developers' in this Defence is used in this sense. Neither they nor others have the power to force users in the BTC network to use any particular software. Paragraphs 9-11 and 18 above are repeated.

49.1.2. Each user of the BTC Network chooses and controls the software they use. There is no restriction in the BTC Network on the software that may be used by nodes in order to form part of the network.

49.1.3. Bitcoin Core and other BTC Network software do not use automatic or forced updates.

49.2. The second and third sentences are admitted, save that:

49.2.1. It is denied that these matters are capable of supporting the allegation in the first sentence.

49.2.2. The unidentified and unparticularised allegation implicit in the pejorative label 'so-called' is denied.

49.2.3. There is no common financial interest between the developers by virtue of the payments referred to in paragraph 24 or otherwise.

49.2.4. There are many other contributors to Bitcoin Core (not named as defendants by TTL) who also receive the payments referred to in paragraph 24.

50. As to paragraph 25:

50.1. The words '*in effect*' in the first sentence are both ambiguous and an implicit acknowledgment that developers do not in fact control the network in question.

The first sentence is in any event denied for the reasons pleaded at paragraph 49 above.

50.2. Paragraph 25(a) is not admitted.

50.3. Paragraph 25(b) is denied. Paragraph 49 above is repeated. Further, whilst it is admitted that all of the Enyo Defendants have contributed to the development of BTC Core at different times and in different respects, it is denied that the Second, Third, Sixth, Tenth and Twelfth Defendants remain active contributors to BTC Core. As to this:

50.3.1. The Second Defendant ceased making contributions in January 2021;

50.3.2. The Third Defendant ceased making contributions in January 2021;

50.3.3. The Sixth Defendant ceased making contributions in December 2021;

50.3.4. The Eleventh Defendant ceased making contributions in March 2017; and

50.3.5. The Twelfth Defendant ceased making contributions in February 2019.

51. As to paragraph 26:

51.1. Each sentence of paragraph 26(a) is denied. Paragraph 49.1 above is repeated.

51.2. Paragraphs 26(b) and 26(c) are vague and, pending proper particularisation, are not admitted.

52. As to paragraph 27:

52.1. The GitHub repository used by Bitcoin Core (the '**BTC GitHub**') is a commercial web service provided by Microsoft to aid collaboration in software development.

52.2. It is admitted that the BTC GitHub is the platform on which node software that is compatible with the BTC Network is developed. It is not the only such source. There are other repositories which contain mirrors of the software including older versions of Bitcoin Core.

52.3. The ability to control the BTC GitHub does not give the person who has such control the ability to control the BTC Network or to require nodes in the BTC Network to use the software on the BTC GitHub (or any other software). The BTC Network is controlled by all the Bitcoin users through the selection of the Consensus Rules that their computers apply (i.e. the node software that they choose to run).

52.4. It is admitted that certain of the Enyo Defendants have (or have had) credentials that enable them to merge changes into the BTC GitHub page. These are:

52.4.1. The Second Defendant, who had access credentials from June 2011 until February 2023;

52.4.2. The Third Defendant, who had access credentials from November 2015 until October 2021;

52.4.3. The Fourth Defendant, who has had access credentials from May 2011 (and still holds those credentials);

52.4.4. The Fifth Defendant, who had access credentials from April 2014 until February 2023;

52.4.5. The Sixth Defendant, who had access credentials from December 2018 until September 2019;

52.4.6. The Seventh Defendant, who has had access credentials from June 2019 (and still holds those credentials);

52.4.7. The Twelfth Defendant, who had access credentials from February 2012 until December 2015

52.5. The Eighth, Ninth, Tenth and Eleventh Defendants have never held access credentials that enabled them to merge changes into the BTC GitHub page.

52.6. In the premises, paragraph 27 is denied, save that the last sentence is not admitted.

53. As to paragraph 28:

53.1. The first two sentences are embarrassing in that they do not identify what '*very substantial power*' the developers have, in respect of what they exercise '*a substantial degree of discretion*' or what '*choices*' they are able to make. Without prejudice to the foregoing, the first two sentences are denied, for the reasons pleaded at 49-52 above.

53.2. As to paragraph 28(a):

53.2.1. The first sentence is admitted.

53.2.2. It is denied that Dr Wright had any role or did anything to fix the bug.

53.2.3. Satoshi (not Dr Wright) published a new version of the Bitcoin client to fix the bug and published a forum post identifying steps individual users could take to fix the issue on their individual nodes.

53.2.4. Individual users were not obliged to adopt these recommendations but it was rational for them to do so because it was not in the interests of any user for the bug not to be fixed.

53.2.5. Individual users therefore chose to adopt Satoshi's recommendations.

53.2.6. It is denied, if so alleged, that a similar bug could, were it to arise today, be resolved in a similar fashion. The incident referred to above took place only 18 months after Bitcoin's inception when the BTC Network and the value of Bitcoin were both a fraction of what they are today.

53.2.7. Satoshi, as the inventor of Bitcoin, had more influence over users than any of the Enyo Defendants. It is in any event denied, if so alleged, that even a recommendation by Satoshi would persuade users to implement the software change that TTL seeks.

53.2.8. In the premises, and save as aforesaid, paragraph 28(a) is denied.

53.3. As to paragraph 28(b):

53.3.1. The first sentence is denied. Developers do not usually have the ability to determine whether any alleged fraud has in fact been committed.

Even if they did, developers do not have the ability to reverse the fraud whether as alleged or otherwise, because they have no power to compel users to use any particular software, as to which paragraph 67.5 below is repeated.

53.3.2. The second sentence is denied. It would appear to be yet another repetition (this time of paragraph 21), as to which paragraph 46 above is repeated.

F. TTL'S ALLEGED OWNERSHIP OF THE BITCOIN IN THE ADDRESSES

54. It is to be inferred that neither TTL nor Dr Wright owns, or has ever owned, the Bitcoin in the Addresses (save where otherwise specified, all references below to Dr Wright's alleged ownership of the Bitcoin in the Addresses include alleged ownership by TTL or any other entity allegedly related to Dr Wright). In particular:

54.1. There are no genuine contemporaneous records of the alleged purchase of the Bitcoin at the Addresses.

54.2. The purchase order submitted by Dr Wright in these proceedings purportedly as evidence of the alleged purchase of the Bitcoin at the 1Feex Address is a forgery. In particular:

54.2.1. The purported purchase order is based on a free online template that was released in 2015 (four years after the alleged purchase).

54.2.2. It states that there is a mining fee of US$75, but no such fee is shown on the BTC Blockchain.

54.2.3. It states that 80,000 Bitcoin was purchased but the BTC Bitcoin shows only 79,956 Bitcoin to have been transferred.

54.2.4. The address listed in the purchase order is lowercase. Since Bitcoin addresses are case sensitive, this particular address is invalid and would not have worked.

54.2.5. The price on the purchase order of $21.01 does not reflect the market price of Bitcoin as at the date of 27 February 2011.

54.3. 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. This Bitcoin could not therefore have been purchased by Dr Wright in March 2011.

54.4. In the course of an investigation by the Australian Tax Office, Dr Wright was asked by the ATO to prove control of Bitcoin at the 1Feex and 12ib7 addresses by using the message signing feature. The owner of Bitcoin at those addresses would have been able to do this. Dr Wright failed to do so.

54.5. Dr Wright chose not to challenge the finding of the ATO that Dr Wright has never had any legal or equitable interest in Bitcoin.

54.6. Dr Wright was ordered by a Florida court in the proceedings referred to at sub-paragraph 54.9.2 below to provide a list of his Bitcoin ownership as at 31 December 2013. Dr Wright filed a list on 14 January 2020 containing 16,000 addresses which did not include either of the two Addresses.

54.7. Draft financial statements of TTL for the period from incorporation in July 2011 until May 2017 did not record ownership of the Bitcoin at the Addresses or any Bitcoin.

54.8. On 8 May 2017, Dr Wright was asked by the Registered Agent of TTL whether TTL had any assets. Dr Wright's response was: '*The shares in DeMorgan Pte Ltd*'. He did not identify either of the Addresses as an asset owned by TTL.

54.9. Dr Wright has fabricated documents or otherwise provided deliberately false evidence on numerous prior occasions (including documents or evidence concerning his alleged ownership of digital assets). In particular:

54.9.1. Dr Wright forged or altered numerous documents in an Australian Tax Office investigation relating to his attempt to claim tax rebates regarding his purported research and development into Bitcoin. For example and without prejudice to the generality of the foregoing: (i) Dr Wright submitted several backdated invoices to the ATO; (ii) Dr Wright fabricated an email from ATO Officer Celeste Salem to him that was never sent; (iii) Dr Wright changed the time and content of an email sent

to him by ATO Officer Hao Khuu; (iv) Dr Wright changed the content of an email sent to him by ATO Officer Brigid Kinloch; (v) Dr Wright provided the ATO with a purported email sent to him from markferrier@hotmail.com which references a sub-domain (albaraka-bank.asia) that did not exist on the date of the purported email, 12 October 2013; and (vi) Dr Wright provided the ATO with two versions of an otherwise identical purported email to him from David Kleiman, one of which is dated 17 October 2014, even though Mr Kleiman died in April 2013.

54.9.2. Proceedings were brought against Dr Wright in the United States District Court for the Southern District of Florida by the personal representative of Mr Kleiman and by a company co-founded by Mr Kleiman and Dr Wright. In those proceedings: (i) Dr Wright submitted forged or intentionally altered documents, including a backdated version of a deed of trust for the Tulip Trust; and (ii) Dr Wright gave knowingly false evidence about (among other things) the Tulip Trust and his inability to verify his alleged Bitcoin holdings.

54.9.3. In the Florida proceedings referred to above, Dr Wright was ordered to provide a list of his Bitcoin ownership as at 31 December 2013. This list included at least 145 addresses that were in fact controlled by other individuals with no relation to Wright. Those individuals signed the relevant addresses (using the private keys associated with them, which only the owner could do) and published a message saying in part '*Craig Steven Wright is a liar and a fraud*'.

54.9.4. In the Florida proceedings, Dr Wright disclosed a paper wallet purporting to relate to the 1Feex Address. The paper wallet was a forgery. In particular: (i) the font on the document is misaligned and does not contain the embossing effect shown on a genuine paper wallet; (ii) the QR code is misaligned (from which it is to be inferred that it was pasted in from an online QR code generator); and (iii) the document disclosed by Dr Wright contains an apparently unique background pattern intended to prevent forgery. This feature was first implemented

in 2014. It is inferred that the unique background pattern on the document was taken from a genuine paper wallet which was then altered to appear to be a wallet containing the 1Feex Address.

54.9.5. Dr Wright fabricated a purchase order submitted in these proceedings as purported evidence of the purchase of Bitcoin at the 1Feex Address, as to which paragraph 54.2 above is repeated.

54.9.6. On 17 April 2019, Dr Wright issued a libel claim in the Queen's Bench Division (as it then was) against Peter McCormack, a journalist, in respect of Mr McCormack's tweets that Dr Wright is not Satoshi but rather a fraud. In those proceedings, Dr Wright signed a statement of truth in a pleading that alleged, and gave evidence, that he had been invited to speak at ten specified academic conferences, in many instances following a successful submission by him of proposed academic papers for blind peer review. This was false and known by Dr Wright to be false. For example, and without prejudice to the generality of the foregoing, the paper Dr Wright submitted to a conference in Hanoi in April 2019 had been rejected by all three peer reviewers who responded and Dr Wright had been notified of this rejection.

54.9.7. In a claim commenced against him in Norway by Mr Granath, Dr Wright forged or intentionally altered documents including what he claimed was an early version of the White Paper but which had in fact been deliberately altered with a view to giving readers the false impression that it had been created earlier than it was.

55. As to paragraph 29:

55.1. As to the first sentence:

55.1.1. Paragraph 54 above is repeated. In the premises, it is denied that TTL owns the Bitcoin in the Addresses.

55.1.2. Even if, which is denied, Dr Wright did at any stage own the Bitcoin at either or both of the Addresses, it is not admitted TTL was the legal (or, if alleged, beneficial) owner when the alleged hack occurred.

55.1.3. Save as aforesaid, the first sentence is not admitted.

55.2. Paragraphs 29(a) and 29(b) are admitted.

56. Paragraph 30 is embarrassing. It does not identify the person or entity who is alleged to have purchased the Bitcoin in the 1Feex Address, nor the purchase price, nor how this person (if not TTL) then transferred the Bitcoin to TTL. Without prejudice to the foregoing:

56.1. Paragraph 54 above is repeated.

56.2. The WMIRK exchange service did not begin dealing in Bitcoin until late 2013. The 1Feex Address could not therefore have been purchased from WMIRK in late February 2011.

56.3. In the premises, paragraph 30 is denied.

57. Paragraph 31 is admitted but it is denied that Dr Wright or TTL is the owner of the Bitcoin at the 12ib7 Address, as to which paragraph 54 above is repeated.

58. As to paragraph 32, the tendentious defined term 'TTL Private Keys' is not adopted because TTL was never the owner of the Bitcoin at the Addresses and never had the private keys for those addresses. This Defence will instead use the defined term '**Relevant Private Keys**'. Save as aforesaid, paragraph 32 is admitted.

59. Paragraph 33 is admitted.

60. As to paragraph 34:

60.1. The first sentence is admitted.

60.2. The second sentence is denied. The owner of Bitcoin at any given address is the holder of the private key for that address. Paragraph 45.3 above is repeated.

G. ALLEGED THEFT OF THE RELEVANT PRIVATE KEYS

61. As to paragraph 35:

61.1. The implicit allegation in the first sentence that there was a misappropriation is denied, as to which paragraph 64 below is repeated.

61.2. Dr Wright never had the Relevant Private Keys. Paragraphs 54 and 58 above are repeated.

61.3. Even if, which is denied, Dr Wright had the Relevant Private Keys or the Keys Access Material, it is not admitted that he held them 'on behalf of' TTL (whatever that vague allegation means) or that he stored them as alleged at paragraph 35(a).

61.4. Save as aforesaid, paragraph 35 is not admitted.

62. As to paragraph 36:

62.1. The first sentence is not admitted.

62.2. Paragraph 54 above is repeated.

62.3. Even if, which is denied, Dr Wright had the Relevant Private Keys or the Keys Access Material, it is to be inferred that they were not stolen as alleged because:

62.3.1. The Bitcoin at the Addresses has not been moved since 2011.

62.3.2. Dr Wright claims to have wiped his hard drive shortly after the alleged Hack, which he would not have done had the Relevant Private Keys or the Keys Access Material been stolen.

62.3.3. Dr Wright did not contact Microsoft or Google to attempt to recover the Relevant Private Keys or the Keys Access Material following the alleged Hack.

62.3.4. Dr Wright does not claim to have reported the alleged Hack to the police until the following day, i.e. 9 February 2020.

62.4. In the premises, the second and third sentences are denied.

63. As to paragraph 37:

63.1. The first two sentences are not admitted.

63.2. The third sentence is noted.

63.3. The fourth sentence is not a proper plea.

64. As to paragraph 38:

64.1. It is denied that there was any misappropriation of the Relevant Private Keys and Keys Access Material. Paragraph 62 above is repeated.

64.2. The matter is claimed to have been reported to the Surrey Police only on 9 February 2020, even though the alleged Hack is alleged to have been discovered on 8 February 2020.

64.3. Save as aforesaid, paragraph 38 is not admitted.

65. As to paragraph 39:

65.1. It is admitted and averred that TTL does not have possession of or access to the Relevant Private Keys and that it is unable to deal with the Bitcoin at the Addresses. The implicit allegation that TTL once had possession of or access to the Relevant Private Keys and the Keys Access Material is denied.

65.2. The allegation that TTL 'remains' the owner of the Bitcoin in the Addresses (and the implicit allegation that it became the owner on some prior date) is denied. Paragraph 54 above is repeated.

66. Paragraph 40 is admitted, save that the implicit allegation that there was a misappropriation of the Relevant Private Keys and the Keys Access Material is denied, as to which paragraph 54 above is repeated.

H. CLAIMS AGAINST THE DEVELOPERS: ALLEGED FIDUCIARY OBLIGATIONS

(1) Fiduciary duties allegedly owed by the Developers to TTL

67. As to paragraph 41:

67.1. The first and second sentences are denied for the reasons set out below. It is

further averred that the alleged fiduciary duties pleaded in the first and second sentences are in any event inconsistent with (alternatively expressly excluded by) the MIT Licence under which Bitcoin Core is released, as pleaded at paragraph 10 above.

67.2. As to paragraph 41(a):

67.2.1. The first sentence is denied. It is wholly unparticularised, save for a cross-reference in the second sentence to paragraphs 24-28, as to which paragraphs 49-53 above are repeated.

67.2.2. The third sentence is denied. The role of developers has been set out at paragraph 49 above. The use of the words '*in effect*' is an implicit recognition of the fact that developers do not in fact have what they are alleged in this sentence to have.

67.2.3. The fourth sentence is admitted. It is averred that the Bitcoin System is designed to require the use of private keys. All users (alternatively, all reasonable users) of that system are aware that it is so designed. It would be contrary to the foundational principles of the Bitcoin System, which include security, immutability, anonymity and the absence of a trusted third party, for the system to be changed to permit a so-called owner of Bitcoin to transact without using its private key (irrespective of the reason why it does not or cannot use the private key).

67.2.4. Even if, which is denied, developers do have some or substantial power over the system in which digital assets are held, it is denied that they owe any fiduciary duties to TTL or anyone else as a result. There is no entrustment of any property to the developers; and in the cryptocurrency community there is and can be no reasonable expectation that developers (whatever power they may or may not have) will act in the interests of the owner of Bitcoin to the exclusion of their own interest or that of a third party.

67.2.5. Save as aforesaid, paragraph 41(a) is denied.

67.3. As to paragraph 41(b):

67.3.1. The first sentence is denied. Developers do not have any relevant powers or discretions because it is for each individual node in the Network to decide what software to use. Paragraph 46.2 above is repeated.

67.3.2. As to the second sentence, it is admitted that the interests of the owners of Bitcoin can and frequently will be significant in monetary terms.

67.3.3. As to the third sentence, the assets held at the Addresses were worth approximately £2.6 billion as at 26 April 2023. It is denied that they are or ever have been the assets of TTL, as to which paragraph 54 above is repeated.

67.4. Each sentence of paragraph 41(c) is denied. There is no entrustment of any property by owners, whether to the developers or to anyone else. Owners have, and are designed to have, the ability to deal in that property only by using their private keys.

67.5. Paragraph 41(d) is denied. A reasonable person purchasing Bitcoin would be familiar with the foundational principles of security, immutability, the absence of a trusted third party and anonymity. Such a person would accordingly be aware that the question of developers acting capriciously (*a fortiori* for the other adjectives used in paragraph 40(d)) cannot arise for they have no power to compel users to use any particular software.

67.6. As to paragraph 41(e), which cross-refers to paragraph 24, paragraph 49 above is repeated. It is denied that the payment received by developers is 'substantial', an allegation that is made without distinguishing between different networks or between different developers within a network. It is also denied that the receipt of payment, if any, is relevant to the question whether developers owe fiduciary duties to TTL.

68. Paragraph 42 (including its sub-paragraphs) is denied for the reasons pleaded at paragraph 67 above and further below.

69. As to paragraph 43:

69.1. As to paragraph 43(a), paragraph 68 above is repeated.

69.2. Paragraphs 43(b) and 43(c) are denied. In particular:

69.2.1. It is impossible for either of the things pleaded at paragraphs 43(b) and 43(c) to be done unless new software is created and adopted.

69.2.2. While it is possible for someone, including Dr Wright, to create such software, no one, including the developers, has the power to require users to adopt it. Paragraph 67.5 above is repeated. Any attempt by the developers to persuade users to adopt it (whether as a result of a court order or otherwise), if it had any effect at all, would lead to a hard fork and a substantial number of users would reject such a proposal as contrary to the foundational principles of the Bitcoin System.

69.2.3. Even if (contrary to the above) any such software were to be adopted by users, it would only grant access to coins on the new forked cryptocurrency (which would likely be worthless or of limited value), not to the coins that TTL alleges to have owned and lost.

69.2.4. A hard fork is undesirable because it would result in significant costs to other users of the BTC Network and affect the value of BTC. Paragraph 21.4 above is repeated.

69.2.5. As to the cross-reference to paragraph 28, paragraph 53 above is repeated.

69.3. Paragraph 43(d) is admitted, save that it is denied, for the reasons set out at sub-paragraph 46.2 above, that there are '*steps open*' to the developers that would give the so-called true owner access to its Bitcoin. It is averred that there is nothing anomalous about the inability of a so-called owner to access Bitcoin without using private keys because the Bitcoin System is designed to permit access only with private keys.

69.4. As to paragraph 43(e), the so-called owner would be able to sue the person by whom it was defrauded if that person can be identified and seek personal remedies (e.g. damages). It is denied that there are any steps open to the

developers that would restore to the so-called owner the Bitcoin of which it was defrauded. The steps proposed by TTL would not achieve this objective for the reasons set out at sub-paragraph 69.2 above.

69.5. As to paragraph 43(f), it is admitted that developers make changes to the software from time to time. The unparticularised allegation that they do so when it is in their interests to do so is, pending proper particularisation, not admitted; but it is averred that the allegation is inconsistent with the existence of any fiduciary duty. It is denied, if alleged, that developers have the power to impose any software changes they may make on users or take any other steps to require users to adopt those changes.

70. Paragraph 44 is yet another instance of an inappropriate plea that belongs, if anywhere, in a response to a Law Commission consultation paper rather than in a statement of case. The Enyo Defendants do not intend to include similarly inappropriate material in their Defence and plead below only to the (few) allegations of fact that are to be found in this paragraph. For the avoidance of doubt, their case is that the matters pleaded in paragraph 44, even if they are true, are irrelevant to the question whether developers owe fiduciary duties under the established principles of equity in English law.

70.1. Paragraph 44(a) is admitted.

70.2. Paragraph 44(b) is denied. Paragraphs 45 and 48 above are repeated.

70.3. Paragraph 44(c) is particularly embarrassing (in its inclusion in a statement of case). Paragraph 3 above is repeated. It is in any event denied for the reasons pleaded at paragraphs 45 and 48 above.

70.4. Paragraph 44(d) is denied. As to the allegation that it is 'possible' to reverse the effect of the alleged fraud, that is denied for the reasons set out at paragraph 69 above.

70.5. Paragraph 44(e) is particularly embarrassing (in its inclusion in a statement of case).

70.6. As to paragraph 44(f), paragraph 70.5 is repeated. The vague and imprecise phrase '*seriousness of the services*' is not understood.

71. In the premises, paragraph 45 (including its sub-paragraphs) is denied. In particular, not only is there no obligation on developers to provide the remedies sought in paragraphs 45(a)-(c), those remedies are unattainable because developers do not have the ability to provide them. Paragraph 69 above is repeated. Further and specifically:

71.1. The peremptory orders sought are in any event too widely framed, imprecise and unclear.

71.2. The peremptory order sought to the effect that the Defendants take all steps to reverse the (alleged) fraud is especially objectionable on grounds of scope, imprecision and lack of proportionality

71.3. If, which is denied, the Defendants should be subject to any peremptory order is must be limited to acts or instructions which are clearly defined and of clear ambit

(2) <u>Alleged breach of fiduciary duty</u>

72. In the premises, paragraph 46 is denied. Even if, which is denied, there would otherwise be a breach of fiduciary duty as alleged at paragraph 46, it is averred that the duty in question does not arise unless a court order is first obtained requiring developers to take the steps specified in paragraph 45. If, as TTL alleges at paragraph 46, a prior court order were not required, developers would be under an obligation to adjudicate on rival claims to Bitcoin, which is again contrary to the foundational principles of the Bitcoin System of which all reasonable users are aware.

73. As to paragraph 47:

73.1. The first sentence, which appears to be a repetition of the first sentence of paragraph 46, is denied and paragraph 72 above is repeated.

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

73.3. The third sentence is denied. Even if TTL were to obtain such a declaration of ownership, the Enyo Defendants would not be in breach of duty because there is, for the reasons pleaded above, no duty as alleged.

74. In the premises, paragraphs 48-50 are denied. TTL is not entitled to the remedy sought

or to any remedy.

I. CLAIMS AGAINST THE DEVELOPERS: DUTY OF CARE

75. Paragraphs 51 and 52 are denied. In particular:

75.1. The allegation that the developers voluntarily assumed responsibility to TTL is embarrassing in that the alleged act giving rise to or constituting the assumption of responsibility is not identified or particularised. It is in any event denied because any voluntary assumption of responsibility is inconsistent with (alternatively expressly excluded by) the MIT Licence under which Bitcoin Core is released, as pleaded at paragraph 10 above.

75.2. As to the cross-reference in paragraph 52 to paragraphs 41-45, paragraphs 67-71 above are repeated.

75.3. As to paragraph 52(a), it is denied that the duty is an incremental extension of scenarios (which TTL does not identify) in which a duty has been found to exist.

75.4. Paragraph 52(b) is denied. It is not reasonably foreseeable to developers that there is any step that it is within their power to take that could achieve the objective TTL wishes to achieve; nor is it reasonably foreseeable to developers that any user of the Bitcoin System would rely on them to take any such step and suffer loss if they do not.

75.5. Paragraph 53(c) is denied. In particular:

75.5.1. There is no special or other relationship between developers and an individual user of the Bitcoin System.

75.5.2. The proposed duty of care would give rise to indeterminate liability, including as it would any user of cryptocurrency wherever domiciled or resident even if they have had no dealings with any particular developer.

75.5.3. The proposed duty of care would: (a) impose on developers affirmative rather than merely negative duties; (b) illegitimately interfere with their freedom of speech; (c) damage their reputation in the cryptocurrency community; (d) inevitably conflict with duties potentially owed to other

users; and (e) lead to a hard fork if they were to attempt to comply with the alleged duty, causing significant harm to the relevant network.

(1) Alleged breach of duty

76. In the premises, paragraphs 53-55 are denied.

77. It is denied that the Claimant is entitled to the relief sought or to any relief.

James Ramsden KC
Niranjan Venkatesan

Statements of Truth

The Second to Twelfth Defendants believe that the facts stated in this defence are true. The Second to Twelfth Defendants understand that proceedings for contempt of court may be brought against anyone who makes, or causes to be made, a false statement in a document verified by a statement of truth without an honest belief in its truth.

I am authorised to sign this defence on behalf of the Second to Twelfth Defendants.

Signed:……..

Name: Timothy Elliss

Position: Partner, Enyo Law LLP (Legal Representative for Second to Twelfth Defendants)

Date: 26 April 2023