

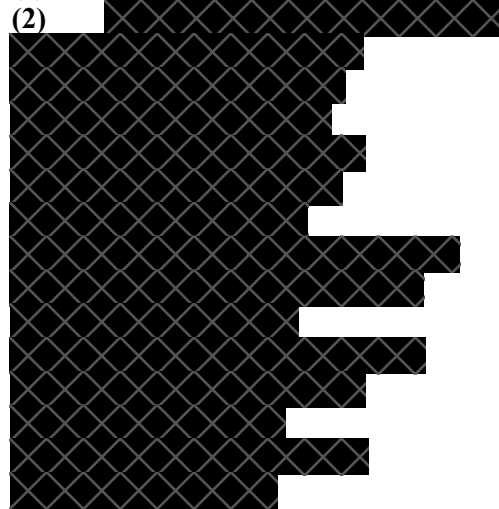
B E T W E E N : -

TULIP TRADING LIMITED (a Seychelles company)

Claimant

- and -

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

(2) A large rectangular area of text is completely redacted with a black cross-hatch pattern. It is positioned to the left of the 'Defendants' label.

Defendants

**DEFENCE OF THE
FIFTEENTH AND SIXTEENTH DEFENDANTS**

A.1 SUMMARY

1. This claim is both fraudulent and legally misconceived.
2. The Claimant seeks an Order intended to give it ownership of cryptocurrency worth billions of US dollars, alternatively damages or equitable compensation in that sum. It never owned or controlled that cryptocurrency in the first place, and the evidence on which it relies is manufactured.
3. It has also brought this claim against the wrong defendants: it has failed to claim against the various individuals who have actually asserted competing claims to the coins (and any judgment would accordingly not bind such parties). The Defendants, by contrast, have never claimed

ownership.¹ Instead, the Claimant is targeting them on the alleged basis that they have the power to give it access to the coins. The true reason for this claim is, perhaps, more accurately illustrated by a tweet from the Claimant's Dr Wright, where he stated: "*I will personally hunt every dev until they are broke, bankrupt and alone before I lost*". This litigation appears designed to threaten and frighten software developers away from contributing towards any cryptocurrencies which Dr Wright does not endorse, and thereby to promote the BSV blockchain with which he is closely associated.

4. As to the Claimant's legal case, this rests on an allegation that the Defendants owe it (and, by necessary implication, all owners of cryptocurrency worldwide) a fiduciary duty to make changes to the underlying rules of the system whenever access to cryptocurrency is lost. That would not only see the disparate, private individual Defendants acting as worldwide guarantors and bailiffs to the entire cryptocurrency system, but would also have them change the very rules by which the fiduciary relationship is said to have arisen. It is inconceivable that a fiduciary duty could exist to do an act which is inconsistent with the very rules giving rise to that fiduciary relationship.
5. The position of the Fifteenth and Sixteenth Defendants is even more pronounced: it is common ground that the creation of the eCash blockchain (referred to by the Claimant as Bitcoin Cash ABC) did not take place until (i) many years after Tulip's alleged purchase, and (ii) several months after the alleged hack. The claim against the Fifteenth and Sixteenth Defendants therefore consists of the generic proposition that whenever any fork takes place on any network giving rise to any new blockchain, irrespective of who creates that fork and for what purpose, fiduciary duties must thereby immediately arise in favour of all 'owners' of coin on that new blockchain. The claim is hopeless.
6. Moreover, the Fifteenth and Sixteenth Defendants do not have the powers ascribed to them. Multiple versions of software can be (and are currently) run simultaneously on the eCash blockchain, anyone can propose software changes, and the Fifteenth and Sixteenth Defendants have no power to compel network participants to run any particular software. The Fifteenth and Sixteenth Defendants are therefore in no better position than the Claimant to propose the changes sought in this claim. In reality, however, the proposed changes would never be accepted by nodes who actually build the blockchain and who are largely anonymous and wholly autonomous. The relief sought by this claim is thus highly unlikely ever to materialise in practice and any Order would be futile.

¹ It is noted that Dr Wright's evidence in support of TTL's application to serve out of the jurisdiction suggested that "*ownership is an issue on which I do not consider that the developers have standing as they do not claim to own the assets*".

7. The relief sought would also, if granted, put the Defendants at considerable risk of worldwide civil and criminal actions from (*inter alia*) competing claimants who have not been included as defendants to this action and who would therefore not be bound by any judgment.
8. The claim is, moreover, contrary to the Defendants' national and/or constitutional rights, and their participation in these proceedings is accordingly expressly under protest. The Fifteenth and Sixteenth Defendants do not accept that the English Courts are properly to be regarded as having jurisdiction (whether personal, subject matter or otherwise). There is no proper basis for a claim of this nature in the English Courts: it is a claim by an allegedly Seychelles-registered company run by an Australian national against ██████████ in respect of cryptocurrency which, on the Claimant's own case, can never have been controlled by it in this jurisdiction given that the relevant cryptocurrency had not even come into existence by the time of the hack by which the Claimant alleges that it lost control. Moreover, the imposition in those circumstances of English legal duties against the Defendants would amount to wholly improper overreach in conflict with the Defendants' own national legal protections. The Fifteenth and Sixteenth Defendants expressly reserve any and all rights in that regard, both in these and in any future proceedings.

A.2 Preliminary

9. In this Defence:
 - 9.1. references to paragraph numbers are, unless otherwise stated, references to numbered paragraphs of the Amended Particulars of Claim dated 13 February 2023.
 - 9.2. abbreviations used in the Amended Particulars of Claim are adopted unless otherwise stated.
 - 9.3. no admissions are made through the use of any abbreviations, headings or sub-headings that have been employed from the Amended Particulars of Claim, which are included for convenience only.
10. Except as stated below, and except where it contains admissions, the Fifteenth and Sixteenth Defendants require the Claimant to prove the matters set out in the Amended Particulars of Claim.
11. The introduction contained at paragraphs 1 and 2 of the Amended Particulars of Claim is noted.
 - 11.1. Whilst the term "*Networks*" is used imprecisely in the Particulars of Claim, and is not apt to describe the blockchains created by nodes or the transactions recorded thereon (as

appears to be intended), it is used in this Defence for convenience of responding to the allegations raised. No admissions are made thereby.

11.2. The term “*Bitcoin Cash ABC*” is also used erroneously: the relevant blockchain is known as “*eCash*”; and “*Bitcoin ABC*” is one of multiple possible versions of software that can be used to build on the eCash blockchain, as further described below. TTL consistently fails to distinguish between the blockchain and the software which can be run in respect of it. The reference to “*Bitcoin Cash ABC*” and “*ABC*” in paragraph 2 is understood to be a reference to the eCash blockchain.

11.3. The Fifteenth and Sixteenth Defendants will likewise refer as necessary at trial to all documents referred to within the Statements of Case in these proceedings.

B PARTIES

12. The Claimant, Tulip Trading Limited (“**TTL**”), is a company incorporated in the Republic of Seychelles. TTL has failed to particularise what “*certain digital assets*” it is alleged to own. It is denied that it is the owner of the coins claimed in these proceedings. Paragraph 3 is otherwise not admitted.

13. The First Defendant (“**the Bitcoin Association**”) is closely associated with Dr Wright and is believed to have been included within this claim in an attempt to lend credibility to the allegations made and the relief sought. The Second to Fourteenth Defendants are private individuals.

14. The Fifteenth Defendant, [REDACTED]. The Sixteenth Defendant, [REDACTED]. It is denied that they have the roles and powers attributed to them by TTL, as further particularised in this Defence.

15. Save as set out above, paragraph 4 is not admitted.

C BITCOIN

(i) The White Paper

16. On 31 October 2008, one or more individuals under the pseudonym “*Satoshi Nakamoto*” published a White Paper entitled “*Bitcoin: A Peer-to-Peer Electronic Cash System*” (“**the White Paper**”). The abstract (with **emphasis** added) reads as follows:

*A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. **We propose a solution to the double-spending problem using a peer-to-peer network.** The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. **The network itself requires minimal structure.** Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.*

17. The concept was thus for electronic transactions to be recorded within groups of data called “*blocks*” that are linked through cryptography, resulting in a “*chain*” of blocks referred to as a “*blockchain*”. The blockchain forms a permanent historical ledger of transactions involving the relevant coins.
18. The White Paper made clear:
 - 18.1. In section 1 (‘Introduction’) that it was seeking to remove the need for “*financial institutions serving as trusted third parties to process electronic payments*” and to enable “*Completely non-reversible transactions*” without the possibility of mediation of disputes. Such mediation was said to, “*increase[...] transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions*”. Its proposal to achieve this aim was, “*an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party*”.
 - 18.2. In section 2 (‘Transactions’) that:
 - (a) An electronic coin is defined as “*a chain of digital signatures*”.
 - (b) Each owner would transfer the coin “*by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin*”. That process requires the use of a private key held only by the owner.
 - (c) All transactions would “*publicly announced*” so that all transactions would be known, which would assist in preventing double-spending.
 - 18.3. In sections 3 (‘Timestamp Server’) and 4 (‘Proof-of-Work’) that the process would be achieved with a timestamp server “*taking a hash of a block of items to be timestamped and widely publishing the hash*”. On a peer-to-peer basis, this would employ a proof-of-work

system with approved blocks forming an interrelated chain, new blocks being added to the end of the chain indefinitely. The chain could not be undone provided that *“the majority CPU power is controlled by honest nodes”* when approving the blocks.

18.4. In section 5 (‘Network’) that there are six *“steps to run the network”* carried out by nodes:

- 1) *New transactions are broadcast to all nodes.*
- 2) *Each node collects new transactions into a block.*
- 3) *Each node works on finding a difficult proof-of-work for its block.*
- 4) *When a node finds a proof-of-work, it broadcasts the block to all nodes.*
- 5) *Nodes accept the block only if all transactions in it are valid and not already spent.*
- 6) *Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.*

18.5. In section 6 (‘Incentive’) that the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block, thereby adding *“an incentive for nodes to support the network”* as well as providing *“a way to initially distribute coins into circulation, since there is no central authority to issue them”*.

18.6. In section 10 (‘Privacy’) that anonymity of ownership would be maintained *“by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone”*.

19. Whilst the code which was subsequently developed to give effect to the proposals in the White Paper could be changed in various ways, there were certain fundamental principles (as set out above and further described in paragraph 23 below) which were immutable. As detailed further below, the relief sought in this claim seeks fundamentally to change those immutable principles.

(ii) Bitcoin as a supposed digital asset & the blockchain

20. Following publication of the White Paper, computer code was developed to realise the concept set out therein and the original Bitcoin blockchain came into being. In particular:

20.1. The blockchain comprises the public announcement of transactions, with such transactions being collected into blocks by computers known as *“nodes”* in a process known as *“mining”*. A block is broadcast and then checked by other nodes. If all transactions are valid, the block will be accepted by other nodes and will then form the foundation on which the next block is built, thereby creating the chain of publicly announced transactions. The blockchain is publicly viewable, and copies are held individually by nodes. There is no central repository where the blockchain is stored and accessed; it is simply a communal public record of transactions.

- 20.2. The electronic coins recorded on that blockchain comprise chains of digital signatures. Each coin therefore has no intrinsic value, but only such value as conferred by the market of users seeking to buy and sell that chain of digital signatures at any given time.
- 20.3. There is no means of “*accessing*” a coin, since it is not a tangible asset. It can simply be transferred. Any transfer can only take place with the use of a private key. Once transferred, the coin ceases to exist and a new coin is created, since the chain of digital signatures which make the coin changes upon transfer.
- 20.4. Whilst transactions can be seen on the blockchain, the identity of those taking part in transactions is unknown and anonymous. Knowledge of ‘owners’ is not known (unless publicly declared by that ‘owner’). That is an important principle underlying the system, and there have been well-publicised examples of threats and attacks on people known to control cryptocurrency.
21. It is also possible to make “*off chain*” transfers of coin. Off-chain transfers are transactions in respect of coin made by a private arrangement which is not recorded on the blockchain (and where no new private key or other data parameters are generated).
22. The Particulars of Claim do not define the word “*Bitcoin*” by reference to any specific blockchain. Moreover, as above, the use of the term “*Network*” is liable to mislead. Those terms are used without admission and for convenience only. Nevertheless, the various cryptocurrencies underlying the present claim are all understood to be governed by the same immutable basic principles from the White Paper as set out above.
23. When a person or entity ‘purchases’ any Bitcoin, they are (a) buying the ability to control a chain of digital signatures which have been (and can only be) generated and operated with the specific system of rules governing that Network; and thus (b) necessarily accepting the fundamental rules of that Network. In particular, users necessarily accept the fundamental rules in the White Paper that:
- 23.1. The Network operates “*without the need for a trusted third party*”;
- 23.2. A valid private key is needed in order to transfer any coin on the blockchain;
- 23.3. Transactions on the blockchain are “*completely non-reversible*”;
- 23.4. There is no possibility of external, third-party mediation of disputes; and
- 23.5. ‘Owners’ are entitled to remain anonymous.

24. The present claim, and the duties which TTL alleges, are inconsistent with every one of those fundamental rules.

25. In the premises, and save as set out above:

25.1. As to paragraph 5, the term “*token*” is apt to mislead, since each coin is a chain of digital signatures recorded in the blockchain, and there is no tangible representation of that coin. This Defence employs the term “*coin*”, which is the term used in the White Paper. It is denied that cash is a suitable analogy in view of the system rules set out above.

25.2. As to paragraph 6, certain third party platforms enable the exchange of currencies, including cryptocurrencies (so-called due to their use of cryptography, and not due to any confusion with encryption as incorrectly suggested by Dr Wright in his evidence supporting service out of the jurisdiction). Bitcoin is not directly ‘held’ on such platforms (if that term is intended to connote the user of the platform being recorded as transferee on the relevant blockchain). Instead, the platform owner itself is recorded as the transferee on the relevant blockchain, and the users of that platform then make internal transfers within and governed by the rules of that platform. Bitcoin can be exchanged on those platforms for whatever other currencies (including but not limited to cryptocurrencies) are provided for by the platform. The user will not need or use a private key; they will simply log into their trading account on the relevant platform. Each platform, of course, differs in the means of operation, but is in any event unlikely to be relevant to the present claim.

25.3. Insofar as “*Bitcoin*” is intended to refer to BTC, it is admitted that each Bitcoin is comprised of 100 million sub-units, known as Satoshis. However, eCash conducted a redenomination such that 1XEC is only 100 Satoshis.

25.4. As to paragraph 8, the blockchains do not record off-chain transfers, as described in paragraph 21 above. The analogy with a physical ledger is limited.

25.5. Paragraph 9 is admitted and averred. Anonymity of ownership is a fundamental principle underpinning the systems.

25.6. Paragraphs 5 to 9 are otherwise admitted as high level descriptions.

(iii) The role of nodes / miners

26. Nodes are devices or computers used by any number of private individuals, pools of individuals, or businesses around the globe voluntarily participating in a Network from time to time by downloading and running freely-available software. References in this Defence to actions and

decisions taken by nodes are (where implied by the context) references to actions and decisions taken by those controlling such nodes.

27. All nodes participate in the functioning of the Network, including by downloading applicable software and verifying blocks and the transactions within.
28. By contrast, only certain nodes produce new blocks (i.e. the process known as ‘mining’, described above). Those nodes are generally known as “*mining nodes*”. Mining nodes work independently in attempting to solve cryptographic hash equations generated by each transfer. They are incentivised to compete with each other to solve new blocks first, in order thereby to receive a reward in the form of new coins and/or a transfer fee. The mining nodes thus collect new transactions into blocks, find proofs-of work and broadcast the blocks to all nodes.
29. Nodes carry out their operations through the use of software (i.e. digital code).
 - 29.1. Provided the nodes use the same software, they are able to recognise each other and operate according to the same system rules, such that the work carried out will interrelate and mesh together. Certain minor changes to the software can also sometimes be made without impact, such that nodes using both the old and amended software can continue to operate in respect of the same blockchain (a process known as a “*soft fork*”). This means that different nodes can run different versions of software in respect of the same blockchain as long as those software versions are compatible and do not differ in a material way.
 - 29.2. If, by contrast, a node starts to operate materially different software, it would no longer be recognised by and operate with the other nodes. Any blocks it created would likewise not be recognised by other nodes operating the original software. Instead, it would only be recognised by other nodes operating that materially different software, and it would thereby create a new and distinct extension to the existing blockchain (known as a “*hard fork*” or “*blockchain fork*”) by creating blocks governed by those different rules.
30. Anybody can propose changes to the software run by nodes (and, indeed, nodes can apply their own changes without input from any third party). Changes might be proposed to fix bugs or weaknesses in the system. Others might be of a more fundamental nature.
31. Nodes cannot be compelled to download amended software and are at liberty to continue running unamended versions if they disagree with any change made. If consensus is not reached between all nodes in respect of a material change to the software they are running, a hard fork may result in the manner described above. In that situation:

- 31.1. The nodes which continue to run the original software will continue to build an extension to the blockchain based on those original rules; and
- 31.2. The nodes which run amended software will build a different extension to the blockchain based on those amended rules.

In that way, the blockchain up to the date of the fork will remain identical, but from the date of the fork it will diverge. Each branch of the fork thereafter progresses independently and any transactions on one branch are entirely distinct from transactions on the other.

32. Where either the original or the amended software is insufficiently popular among either (a) those wishing to execute transactions or (b) nodes accepting transactions through the creation of new blocks, the blockchain built following a hard fork using that software will have little value and is likely to become defunct. Coins (i.e. chains of digital signatures) will still exist on that blockchain, but users may attribute little or no value to them and cease to transact, and/or transactions may cease because nodes will have insufficient incentive to continue mining.
33. The relevant software run by the nodes is open-source and publicly accessible. That means it can be downloaded by (a) nodes, in order to run it and thereby participate in the process described above; and (b) anyone else who might wish to inspect it, use it or change it. However, in order that nodes can be sure that the software version they are downloading reflects the current general consensus of, and will work on, a relevant Network, they will usually seek to download a ‘static’ version of the software from a trusted source which will not have been subject to unknown unidentified and/or potentially harmful amendments.
 - 33.1. The static version can be downloaded by anyone at any time. Any downloaded copy will not be password-protected and can therefore be amended on an individual “local” basis. Indeed, nodes themselves might amend the software they intend to run for various reasons, including the desire to add features specific to their business that do not materially impact consensus, and/or to use programming language more familiar to their business. Any amended version could then itself be made publicly accessible, either with the intention of encouraging others to use or benefit from those amendments, or encouraging others to assist in reviewing and working on the updated version going forward; or even of creating a new blockchain (if the amendments are material).
 - 33.2. How the static versions might be protected from unauthorised changes (if at all) varies depending on the specific version of the software. The position in respect of Bitcoin ABC is described below.

34. There is also software common in the industry called “*git*” that is used to track and share software changes. Website platforms such as GitHub and GitLab have various features which can allow software developers to collaborate, share ideas and propose changes so that widespread consideration can be given to any proposed changes to the static file.
35. Where a new blockchain results from a hard fork (through the process described in paragraphs 29.2 and 31 above) any nodes wishing to participate on that new blockchain will then need to use software compatible with the new changes, such that a ‘static’ version of the new software (or software materially the same as the new software) will then again generally be needed for downloading from a trusted source.
36. A large number of forks have taken place since the original Network was set up:
- 36.1. As described above, a hard fork will result whenever any software with material amendments is run (even if only run by a limited number of nodes). That has taken place many times over the years, both deliberately and as a result of error or failed experiment. However, unless the software underlying the new fork is run by a sufficient number of nodes, the fork (and any coin held on it) will have little or no commercial value and mining is likely to cease, given that the time and/or cost of mining would in those circumstances be wasted.
- 36.2. More significant forks include those forming part of this claim. Others also exist. Where the main hard forks have taken place, they have usually resulted from a difference of principle between Network participants, with some nodes agreeing with amendments and some declining to run them. The main forks are illustrated in the diagram appended to the Fourteenth Defendant’s Defence.²
37. The entitlement for anyone to amend the underlying software is made clear in the terms of the MIT Licence (“**the MIT Licence**”), under which the original bitcoin software as well as the versions for the subsequent forks have been released. The MIT Licence is one of a number of commonly-used generic licences under which open source software is released. It is expressly or impliedly accepted by users of the underlying software, including those who purchase coin created using software subject to the MIT Licence. The MIT Licence provides:

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

² Save that the ticker for eCash is now XEC, rather than BCHA.

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS 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.

38. In the premises, and save as set out above:

38.1. The last sentence of paragraph 10 is denied. Nodes control the network by their decision, in consensus with others, to run specific software. Nodes cannot be compelled to use any particular software and, where enough decide to run materially different software, a hard fork may result. There are no others, at least in respect of eCash, "*who do exercise control*". Indeed, TTL's case on control by others is expressly contrary to the rules set out the White Paper, which expressed the system to be a "*peer-to-peer*" network which would operate "*without the need for a trusted third party*". Not all nodes carry out mining.

38.2. Paragraph 10 and 11 are otherwise admitted as high level descriptions.

39. Save that it is denied that there are "*only a small number of nodes*" operating on the eCash blockchain, paragraph 12 is not admitted. TTL fails to identify the Network to which it is referring, fails to define what is meant in context by the description "*small*", and fails to plead any "*example*" by reference to the eCash blockchain. In fact, the number of nodes operating on the eCash blockchain is unknown: only those that run publicly (contrasted with those behind firewalls) can be ascertained. As to those, there are generally around 100 (and specifically 84 as at the date of this Defence) ascertainable. The allegation in any event supports the case set out above, i.e. that it is the nodes which decide which software to run and which therefore control the network.

(iv) Addresses on the blockchain

40. As to paragraph 13:

40.1. It is admitted that coins (i.e. chains of digital signatures) are registered to public addresses on the eCash blockchain. The public addresses do not hold a balance are not analogous to a bank account number.

40.2. TTL's description of unspent transaction outputs ("UTXOs") as analogous to unspent cash in hand is an oversimplification and misleading.

- (a) Transactions are made up of inputs and outputs.
- (b) When a transaction takes place, a transferor takes one or more UTXOs (which serve as the input) and provides his or her associated digital signature.
- (c) At that point, those UTXO(s) are considered as 'spent' and no longer usable, and new UTXO(s) are created in their place (which serve as the output).
- (d) The quantity of UTXOs in a given transaction can be illustrated by the following equation: $[Sum(input\ UTXOs) = Sum(output\ UTXOs) - fee]$. Thus, if the transferee is to take the full value of the input UTXO(s) (taking into account any applicable Network fee), output UTXO(s) with the same value will be registered to the public address of the transferee. If, by contrast, the transferee is only to take part of the value of an input UTXO, it will be 'broken up' by the creation of multiple lower-value output UTXOs which together add up to the value of the input UTXO. Output UTXOs reflecting the transaction value will be registered to the public address of the transferee, and the surplus UTXOs will be registered to a public address (often a new address) of the transferor.
- (e) The output UTXO(s) can then be spent in new transactions later (in which they become the input UTXO(s)).
- (f) UTXOs registered at a given public address can be added up to ascertain the total sum of Bitcoin registered to the user of that address. The total is the amount of Bitcoin available to be transferred from that address.

40.3. Except that an uppercase 'F' is required to be valid on the eCash blockchain (rather than lowercase as alleged), it is admitted that UTXOs are registered at both the 1Feex and 12ib7 addresses on the eCash blockchain.

40.4. Paragraph 13 is otherwise denied.

(v) The existence of multiple blockchains

41. As set out above, where nodes elect to use materially divergent software, hard forks to the blockchain can take place. In the years since the creation of the original Network, a number of

hard forks have taken place. These are not limited to the four Networks forming the basis of this claim. Many other hard forks, some significant, have taken place.

42. The first major hard fork to produce a long-term viable blockchain took place on 1 August 2017, when the BCH blockchain was created. Various further hard forks subsequently took place, both from the original blockchain and from the BCH blockchain. On 15 November 2018, a fork took place from the BCH blockchain, giving rise to the BSV blockchain. On 15 November 2020, another hard fork from the BCH blockchain took place, giving rise to the eCash blockchain.
43. In the premises, and save as set out above:
 - 43.1. The first sentence of paragraph 14 is denied. There are more than four Networks. The remainder of the paragraph is admitted as a high level summary.
 - 43.2. Sub-paragraph 14.a. is denied. BSV was created on 15 November 2018 as a hard fork from the BCH blockchain (using Bitcoin ABC software which at that time operated on the BCH blockchain and from which material amendments were then made to create the BSV blockchain). Moreover, the suggestion that the Networks “*had no permission to copy the original blockchain*” is not understood: the software underpinning the transactions in the blockchain was subject to the permissions in the MIT Licence; and the blockchain itself is merely a public record of transactions which is in no sense protected against being ‘copied’ (which is in any event a misdescription of the mechanics by which a new blockchain comes into being, as described above).
 - 43.3. Sub-paragraph 14.b. is admitted a high level summary.
 - 43.4. Sub-paragraph 14.c. reflects a difference of terminology and is accordingly denied. Where TTL refers to an “*airdrop*” it will be treated for the remainder of this Defence as a reference to a “*hard fork*”. It is also incorrect to refer to the “*copying*” of the blockchain: in reality, nodes operating new software simply continue to build on the existing blockchain but using a new protocol incompatible with the previous rules, thereby giving rise to the blockchain fork.
 - 43.5. Paragraph 15 is admitted as a high level summary.
 - 43.6. Sub-paragraph 15.a. is denied. The BCH blockchain did not apply the same protocols as before: it arose from a hard fork which increased the block size limit. It cannot therefore be regarded as the “*original version*” (to the extent relevant to this claim).

43.7. Sub-paragraph 15.b is denied. The BTC blockchain continued operating the same protocols as previously.

43.8. As to sub-paragraph 15.c, it is not understood what TTL intends by the word “*hold*”. Those who had access to coin registered at an address on a blockchain before a hard fork by use of their private key will have access to coin registered at the same address on the new blockchain after the fork by use of the same private key.

(a) Questions of ownership are a legal issue which will vary depending on jurisdiction (and references to ownership in this Defence are to be construed accordingly) and are therefore not admitted. As a matter of English law, it is denied that coins constitute property that can be “*owned*”. They merely comprise publicly recorded data which can, with the use of a private key, be replaced with different publicly recorded data for value in a willing market. ‘Purchasing’ coins thus merely amounts to paying someone with a private key to cause the creation of a new data set attaching to a different private key controlled by the payor. The fact that such actions and data creation might be exchanged for value does not make it property which can be owned. The claim accordingly fails to overcome this initial threshold.

(b) The remainder of this Defence proceeds on the alternative basis (which is denied) that, contrary to the above, ownership of coins can be established as a matter of English law.

(c) Paragraph 15.c. is otherwise admitted as a high level summary.

43.9. Paragraph 16 is admitted as set out above.

43.10. Sub-paragraph 16.a. is denied. The BSV blockchain was a fork from the BCH blockchain and not the original version of Bitcoin. Paragraph 43.2 above is repeated. The reference “*software developers... apply[ing] the same operating protocols as before*” is not understood. Developers do not apply any protocols; it is the nodes which operate the software.

43.11. Sub-paragraph 16.b. is denied. The BCH blockchain continued as before. Again, the reference to developers using different protocols is misconceived: it is nodes which select which software/protocols to run.

43.12. Paragraph 17 is admitted save that, pending proper particulars, it is not admitted that there was a “*disagreement*” between the Fourteenth and Fifteenth Defendants. In fact, the Bitcoin ABC software had previously been the main trusted software used for the BCH

blockchain but a separate competing software version called Bitcoin Cash Node emerged. This was intended to, and ultimately did, supplant Bitcoin ABC as the principal implementation for the BCH blockchain. Updates continued to be made to the Bitcoin ABC software, however, and some changes were subsequently made which were incompatible with Bitcoin Cash Node. The result was a blockchain fork on 15 November 2020.

(vi) The eCash blockchain

44. As described above, following the fork on 15 November 2020, the eCash blockchain came into being. That fork arose from an amendment to software use on the BCH blockchain.
45. Consistent with the principles outlined above, any number of software versions can be run by nodes building on the eCash blockchain, provided the software does not introduce differences in respects material to the rules of the blockchain.
 - 45.1. The most widespread software currently used is known as Bitcoin ABC, which is a further amended version of the original and subsequently amended version of bitcoin software. Bitcoin ABC is published and used subject to the MIT Licence. A number of updates to Bitcoin ABC have been made since the eCash blockchain came into being, and multiple versions (currently understood to number at least 16) remain in use by nodes.
 - 45.2. Some nodes also create their own custom software for various reasons, including the desire to add features specific to their business that do not materially impact consensus, and/or to use programming language more familiar to their business.
 - 45.3. Software versions other than Bitcoin ABC are also possible, provided they remain consistent with the same underlying consensus rules. It is understood that at least two (BCash and RaiPay) are currently in use on the eCash blockchain.
46. The Bitcoin ABC software is not subject to a hierarchical approval process: amendments can be made by anyone registered as a ‘reviewer’. In particular:
 - 46.1. The ‘static’ software is published on various platforms, including Github, Dockerhub, Launchpad.net and Archlinux User Repository.
 - 46.2. A software amendment is developed by an individual/business on their local computer.

- 46.3. That amendment is then submitted through “*Phabricator*” (a web-based development collaboration tool) to enable other reviewers to review the proposed amendment. Comments can be provided in a peer-review process.
- 46.4. Once at least one reviewer has approved the proposed amendment, and no reviewer has rejected it, the amendment can be put into effect. The approved changes are applied to a “*git repository*” and released approximately every two weeks by way of automatic update to the software.
- 46.5. Upon release, the updated ‘static’ software is then published on the same platforms described above, together with release notes explaining the most recent changes.
- 46.6. Anyone concerned with a change that has already been made can do a “*post review*” and amend unacceptable changes in a “*fix forward*” manner, using the same process described above. That would of course apply equally to the changes sought by this claim: if such changes were made to the Bitcoin ABC software, they could immediately be changed back or removed by other users who might disagree with them. Since these proceedings operate *in personam* only, such users would not be bound by any Judgment.
47. There are a number of contributors to software development for Bitcoin ABC at any given time. It is understood that the claim against the Fifteenth and Sixteenth Defendants is premised on recent (unparticularised) work supposedly carried out by them. Insofar as TTL seeks to amend its claim in order to rely upon any historic work carried out by either the Fifteenth or the Sixteenth Defendant (which is not presently alleged), the Fifteenth and Sixteenth Defendants reserve their right to plead that the claim is directed at the wrong persons.
48. As with the other blockchains, nodes on the eCash blockchain decide which software to run. If they choose to run Bitcoin ABC software, they can then choose which version of that software to use. They may select a particular version because, over time, they have grown to trust the software and the people contributing to it. Equally, they might reject a particular version because they disagree with a particular change that has been made (as was the case with the various forks described above).
- (vii) Lack of encryption and the use of ‘private keys’**
49. Paragraph 18 is admitted.
50. Paragraph 19 is inaccurate and accordingly denied. As set out in the White Paper and above, the requirement to use a private key to effect a transfer is fundamental to the design of the blockchain. On-chain transactions are thus not “*typically...signed off*” using private keys; they can only be

made through the use of the private key. That is one of the system rules necessarily accepted through the purchase of Bitcoin.

51. The private key is used in the manner set out in paragraph 18.2(b) above. Thus it does not provide “*access*” to the coin, since the coin is merely an intangible chain of digital signatures. It simply enables that chain to be transferred. Knowledge of the private key does not itself connote ownership (for example, the key might be shared with a number of people; an off-chain transfer might take place with the transferor retaining knowledge of the key; etc) but knowledge of the key and any ownership (if, indeed, ownership is legally possible) will usually go hand in hand. The fact that any such ownership is anonymous and transfers can only be effected with the use of the private key has given rise to the well-known saying, “*not your keys, not your coins*”. There is no proper analogy with a physical key used to open a safe. If a party has no private key, they have no entitlement to effect a transfer on the blockchain. Paragraph 20 is otherwise denied.
52. Aside from being inconsistent with the fundamental principles governing the system, removing the need for a private key and/or effecting changes to the code in order to transfer ‘ownership’ between individuals would also create new types of risk, including (a) transfers to non-owners; (b) fraud by transferors in off-chain transfers, who might pass over a private key but then seek to recover the same money without a private key; and (c) fraud by those said to have control over the system and ability to transfer. The present system is designed in a way which avoids such risks.
53. Paragraph 21 is denied.
 - 53.1. The use of a private key is fundamental to the systems. It is the way in which a transfer is authorised by a transferor without the use of a third party intermediary. Paragraphs 51 and 52 above are repeated.
 - 53.2. Controllers or ‘owners’ of coin are anonymous and are entitled to remain as such, that being one of the fundamental rules of the system when their coin was purchased and by which it was created. Controllers or ‘owners’ can be located anywhere in the world, and there is no proper way to ascertain the “*legitimate owner*” as alleged.
 - 53.3. Any changes to software would need to be accepted and adopted by nodes. Developers cannot compel the use of any particular software. It is highly unlikely that any material number of nodes would accept the changes proposed by TTL, such changes being wholly inconsistent with the fundamental rules on which the entire system is based. Any nodes which did accept the proposed changes would lead to a further fork and a new blockchain with no or little value.

- 53.4. In any event, TTL has failed to particularise the specific software changes which it seeks. Given that, as set out above, the underlying software is publicly available, TTL is entitled to make any changes it wishes to the software and to seek to persuade nodes to run that amended software. It has made no such attempt, at least in respect of the eCash blockchain. No claim can properly be advanced by TTL for amendments to the software without specifying precisely and in terms what code amendments are being requested.
54. Save that it is not possible to “own” a public address, paragraph 22 is admitted.
55. As to paragraph 23:
- 55.1. The first sentence is not admitted.
- 55.2. The popular reference to Bitcoin being “lost” is a reference to the loss of the private key.
- 55.3. It is admitted that the loss of a private key does not affect the ongoing record of the coin on the blockchain. Legal title to the coin (if any) thus remains unchanged.
- 55.4. Paragraph 23 is otherwise denied. There is no proper analogy with a locked safe. The loss (in whatever manner) of a private key simply means that a person who was previously able to effect a transfer by generating a new data set can no longer do so. That is entirely in accordance with the rules of the system, and a risk voluntarily assumed by anyone seeking to transact in the coins.

(viii) The role of Developers

56. Whilst paragraphs 24 to 28 make allegations broadly against all Defendants, this Defence responds only insofar as the allegations concern the Fifteenth and Sixteenth Defendants.
57. Paragraphs 24 and 25 are denied. Neither the Fifteenth nor Sixteenth Defendant (whether alone or together) controls the eCash blockchain. The position in respect of the Bitcoin ABC software is described above, and neither have been sponsored or otherwise remunerated in respect thereto since the fork by which the eCash blockchain came into being. Paragraphs 44 to 48 above are repeated.
58. As to paragraph 26:
- 58.1. Sub-paragraph 26.a. is denied. Neither the Fifteenth nor Sixteenth Defendant (whether alone or together) makes decisions about the software to be applied in relation to the eCash blockchain. As described above, nodes decide which software to run in respect of the eCash blockchain and there are currently a number of versions of software being run.

- 58.2. Sub-paragraph 26.b. is insufficiently particularised and not understood. TTL has failed to particularise the “*system*” to which it is referring. The eCash blockchain itself is not security tested. The Bitcoin ABC software can be checked for security flaws by anyone.
- 58.3. Sub-paragraph 26.c. is denied. The Fifteenth and Sixteenth Defendants are unable to “*ensure*” that nodes implement any particular software for the reasons described above. Running any new code is entirely at their own election. Indeed, it is not even possible to contact nodes unless those running them have provided the means of doing so.
59. As to paragraph 27:
- 59.1. As described above, anyone may propose or design changes to software. That includes uploading the proposals through platforms or tools such as Phabricator. In respect of the Bitcoin ABC software, proposed amendments can be approved by any reviewer. Once approved, the amendments are automatically included within new releases.
- 59.2. However, for that amended software to take effect, the changes must then be accepted by nodes. A change such as that proposed by TTL in this litigation is unlikely to be accepted.
- 59.3. The position in respect of BSV is not admitted.
- 59.4. Paragraph 27 is otherwise denied.
60. Paragraph 28 is denied. The Fifteenth and Sixteenth Defendants do not have the power attributed to them, nor do they exercise any discretion or make choices in relation to the eCash blockchain. As regards the Bitcoin ABC software, they have no greater power to make and approve changes than any other reviewer. As to the sub-paragraphs:
- 60.1. On 15 August 2010 an amendment to the software was made by Satoshi Nakamoto amounting to a ‘soft fork’ in order to rectify the improper creation of over 184 billion coins. To be effective, the change had to be (and was) accepted by the vast majority of nodes running software at the time. Sub-paragraph 28.a. is otherwise denied.
- 60.2. Sub-paragraph 28.b. is denied. The Fifteenth and Sixteenth Defendants are unable to “*ensure*” anything in respect of an alleged fraud. In line with the White Paper, all transactions are recorded on the blockchain, transactions are irreversible, ownership is anonymous, there is no mediation of disputes, and there is no trusted third party. Thus, the Fifteenth and Sixteenth Defendants have no knowledge of the true owners of coins, would be unable to ascertain whether or not a fraud had taken place, cannot reverse transactions and cannot mediate disputes. Moreover, they have no control over the software run by

nodes. As described above, anybody (including TTL) can amend the software and seek to persuade nodes to accept it. Given that the proposed changes are contrary to the fundamental principles in the White Paper, such changes are highly unlikely to be accepted.

60.3. Sub-paragraph 28.c. is denied. The use of the relevant private key is the only way in which an on-chain transaction can take place. Aside from making a transaction using the private key, there is no such thing as “*access*” to the coins. The reference to encryption is not understood: the blockchain is public; and a user can record their private key in any medium they wish.

D TTL’S ALLEGED OWNERSHIP

61. As to paragraph 29:

61.1. It is denied that TTL owns, or has ever owned, the Bitcoin in the Addresses. Ongoing statements to the contrary are fraudulent and amount to perjury and/or contempt of court by Dr Wright, and the Fifteenth and Sixteenth Defendants reserve the right to seek such sanctions as are appropriate in respect thereof following trial. Even the first statement of Mr Cain in support of TTL’s application to serve out of the jurisdiction (on which the Fifteenth and Sixteenth Defendants will rely) identifies a number of matters which are inconsistent with TTL’s claim ever to have owned coins registered at the Addresses.

61.2. TTL has failed to particularise the “*many others*” it is alleged to own, and the Fifteenth and Sixteenth Defendants are accordingly unable to respond.

61.3. Subject to paragraph 25.3 above and the denomination of 100 Satoshis per “*token*”, the quantity of “*tokens*” on the eCash blockchain in respect of the Addresses is admitted. The value at the date of the Particulars of Claim is not admitted.

61.4. Paragraph is otherwise denied.

62. Paragraph 30 is denied. Contrary to TTL’s security for costs evidence which stated that the coins “*have been owned by TTL since at least 2011*”, and contrary to paragraph 30, TTL did not exist in 2011, nor did WMIRK.com deal in Bitcoin at that time. The purchase order relied on by TTL and Dr Wright is a forgery. In fact, the coins registered to the 1Feex address are understood to have been stolen from the Mt Gox exchange.

63. Paragraph 31 is admitted; its relevance is denied. TTL has failed to particularise when and how it claims to have taken ownership of the coin in the 12ib7 address. TTL did not exist in 2010. It is denied (if intended to be alleged) that the transactions identified in paragraph 31 were carried out by or on behalf of TTL.
64. As to paragraph 32:
- 64.1. It is admitted that (a) all on-chain transfers associated with the Addresses, and (b) the remaining coin associated with those Addresses, are recorded on the eCash blockchain, in line with the underlying rules of the system as described above.
- 64.2. It is admitted that the coin in the Addresses pre-dates the various hard forks relevant to this claim (including the emergence of the eCash blockchain) and remains registered to the Addresses as at the date of this Defence.
- 64.3. Sub-paragraph 32.b. inaccurately characterises the nature of the hard forks. As at the date of each hard fork, nodes continue to build onto the existing blockchain, albeit using different software. Accordingly, the same data will be recorded on the blockchain up to the date of the hard fork. That means that the same public addresses are found on the new blockchain, the same quantity of coin will be registered to those addresses, and the same private keys will apply to those addresses. Coin on each of the blockchains can thereafter be dealt with independently. Paragraph 31 above is repeated.
- 64.4. Ownership (including whether an owner of coin on a particular blockchain will also become an owner of coin on any additional blockchain which results from a hard fork of the first) is a legal issue which will vary depending on jurisdiction. Paragraph 43.8(a) above is repeated.
- 64.5. Paragraph 32 is otherwise not admitted.
65. Paragraph 33 is admitted save that, to the extent alleged, it is not admitted why dust payments were made to the Addresses. The potential for a known 'owner' to be subject to blackmail or other attacks is one reason why anonymity is a key principle underpinning the system.
66. As to paragraph 34, it is admitted that there have never been any transfers from the Addresses on the eCash blockchain. Paragraph 34 is otherwise denied. TTL is not and has never been the owner.

E THE ALLEGED THEFT

67. Paragraph 35 is denied. Neither Dr Wright nor TTL have ever held the private keys (or means of accessing the private keys) associated with the Addresses, for the reasons set out above. It is noted that TTL alleges that the private keys to the Addresses were contained in an encrypted wallet.dat files. Only Bitcoin Core and its derivatives use wallet.dat files, meaning that the keys in question must have been kept in an MIT licensed wallet. It is therefore to be inferred that TTL and/or others acting on its behalf expressly accepted the terms of the MIT Licence.
68. As to paragraphs 36 and 37:
- 68.1. Whilst the Fifteenth and Sixteenth Defendants have no direct knowledge as to whether Dr Wright's computer and/or network were unlawfully accessed between 5 and 8 February 2020, it is to be inferred from the circumstances that no such hack took place. In particular:
- (a) It is denied that Dr Wright's computer and/or network contained the private keys (or means of accessing the private keys) associated with the Addresses.
 - (b) Nobody with the knowledge which Dr Wright claims to enjoy would wipe their hard drives rather than disconnect them from the network (particularly in view of the nature of the information said to be held on the relevant computer(s)), or fail to attempt to restore the data from the One Drive and/or Google Cloud. It is noted that Dr Wright claims to have been "*unable to locate a record as to which files had been accessed and/or wiped during the hack as the system logs had been erased*" but has failed to specify what record he would have expected to have found.
 - (c) In or around February or March 2020, Dr Wright procured a report from Mr John Douglas of First Response, an IT forensics expert, who attended Dr Wright's home and performed an investigation. Mr Douglas was only able to produce a very brief report and it is accordingly to be inferred that he found no evidence of a hack.
- 68.2. In the premises, it is denied that the alleged hackers deleted and/or copied the private keys or any associated access information. TTL fails to particularise what other "*information and assets*" are alleged to have been stolen. The third and fourth sentences of paragraph 37 are not relevant to the present claim.
- 68.3. Paragraphs 36 and 37 are otherwise denied.

69. As to paragraph 38:
- 69.1. The alleged misappropriation is denied for the reasons set out above. The so-called ‘discovery’ is thus a fabrication.
- 69.2. TTL has failed to particularise the steps allegedly taken to secure Dr Wright’s personal computer. Insofar as Dr Wright wiped the hard drive, he did so to hide the fact that (a) he did not have the private keys to the Addresses and/or (b) the alleged hack did not take place.
- 69.3. To the extent that Dr Wright reported the alleged misappropriation to the Surrey Police (which is not admitted), this was a false claim. TTL has also failed to particularise the outcome of any investigation carried out by the Surrey Police.
- 69.4. By paragraph 35(a), TTL alleges that the private keys were backed up on Dr Wright’s OneDrive and Google Cloud. TTL has failed to particularise why such data was not restored upon the alleged loss.
- 69.5. Paragraph 38 is otherwise denied.
70. In the premises, save that it is admitted that TTL does not have (and has never had) possession of the private keys or means of accessing them, paragraph 39 is denied.
71. As to paragraph 40, TTL has failed to particularise which “*various*” Developers are alleged to have been sent a notice on 12 June 2020. It is admitted that a letter of that date was sent to the Fifteenth Defendant; it is not admitted that a letter of that date was sent to the Sixteenth Defendant at that time. It is admitted that a letter before action dated 24 February 2021 was sent to the Fifteenth and Sixteenth Defendants and that neither have accepted the existence of the alleged fiduciary or tortious duties, or agreed to take the steps requested. Paragraph 40 is otherwise denied.

F ALLEGED FIDUCIARY OBLIGATIONS

(i) Alleged fiduciary duties

72. Paragraphs 41 to 45 are denied. The Fifteenth and Sixteenth Defendants rely on the entirety of this Defence, and plead further below, without prejudice to the generality of such denial.

- 72.1. The Fifteenth and Sixteenth Defendants have no relationship whatsoever with TTL. Prior to the claim forming the subject of these proceedings, they had never communicated with it and were unaware of its existence.
- 72.2. The Fifteenth and Sixteenth Defendants do not act as remunerated developers vis-à-vis the eCash blockchain. The suggestion in TTL's security for costs evidence that, "*TTL has at all times proceeded on the assumption that the Defendants would be entitled to reasonable compensation for developing and implementing the required software*" is therefore wrong as a matter of fact (unless TTL is proposing to pay the Defendants for any software amendments).
- 72.3. On TTL's own case, the creation of the eCash blockchain and the alleged hack both took place long after it claims to have obtained coins on the original bitcoin blockchain. TTL has never purchased any coin on the eCash blockchain and, on its own case, did not even have access to or control over the cryptocurrency at the Addresses as at the date of the hard fork giving rise to the eCash blockchain. TTL never entrusted or placed any property into the care of anyone involved with the eCash blockchain (and certainly not the Fifteenth and Sixteenth Defendants).
- 72.4. Developers do not in any event have the power ascribed to them by TTL. Software developers merely propose software changes. Those changes must achieve market consensus and be adopted by nodes in order to take effect. The Fifteenth and Sixteenth Defendants are in no better position than TTL and/or Dr Wright (a self-professed software developer and someone with control over nChain) to propose the changes sought by TTL in this claim. They are equally likely to be rejected by nodes, for the reasons set out above. There is no imbalance as alleged.
- 72.5. A fiduciary duty does not arise in the abstract; it is a duty of fidelity and loyalty in the execution of existing obligations. It cannot be invoked in favour of a standalone obligation to act, or to enlarge the scope of other duties. Neither the Fifteenth nor Sixteenth Defendant undertakes acts of the same kind as claimed as relief in these proceedings.
- 72.6. A refusal to act in the manner sought by this claim would not in any event be capricious, unreasonable or disloyal, since an inability to effect a transfer without a private key is a fundamental system rule.
- 72.7. Any coins on the eCash blockchain are chains of digital signatures which exist only within the parameters of the system rules. The alleged fiduciary duties are likewise said to arise as an incidence of the rules by which the system operates. Those rules included (*inter alia*)

(i) anonymity of ownership, (ii) irreversibility of transactions, (iii) the requirement for a private key in order to transfer bitcoin, and (iv) no mediation of disputes. There can be no fiduciary duty to do an act (including amending the software or the data comprising the coins) in a manner which is inconsistent with the very rules by which that fiduciary relationship allegedly arose.

72.8. If developers had fiduciary duties to TTL, it would follow that they had duties to all 'owners'. Any changes to the software, however, would cause detriment to those other owners, for at least the following reasons: (i) they would be changes to the fundamental rules under which the owners had bought; (ii) they could negatively impact the value of the coins held by other owners, including by reintroducing large amounts of coins into the market and thus depreciating the value of existing coins; (iii) they would undermine the need for a private key; (iv) they would compel owners to step forward and abandon their anonymity whenever a claim was made in respect of coins registered to their public addresses; and (v) they would undermine the principle of irreversibility of transactions, which is important to many owners. The proposed changes would therefore be inconsistent with duties owed (on TTL's case) to other owners. The above factors militate against the imposition of the pleaded fiduciary duty.

72.9. The software through which coins are created and transacted, the alleged participation by TTL in such transactions, and/or the wallet by which the private keys were held, were expressly and/or impliedly subject to the MIT Licence, which precludes any claim or duties of the nature pleaded.

72.10. Owners are a fluctuating class of individuals and entities. Their transfer may be reflected on the blockchain or might have been agreed off-chain. Indeed, TTL claims to have taken ownership by way of off-chain transfer.

72.11. Developers are also a fluctuating class of individuals and entities. Indeed, TTL claims that Dr Wright was previously (but is no longer) a developer under the anonymous pseudonym "*Satoshi Nakamoto*". There can be no basis for imposing an obligation which would require them to continue to be involved and make changes when required by owners, when they have given no previous commitment or assurance that they would do so and their previous involvement may well have been intermittent.

72.12. Developers are also based all around the world, often with no connection to England and Wales. There is no justification for the extra-territorial, international application of English law rights and obligations to all users of the Bitcoin system worldwide. That is particularly

so in circumstances where such obligations could conflict with the Defendants' own national and/or constitutional rights. The Fifteenth and Sixteenth Defendants expressly deny that they are subject to English legal obligations in respect of any development activities they have carried out.

72.13. The alleged duty would, contrary to authority, involve the taking of extensive positive actions. Any breach is a pure omission. TTL says that, the private key having been lost, the Defendants should positively take action that would have the effect of permitting TTL to regain its ability to access its Bitcoin. Indeed:

- (a) As regards the primary claim, developers would be under extensive investigatory and judicial obligations, after which they would have to carry out extensive drafting of computer code in order to attempt to give effect to the claim. The primary claim thus seeks to put them in the position of police, judiciary and bailiffs.
- (b) As regards the secondary claim added by amendment, upon receipt of a Court judgment confirming ownership, developers would still be under obligations (as 'bailiff') to carry out extensive drafting of computer code in order to attempt to give effect to the claim. Moreover, an obligation to comply with a Court Order does not in any event give rise to a fiduciary duty to act as a matter of law.
- (c) On either case, they would be required to write and publish updates each and every time any owner no longer had access to its private key. There is no pleaded limitation on the ability of an owner to require these changes to be put into effect, such that any number of owners could require software changes any number of times.

72.14. Moreover, the steps which the Defendants would have to take to fulfil such obligations (in respect of which no remuneration would be paid) are impossible.

- (a) In acting as 'police', it would be impossible for the private individuals subject to this claim to investigate and determine ownership of the global supply of Bitcoin in respect of anyone who claimed to be unable to access their coin: 'ownership' is anonymous; millions of claims could be advanced; the Defendants would be wholly reliant on information submitted by third parties and would have no means of notifying all potential competing owners globally; they would have insufficient resources to carry out these tasks. True 'owners' may not wish to waive their entitlement to anonymity; and some may not even keep track of the specific addresses they control since that can be managed by their wallet software.

- (b) In acting as 'judiciary', it would be impossible for the Defendants to determinate conclusively whether a given claimant was the true owner or not, for all the reasons set out above. Moreover, they have no authority to carry out such judicial activities, and there is no mechanism in the event that different conclusions were reached by different Defendants on the facts available to them. There would be none of the usual judicial protections for claimants (such as right to appeal and right to a fair hearing) and no legal protection for those individuals exercising this quasi-judicial role against proceedings brought by dissatisfied claimants.
- (c) In acting as bailiff (giving effect to the investigatory and judicial stages above in respect of coin not claimed by the Defendants), this amounts to a kind of specific performance which would require the writing of new digital code (effectively a design obligation), in a way which could not be prescribed in any satisfactory way by Court order (there being no 'one way' to write such code), and thereafter seeking to compel users of the software around the world to download and use that amended digital code (despite users being at liberty to use whatever software/updates they want).
- (d) Any such software amendments would also be wholly ineffective unless accepted by the majority of nodes. For the reasons set out above, that is unlikely. The reputations of the Fifteenth and Sixteenth Defendants would, however, be negatively affected.
- (e) Moreover, even if the Defendants could effect any such transfer, they would be unlawfully interfering with the ability of a controller of the private key to transact for value and/or expropriating a true 'owner' of their property (to the extent that the law recognises such ownership), and could face civil and criminal actions across the world as a result of such expropriation and/or carrying out regulated transfer activities.

72.15. In the present case, the alleged liability would arise from losses allegedly caused by the conduct of a third party. TTL does not allege that the Defendants were responsible for the loss of the private key. It also does not suggest that the Defendants could or should have prevented the loss of its private key. TTL seeks steps to counteract third party conduct. The law imposes no such liability.

72.16. The alleged duty would be owed to the world at large and in respect of unknown or unpredictable sums of money. Anybody in the world can buy Bitcoin, including both on-

and off-chain transfers. Bitcoin can be stored (i.e. left undisturbed on the Blockchain) for an indeterminate period of time. Anybody in the world can lose access to their private key (through anything from fraud to forgetfulness). The alleged duties would thus be owed to the world at large. The alleged duty is accordingly within the four corners of the prohibition against “*liability in an indeterminate amount for an indeterminate time to an indeterminate class*”.

72.17. Any Court order as to ownership would take effect *in personam* only, and could not be relied upon by developers as binding any other potential claimants. The recognition of a duty in those circumstances would thereby involve developers in an indeterminate liability to potential claimants if they fail to transfer such property, and an equally indeterminate liability to other potential claimants if they do so.

72.18. There are no similar duties recognised as a matter of English law, and any such duties would not be an incremental extension.

72.19. Controllers and/or ‘owners’, including TTL, have the power to secure and/or back up their private keys. They can also insure against loss, and can take actions against the alleged hackers. By contrast, it is unlikely that any, or any adequate, insurance could be obtained by the Fifteenth and Sixteenth Defendants for the type and quantum of potential liability in question.

72.20. By allegedly participating in a global system such as Bitcoin, TTL thereby accepted the fundamental rules governing the system, including those identified in paragraph 23 above. It ought not to be permitted to go behind those rules simply because they no longer suit it.

73. As regards paragraph 42, developers do not have any powers or decisions in relation to taking the steps alleged for the reasons set out above. Those steps would be contrary to the fundamental system rules. Paragraph 42(b) is not relevant to the present claim, TTL having pleaded that no fraudulent transaction has taken place. The coins at the Addresses have not been transferred.

74. As to paragraph 44, there is no public policy imperative in favour of the alleged duties. On the contrary, whilst public policy considerations are in any event irrelevant, they in fact militate against the imposition of any such duty. As to the sub-paragraphs:

74.1. Save that it is admitted that Bitcoin is traded globally, sub-paragraph 44.a. is not admitted.

74.2. Sub-paragraph 44.b. is denied. The use of a private key is fundamental to the operation of the system and is a rule which, on TTL’s own case, was or ought to have been known to it at the time of obtaining its coins. That is reasonable in order (*inter alia*) to reduce transfer

costs and avoid the need for intermediaries, together with the further matters set out in paragraph 18.1 above. It is incumbent on an person in possession of a private key to secure it and/or back it up (as TTL and/or Dr Wright was well aware).

74.3. Sub-paragraph 44.c. is denied. The analogy is inapposite; and it would not in any event be capricious to hold an owner to the known and accepted rule by which a transfer of coin can only be made by using a private key. Moreover, for the reasons set out above, the Fifteenth and Sixteenth Defendants do not have the powers ascribed to them.

74.4. Sub-paragraphs 44.d. and e. are misconceived. The blockchains are not easily amenable to manipulation by fraudsters. Indeed, Mr Cain's first statement in support of TTL's application to serve out of the jurisdiction confirmed at paragraph 21 that, "*As it is a single ledger which **cannot be cheated or manipulated**, the Blockchain protects against double spending and corrupted files*". Even on TTL's case, its coin has not been moved. The sub-paragraphs are otherwise denied. Moreover, the present claim has nothing to do with any "*lawless use of Bitcoin*" or its alleged "*use on the dark web and in transactions relating to illegal and immoral activities*" which are not admitted and in any event irrelevant.

74.5. Sub-paragraph 44.f. is misconceived. The Fifteenth and Sixteenth Defendants do not provide services as alleged. Public policy militates in favour of holding a party to the rules of a system which it has, by its alleged transaction, accepted.

75. Paragraph 45 is insufficiently particularised. TTL has failed to set out: (i) the precise content of any amendments it contends are required to any software used on the eCash blockchain; or (ii) how such amendments should be made effective by nodes. The allegations in sub-paragraphs 45.a., b., and c. are so vague as to be embarrassing. The Fifteenth and Sixteenth Defendants in any event have no power to carry out the actions pleaded.

(ii) Alleged breach of fiduciary duty

76. It is denied that the Fifteenth and/or Sixteenth Defendants are in breach of duty, whether as alleged or at all.

77. As to paragraph 46:

77.1. It is admitted that neither the Fifteenth nor the Sixteenth Defendants have taken any of the steps set out in paragraph 45 of the Amended Particulars of Claim. For the reasons set out above, they neither have the power nor the duty to do so. Sub-paragraph 46.a. is otherwise denied.

- 77.2. Sub-paragraph 46.b. is insufficiently particularised. TTL has failed to set out what other “steps” it alleges ought to have been taken; it is common ground that the coins at the Addresses has not been moved; and the Fifteenth and Sixteenth Defendants in any event have neither the power nor the duty to take any action.
- 77.3. The inability to execute a transaction is the inevitable consequence, known and accepted by TTL, of the loss of a private key. That does not in law amount to recoverable loss. Indeed, TTL has not even pleaded an intention to make any transfer.
- 77.4. As set out above, having considered TTL’s claim, the Fifteenth and Sixteenth Defendants do not in any event consider TTL to be the rightful ‘owner’ of the coin registered at the Addresses (if ownership is, contrary to the above, possible in law). Accordingly, even if a duty had arisen in favour of a true owner, the Fifteenth and Sixteenth Defendants cannot be in breach having reasonably reached the conclusion that any software change would expropriate the true owner. The Fifteenth and Sixteenth Defendants will further rely on the matters set out in paragraph 83.6 below.
- 77.5. In any event, even if the Fifteenth and Sixteenth Defendants had taken the steps alleged, they would have no meaningful effect, since such changes are unlikely to be accepted by any material number of nodes operating on the eCash blockchain. In those circumstances, the Fifteenth and Sixteenth Defendants can have caused no loss.
- 77.6. Paragraph 46 is otherwise denied.
78. Paragraph 47 is denied for the reasons set out above. Moreover:
- 78.1. TTL has failed to particularise the basis on which it is alleged that the receipt of a declaration on ownership would immediately place the Fifteenth and Sixteenth Defendants in breach of duty. This is denied.
- 78.2. It is moreover denied, if intended to be alleged, that any declaration as to ownership would create a duty on the part of the Fifteenth and Sixteenth Defendants where no such duty existed previously.
- 78.3. The Court is not able to make an *in rem* determination of ownership in the present proceedings. TTL has also failed to add the other individuals who have asserted claims to ownership of the same coins. In the premises, receipt of an order as to ownership in these proceedings will not be binding on any third parties and will accordingly not be conclusive as to ownership. TTL ought not to be permitted to seek relief effectively amounting to *in rem* relief, and the Fifteenth and Sixteenth Defendants could not properly be regarded as

having acted unreasonably, irrationally and/or capriciously, in those circumstances. The Fifteenth and Sixteenth Defendants will further rely on the matters set out in paragraph 83.6 below.

79. Paragraphs 48 and 49 are denied for the reasons set out in this Defence. Moreover:
- 79.1. TTL has failed properly to particularise the “steps” sought by way of relief. Paragraph 75 above is repeated. Any such steps would in any event be impossible, as further particularised above.
- 79.2. TTL has failed to particularise the quantum of compensation sought and/or the basis for such a figure. Bitcoin is a highly volatile market and TTL has at no time indicated an intention to transfer any of the coin in the Addresses to others in the market for value. Moreover, any attempt to transfer the entirety of the coin in the Addresses is itself likely to cause a significant decrease in the market value of coins (on account of the increased available supply thereby caused).
- 79.3. No orders should be granted in any event on account of TTL’s own failure adequately to secure and/or back up its alleged private key; its wiping of its hard disk; and/or its failure to restore its alleged private key from Dr Wright’s OneDrive and/or Google Cloud. Had it done so, the present claim would not have been necessary. To the extent that TTL relies on any alleged hardware or router said to have been physically placed in its premises, the Fifteenth and Sixteenth Defendants will likewise rely on TTL’s failure to identify such item in advance of the alleged hack.
- 79.4. An inability to access coins without the private key does not constitute loss: it is merely the known, accepted and inevitable outcome of the rules of the system and by which the relevant coin was created and/or transferred.
- 79.5. The Fifteenth and Sixteenth Defendants have obtained no benefit from TTL or its alleged coins; have not been remunerated to carry out the actions claimed; and ought not to be subject to any order for equitable compensation or an account.
80. Save that it is admitted that the Fifteenth and Sixteenth Defendants have not accepted that TTL owns the coins in the Addresses, paragraph 50 is denied for the reasons set out in this Defence. Moreover, the claim will operate *in personam* only. It will not bind any rival claimants, and (despite being aware that such rival claimants exist) TTL has not sought to add them as defendants. The Order sought, by contrast, would effectively amount to *in rem* relief, since TTL thereby seeks the immediate transfer of coins out of the hands of any other owner. The Fifteenth

and Sixteenth Defendants have no competing interest in the coins and/or Addresses subject to this claim. This claim is thus akin to commencing a claim against bailiffs to compel them to seize and transfer property, despite the bailiffs having no knowledge of the underlying claim and having no interest in the property to be transferred. No such order would be appropriate; would amount to an order against a non-party and would breach such non-party's right to a fair trial.

G ALLEGED TORTIOUS DUTY

(i) Alleged tortious duties

81. Paragraphs 51 and 52 are denied. The Fifteenth and Sixteenth Defendants rely on the entirety of this Defence, and plead further below, without prejudice to the generality of such denial.

81.1. Where a case does not fit within an established category of liability, the law can develop only by incremental extension. The duty alleged is not incremental to any scenarios in which a duty of care has previously been found to arise.

81.2. There is in any event no voluntary assumption of responsibility by the Fifteenth and Sixteenth Defendants to TTL, no proximate relationship, and it would not be fair, just or reasonable to impose a duty of care against the Fifteenth and Sixteenth Defendants.

81.3. It is not foreseeable that any harm would be caused to owners on the eCash blockchain. The consequences described by TTL are the inevitable result of the rules underlying the system.

81.4. Paragraphs 72 to 74 above are repeated *mutatis mutandis*.

81.5. Moreover, the alleged losses are purely economic. In such a situation, no common law duty of care can arise in the absence of a special relationship. No "*special relationship*" exists here (and none is alleged).

81.6. TTL is, in truth, seeking to establish through the Courts a wide-ranging regulatory framework for Bitcoin which cannot be accommodated by the common law and which should properly be left for Parliament.

82. The "*arrangements*" and "*steps*" identified in paragraphs 51(a) and (b) are insufficiently particularised. Paragraph 75 above is repeated.

(ii) Alleged breach of duty

83. Paragraphs 53 to 55 are denied.

83.1. No such duty exists. Paragraph 81 above is repeated.

83.2. TTL has failed to particularise the content of any software amendments it contends should have been written by the Fifteenth and Sixteenth Defendants. Paragraph 75 above is repeated.

83.3. The Fifteenth and Sixteenth Defendants are not in breach in any event. Paragraphs 76 to 80 above are repeated *mutatis mutandis*.

83.4. If, by sub-paragraphs 53(a) and (b), TTL seeks to allege a requirement for inclusion within the software of a mechanism for any user to retrieve a private key, that would be a matter which, on its own case, should properly be directed against Dr Wright as the alleged creator of the system. It is noted that, in the jurisdiction application, TTL expressly disavowed that its claim alleged such a broad duty, but was instead limited to an obligation to enable access to the coin subject to this claim.

83.5. The Fifteenth and Sixteenth Defendants have no ability to make the changes sought by TTL. Any software drafted to have such effect would be inconsistent with the fundamental rules of the system and would not be accepted by nodes.

83.6. Moreover, refusing to write such software amendments is reasonable in (*inter alia*) circumstances where (or where the Fifteenth and Sixteenth Defendants reasonably believe that):

- (a) To do so would require considerable time and resource;
- (b) The Fifteenth and Sixteenth Defendants would not be remunerated for doing so;
- (c) The Fifteenth and Sixteenth Defendants' reputations would be damaged;
- (d) The Fifteenth and Sixteenth Defendants reasonably consider that: TTL is not the true owner of the coins at the Addresses and that the claim is fraudulent; the first statement of Mr Cain in support of TTL's application to serve out of the jurisdiction identifies a number of matters which are inconsistent with TTL's claim ever to have owned coins registered at the Addresses; Dr Wright failed, when requested by the Australian Taxation Office, to demonstrate ownership; and the Fifteenth and Sixteenth Defendants are aware of a large number of judicial and quasi-judicial

findings that Dr Wright has previously lied and/or fabricated documents, as well as a large number of online articles and other research indicating that Dr Wright has committed fraud and plagiarism;

- (e) There are in any event competing claims for such coins, none of which TTL has sought to have resolved;
- (f) Any changes by the Fifteenth and Sixteenth Defendants having the effect of dispossessing a potential owner could be subject to civil and/or criminal claims against the Fifteenth and Sixteenth Defendants across the world; and
- (g) Any changes are in any event likely to be of no effect since they would not be accepted by nodes. Accordingly, time spent in writing code would be wasted and of no use.

83.7. No injunctive relief is available to TTL as a matter of law and/or should not be ordered by the Court as a matter of discretion. There is, moreover, no imminent harm which can be identified, the hack having allegedly taken place some years ago and even before the eCash blockchain was created.

83.8. Likewise, TTL is not entitled to any damages. The Fifteenth and Sixteenth Defendants have caused no loss. Any loss results from TTL's own failures identified in paragraph 79.1 above. Further or alternatively, TTL was contributorily negligent in that regard to the full extent of its claim. Further or alternatively, an inability to access coins without the private key does not constitute loss: paragraph 79.4 above is repeated.

H RELIEF

84. It is denied that TTL is entitled to relief, whether as claimed or at all, for the reasons set out in this Defence.

84.1. This is a fraudulent claim. TTL is not the true owner of the coins. Moreover, any declaration as to ownership would operate *in personam* against Defendants who do not themselves claim ownership; and TTL has failed to add any rival claimants to the same coins. The Fifteenth and Sixteenth Defendants are not proper parties to that claim, and any declaration would serve no useful purpose.

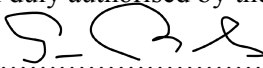
84.2. The claim is in contravention of the Fifteenth and Sixteenth Defendants' national and/or constitutional rights.

- 84.3. There is no proper basis for the pleaded duties, and the Fifteenth and Sixteenth Defendants do not have the powers ascribed to them. There is also a strong likelihood that any orders made in this litigation would have no effect, because the nodes who build the blockchains would not accept the amendments proposed.
- 84.4. TTL has failed to set out with the necessary particularity the software amendments which it seeks by way of relief. The claim as presently pleaded is incapable of giving rise to an injunction or order for specific performance, since the terms of any such order could not be formulated in a manner capable of performance (or, indeed, in a manner in which the Court could ascertain compliance).
- 84.5. Any software change which TTL seeks would not result in access to the coins at the Addresses, but would amount to the deletion of the existing coins and creation of entirely new coins. That is not a remedy available to TTL as a matter of law.
- 84.6. In truth, TTL is responsible for its own alleged losses: the simple answer to this claim is that, in accordance with the rules of the system, any ‘owner’ should keep their private key secure and backed-up; and the consequences if they fail to do so are known, accepted and at their own risk.
85. Since on its own case TTL’s main asset is the coin allegedly held in the Addresses, this litigation must be funded by a third party. It is assumed that it is being funded by Dr Wright (who is, in effect, the *alter ego* of TTL) and/or Mr Calvin Ayre (who has funded Dr Wright’s litigation in the past).

MATTHEW THORNE

STATEMENT OF TRUTH

The Fifteenth and Sixteenth Defendants believe that the facts stated in this Defence are true. I understand that proceedings for contempt of court may be brought against anyone who makes, or causes to be made, a false statement in a document verified by a statement of truth without an honest belief in its truth. I am duly authorised by the Fifteenth and Sixteenth Defendants to sign this statement.

Signed: 

Name: **Samuel Charles Roberts**

Position: **Partner**

Company: **Cooke, Young & Keidan LLP**

Date: **3 May 2023**

Claim No. BL-2021-000313

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

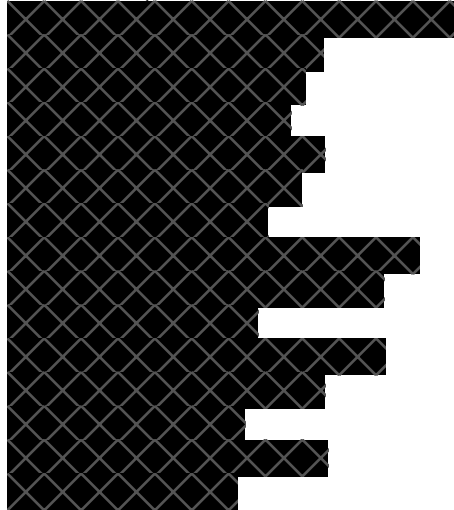
B E T W E E N : -

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

Claimant

- and -

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



Defendants

DEFENCE OF THE
FIFTEENTH AND SIXTEENTH DEFENDANTS

Cooke, Young & Keidan LLP
21 Lombard Street
London
EC3V 9AH

Solicitors for the Fifteenth and Sixteenth Defendants