EIP

Tulip Mania - Can an individual or group be said to have de-facto control over a cryptocurrency network?

(Tulip Trading Limited v Van der Laan and Others [2023] EWCA Civ 83)

In the Dutch Golden Age, circa 1634, the price of tulip bulbs temporarily reached extraordinarily high levels as market speculators fought to profit from this newly-introduced luxury.The price dramatically tanked three years later, and this "tulip mania" would later be held up as an archetype of a speculative bubble in which prices of an asset deviate from its intrinsic value.

Fast forward 400 years, and an ironically named "Tulip Trading" has taken centre stage in a dispute which could have a real impact on the credibility and value of one of the modern day's most speculative assets – cryptocurrency. In a recent article, EIP colleagues Ellen and Mark discussed the English Court of Appeal's ruling in Tulip Trading v Van der Laan and Others, on the subject of whether software developers of a cryptocurrency owe a fiduciary duty to users of the code they write. A key question in this dispute is whether an individual or group can be said to have de-facto control over a cryptocurrency network. In this article, we take a closer look at this question to identify factors that could influence the answer.

Background

As a brief background to the case, the claimant Tulip Trading Limited ("Tulip") claims that it owned approximately $4 billion worth of Bitcoin but, as a result of a hack on the home computer of its CEO, has lost the private encryption keys needed to access the Bitcoin.

Tulip has brought a claim against sixteen core developers involved in the development of the blockchain code underlying Bitcoin, claiming that the developers owe a fiduciary
p2 and/or tortious duty to implement a software patch to restore Tulip's ability to access the Bitcoin. The defendants deny they have such duties, and contend that they have nothing like the power or control that Tulip alleges and that such a duty would be unworkable.

Blockchain

A key issue in this case is whether the control of a cryptocurrency is "decentralised", or whether in fact that control is in the hands of an individual or small group.

Cryptocurrencies are often described as being a decentralised form of currency. This usually refers to the fact that responsibility for verification and recording transactions of the cryptocurrency is shared between many users of a computer network, rather than lying with a central trust body (such as a bank). This decentralisation is typically implemented using blockchain technology.

A blockchain records all of the transactions of the cryptocurrency. This transaction data is stored in units, known as blocks, which are chained together in chronological order. For each new batch of transactions, a new block is created. This new block includes the new transactions, as well as a hash (a unique signature) of the previous block. Including the hash links the new block to all of the previous blocks in the chain so that the new block will only be successfully verified if its transactions follow on from the transactions of the earlier blocks.

According to the blockchain protocol implemented by Bitcoin, the storage of the blockchain and the generation and verification of new blocks is performed by miner software running on nodes of a computer network. Anybody can become a Bitcoin miner by simply downloading a copy of the miner software. A copy of the blockchain is stored by each miner. When a new block is to be added, the transaction data is distributed to all of the miners. The miners compete to be the first to identify a hash of the data in the previous block that meets specific requirements defined by the protocol. Once a miner identifies a hash that meets the requirements, the new block is distributed to the other nodes for verification. If there is consensus on verification between the nodes, the block is added to the blockchain, and the miner is rewarded with newly-minted Bitcoin.

Accordingly, control over the blocks added to the blockchain (and hence control over the record of transactions of the cryptocurrency) is decentralised: it is by consensus among all the miners of the network. If a miner were to act dishonestly, for example by mining a fraudulent block in which the transaction record has been tampered with, then the block would fail verification by the other miners as it would disagree with the transaction data

stored by the other miners. The rogue miner could go on to pursue a sequence of fraudulent blocks, but on their own would be unable to verify blocks at anywhere near the
p3 combined rate of the other miners working to verify a common legitimate block, so the number of blocks in the fraudulent sequence would lag behind the number of blocks in the legitimate sequence. Since only the longest blockchain branch is accepted as valid by the miner software, no one party has control over the blockchain (and hence the record of transactions) provided that no one party controls more than 50% of the total computational power of the miners.

Open source software development

For a typical cryptocurrency (such as Bitcoin), the miner software operating on each of the nodes is maintained as an open source software development project. In such a project, software developers work together to write code, and make the code publicly available under an open source licence. For example, the code of the mining software for Bitcoin is publicly available on the cloud-based software repository GitHub, and is provided under the permissive, open source, MIT License. This license allows anyone to use or modify the code as they see fit, provided certain permissive conditions are complied with.

Open source projects are highly collaborative and community-oriented. Anyone can propose improvements to the code, and these may be taken up. However, in larger projects (such as Bitcoin) typically only a certain group of core developers have "commit access" to the code (that is, password protected access to make changes to the code on GitHub). In the sense that only these developers can make changes to the code listed for the project on GitHub, they can be said to have control over that code.

However, as explained below, the open source nature of the projects may limit the actual control that these core developers have over the cryptocurrency network itself.

Specifically, provided the conditions of the open source license are complied with, other developers are free to modify the miner code and publish their own versions on GitHub. Each miner has discretion to choose which version of the miner code they run. For example, a group of miners could choose to run an older version of the code if a newer version includes changes that the group disagrees with. Different groups of miners can end up running different versions of the miner code, resulting in a so-called "fork" of the blockchain. Forks come in two flavours: soft and hard. A soft fork occurs when two different versions of mining software can successfully verify common blocks, and thus remain compatible so that miners can easily switch between versions. A hard fork, on the other hand, results in different software versions disagreeing over the content of a block to be mined, meaning that the separate versions begin to generate distinct blockchain

branches. If the branches are pursued by different groups of miners, this effectively splits the original cryptocurrency into two different versions, which can have a significant impact on the "real world" value of the cryptocurrency. A fork resulting from an update seeking to refund or otherwise modify transactions would inevitably be a hard fork, as the blocks created on the different branches would disagree on transactions and therefore be incompatible.

Precedence for a cryptocurrency to split into separate versions is provided by the Ethereum hard fork of 2016, in which core developers sought to update the miner code of the Ethereum blockchain to reverse the effect of an evident act of fraud. A majority of miners favoured justice for the victim, and willingly accepted the updated miner code. However, a significant minority of miners, holding sacrosanct the immutability of the blockchain, refused the update and set up a separate open source project to continue using the earlier version of the miner code, spawning a separate cryptocurrency referred to as Ethereum Classic. Both versions coexist to this day, and only the ownership of the Ethereum trademark by the Ethereum Foundation distinguishes one version as the "official" Ethereum cryptocurrency.

The Ethereum hard fork serves as a warning to developers seeking to override the immutability of a cryptocurrency blockchain. Bitcoin itself has undergone similar forks, the most significant giving birth to the popular "Bitcoin Cash" variant.

Factors affecting control over a cryptocurrency network

As discussed above, key to a cryptocurrency network are the miners that record and validate the transactions. In order for the miners to adopt a new version of the miner code (for example a version that includes a software patch to fix a loss), they must be willing to accept it. The control that any particular individual or group has over the cryptocurrency network would therefore also seem to include the influence that the individual or group has over the miners to adopt the new version of the code. In particular, any party seeking to impose such a new version must be able to persuade a large enough majority of the miners to adopt the code to avoid rejection or a crippling chain split. Whether this is possible will likely depend on the nature of the changes that the new version of the code represents, and the willingness of the cryptocurrency community at large to accept those changes. As shown by the Ethereum hard fork, a unilateral action to reverse a loss or act of fraud may be seen by members of the community as going against the core principle of immutability of the blockchain – the principle from which trust (and hence value) in the cryptocurrency arises. The feeling of the community may be complicated further if such an action is performed at the behest of an English court, raising moral issues and also a practical question as to the extent to

which the court could enforce a judgment in favour of the claimant.

p5 In conclusion, while it seems in principle possible that an individual or group could have the power to reverse a loss of cryptocurrency, determining whether this is possible in practice would seem to require consideration of case-specific factors beyond merely whether the individual/group has 'commit access' to make changes to the miner code.

What next?

The Court of Appeal has ruled that the question of whether an individual or group has de-facto control of a cryptocurrency network, and the contingent question of whether its developers can owe a fiduciary duty, constitute a serious issue to be tried, and can therefore proceed to trial. The international cryptocurrency community will be watching the case with great interest.