KEY POINTS

- Software developers should not be held to owe a fiduciary duty to grant an owner access to its Bitcoin where that owner has lost its private key.
- Even taking Tulip Trading Limited's (TTL) factual case at face value (as was required in the jurisdiction challenge), there is no basis for recognising that fiduciary duty. It is very different from a duty to fix software bugs since the absolute requirement for a private key is a fundamental security feature of the system.
- In any event, TTL's factual case does not reflect the reality of the Bitcoin system. Power is diffused between multiple constituencies. So, developers should not be regarded as fiduciaries at all.

Feature

Author Mohamed Sacranie

Blue pill or red pill? Into the *Tulip Trading* rabbit hole

If someone steals my 10 pound note, I would have to go after that person to recover it. Digital money is different since victims might also be able to ask a bank to intervene. But what about where Bitcoin (or its private key) is stolen? Since Bitcoin is (meant to be) decentralised, there is no bank. But should Bitcoin software developers intervene? In *Tulip Trading Limited v Van Der Laan and ors* [2023] EWCA Civ 83, the Court of Appeal said they might have to. This article disagrees (the views are the author's own).

In *The Matrix*, Morpheus offered Neo the following choice:

> "You take the blue pill, the story ends. You wake up in your bed and believe whatever you want to believe. You take the red pill, you stay in Wonderland, and I show you how deep the rabbit hole goes. Remember, all I'm offering is the truth. Nothing more."

The *Tulip Trading* case offers us a similar choice. We have two options when considering the question whether Bitcoin developers owe a fiduciary duty to grant an owner access to its Bitcoin where that owner has lost its private key:

- **The Blue Pill** precludes factual investigation. Instead Tulip Trading Limited's (TTL) factual case regarding the nature of the Bitcoin system is taken at face value (ie the story ends there). In the jurisdiction challenge, we have to take the blue pill.
- **The Red Pill** means diving into the Bitcoin rabbit hole and investigating whether TTL's factual case reflects the reality of the Bitcoin system. The red pill – which offers the truth – will be taken at trial.

Neo's choice in the Matrix would inevitably lead him to different destinations. However, this article will argue that whichever pill you take, the ultimate conclusion is the same: Bitcoin developers do not owe a fiduciary duty to grant TTL access to its Bitcoin.

WHAT IS BITCOIN?

The cryptocurrency Bitcoin (ie BTC) was created in 2009 by the pseudonymous Satoshi Nakamoto. The Bitcoin system consists of:[1]

- **A decentralised peer-to-peer network of nodes** run by participants. Nodes may perform one or more of various functions which include: mining, routing and maintaining a copy of the blockchain. Participants that run mining nodes are referred to as miners.
- A type of distributed ledger (ie a **blockchain**) which records transactions.
- **Software** run by nodes. There are multiple compatible software options but Bitcoin Core is currently the most popular. This point should not be confused with the separate point that there are multiple systems (eg the Bitcoin system, Bitcoin Cash system, Bitcoin Satoshi Vision system).

The Bitcoin system is decentralised in various ways:

- The blockchain is distributed so that no single node is in control of it.
- Mining ensures that no single entity is relied upon to validate and confirm transactions and update the blockchain.
- The software is open source: anyone can view it, propose changes or copy it.

From 2009 onwards, a community of developers began contributing to the software. The original software was not perfect. For example, Bitcoin's total supply is capped at 21 million but in August 2010 a hacker exploited a bug to produce 184 billion Bitcoin. This was quickly fixed by Satoshi.

Satoshi's final contribution to the software was in December 2010. Shortly thereafter, in April 2011, Satoshi announced their departure from Bitcoin. Satoshi's identity remains a mystery.

THE BLOCKSIZE WAR

Bitcoin blocks have a size limit. From around 2015, the existing 1MB limit caused problems; increased adoption meant more transactions which resulted in delays and increased fees. There were competing solutions:

- **Increase the blocksize limit**: This was a hard fork proposal (ie it violates an existing rule in the software). Without unanimous support, this proposal would split the blockchain (ie a chain-split).
- **Segregated Witness (SegWit)**: This soft fork proposal solved the problem by creating a new transaction format. A soft fork proposal will not result in a chain-split provided it is supported by a majority of mining power.

Disagreements led to chain-splits and the creation of new cryptocurrencies: Bitcoin Cash (BCH) in 2017, Bitcoin Satoshi Vision (BSV) in 2018 and BCH ABC in 2020. Common usage of the term "Bitcoin" actually denotes BTC only and this article will adopt that approach.

THE CLAIM

TTL is a Seychelles incorporated company. Its CEO is Dr Wright who claims to be Satoshi. That claim is very widely disputed.

Files containing TTL's private keys were hacked and TTL said it was unable to access over £3bn worth of cryptocurrency

(ie Bitcoin, BCH, BSV and BCH ABC). Instead of pursuing the anonymous hackers, TTL sued the defendant developers. TTL claimed that they control the relevant networks and therefore owe it fiduciary and/or tortious duties to assist it in regaining access.

This article will focus on TTL's amended case on fiduciary duties as put before the Court of Appeal [81]. The fiduciary duty would arise when it is established that the true owner is unable to access their cryptocurrency because their private key has been stolen. The duty is to introduce a code update which grants the owner access.

BLUE PILL: THE JURISDICTION CHALLENGE

Almost all the defendants challenged jurisdiction. There is a three-stage test for permission to serve out. This section will focus on the first stage and more specifically on the following question: *Is there a serious issue to be tried on whether the BTC defendant developers owe the alleged fiduciary duties?*

The High Court said no. The Court of Appeal said yes. Who was right? First, we need to take the blue pill which for some may be hard to swallow. The first stage is a summary judgment test so it cannot resolve the factual question whether the Bitcoin system is decentralised. We will therefore take TTL's factual case at face value and make the following four assumptions in its favour: (i) the BTC developers are a sufficiently well-defined group; (ii) the BTC developers control the software; (iii) the BTC developers control the network; and (iv) the BTC developers are able to implement a software patch to allow TTL to access its Bitcoin.

The Court of Appeal summarised its analysis as follows:

> "… [T]here is, it seems to me, a realistic argument along the following lines. The developers of a given network are a sufficiently well defined group to be capable of being subject to fiduciary duties. Viewed objectively the developers have undertaken a role which involves making discretionary decisions and exercising power for and on behalf of other people, in relation to property owned by those other people. That property has been entrusted into the care of the developers. The developers therefore are fiduciaries. The essence of that duty is single minded loyalty to the users of bitcoin software. The content of the duties includes a duty not to act in their own self-interest and also involves a duty to act in positive ways in certain circumstances. It may also, realistically, include a duty to act to introduce code so that an owner's bitcoin can be transferred to safety in the circumstances alleged by Tulip." [86]

The Court of Appeal justified the final sentence on the basis that a positive duty to fix software bugs is sufficiently similar to a positive duty to implement the patch requested by TTL. In both, the nature of the activity required to fulfil the duty is the same, ie a code update [85]. In the former scenario (regarding software bugs), there may be disagreement amongst owners over whether the alleged bug is a bug and/or how to fix it [31]. The developers make the ultimate decision and the informed consent of owners as a whole to developers exercising that authority in good faith can be inferred from the circumstances. Thus, the developers' decision will not breach the fiduciary duty of single minded loyalty owed to owners as a whole [80]. Since developers are entrusted by owners with decision-making, it follows that a good faith decision by developers to implement TTL's requested patch will not breach their fiduciary duty of single-minded loyalty owed to owners as a whole (even if some owners object to that patch) [84].

This analysis is problematic because it relies on a flawed analogy between software bugs and the inability to transfer Bitcoin without a private key. Consider the following non-exhaustive spectrum of situations where developers might be asked to make a software change, see Figure 1 below.

(1) **The Obvious Bug Scenario**: On one end, you have obvious errors in the software where everyone agrees that there is a problem. An example of this is the 184bn Bitcoin incident.

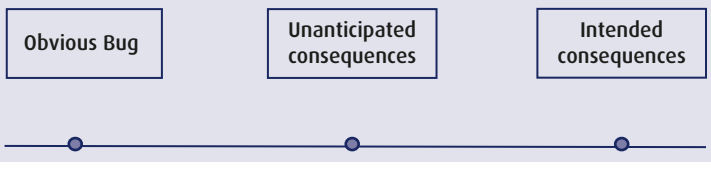
(2) **The Unanticipated Consequences Scenario**: In the middle, you have intentional design features which give rise to unanticipated consequences. An example of this is the 1MB blocksize limit. There may be disagreements over whether there is a problem at all as well as over the solutions.

In both (1) and (2), since we have to assume that the developers control the networks (as we have taken the blue pill), they may be under a fiduciary duty to consider the situation (which may or may not require action). Since they are entrusted with decision making for the benefit of owners as a whole, a decision made in good faith will not breach their fiduciary duty of single-minded loyalty owed to owners (even if some owners disagree).

(3) **The Intended Consequences Scenario**: On the other end, you have intentional design features which give rise to intended consequences. An example is the inability to transfer Bitcoin without a private key. That this consequence was intended can be established without controversial factual investigation. First, both the Court of Appeal and TTL accepted that "as the Bitcoin software is currently coded, a user cannot transfer bitcoin on the blockchain other than with the relevant private key" [38]. Second, the Bitcoin White Paper explains in its introduction that a key aim of the Bitcoin system is to create completely non-reversible transactions (ie transactions that cannot be undone without the consent of the recipient who now holds the relevant private key). Third, in 2009 Satoshi was publicly asked about the topic of lost keys and the possibility of recovering lost coins. Satoshi answered: "Those coins can never be recovered, and the total circulation is less".[2]

Once these distinctions are taken into account, the Court of Appeal's analysis unravels:

FIGURE 1: A NON-EXHAUSTIVE SPECTRUM OF SITUATIONS WHERE DEVELOPERS MIGHT BE ASKED TO MAKE A SOFTWARE CHANGE



- First, the nature of the activity required to fulfil the duty alleged by TTL (ie change how the system is intended to work by transferring Bitcoin without a private key) is fundamentally different to fixing a software bug. Describing both as a mere "code update" (see [85]) is a gross oversimplification.
- Second, whilst it might be possible to infer informed consent of owners as a whole to a software change in an Obvious Bug Scenario and even an Unanticipated Consequences Scenario (since problems with the system might otherwise go unaddressed forever which would be to everyone's detriment), it is not clear at all that it is possible to infer informed consent to a change in an Intended Consequences Scenario. Nothing has gone wrong with the system. It is operating as intended. The inability to transfer Bitcoin without a private key is a fundamental security feature of the system. So, on what basis can consent to a change which undermines that security feature be inferred?
- Third, even if consent can be inferred (so the duty of single minded loyalty is not breached by implementing TTL's software patch), it does not follow that there is a *duty* to implement that patch. It is completely unrealistic to say that Bitcoin owners (let alone the person who created Bitcoin who Dr Wright ironically claims to be) have a legitimate expectation that developers will change how the system was intended to operate. This is a system which owners have voluntarily entered into and the consequences of losing a private key are well known.

So even if TTL's factual case is taken at face value, it does not provide a basis for the alleged fiduciary duty. TTL's case becomes even weaker when we take the red pill and investigate each of TTL's four factual allegations.

RED PILL: WHAT ABOUT TRIAL?

(1) The BTC developers are a sufficiently well-defined group

Bitcoin Core is the most popular software option in the Bitcoin system. It is open source, and anyone can contribute. Therefore, the group of Bitcoin Core developers is necessarily not well-defined. The group of developers of software used within the Bitcoin system generally (there are multiple options) is even less well-defined.

TTL targets its claim at certain Bitcoin Core developers. It says those developers hold the passwords and are therefore able to introduce changes to the source code repository on GitHub [29]. Developers with this access are referred to as repository maintainers.

But not all of those defendant developers are maintainers. Some of them have never been maintainers and others were no longer maintainers as at the date of the claim. So TTL's claim extends beyond maintainers but to whom? That is unclear. Perhaps as the High Court observed, it extends to developers who TTL says exert "significant influence" over the Bitcoin network.[3] What do "influence" and "significant" mean? When does influence cease to exist? What about other non-developer constituencies who might have significant influence?

Therefore, even on TTL's case, the class of developers is not well-defined. Some writers have argued that it is impossible for courts to provide a definition that clearly delineates which developers are influential enough to warrant the imposition of fiduciary duties.[4]

(2) The BTC developers control the software

The process of Bitcoin Core software development is as follows:[5]

- For ordinary changes: A proposal by a contributor is peer reviewed by the community of developers. Maintainers then determine, based upon comments from reviewers, whether the proposal is in line with the general principles of Bitcoin Core, meets the minimum standards, and has achieved consensus. Consensus is more accurately described as "rough consensus" (ie where all objections have been addressed but not necessarily accommodated).[6]
- For significant changes, the requirements are similar but stricter. For example, the proposal must be accompanied by a widely discussed Bitcoin Improvement Proposal (BIP) (ie a detailed technical design document).

TTL asserts that the maintainers have unbounded discretion in deciding whether a proposal should be merged into the repository. However, that ignores two things:

(1) the expectation of the wider development community is that maintainers should be mere facilitators or performing a "janitorial role";[7] and
(2) all GitHub proposals are publicly available and the peer review is public.

This transparency creates accountability.[8]

(3) The BTC developers control the networks

The Court of Appeal considered that because software is all there is (and the developers control that software), the developers control the networks [72]. There are a few problems with this. First, there are multiple software options within the Bitcoin system. Bitcoin Core is currently the most popular but that is only because most nodes choose to run it. Second, there are other components of the Bitcoin system including the network of participants. The participants are just one part of a wider set of constituencies which also includes developers, exchanges, merchants and end users.[9] These constituencies can and do exert influence on the system.

If maintainers introduced a controversial change into Bitcoin Core, participants are free to not upgrade to the new version (there is no automatic upgrade mechanism) or to run an alternative software option (Bitcoin Core is released under the open source MIT License, so the alternative software could even be a copied or modified version of Bitcoin Core). This might give rise to a chain-split. Which branch succeeds as the main chain will depend on various factors including: (i) whether the majority of mining power upgrades to the new version of Bitcoin Core; and (ii) which chain other constituencies (ie users, exchanges etc) choose for their economic activity. The latter may influence the former since the miners will want to avoid mining a worthless coin.[10]

There are numerous incidents which demonstrate that no constituency (including developers) can unilaterally impose its will on the others.

Example 1: Bitcoin's March 2013 Hard Fork

In March 2013, a hard fork occurred because nodes were running two different versions of the software. As Angela Walch has observed:

Feature

Biog box
Mohamed Sacranie is a litigation associate at Allen & Overy LLP specialising in crypto disputes. His interest in Bitcoin was sparked by his late father's contagious passion and vision for Bitcoin as a powerful tool with the potential to create profound change.
Email: mohamed.sacranie@allenovery.com

> "When the software developers realized that the fork was occurring, they quickly contacted miners on the network to persuade them to support one of the two disparate ledgers."[11]

Surprisingly, the Court of Appeal considered that the Walch article provided "independent support" for TTL's factual case [36]. But even Walch accepts that the developers cannot act unilaterally and need to work with miners.

Example 2: 2017 User Activated Soft Fork

In 2017, Bitcoin faced several technical issues. SegWit solved these issues but was opposed by many of the significant miners and some highly influential developers. There were suspicions that some miners opposed SegWit because it fixed a vulnerability that they were exploiting to increase their efficiency. Since, soft forks typically require a large miner majority to flag support in order to be activated, this is an example of a situation where a powerful constituency might be exerting its influence to further its own interests at the expense of others.

Shaolinfry (a pseudonymous developer who was not a maintainer) proposed a user activated soft fork (UASF) which, if implemented by nodes, would give miners an ultimatum: signal support for SegWit by 1 August 2017 or we will start rejecting your blocks. This was highly controversial and was openly criticised by some influential Bitcoin Core developers. It was therefore incorporated into an alternative software option.

The UASF presented a significant threat to miners. The miners therefore started signalling support for SegWit in advance of 1 August 2017 which made the UASF no longer necessary. Nodes were therefore able to exert significant influence through the mere threat of the UASF.[12]

(4) The BTC developers are able to implement TTL's software patch

If maintainers were to merge TTL's software patch into the Bitcoin Core repository, participants may refuse to upgrade to the new software or opt for another software option.

TTL argues that would not happen because it is not in the participants' commercial interests. However, this assumes (without providing any justification) that a majority of participants and wider constituencies would upgrade to the new software with the result that participants who do not upgrade are left on a minority chain. Given the controversial nature of TTL's software patch (including the potential for it to undermine security), it is very likely that the majority would not upgrade. All TTL's patch would achieve is the creation of a minority chain with a likely worthless coin.

THE IMPLICATIONS

There are therefore strong arguments that the BTC developers do not owe any fiduciary duties at all:

- The class of developers is not sufficiently well-defined even on TTL's case.
- Power in the Bitcoin system is diffused between multiple constituencies.[13] The system is designed (and contains sufficient safeguards) to protect these constituencies from one another since unilateral decisions cannot be imposed.
- More specifically, Bitcoin Core developers do not control the network. Their position as developers of the most popular software option in the Bitcoin system is conditional upon the consent of the other constituencies. In the event of a loss of faith in a development team or Bitcoin Core for any reason (eg failure to fix a bug), participants can choose another software option.

Fiduciary duties are therefore not required. Imposing them would have significant downsides including deterring developers from becoming involved at all. The duty alleged by TTL is particularly problematic since the English courts, by recognising it, would be dictating how the Bitcoin system should operate. That is a matter for the constituencies to resolve between themselves.

This also has significance beyond fiduciary duties. It has been argued elsewhere that the *lex situs* of a crypto-token should be where the majority of "core software developers" are based because the key connecting factor for jurisdiction is power over an asset and the core developers have that power.[14] However, that does not work for Bitcoin:

- "core software developers" is indefinable;
- potential candidates may be located all over the place; and
- power is actually diffused amongst multiple constituencies.

Finally, reasoning by analogy (eg the safe to which a key has been lost) is unhelpful because the Bitcoin system operates on unique principles. Bitcoin prioritises security and therefore preserves the sanctity of transactions as a system feature. Responsibility is placed on owners to safeguard their Bitcoin (or to go after the hackers) and not on developers to recover it for them. ■

1 Andreas Antonopoulos, *Mastering Bitcoin* (2nd ed 2018), p 2.
2 https://bitcointalk.org/index.php?topic=13.msg46#msg46
3 *Tulip Trading Ltd v Bitcoin Association for BSV & ors* [2022] EWHC 667 (Ch) at [33].
4 Haque et al 'Blockchain Development and Fiduciary Duty', Stanford Journal of Blockchain Law and Policy, 2019, Vol 2.2 at p 184.
5 Contributing to Bitcoin Core (available at https://github.com/bitcoin/bitcoin/blob/master/CONTRIBUTING.md) and BIP-0002 (available at https://github.com/bitcoin/bips/blob/master/bip-0002.mediawiki)
6 Alex B, 'The Tao of Bitcoin Development' (available at https://medium.com/@bergealex4/the-tao-of-bitcoin-development-ff093c6155cd)
7 https://bitcoincore.org/en/about/#:~:text=Maintainers,line%20with%20the%20project%20goals)
8 Haque et al (n 4), p 160.
9 Antonopoulos (n 1), p 283.
10 Haque et al (n 4), p 163.
11 Angela Walch, 'In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains' (19 July 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3203198
12 Suleiman Sacranie, 'Bitcoin Viewed From the Perspective of Marx's Vision of Communism', 2020; and Haque et al (n 4), p 164.
13 Antonopoulos (n 1), pp 283-284.
14 Amy Held, 'Cryptoassets as property under English law Pt II: ownership, situs and the circular question of jurisdiction', (2023) 4 JIBFL 236.