Bitcoin: trust the code, or trust the law?

Malcolm Dowden & Owen Afriye examine private keys, hacking & duties of care in *Tulip Trading v Bitcoin Association*

IN BRIEF

- In March, the High Court dismissed a claim brought against crypto software developers alleging that they owed a duty of care to assist the claimant in regaining access to a large amount of Bitcoin which was lost on the developers' networks.
- Although it has left open certain very limited potential routes to liability and remedy, the judgment reinforces concerns that tort and common law may be proving themselves incapable of adapting to new technologies.

A founding principle of Bitcoin was set out in *Bitcoin: A Peer-to-Peer Electronic Cash System* (the 'White Paper') published in October 2008 under the name of Satoshi Nakamoto. It led with the assertion: 'What is needed is 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'. That explicit commitment to 'cryptographic proof' instead of trust reflected the 'code is law' philosophy articulated by Lawrence Lessig in 2000. Logically pursued, 'code is law' amounts to a rejection of central governments, central banks or reliance on judicial systems. For purists, the person entitled to hold and transact from a particular wallet is the person able to apply the relevant private key. So what happens if a key is lost, whether through hacking or carelessness? Should the 'owner' of Bitcoin or any similar cryptoasset be able to look to the court system of a particular jurisdiction for a remedy that would replace or reinstate their means of access once a private key has been lost? That was the question put to the High Court by Dr Craig Wright, who has publicly claimed to be 'Satoshi Nakamoto', author of the White Paper.

In *Tulip Trading Ltd (a Seychelles company) v Van Der Laan and others* [2022] EWHC 667 (Ch), [2022] All ER (D) 106 (Mar), the court brushed aside claims brought against crypto software developers alleging that they owed a fiduciary and/or tortious duty of care to assist the claimant in regaining control and access to a large amount of Bitcoin which was lost (allegedly through a hack) on the developers' networks.

Although the court rejected the existence of a fiduciary duty or a common law duty of care on the facts, the judgment left the door open for such relationships to be found in certain, very limited circumstances. For example, a developer making software changes might be taken to have assumed more responsibility and duties to their software users—including, taking reasonable care to:

- not harm the interests of users, for example, by introducing malicious software bugs or other actions that may compromise the security of the relevant network/software; and
- address bugs or other defects that arise in the course of operation of the system and which threaten that operation.

Although it has left open that narrow potential route to liability and remedy, the judgment reinforces concerns that tort and common law may be proving themselves incapable of adapting to, and of accommodating, new technologies and inherently international/cross-border business and commercial structures. It potentially fuels the view that legislation and regulation are the only viable route, but that any such legislation and regulation must reflect international cooperation. Unless that cooperation is global and comprehensive, it has limited chance of being effective.

So, does that leave Bitcoin and other cryptocurrencies outside the reach of conventional law? The answer to that question is currently still being unravelled, so it will be interesting to see how the legal developments in this space (inside and outside the courtroom) will progress in the coming years, particularly in view of the extreme recent volatility of Bitcoin and other cryptocurrencies, which may well leave many investors holding a loss.

Background

The claimant, Tulip Trading Limited (TTL) (a holding company of Dr Craig Wright, incorporated in the Seychelles) claimed that a substantial amount of Bitcoin

(approximately worth £1.1m) which TTL purportedly owned, was subject to a computer hack at Dr Wright's home in February 2020. As a result, TTL claimed that the 'private keys' which were needed to gain access to the Bitcoin had been stolen and deleted from Dr Wright's computer, and thus TTL was no longer able to access or control the Bitcoin.

As the Bitcoin in question had not been taken or transferred from its original location (but merely TTL was locked out from accessing it due to the lost keys), TTL issued proceedings against the 16 core developers (the defendants) who controlled software in respect of the BSV, BTC, BCH and BCH ABC networks on which the Bitcoin was stored ('the networks'), rather than pursuing the alleged hackers.

TTL claimed that the defendants owe it fiduciary and/or tortious duties to assist it in regaining control and use of the Bitcoin, and that it would not be technically difficult for the defendants to write and implement a software 'patch' enabling TTL to regain control of it. TTL also sought equitable compensation or damages if the former was not successful.

None of the defendants were based in the jurisdiction of England and Wales. The judgment was an interim application rather than a full trial, and specifically related to a number of the defendants' (the second to 12th, 15th and 16th) challenge to the court's jurisdiction and ability to permit service outside England and Wales.

In order for the defendants to succeed with their jurisdictional application, the court expressed that the following requirements had to be satisfied:

(1) whether there was a serious issue to be tried;
(2) whether there was a good arguable case that the case fell within one or more of the jurisdictional gateways set out in CPR PD 6B, para 3.1; and
(3) whether, in all the circumstances:
    (i) England is clearly or distinctly the appropriate forum for the trial of the dispute; and
    (ii) the court ought to exercise its discretion to permit service of the proceedings out of the jurisdiction.

Judgment

The claim failed at the first limb—*whether there was a serious issue to be tried*—as the court could not establish that the claim had a real prospect of success.

The standard followed by the court was as follows:

> 'The claim must be more than merely arguable. Whilst the court must not conduct a mini-trial, it must take account of the available evidence and also evidence that can reasonably be expected to be available at trial. But there may be a point of law on which the court should "grasp the nettle". The court should not allow the case to proceed because something may turn up' (at [37]).

In particular, the court focused on whether TTL had a real prospect of proving the existence of fiduciary or tortious duties owed by the defendants.

Fiduciary duty

The court concluded that TTL did not have a realistic prospect of establishing that the defendants breached any fiduciary duties owed to TTL. Reasons for this included:

- Bitcoin owners could not realistically be described as having entrusted their property to a fluctuating, and unidentified, body of software developers;
- the distinguishing feature or defining characteristic of a fiduciary relationship is the obligation of 'undivided loyalty'. However, the steps that TTL required the defendants to take (such as bespoke amends to the networks so TTL could recover the Bitcoin) would only benefit TTL, rather than the other users of the networks (who would more likely benefit from a general systematic software change). The court even argued that the changes sought by TTL could even be disadvantageous to other uses of the networks, specifically any potential rival claimants to the Bitcoin; and
- TTL's demands could have exposed the defendants to risks: eg if the defendants went ahead and created the software patch for TTL, there would be a possibility that potential rival claimants to the Bitcoin would have a legitimate claim against the defendants.

Duty of care

Again, the court dismissed claims that the defendants were in breach of a duty of care owed to TTL. The court followed guidance by the Supreme Court which suggested that when identifying whether a duty of care exists, an incremental approach should be adopted, based on an analogy with established categories of liability. On that basis, the court particularly noted:

- the loss suffered by TTL was purely economic loss and there was no element of physical harm to person or property. As such, no common law duty of care could arise in the absence of a special relationship between the parties;
- the complaints made by TTL related to failures by the defendants to act. However, there is no general duty to protect other from harm. In addition, the law generally imposes no duty of care to prevent third parties causing loss or damage, or for injury or damage caused by a third party;
- the defendants' alleged duties of care would be owed to a potentially unknown and unlimited class of people, meaning that there would be no restriction in the number of claims that could be brought against the defendants by those alleging their private keys were lost or stolen;
- the defendants' scope of the duty of care would be open-ended, requiring them to investigate and address any and all such claims—and given the anonymity of the system, would have poised a challenging task in practice; and
- similarly as with the claim for fiduciary duty, the defendants are a fluctuating body of individuals. Therefore there was no basis for imposing obligations on them to continue to be involved and make changes to the network when they have given no previous commitment or assurances in this regards.

The real Satoshi Nakamoto?

An interesting strand to this case is Dr Wright's claim that he is Satoshi Nakamoto—the author of the White Paper.

If Dr Wright is (as he claims) Satoshi Nakamoto, then bringing a claim in the English court was a fundamental departure from the guiding principles of his own White Paper.

The essence of the White Paper (and the philosophy underpinning Bitcoin) is a peer-to-peer network in which trust is placed in the coding and its consequences rather than in any central government, bank or judicial system. However, Dr Wright was asking the court to order the defendants to write a patch that would either create a new wallet and private key, into which the 'lost' Bitcoin would be placed, or to create a replacement for the 'lost' private keys said to have been hacked. Essentially, Dr Wright was seeking a radical departure from the founding principles and assumptions of Bitcoin to resolve his own individual problem. From an individual perspective, the claim failed. For adherents to 'code is law', it looks more like a victory. NLJ

Malcolm Dowden, partner in data privacy, cybersecurity & digital assets, & **Owen Afriye**, trainee solicitor, Squire Patton Boggs (*www.squirepattonboggs.com*).