Client Alert

Akin Gump
STRAUSS HAUER & FELD LLP

Tulip Mania—Do Blockchain Developers Owe Duties to the Owners of Crypto Assets?

April 12, 2022

Dubai, and the Dubai International Financial Centre (DIFC) specifically, is positioning itself as the centre of the blockchain world. Developers, blockchain networks and major exchanges such as Binance are basing themselves in Dubai *en masse* and the DIFC Court has launched a specialised court for the digital economy which will hear disputes relating to blockchain technologies and smart contracts. As the size and complexity of the industry evolve, and the number of disputes increases, so too must DIFC law.

To that end, a recent case in the English High Court, *Tulip Trading Limited v Bitcoin Association for BSV & Ors* [2022] EWHC 667, addressed a fundamental, unsettled question in the blockchain space: whether the developers of a decentralised blockchain network such as Bitcoin owe legal duties to owners of the crypto assets in the network. The Judgment, although a summary determination only, followed a three-day hearing and the filing of extensive evidence and authority and was well reasoned and carefully considered. It will provide helpful guidance for DIFC Courts grappling with similar issues, particularly given that DIFC law regarding negligence and fiduciary duties closely mirrors the law of England and Wales.

The Facts

The claimant, Tulip Trading Limited ("TTL"), is a company incorporated in the Seychelles. Its ultimate owners are Dr. Craig Wright and his family. Dr. Wright famously (and controversially) claims he is Satoshi Nakamoto, the anonymous creator of Bitcoin. Dr. Wright is also the CEO of TTL and has resided in England since 2015.

The defendants were said to be the core developers and/or controllers of four digital asset networks related to Bitcoin (the "Networks"), including Bitcoin Core, the software which powers the Bitcoin network (the "Defendants"). None of the Defendants was based in England and Wales.

TTL maintained that it is the rightful owner of approximately USD 4 billion of Bitcoin. The private keys to the Bitcoin had been held securely by Dr. Wright in England, until Dr. Wright's computer system was hacked by an unknown third-party and all records of the private keys were deleted. This meant TTL could not access or use the Bitcoin.

Contact Information

If you have any queries or concerns about DIFC law in this area, the experienced team at Akin Gump is on hand to assist.

Graham Lovett
Partner
glovett@akingump.com
Dubai
+971 4.317.3040

Michael Stewart
Associate
stewartm@akingump.com
Dubai
+971 4.317.3044

TTL argued that the Defendants were in control of the Networks and in particular, had the power to return control of the hacked Bitcoin to TTL via a software patch. TTL claimed that the Defendants owed it fiduciary and/or tortious duties, pursuant to which they were required to take positive steps to assist TTL in regaining control and use of its Bitcoin.

The Defendants disputed this, claiming that control and operation of Bitcoin are decentralised. The Defendants were instead past or present members of a very large, shifting group of contributors without an organisation or structure. Further, any change they were able to propose to address TTL's complaint would be ineffective, as miners (i.e., the nodes which validate blocks for entry onto the blockchain) could refuse to adopt any change.

The Legal Context

In May 2021, the Court had granted TTL permission to serve out the claim form on the Defendants (the "Service Out Order"). The Defendants challenged the Service Out Order. The Court's role was therefore to reconsider, effectively by rehearing, whether permission to serve out should have been given. Three criteria must be satisfied to grant permission to serve out:

1. There is a serious issue to be tried.
2. There is a good, arguable case that the claim fell within one or more of the jurisdictional gateways.
3. In all the circumstances, the Courts of England and Wales are the appropriate forum.

The Court set aside the Service Out Order on the basis of the first criteria – i.e., there was no serious issue to be tried. The Court went on to find that criteria 2 and 3 would have been met in the circumstances.

The Decision

The crux of the case was whether software developers in a decentralised system owed fiduciary and/or tortious duties to owners to assist with recovery of lost or stolen digital assets. Ultimately, the Court found that TTL's argument that it was owed fiduciary and/or tortious duties by the Defendant developers was too weak for service out to be permitted.

Fiduciary Duties

At common law, a fiduciary is someone who acts on behalf of another in circumstances which give rise to an obligation of trust and confidence. The distinguishing feature of the relationship is the obligation of loyalty – the principal is entitled to the single-minded loyalty of their fiduciary, who must forgo their own interests. DIFC law essentially codifies this position in Part 8 of the DIFC Law of Obligations.

TTL accepted that the Defendants were not in a category previously recognised as owing fiduciary duties. However, the established categories of fiduciary relationships are not locked. Whether a fiduciary relationship arises will depend on the particular

circumstances. TTL argued that there was a fiduciary duty on the Defendants to assist TTL to recover its Bitcoin given the following:

1. The Defendants had complete control over the Networks, including the power to amend the protocol to allow owners to recover control of their assets or reverse a fraudulent transaction.
2. Owners had no control, save for the ability to use their private keys.
3. Owners of digital assets entrusted the care of their property to the Defendants and were vulnerable to abuse by them, including the destruction of the value of the assets.

The Defendants said none of these features met the loyalty requirement. They emphasised that TTL's case would involve the imposition of a broad duty to take action in respect of one owner, potentially at the expense of other owners. The fact that the duty was a positive one (i.e., to take actual steps rather than to refrain from doing something) also tended against the existence of a duty.

The Court agreed with the Defendants and made the following observations:

1. The foundation of TTL's case was the alleged imbalance of power, combined with an entrustment of property to the Defendants. While these are common features of a fiduciary relationship, they are not alone sufficient for the establishment of a duty. Further, Bitcoin owners cannot realistically be described as entrusting their property to a fluctuating, unidentified body of software developers.
2. This was not a case where, in making a software update, the Defendants acted in their own interests and contrary to the interests of owners, for example, by introducing a bug or feature that compromised owners' security but somehow benefited the Defendants. Critically, the Court said it was "conceivable" that there was an assumption of responsibility in such a case and some form of duty may exist. This observation is likely to be a hotly contested topic in the future. The blockchain and digital asset space is replete with scams and 'rug-pulls' perpetrated by protocol founders and developers at the expense of owners. The Court suggested that, in circumstances where there is deliberate conduct by developers at the expense of owners, a duty may exist.
3. Really, TTL was saying there was an assumption of responsibility merely because the developers had the **ability** to make changes, irrespective of whether they were actually engaged in making changes, and in the absence of a contractual or other obligation to do so. This was a difficult argument.
4. Bitcoin developers are a fluctuating body of individuals with no organisation or structure. They could not owe continuing obligations to remain as developers and make future updates when it may be in the interests of owners. This too will be a hotly contested area in future litigation in blockchain. Who is responsible for acts when a network is decentralised? How do you pin down an anonymous, multijurisdictional, amorphous group of individuals?
5. Owners themselves are an anonymous and fluctuating class with whom the Defendants have no direct communication and no contractual relationship. It was difficult for a fiduciary relationship to arise in those circumstances.

6. TTL was seeking to impose an expansive positive duty to alter software to allow TTL to regain control over assets. Fiduciary duties which require positive steps are generally limited in nature – e.g., an obligation to disclose wrongdoing.
7. The most fundamental difficulty of TTL's case, however, was that the steps TTL required the Defendants to take would be for its benefit alone and not for the benefit of any other users. This was in conflict with the principle of undivided loyalty where a fiduciary has multiple principals. The Court made two points here:
    A. A fundamental feature of the Networks is that digital assets are accessed and transferred through the use of private keys. This is the general expectation of users. TTL effectively sought to bypass this. Some users/owners may not agree that a system change that allowed digital assets to be accessed and controlled without private keys accorded with their interest.
    B. TTL's alleged duty would have the effect of putting the Defendant developers at significant risk – for instance, rival claimants to the assets could sue the Defendants outside of an English court, claiming a failure to act in their interest.

Overall, the Court found that there was not a serious issue to be tried regarding the existence of a fiduciary duty. In concluding, the Court did, however, note that a holder of digital assets on a network will have certain expectations, for example about security and private keys, the efficacy of 'proof of work' process and anonymity. A software change that compromised those might engender some ground for complaint by users, although it may not be fiduciary in character.

Again, this is an important observation – the Court is recognising that in certain circumstances there may well be obligations owed by developers to owners. Developers should therefore be cautious about altering the fundamental features of a protocol or upending the legitimate expectations of users.

Tortious Duties

TTL also claimed that the Defendants were in breach of a duty of care (i.e., were negligent) in failing to (i) code a mechanism for recovery of Bitcoin where a private key had been lost or stolen, (ii) include sufficient safeguards against wrongdoing by third parties and (iii) take steps to give TTL access to its Bitcoin or otherwise protect TTL against fraud.

Under English law, a defendant is liable in negligence if (i) it owes a duty of care to a claimant, (ii) it breaches that duty of care and (iii) the breach caused loss to the claimant. In identifying whether a duty of care exists, an incremental approach should be adopted, based on an analogy with established categories of liability. While not universally required criteria, the following three factors are important touchstones:

1. Foreseeability of harm.
2. Sufficient proximity between a claimant and a defendant.
3. Imposition of a duty is fair, just and reasonable in the circumstances.

For claims relating to pure economic loss (which is what TTL's claim was), no duty of care can arise unless there is a special relationship. That relationship is generally created where there has been an assumption of responsibility by a defendant.

The law generally imposes no duty of care to prevent harm from a third party (e.g., the hacker who took TTL's keys). The exception to this is where there has been an assumption of responsibility to prevent against such harm or where the risk of harm is created by the defendant.

As with fiduciary duties, the above common law principles are by and large codified into DIFC law – see Chapter 2 of the DIFC Law of Obligations.

TTL's argued that while novel, its claim was a permissible incremental extension of the law of negligence. The three criteria above were satisfied and a special relationship existed. Its case came down to three arguments:

1. There was a fiduciary relationship between TTL and the Defendants, which was sufficient to establish a duty of care in tort according to previous cases. There was the requisite special relationship because the Defendants had voluntarily assumed responsibility by their control of the Networks.
2. Previous case law suggested that a financial institution may have a duty to customers to prevent fraudulent transactions. The Networks were equivalent to financial institutions (e.g., banks), and the absence of a contractual relationship did not make any difference. Funds were being entrusted to controllers of the Networks, who profited from their activities.
3. There were strong public policy considerations in support of the existence of a duty, as otherwise owners would be illegitimately deprived of their digital assets without recourse.

The Defendants argued that TTL was overly relying on policy considerations and that the scope of the proposed duty was far too broad. TTL's case required a duty to take positive steps to protect TTL not only from harm by a third party (theft of private keys) but from harm to itself (loss of private keys).

The Court found that there was no real prospect of a duty of care existing in the circumstances. The following observations from the Court were of particular interest:

1. The Court had already found that the existence of a fiduciary duty was not realistically arguable, so the existence of a tortious duty on that basis was rejected.
2. There was no special relationship. It might have been arguable that when making software changes, developers assume a level of responsibility to ensure that they take reasonable care not to harm the interests of users, for example by introducing malicious software or a bug. It is conceivable that there may even be a positive duty on developers who exercise control over a network to address bugs or other defects that arise in the course of operation of the network. However, that was not the complaint in this case. Again, this is an important acknowledgement from the Court. If developed further in future cases, it would have significant implications in the blockchain space. In the decentralised finance sector in particular, exploits by third parties using bugs or other vulnerabilities in a protocol's code are common. Often these exploits result in a significant, sometimes permanent depreciation in the protocol's token. The Court is saying that there may be a duty on developers to (1) prevent bugs and malicious code when updating or changing code and (2) proactively seek out and address bugs/vulnerabilities in existing code. A failure to do either could sound in liability for developers.

3. The failures alleged by TTL were failures to change how the Networks worked, and are intended to work, rather than to address a known defect. There was no allegation that any of the Defendants had any involvement in the alleged hack or had done anything to create or increase a risk of harm. TTL was seeking a positive, ongoing duty to safeguard owners in circumstances where (i) no actual software development was necessarily occurring and (ii) there was no known bug or defect preventing the software from operating as anticipated.
4. The analogy between Network developers and digital asset owners on the one hand and a financial institution and its customers on the other was not a good one. In the latter, the existence of a contract was of critical importance, as was the fact that the bank was acting as a payment agent. Here, there was no contract and no such agency (although cf. *Hedley Byrne & Co Ltd v Heller & Partners Ltd* [1964] AC 465 regarding the existence of a duty of care despite there being no contract).
5. The potential class of persons to whom the duty would be owed was unknown and potentially unlimited. There was no real restriction on the number of claims that would be advanced against the Defendants by persons who had allegedly lost their private keys or had them stolen.
6. The open-ended scope of the duty was unduly burdensome for the Defendants. The Defendants would be obliged to investigate and address any claim that a person had lost their private keys or had them stolen. This was virtually impossible in an anonymised, decentralised system.
7. Owners of digital assets are capable of taking steps to protect themselves against the loss of private keys, for example by keeping copies in multiple locations or by insurance.
8. The Network developers are a fluctuating body of individuals. Even if the Defendants currently had control of the Networks, they may not in the future.
9. Policy considerations alone cannot provide a foundation for a duty of care.

Other Interesting Observations

Three additional points of interest were raised by the Judgment:

1. TTL maintained that Bitcoin constituted property. The Court endorsed the argument, referring to previous High Court decisions and the *Legal Statement on Cryptoassets and Smart Contracts* published by the UK Jurisdiction Taskforce in November 2019.
2. The Court said it was reasonably arguable that digital assets are 'located' in the place where the person or company who owns it resides. For a company, this will be where it conducts its business, rather than where it is incorporated. If this principle evolves, it will have significant implications on conflict of laws.
3. Express disclaimers of liability in a software license may prevent a duty from arising, depending on the circumstances.

Conclusion

Developers can breathe a sigh of relief – the Court did not think a legal duty to assist an owner to recover lost or stolen Bitcoin was realistically arguable. That said, there was a suggestion that developers may owe owners a duty of care in certain

circumstances, such as where they are taking positive steps to alter code or are engaged in acts in their interest but contrary to owners' interests. Developers may also have a duty to find bugs and vulnerabilities in existing code.

All of this is, for now, theoretical, particularly as the case (like many in the blockchain space) was a summary determination only. However, as the nascent blockchain and digital asset space expands, the law will have to address these and other difficult issues. Chief amongst those is the question of how liability for harm will be imposed, and on whom, in a network that relies on self-custody of assets, has no centralised authority and where many users, owners and developers are multijurisdictional and in large part anonymous. Further complexity arises when an owner's assets are, in fact, held by a third-party custodian – for example, an exchange such as Binance or Coinbase. To whom would a developer owe a duty in that circumstance?

The DIFC Court will be at the forefront of this evolution, given the dedicated digital economy court and the nexus to the DIFC that will be created by the influx into the DIFC of participants in the digital economy. For now, it is very much a case of 'watch this space'.

akingump.com