

Recent High Court Judgments Demonstrate Adaptability of English Law to Blockchain and Cryptocurrency Commercial Disputes

9 May 2022

Introduction

When businesses started to adopt the internet in the 1990s, there was much academic commentary at the time about how the law would cope with a system that “*cut across territorial borders, creating a new realm of human activity and undermining the feasibility—and legitimacy—of laws based on geographic boundaries*”¹. In fact, English law showed itself to be highly adaptable to disputes concerning the internet. A notable example of this was the landmark case of *Godfrey v Demon Internet Service QBD*, [1999] 4 All ER 342, in which the Court held that an internet service provider could be liable for a defamatory posting transmitted on its news-server.

In more recent years, blockchain and the associated virtual assets (e.g. cryptocurrencies and tokens) have crept into mainstream business use and consumer markets and, of course, have been the subject of wild speculation and price fluctuation. Renowned for its “decentralised” and “anonymous” characteristics, questions are once again being asked about how the law will approach disputes concerning this technology and asset class. The law is developing and remains unsettled in this area. However, some recent cases have indicated that the English courts have again been adept at applying traditional legal principles to these technologies and new asset classes. In this update, we take a look at those cases and discuss some important developments.

Key takeaways are:

- Blockchain developers do not owe fiduciary or tortious duties to those who use their networks to store or trade crypto assets.
- Bitcoin is not currently suitable for security for costs due to the high level of volatility in its value. However, the court has left the door open for less volatile

¹ *Law and Borders: The Rise of Law in Cyberspace*; Stanford Law Review, Vol. 48, No. 5 (May, 1996), pp. 1367–1402.

cryptocurrencies or central bank digital currencies to be used as permissible forms of security.

- The English Court is willing to grant a number of remedies in relation to cryptocurrencies, such as third-party debt orders and freezing orders.
- Contracts under which parties agree to a reciprocal cryptocurrency swapping structure do not give rise to a trust, though on different facts, a trust over cryptocurrency may arise.

Duties of Crypto Developers and Use of Bitcoin to Provide Security for Costs

Tulip Trading Limited v Bitcoin Association for BSV and others was the first case in which the English Court considered the duties owed by cryptocurrency software developers to crypto owners.

Background

The defendants (all of whom were based outside England & Wales) were the developers/controllers of the software of four blockchain networks (the "Networks"). Network users stored digital assets on the Networks and traded them using "private keys". The beneficial owner of the claimant was a Network user. He alleged that he was hacked, with the result that that he was no longer able to control, or use, a significant amount of bitcoin (the "Assets"), as the private keys (which would allow dealings in the Assets) had been removed. This resulted in economic loss to the claimant. There was no suggestion that the defendants were involved in the alleged hack. Rather, the claimant's case was that the defendants owed it fiduciary and/or tortious duties to re-write the Networks' software so as to regain control and use of the Assets. The defendants challenged this on the basis that the Networks were decentralised and therefore any rewrite would result in a "fork" in the network, as miners would refuse to run the update and instead continue to run earlier versions of the software.

At a preliminary hearing, the court ordered the provision of security as the claimant had failed to show that it could pay the defendants' costs.

Bitcoin Not Currently Suitable as Security for Costs Due to Its Volatility

In a [judgment](#) dealing with the consequential matters arising out of the security for costs application (*Tulip Trading Limited v Bitcoin Association for BSV and others* [2022] EWHC 2 (Ch)), the High Court did not allow the claimant to use bitcoin to provide security for costs due to its volatility; however, it did not conclusively rule out the use of

cryptocurrencies to provide security for costs. The claimant had proposed that it provide security by way of transferring bitcoin to its solicitors to the value of the security ordered plus a 10% "buffer" to address the volatility in the value of the bitcoin. The draft order also included a mechanism for topping up the value of the bitcoin. However, the Court found that bitcoin did not currently satisfy the test for using an alternative form of security on the basis that: (i) the defendants' security could become "*effectively valueless*" in the event of a fall in the value of bitcoin; and (ii) the buffer and top-up provisions did not adequately mitigate the volatility risk. However, the focus in this case was on "*the high level of volatility in the value of Bitcoin*". It remains an open question, therefore, whether less volatile cryptocurrencies or central bank digital currencies can be used to provide security for costs, or whether bitcoin will be a permissible form of security if its value stabilises in the future.

The court subsequently issued an additional [judgment](#) in the same matter dealing with a jurisdictional challenge made by some of the defendants (*Tulip Trading Limited v Bitcoin Association for BSV and others* [2022] EWHC 667 (Ch)). The court set aside an order granting permission to serve the claim form on the defendants out of the jurisdiction on the basis that the claimant had not established a serious issue to be tried on the merits.

Crypto Developers Do Not Owe Fiduciary Duties to Owners

The claimant advanced a case on the basis of: (i) an "*alleged significant imbalance of power*" between the defendants and the claimant, with the result that the defendants had "*complete power*" over the Networks, while the claimant had "*no control other than the ability to use their private keys*"; and (ii) the fact that the claimant had entrusted its property to the defendants. The Court disagreed that a fiduciary relationship existed on the facts of this case because:

- Imbalance of power not a condition for a fiduciary relationship. The Court held that "*whilst an imbalance of power, together with vulnerability to abuse of that power, is often a feature of fiduciary relationships and may in broad terms be a rationale for the concept, it is not a defining characteristic and is certainly not a sufficient condition for the existence of the duty*".
- Fluctuating body of individuals. The Court found that, given that crypto developers are a "*fluctuating, and unidentified*" body of individuals, it was unrealistic to:
 - (i) impose continuing obligations on them to, for example, remain as developers and make future updates whenever it might be in the interests of crypto owners to do so;
 - and (ii) describe crypto owners as entrusting their property to this body of individuals.

- Conflict between the defendants' alleged duties to the claimant and the other crypto owners. The claimant's case was that there was a fiduciary quality to the relationship between the crypto developers and all crypto owners/users of the Networks, including itself. However, the software change it was requesting was not one that could be regarded as being for the benefit of all crypto owners on the Networks. Instead, it was seeking to bypass the fundamental feature of the Networks that digital assets were transferred through the use of private keys. The Court therefore found that there was "a real risk [to the defendant] that acceding to [the claimant's] demands would not be consistent with a [fiduciary's] duty of single-minded loyalty owed to other users".
- Any declaration of ownership by the Court would operate in personam and not in rem. The Court therefore found that if the defendants rewrote the software as the claimant was requesting, a rival claimant to the Assets could have a legitimate complaint against the defendants, which would not necessarily be brought in the English Courts and against which they would not be protected.

Crypto Developers Do Not Owe Tortious Duties to Owners

As with fiduciary duties, the Court found that crypto developers do not owe a common law duty of care to those who use their networks to store or trade crypto assets. The Court found that the imposition of a duty of care in this case would not be an incremental extension of the law, and would not be fair, just and reasonable, for the following reasons:

- Lack of a special relationship between crypto developers and crypto owners. Given the absence of a fiduciary relationship between the crypto developers and crypto owners, there was similarly no special relationship to found a duty of care in respect of economic loss.
- Lack of a positive responsibility for crypto developers to safeguard crypto owners. Even if it could be argued that the defendants had assumed some level of responsibility as a result of a role they had taken on in relation to the relevant Network, this did not extend to a requirement to take positive action to make changes, particularly in circumstances where there was no known defect preventing the software from operating as anticipated.
- Harm inflicted by third parties. The defendants did not have control over the alleged hackers and because the loss caused was purely economic, there were even more limited grounds for the Court to find that an exception applied to the general rule that no liability will arise for damage caused by a third party.

- Any declaration of ownership by the Court would operate *in personam* and not *in rem*. The Court found, as with fiduciary duties, that there was a real risk that rival claimants to the Assets could make a claim against the defendants, against which they would not be protected.
- Duty owed to unknown and potentially unlimited class. The Court considered that if it found that a duty of care existed, this would be owed to an “*unknown and potentially unlimited*” class. Case law had shown that this would be a consideration mitigating against the existence of a duty of care.
- Steps to protect against loss. The Court found that it was “*far from obvious that the Defendants could take steps to protect themselves by insurance*”. By contrast, it found that the crypto owners could take steps to protect themselves against the loss of “private keys” “*by keeping copies in different locations, and possibly by insurance*”.
- Fluctuating body of individuals. The Court found, as with fiduciary duties, that it was unfair to impose a duty of care on a fluctuating body of individuals.
- Public policy. Although the claimant had rightly argued that the issues raised significant public policy concerns, this could not, by itself, provide a foundation for the existence of a duty for which there was no realistically arguable basis under existing law.
- Relationship between developers and crypto owners was not analogous to that between a bank and customer. The claimant had tried to rely, by analogy, on previous case law that financial institutions may have a duty of care to customers to prevent fraudulent transactions. The Court rejected this, finding that “[t]he starting point for that duty of care is the contractual relationship between the bank and its customer, and the fact that a banker acts as agent of the customer in executing payment instructions. The duty is owed only to the bank’s customer, and not to a wider class”.

Crypto Developers May Owe Some Duties to Owners

Despite these findings, the Court accepted that there may be some, limited circumstances where developers would owe “*some form of duty*” to owners, including:

- a responsibility that arises when “*making an update to the software ... in their own interests and contrary to the interests of owners, for example in introducing for their own advantage a bug or feature that compromised owners’ security but served their own purposes*”;

- a “responsibility to ensure that they take reasonable care not to harm the interests of users, for example by introducing a malicious software bug or doing something else that compromised the security of the [n]etwork”; and
- a duty, if they exercise control over a network, “to address bugs or other defects that arise in the course of operation of the system and which threaten that operation”.

The Court also flagged that crypto owners “have certain expectations, for example about the security of the Network and private keys, the efficacy of the ‘proof of work’ processes and indeed anonymity”. The Court held that “software change that compromised these might engender some cause for complaint by” crypto owners.

The Court then went on to address whether the claimant’s claim fell within one or more of the CPR jurisdictional gateways in the event of an appeal. It made some noteworthy *obiter* comments, including seemingly casting doubt on the finding in *Ion Science Ltd v Persons Unknown* (unreported, 21 December 2020) that, “[t]he *lex situs* of a crypto asset is determined by the place where the person who owns it is domiciled in the present case”. The Court instead appeared to suggest that residence was the correct test to be applied.

This case highlights the need for crypto owners to take every measure to protect against the theft or loss of their assets. However, while crypto developers can take comfort in the knowledge that they do not owe fiduciary or tortious duties to crypto owners, this does not mean they should not take action in the event a crypto owner loses control of its assets. Indeed, one defendant in *Tulip Trading, the BSV Bitcoin Association*, has released a [statement](#) that the “digital currency and blockchain industry should strive to develop technical mechanisms and industry best practices to provide remedies, upon valid proof of ownership and with judicial due process, to restore control of lost or stolen coins to their rightful owner ... to engender more confidence in ... and lead to wider adoption of Bitcoin’s innovative technology”. In addition, developers should note the, presently limited, circumstances in which they may be found to owe a duty to owners, including a responsibility to take reasonable care not to harm the interests of network users.

Equitable Remedies Available in Relation to Cryptocurrencies

Other recent case law has shown that the English Court is willing to impose a wide variety of remedies in relation to cryptocurrencies.

Interim Third-Party Debt Order

In [Ion Science Ltd v Persons Unknown](#) (unreported, 28 January 2022), the High Court for the first time granted an interim third-party debt order in relation to cryptocurrency.

This builds on previous case law treating cryptocurrencies as property under English law (as mentioned above), with the result that cryptocurrencies can be the subject of proprietary claims and can be traced.

Other Remedies

The claimant in [Sally Jayne Danisz v \(1\) Persons Unknown \(2\) Huobi Global Limited \(trading as Huobi\)](#) [2022] EWHC 280 (QB) alleged that her bitcoin had been misappropriated by the first defendant; an expert had traced the bitcoin to a cryptocurrency end-wallet at the exchange of the second defendant. Following the claimant's application, the court granted the following remedies:

- A prohibitory interim injunction. Preventing both defendants from dealing with the bitcoin.
- A worldwide freezing order ("WFO"). Prohibiting the first defendant from unjustifiably disposing of, or otherwise dealing with, the bitcoin in the cryptocurrency end-wallet.
- A bankers trust disclosure order. Compelling the second defendant to disclose certain payment-related information about account holders of the end-wallet.

These cases demonstrate the readiness of the English courts to grant an extensive range of remedies in relation to cryptocurrencies. Crypto owners should take note of the various protections available against fraud and other wrongdoing. In particular, victims of crypto-fraud will benefit from the fact that cryptocurrencies can be the subject of proprietary claims and can be traced.

Trusts

[Wang v Darby](#) [2021] EWHC 3054 (Comm) was the first contested hearing in the English jurisdiction dealing with the question of whether a trust existed over cryptocurrency. The Court held that contracts under which the parties had agreed a reciprocal cryptocurrency swapping structure did not give rise to the existence of any type of trust (express, Quistclose-resulting or constructive). This was for at least the following reasons:

- The "essential economic reciprocity of the transactions".
- Transactional element. The claimant could not identify a case in which a beneficiary under a trust was "*obliged to transfer ... economic value to the trustee in order to obtain*

the trust property”. Rather, a beneficiary “has an interest in and right to receive the trust property, not an option to (re-)acquire it for value”. This “transactional element” was “inimical to the concept of a trust”.

- Sale and re-purchase. The Court found that “the pleaded characterisation of [the claimant]’s restoration obligation as one of sale or purchase back [wa]s fatal to any trust analysis” because “a sale/purchase back of an asset (akin to the ‘off leg’ in a repo transaction) presupposes its original or prior sale/purchase in the other direction (akin to the ‘on leg’ in a repo transaction)”.
- Full transfer of ownership. The transfer of bitcoins to the claimant from the defendant “was a full transfer of ownership”. A trust over the cryptocurrency would therefore “impose asymmetry in this reciprocal capital-swapping arrangement”.
- Quistclose-resulting trust. The Court noted that no case was identified in which a Quistclose-resulting trust “arose over property transferred as part of reciprocal exchange of assets and on terms whereby its re-transfer was expressly conditional upon a reciprocal or equivalent re-transfer of value from beneficiary to trustee”. In other words, the Court found that economic reciprocity precluded the existence of a trust.
- Constructive trust. The Court noted it was “difficult to see how a constructive trust as pleaded could arise in respect of entirely fungible and non-identifiable digital assets. There is no obvious analogy to a specifically-enforceable contract for the sale of land or some unique or sufficiently rare piece or parcel of personal property”. It went on to state that it was “impossible to say that [the defendant’s] conditional obligation to return [the cryptocurrency] after the minimum contractual period would be enforceable by decree of specific performance given the entirely fungible and non-identifiable nature of such digital currency”.

Importantly, the Court did not, however, rule out the possibility that a trust over cryptocurrency could arise on different facts. The Court observed, obiter, that “the transfer of digital assets from one account-holder to another for the purpose of baking or stake bonding [akin to ‘mining’ and ‘farming’ in other crypto contexts] could involve or constitute a trust” but that this would “depend on all the circumstances”. In particular, its comments in relation to constructive trusts suggest that a trust over non-fungible and identifiable digital assets such as non-fungible tokens (or “NFTs”) may be possible.

The Court went on to find that a personal claim for breach of fiduciary duties arising from the “nature and terms of the contracts” could “have a real or reasonable prospect of success”. It also granted the claimant’s application to continue a WFO against the defendant. The Court has recently issued a further [judgment](#) in this matter removing the legal and living expenses exceptions to the WFO on the basis that the defendant had

access to cryptocurrency with a current value “*far in excess*” of the maximum sums the subject of the WFO, meaning he was able to meet both his living and legal expenses.

Commentary

The theme that emerges from these cases is the adaptability of English law to commercial cases concerning blockchain and cryptocurrencies and, indeed, more generally the versatility of the common law system. As the law continues to develop in this area (whether in tandem with regulatory developments or independently), this is likely to further legitimise the commercial and consumer uses of blockchain and investment in crypto technology.

Debevoise will continue to monitor further legal developments in this interesting area. If you would like to talk about any of the issues discussed in this bulletin, please do not hesitate to contact any of the authors.

* * *

Please do not hesitate to contact us with any questions.

LONDON



Christopher Boyne
cboyne@debevoise.com



Patrick Swain
pswain@debevoise.com



Ralph Sellar
rsellar@debevoise.com



Luke Duggan
lduggan@debevoise.com



Olivia Collin
(Trainee Associate)
ocollin@debevoise.com