KEY POINTS

- Although traditional methods of enforcement may be effective against cryptoassets, there remains the "hard question" of how that can be done without access to the private key.
- It may be possible to order software developers of cryptoasset networks to develop and implement software which would translate court orders into machine readable format and enable the network to transfer cryptoassets in accordance with the terms of such orders without the authorisation of the private key.
- However, even if such remedies could be obtained, their implementation may lead to a "fork" in the network, with one branch accepting the court orders and the other ignoring them. Ultimately market forces are likely to determine the relative success of one fork over the other.

Feature

Author John Lee

The endgame: issues in enforcement against cryptoassets

This article considers the possibility of recovering cryptoassets without the authorisation of the private key.

INTRODUCTION

The recovery of assets or monetary damages will be the ultimate goal of most commercial claimants who decide to embark upon (often costly) litigation. That is no different in the world of crypto disputes. However, particular difficulties may arise when seeking to enforce a judgment against cryptoassets, given their peculiar technological features. They range from ascertaining the identity of the defendant (particularly in cases of fraud), as well as that of any third-parties who have become mixed up in the dispute, to identification of cryptoassets against which a final judgment can be enforced. Perhaps the most challenging of all is enforcement against cryptoassets without access to the private key.

This article considers some conventional, as well as more novel, solutions to common problems which may arise when seeking to enforce a judgment specifically against cryptoassets.[1]

CONVENTIONAL ENFORCEMENT METHODS

In many circumstances, conventional methods of enforcement should be capable of delivering a claimant's ultimate goal of enforcement against cryptoassets, which are often the most easily identifiable of a defendant's assets, given the public nature of the distributed ledgers recording their transfers.[2] Whether it will be successful will be down partly to effective litigation strategy, but also to good fortune.

As for strategy, where there is a risk of dissipation of assets – as there often is in cases of fraud – time is of the essence. This means that obtaining *interim* proprietary and/or freezing injunctions against the defendant and/or any third-parties who hold the cryptoassets in question is likely to prove crucial when it comes to enforcement of any final judgment. In order to be in a position to make such applications, a claimant is likely to have to carry out thorough forensic investigations relating to the identity and whereabouts of the defendant, as well as any third-party holders of the assets. Whilst a claimant may not be able to identify a defendant at this stage – in which case, the English courts have been prepared to grant proprietary and freezing injunctions against "persons unknown"[3] – *Norwich Pharmacal*[4] and *Bankers Trust*[5] orders have also been sought and obtained against third-parties who have been identified as holding the relevant (in many cases, wrongfully appropriated) cryptoassets, with a view to obtaining further information about the defendant.[6] Whilst there currently exists some doubt as to whether such orders can be made against parties outside the jurisdiction, Gateway 23 in CPR Practice Direction 6B (which will come into effect on 1 October 2022) will permit the service out of the jurisdiction of a Pt 8 claim for disclosure of information regarding the true identity of a potential defendant or what has become of the property of a claimant in aid of proceedings which it is intended to commence, without the need to commence Pt 7 proceedings against persons unknown.[7]

There are further tools in the claimant's arsenal, including orders ancillary to a freezing order requiring the disclosure of details of the defendant's assets[8] and, post-substantive judgment, an oral examination in court of a judgment debtor in aid of enforcement under CPR Pt 71 (albeit this latter procedure cannot be used against persons outside the jurisdiction).

Now to good fortune. A claimant usually has the best chance of successfully enforcing a judgment where the cryptoassets to be enforced against are held by reputable third-parties as custodian[9] for the defendant, for example, centralised crypto exchanges, with a presence in the jurisdiction. To the extent that the claimant is able to establish a proprietary interest in the cryptoassets held by the third-party, it ought to be able to assert a proprietary claim over those assets. Alternatively, even if no proprietary interest can be established, the claimant might be able to obtain a charging order against the cryptoassets, to the extent that they are held on trust by the third-party on behalf of the defendant.[10] (For completeness, in *Ion Science Ltd v Persons Unknown and others* (2022) (unreported) a third-party debt order was obtained against a crypto exchange. However, third-party debt orders are available only in respect of "money"[11] and it is unlikely that cryptoassets currently function as or should legally be treated as money.[12])

If, however, the relevant cryptoassets are held directly by the defendant, enforcement against those assets may prove more difficult. Sufficient commercial and legal pressure (for example, through the instigation of committal proceedings) may result in the defendant satisfying a judgment by returning the assets to the claimant or the proceeds of the sale thereof, as the case may be. In the face of the most recalcitrant of defendants, however, options appear limited. The appointment of a receiver by way of equitable execution[13] will prove futile without access to the relevant private key. As a last-ditch effort, a claimant may seek a search order of the defendant's premises.[14] However, in addition to the very high bar that needs to be met in order to obtain such a draconian, without-notice order, there is no guarantee that the defendant will have kept a copy the relevant private key[15] in either hard-copy or electronic form.

So is there anything more a claimant can do in such a situation, or where the defendant is yet to be found?

A NOVEL SOLUTION?

The orthodox view appears to be that, both as a matter of *fact* and *law*, there is no way of enforcing a judgment against a cryptoasset without access to the relevant private key. In order to challenge this view, one needs to look under the bonnet of cryptoassets and how they function.

The nature of distributed consensus

There are certainly no *physical* constraints on a transaction being recorded on a distributed ledger system without authentication using the relevant private key. At one level, cryptoasset transactions are merely data entries on electronic ledgers, which could be so recorded if all participants agreed to do so. Therefore, what is essential for the integrity of distributed ledger systems – that is, ensuring that they follow the "rules" or "protocols" they purport to adhere to – is their *consensus mechanism*.

Taking the Bitcoin network as the simplest and paradigm example, it achieves distributed consensus through a so-called "proof-of-work" consensus mechanism. This protocol, through "mining rewards", incentivises validators ("miners") of the ledger records to build consensus around and to propagate those records which *do* conform to the "rules of the game" – for example, that aside from mining rewards, new bitcoins cannot be created, that one can only transfer the bitcoin(s) that one holds and no more, and that they may only be transferred from one address to another if the transfer instruction is authenticated by the private key – and to reject and discard those (purported) instructions or records which, whether through malicious intent or simple error, do not.

One may then pose the following question: is there a world in which the validators and the wider community of users,[16] will accept the transfer instruction of a cryptoasset, which falls short of having been authenticated with the private key? There is no conceptual incoherence in this idea; after all, any protocol governing the functioning of a distributed ledger system is not an immutable monolith, but an organic thing whose existence depends (only) on consensus. New rules can always be proposed and it is merely a *question of fact* whether or not they attract sufficient support such that they are adopted by a sufficiently large number of participants. The outcome will no doubt depend on a host of factors, including technical, commercial, economic and political (in both the narrow and wider senses) considerations. Furthermore, a proposed rule change may not necessarily result in a binary outcome of either no adoption, in which case the old rules continue to prevail, or universal adoption, in which case the old rules are supplanted by the new rules.

Rather, there may – at least initially – be a "fork", whereby one contingent of participants continue with the old rules, whilst the other adopts the new ones.

The DAO hack

Furthermore, there is an infamous and perhaps easily forgotten precedent for the transfer of cryptoassets without authorisation with the private key in relation to Ethereum, currently the second largest and well-known cryptoasset network. In 2016, "The DAO", a so-called "decentralised autonomous organisation" operating as a smart contract[17] on the Ethereum network, was hacked,[18] leading to the transfer of 3.6 million ether[19] to the hackers' addresses. The orthodox view was that, without the hackers' private keys, the appropriated cryptoassets could not be transferred back to The DAO. However, given the vast negative publicity and public pressure from a large number of original investors in The DAO, certain founders and/or lead developers of Ethereum – including Vitalik Buterin – proposed a "rewinding of the clock", essentially manually "erasing" the hack and returning the appropriated cryptoassets back to The DAO. This proposal was not universally adopted, and it led to a forking of the Ethereum network into two branches, one being the "purist" ETC (Ethereum Classic) (in which the hackers kept the assets), and the new one being ETH (retaining the original name, Ethereum). It is noteworthy that, despite ETH being the fork which "violated" the rule regarding the requirement for authorisation with a private key, it has since become the more widely adopted and valuable network.

Tulip Trading Ltd v Bitcoin Association for BSV

The case of *Tulip Trading Ltd v Bitcoin Association for BSV and others* [2022] EWHC 667 (Ch) in essence concerned this very issue, albeit the claim was not formally couched in terms of *enforcement* of a judgment against a wrongdoer whose private key could not be obtained. This was because no proceedings had been commenced against the wrongdoer, who had allegedly stolen the claimant's private key to its own cryptoassets, their identity and whereabouts having yet to be identified (para [30]). Instead, a claim was brought *directly* against core software developers of four cryptoasset networks, all forks of bitcoin, namely the:

- Bitcoin Satoshi Vision network (BSV);
- Bitcoin Core network (BTC);
- Bitcoin Cash network (BCH); and
- Bitcoin Cash ABC network (BCH ABC),

based on a duty of care and fiduciary duties "to the effect that they should assist it in regaining control and use of its [crypto-] assets" (para [6]).

The claims against all but the first defendant (who submitted to the jurisdiction of the English courts) were dismissed at first instance at the jurisdictional challenge stage for revealing no real issue to be tried. In summarily rejecting this attempt to impose novel duties on software developers of blockchain networks, the judge noted that: "[i]t is uncontroversial that a fundamental feature of the Networks, at least in their existing form, is that digital assets are transferred through the use of private keys" and that the claimant's claim "effectively seeks to bypass that" (para [78]).

This decision is certainly consistent with the "orthodox" view outlined above. However, the claimant has obtained permission to appeal the decision, given the novel nature of the claims advanced. Furthermore, it may be that a claimant's position would be strengthened if a similar claim were put as one of *enforcement* of an extant final substantive judgment establishing a claimant's proprietary right to the cryptoassets in question. A judgment *in rem*, in contrast to a judgment *in personam*, ought to be capable of being binding on and enforceable against the whole world, and not just the defendant in the initial substantive proceedings.[20]

Recognition of and giving effect to proprietary rights in cryptoassets

There is a wide consensus that under English law, there is a bifurcation of: (i) *factual* control of cryptoassets on a distributed ledger, on one hand; and (ii) the *legal* title to such assets, on the other, and that the former is not necessarily to be regarded as a definitive record of the latter.[21] This means that the question of who has the legal title to any given cryptoasset is essentially justiciable and all the participants within the relevant distributed ledger ecosystem are, in principle, within the reaches of and bound by the law, in this instance, of personal property. Once this threshold has been crossed, it seems that the law should do what it can to give practical effect to the recognition of a claimant's proprietary interest in cryptoassets.

As such, where a judgment *in rem* in respect of certain cryptoassets has been awarded in a claimant's favour, it seems that the law ought to consider the following potential claims, in addition to a breach of duty of care and/or fiduciary duties put forward in *Tulip Trading*, against software developers of the relevant networks who, unlike miners, are usually identifiable, and are in the special position of generally taking the lead on the maintenance of the software on which such networks are run, and proposing any necessary or desirable changes to such software:

- **Dishonest assistance**: In the case of theft of cryptoassets, it is likely that the thief holds the assets (or traceable proceeds thereof) on constructive trust for the victim.[22] Once software developers are on notice of a final judgment of a court of competent jurisdiction to that effect, it may be argued that they are dishonestly assisting the thief's (continued) wrongful appropriation of the cryptoassets by assisting the thief in maintaining control of the assets, instead of doing what they (reasonably) can to facilitate the return of control of those assets to the victim (as to which see below).
- **Conversion:** It may also be argued that the same conduct amounts to wrongful interference with the claimant's property. The defendants to an action for conversion need not have been in direct possession or control of the cryptoassets, if they have in some way acted so as to deny the claimant's legal right to them.[23]

The extension of these causes of action to software developers of permissionless distributed ledger systems would certainly be a novel step in the law. Indeed, as English law currently stands, it is highly unlikely that cryptoassets will be capable of being the subject of a claim in conversion given the ruling in *OBG Ltd v Allan* [2007] UKHL 21 that intangible property is incapable of being possessed. However, it has been argued that the tangibility of a property should not be determinative of whether it can be converted, but rather whether its *functional characteristics* are sufficiently analogous to tangible objects such that it should be capable of being the subject matter of conversion.[24] It is widely recognised that certain cryptoassets *do* exhibit such characteristics and therefore the Law Commission currently considers that "there are good policy arguments for the extension of the tort of conversion to [cryptoassets]",[25] albeit given *OBG*, this is likely to require legislative intervention.

But what would the *remedy* be, and would it be capable of being enforced in practice? In this regard, the terms of a Consent Order entered into between the claimant and the first defendant (the Bitcoin Association for BSV, being the software developer for BSV) in *Tulip Trading* are of interest.[26] In essence, the Bitcoin Association for BSV agreed:

- to develop and make available on its website software for the BSV network which, when implemented by miners on their nodes, will broadcast court orders affecting BSVs (the native cryptoassets on the BSV network) translated into machine readable format (Digitalized Orders) to the miners for freezing or unfreezing of BSVs and for the miners' nodes to implement a Digitalized Order; and
- to use its reasonable endeavours to continue developing and make available on its website software which, when implemented by miners, will enable an entity in whose favour a court order is made to request control of the relevant BSVs.

It seems at least possible that a similar remedy could be sought and obtained from the court against software developers of cryptoasset networks.

However, even if a claimant were to obtain such a remedy, its *practical* efficacy would not be guaranteed. It is considered by many to be a unique design feature and value proposition of certain cryptoassets that they are the "safest" assets, in the sense that they are least vulnerable to corruption and wrongful confiscation, *because* there can be no transfer without the private key. Therefore, even if an order such as the one outlined above were to be obtained, there may be little or no acceptance by the miners and the wider community of the proposal that the relevant cryptoassets should be capable of being transferred in accordance with court orders without authentication by a private key. In that case, a claimant will be left with a pyrrhic victory. Alternatively, it is possible that market forces will regard this kind of "integration" of the rule of law into the base-layer operation of the cryptoasset network as an improvement. In announcing

Biog box
John Lee is a partner in the dispute resolution department at Travers Smith LLP, based in London. Email: john.lee@traverssmith.com

its settlement with Tulip Trading, the Bitcoin Association for BSV stated:

> "We believe that the introduction of such solutions would help to engender more confidence in Bitcoin among everyday users, businesses and government agencies, and lead to wider adoption of Bitcoin's innovative technology. This aligns with our … goal to build a lawful digital currency ecosystem that leverages the capabilities of the Bitcoin public ledger to advance more honesty, transparency and accountability in the world."[27]

As noted above, only time will tell which of the two scenarios will prevail, or if forked networks along these lines will co-exist alongside each other.

CONCLUSION

Claimants are advised to use all conventional interim and other measures available to them in order to have the best chance of enforcing any judgment against identified cryptoassets. In many circumstances, they will lead to success. However, the "hard problem" of enforcement against cryptoassets without access to the private key remains. There is a case for the extension of existing legal principles to participants in distributed ledger networks in order to give full effect, in particular, to proprietary rights in cryptoassets. However, as such networks are at their core creatures of distributed consensus, there may be a limit to the ability of the law to protect and to give effect to such rights. ■

[1] This article is not primarily concerned with enforcement of *personal* remedies against any non-cryptoassets which may be available to satisfy the judgment.

[2] Save for so-called "privacy coins" (such as Zcash), which restrict the public's access to certain information on their blockchain ledgers, despite participation being "permissionless" and consensus remaining distributed through the use of advanced cryptographic techniques such as zero-knowledge proofs.

[3] See, for example: *AA v Persons Unknown* [2019] EWHC 3556 (Comm); *Ion Science Ltd vs Persons Unknown* (2020) (unreported); and *Fetchai Ltd v Persons Unknown* [2021] EWHC 2254 (Comm).

[4] A disclosure order against a third-party who has become "involved" in a wrongdoing where the claimant does not know the identity of the primary wrongdoer: *Norwich Pharmacal v Commissioners of Customs & Excise* [1974] UKHL 6.

[5] An order for the disclosure of confidential documents from (usually) the defendant's bank to support a proprietary claim in cases of fraud: *Bankers Trust Company v Shapira* [1980] 1 WLR 1274.

[6] See, for example: *Mr Dollar Bill Limited v Persons Unknown and Others* [2021] EWHC 2718 (Ch); and *Fetchai Ltd v Persons Unknown* [2021] EWHC 2254 (Comm).

[7] Speech by Judge Mark Pelling QC on *"Issues in crypto currency fraud claims"* delivered on 20 July 2022: https://www.judiciary.uk/announcements/speech-by-judge-mark-pelling-qc-issues-in-crypto-currency-fraud-claims/

[8] *AJ Bekhor & Company Ltd v Bilton* [1981] EWCA Civ 8.

[9] The legal characterisation of any crypto-custody arrangement will depend on its terms and can range from a trust arrangement to a mere contractual obligation on the part of the custodian to return the cryptoassets (or their equivalents) initially deposited by the customer, without the customer retaining any proprietary interest in the original assets deposited.
See: *Ruscoe v Cryptopia* [2020] NZHC 728; and the Law Commission's Consultation Paper (256) on Digital Assets published on 28 July 2022 (the Law Commission Consultation Paper), Chapters 16 and 17.

[10] Charging Orders Act 1979, s 2(1)(a)(ii).

[11] Civil Procedure Rules, r 72.1(1).

[12] For example, as legal tender.

[13] Senior Courts Act 198, s 37(1) and CPR Pt 69.

[14] Formerly called *Anton Piller* orders following *Anton Piller KG v Manufacturing Processes Ltd* [1976] Ch 55. See *Distributori Automatici v Holford Trading Co* [1985] 1 WLR 1066.

[15] Or, alternatively, the "recovery seed phrase" giving access to a wallet containing such a private key.

[16] The vast majority of holders and users of major cryptoassets do not (or no longer) actively participate in the process of validating the ledger records. This is because the rise in the popularity and adoption of certain cryptoassets, and the corresponding rise in their (monetary) value have led to a vastly increased competition in and "professionalisation" of mining activities, making it practically futile for individuals to take part in.

[17] For present purposes, the fact that The DAO operated as a smart contract, as opposed to a simple address (account), is not relevant.

[18] Or more accurately, certain vulnerabilities in the smart contract code were exploited but again this detail does not matter for present purposes.

[19] Ethereum's native cryptoasset.

[20] Bridge et al, *The Law of Personal Property*, (3rd Ed 2022), para 1-056.

[21] See: UK Jurisdiction Taskforce, *Legal Statement on cryptoassets and smart contracts* (November 2019), paras 46 and 131-134; and the Law Commission Consultation Paper, paras 13.7 to 13.9.

[22] See *Armstrong DLW GmbH v Winnington Networks Ltd* [2012] EWHC 10 (Ch) in the context of carbon emissions allowances.

[23] *Clerk & Lindsell on Torts* (23rd ed 2021), para 16-32.

[24] S Green and J Randall, *The Tort of Conversion* (2009), p 107.

[25] The Law Commission Consultation Paper, para 19.103.

[26] Sealed on 6 June 2022.

[27] https://bitcoinassociation.net/bitcoin-association-for-bsv-tulip-trading-ltd-settlement-statement-and-faq/

Further reading:

- Identifying and tracing the origins and flows of cryptocurrency (2019) 3 JIBFL 173.
- Intermediated cryptos: what your exchange-hosted wallet really holds (2020) 8 JIBFL 540.
- LexisPSL: Banking & Finance: Practice Note: The risks of cryptoassets from a financial crime, money laundering and terrorist financing perspective.