LITTLETON

CRYPTOASSETS - OBTAINING ENGLISH FREEZING AND PROPRIETARY INJUNCTIONS IN RELATION TO CYBERFRAUD

by Andrew Maguire

Summary

- The English High Court has ruled that cryptoassets are property under English law. Cryptoassets are not things in possession nor things in action, but a third category of property which English law recognises.
- Worldwide injunctive relief may be granted by the English High Court in relation to Cryptoassets – either proprietary or freezing injunctions.
- The English courts' objective is to provide much needed market confidence and a degree of legal certainty as regards English common law in an area that is critical to the successful development and use of cryptoassets and smart contracts in the global financial services industry and beyond.

Introduction

The theft and misappropriation of cryptoassets, typically Bitcoin, Ethereum and other virtual cryptocurrencies, by fraudsters is becoming increasingly common, and thus the subject-matter of civil fraud litigation. This article considers how parties can obtain the "nuclear weapon" of the worldwide proprietary or freezing order against cryptoassets.

English law does not provide a statutory definition of a cryptoasset or cryptocurrency but

essentially considers it to be a form of decentralised digital currency, providing through cryptography a secure means of transacting, with a verification of asset transfer, and creation of new units of currency. Cryptocurrencies have a unique identity and cannot therefore be directly compared to any other form of investment activity or payment mechanism.

Legal status of cryptoassets in English law –

In obtaining injunctive or other relief in respect of cryptoassets, the first hurdle is to prove that they are "property" in English law.

In *Vorotyntseva v Money-4 Ltd* [2018] EWHC 2596 (Ch), Mr Justice Birss granted a freezing injunction against Nebus, a cryptocurrency trading company, and its directors. Ms Vorotyntseva, who wished to test Nebus's trading platform, had deposited significant quantities of Bitcoin and Ethereum cryptocurrency, worth about £1.5 million with the company. When Ms Vorotyntseva became concerned with the company's operations and, having voiced her concerns, received no credible response from the management, she promptly applied for a worldwide freezing injunction. On the evidence adduced, the court concluded that there was a real risk of assets being dissipated and granted a freezing order against the company and its directors. In the case, it was not argued that cryptocurrency did not constitute, in law, "property".

In *Robertson v Persons unknown* CL-2019-000444, Mrs Justice Moulder granted an asset preservation order (but not the requested freezing order) in respect of cryptocurrency, worth about £1 million at the time, on the coin exchange, Coinbase UK Ltd, holding that there was a serious issue to be tried concerning a proprietary claim. Mr Robertson had responded to a phishing email and transferred 100 Bitcoin to a hacker's wallet. The hacker then transferred 80 of the coins to a third party. The latter transfer was eventually traced to a digital wallet held by Coinbase, a well-known custodian and digital currency exchange. In *AA v Persons Unknown* [2019] EWHC 3556 (Comm), on 19 January 2020 Mr Justice Bryan specifically held, on a without notice application, that cryptoassets were "property" for the purposes of granting proprietary or freezing injunctive relief.

The facts in that case were as follows. In October 2019, hackers, the First and Second Defendants**,** infiltrated the IT system of a Canadian insurance company, which was itself insured against cyber-crime attacks by the Applicant, the Insured**,** and installed malware called BitPaymer, which caused all of the Insured's data and IT systems to become encrypted. The First and Second Defendants subsequently demanded the equivalent of US$950,000 in Bitcoin in return for the decryption software that would allow the Insured to decrypt and regain access to their IT systems.

There was a period of negotiation, conducted on behalf of the Applicant by a specialist intermediary known as an Incident Response Company. Then, in light of the importance of the Insured being able to gain access to its systems, the Applicant arranged for the Bitcoin ransom to be paid, to an electronic address (also known as a "wallet") provided by the First and Second Defendants. Shortly after the payment was made, the Insured received the necessary decryption tools and over a period of several days, was able to regain access to its IT systems.

The Applicant subsequently engaged a third-party company, Chainalysis, Inc., a blockchain investigations company specialising in cryptoasset investigations, to trace the Bitcoin that had been paid to the First and Second Defendants. The investigation revealed that, of the

109.25 Bitcoins that had been transferred as the ransom payment, 13.25 Bitcoins (worth approximately US$120,000 at the time) had been converted into an untraceable paper currency, while the remaining 96 Bitcoins had been transferred to a specific, traceable, wallet, which was found to be linked to an exchange known as Bitfinex, operated by the Third and Fourth Defendants (both registered in the British Virgin Islands).

The Applicant sought a proprietary injunction against the First to Fourth Defendants, as well as ancillary disclosure orders against the Third and Fourth defendants, to require them to verify the identities of the customers who held the Bitcoin wallets in question (i.e. the First and Second Defendants). For the purpose of the application, which Mr Justice Bryan agreed should be heard in private and on a without notice basis (insofar as the First and Second Defendants were concerned), an anonymity order was sought and granted to protect the identities of both the Insured and the Applicant. The Judge granted the Orders as sought, and permitted alternative service of the order, by email, on the Third and Fourth Defendants in the British Virgin Islands.

Shortly before the decision in *AA v Persons Unknown* (above), in November 2019 the UK Jurisdiction Taskforce ("**UKJT**") had produced a Legal Statement on Cryptoassets and Smart Contracts. The UKJT is chaired by Sir Geoffrey Vos, Chancellor. The Legal Statement provides an authoritative, albeit not binding, analysis.

Nonetheless, Mr Justice Bryan referred to the Legal Statement as being an accurate exposition of English law in *AA v Persons Unknown* (above) and said that he considered that crypto assets such as Bitcoin are "property". They meet the four criteria set out in Lord Wilberforce's classic definition of "property" in *National Provincial Bank v Ainsworth* [1965] AC 1175 as being: (i) definable, (ii) identifiable by third parties, (iii) capable in their nature of assumption by third parties, and (iv) having some degree of permanence.

That too, was the conclusion of the Singapore International Commercial Court in *B2C2 Ltd v Quoine PTC Ltd* [2019] SGHC (I) 03, and which was followed on appeal [2020] SGCA(I) 02 at [144], in which it was held that that cryptocurrencies fulfilled Lord Wilberforce's classic definition, so as to amount to "property" in a generic sense.

More recently still, in *Ruscoe v Cryptopia Ltd* (in liq) [2020] NZHC 728, the High Court of New Zealand held, after full argument, that digital assets of a cryptocurrency exchange constituted "property" and (in that case) were held on trusts for accountholders on that exchange.

More recently, on 29 July 2020, in the case of *Toma & True v Murray* [2020] EWHC 2295 (Ch), Mr Robin Vos, sitting as a deputy High Court Judge, followed the *AA v Persons Unknown* test at [62] as to cryptoassets constituting property; as had Mr Justice Zacaroli, at the hearing of the 'without notice' application, on 5 June 2020:

"First, there must be a serious issue to be tried, secondly, if there is a serious issue to be tried, the court must consider whether the balance of convenience lies in granting the relief sought. The balance of convenience involves consideration of the efficacy of damages as an adequate remedy, the adequacy of the cross-undertakings to damages, and the overall balance of convenience including the merits of the proposed claim."

In *Toma & True v Murray*, a Bitcoin sale transaction went badly askew, leaving the claimant sellers without their Bitcoin or the money they were supposed to receive for it. The Sellers issued proceedings for a proprietary injunction in England against the defendant individual who controlled the coin depot account used for the failed transaction. In the proceedings, the Claimants sought to recover their losses via other assets in the defendant's Bitcoin account. However, the claimants, who were unable to provide a sufficient undertaking in damages, sought to freeze all of the assets within the Bitcoin account. The Court refused an application to continue interim injunctions restraining the identified defendant from dealing with bitcoin held in a coin deposit account. Although there was a serious issue to be tried, damages were, in principle, an adequate remedy (the defendant owning an unencumbered property in Dublin worth £4.8m as against the claimants' monetary claim for £120,000), despite the fact that this would convert the claim into a claim for a personal remedy, rather than a proprietary remedy, if the bitcoin was sold. The key reasons being that Bitcoin's value is particularly volatile so that, if the defendant was prevented, by the injunction, from selling further Bitcoin when he chose, he could suffer very significant losses.

For present purposes, it seems that in relation to cryptoassets, the first hurdle can readily be vaulted, in proving that cryptoassets are "property" for the purposes of seeking worldwide freezing or proprietary injunctions.

Seeking an injunction respect of a cryptoasset

As cryptocurrency accounts are wholly different from ordinary bank accounts, because they are decentralised; i.e. not located in one place, but held across a distributive ledger, there is no obvious party on whom to serve proceedings. The question therefore arises as to who should be served? The thief or wrongdoer is the obvious first choice; however, what of other enablers or associates? In *Robertson v Persons Unknown* (above), Mrs Justice Moulder relied upon an analysis provided by a specialist company which is a provider of software to track payment of crypto currency. That analysis tracked 80 Bitcoin to a wallet/account/address held by a crypto currency or coin exchange called "Coinbase".
Practical questions also arise as to the form of disclosure that should be sought from a wrongdoing respondent. The standard form worldwide freezing injunction order requires a respondent to give the "value, location and details of all such assets", but the question arises as to how this applies to cryptocurrencies. As stated above, the defining nature

of a distributive ledger is that cryptocurrencies are not located in one place. Issues will therefore arise as to ascertaining which parties have a private key to the coins and as to whether the coins are held in an exchange or through a third party. It will be necessary to discover the transaction code or hash by which the coins were wrongfully acquired.

How to locate cryptocurrencies

In theory, the tracing of cryptoassets ought to be possible, given that the apparently transparent nature of the blockchain system means that anyone can obtain a copy of every transaction of that particular cryptocurrency by downloading the blockchain. To assist the application for injunctive relief in court, there are "block explorers" by which an applicant can obtain information about cryptocurrency addresses and transactions. This means that an applicant should be able to trace cryptocurrencies from one address to another in permissionless systems, although the position will of course be different in permissioned ones[1].

Governing law

The traditional property rules of private international law, which focus on tangible goods, prescribe that a question as to rights or entitlement should be governed by the law of the place in which the property or claim to property is situated; the *lex situs*.

The very concept of a single *situs* for the asset becomes difficult to apply in the case, firstly, of intangibles, secondly, of digitised assets and, thirdly, of assets constituted on a distributed network or platform. Therefore, the question arises as to which law governs the exercise of seeking to trace and recover the cryptoasset? It may be problematic to use the *lex situs*, because cryptocurrencies are maintained on the decentralised ledger. Feasibly, it could be the *lex fori*, on the basis that the remedy of tracing or restitution is being utilised. Alternatively, it could be the law of the underlying transaction.

It may be that the elective *situs* should be the starting point for any analysis of a conflicts of law approach to virtual tokens. The elective *situs* is the system of law chosen by network participants of the distributed ledger technology ("DLT") or "blockchain" system[2]; provision for which may be included in the terms and conditions of joining the system.

The *lex situs* does not, however, comfortably locate when applied to a DLT system. The *situs* of an asset constituted on a DLT ledger which is, by its very definition, "distributed", is not immediately discernible. A network can span several jurisdictions and, in the case of a ledger which is fully decentralised, there is no central authority or validation point.

1 Permissionless systems are open to the public, and members of the public may affect and verify changes to the ledger. By contrast, in permissioned systems only authorised participants are able to create records and verify changes to the ledger (and different participants may have different authorisations).

2 The European Securities Markets Authority ("ESMA") has observed that DLT systems can be characterised as: (a) records of electronic transactions which are maintained by a shared or "distributed" network of participants (known as "nodes"), thereby forming a distributed validation system; that (b) make extensive use of cryptography i.e. computer-based encryption techniques such as public/private keys and hash functions which are used to store assets and validate transactions on distributed ledgers.

The authors of the Legal Statement suggest that the following factors might be particularly relevant in determining whether English law governs the proprietary aspects of dealings in cryptoassets:

a. Whether any relevant off-chain asset is located in England;
b. Whether there is any centralised control in England;
c. Whether a particular cryptoasset is controlled by particular participant in England (because, for example, a private key is stowred there);
d. Whether the law applicable to the relevant transfer (perhaps by reason of the parties' choice) is English law.

ANDREW MAGUIRE

Littleton Chambers
Temple
London

September 2020