Proskauer

From Cryptic to (Some) Clarity: English Law and Policy Rising to the Challenge of Cryptoassets (Part 2)

Blockchain and the Law Blog on **May 11, 2022**

In the first part of this series of articles, we examined the progress of English law to shape and build an infrastructure to support the development of a secure and certain environment for investment in digital assets. We considered how recent English case law has addressed the questions of whether cryptoassets are property, and whether they can be held on trust.

In this second instalment, we review jurisdictional issues relating to digital assets.

Where are cryptoassets located?

Where assets are located in the eyes of the law is relevant to questions of what governing law applies to them, the Court's determination of its own jurisdiction (including the appropriate forum for a claim to be resolved) and questions of service of court documents outside the jurisdiction. Crypto-disputes raise questions of where cryptocurrency exchanges are located, the identification and location of defendants, and where cryptoassets (which have no traditional physical form) are situated.

The law of the jurisdiction in which property which is subject to litigation is located is referred to as the *lex situs* of the property. In general terms, Courts determine the *lex situs* of land and chattels based on their (physical) location, and in respect of enforceable personal rights over property (known as choses in action) where they are recoverable or can be enforced. Given their intangible nature, determining the *lex situs* of cryptoassets is a question the English Courts have needed to grapple with sooner or later.

The *Ion Science Ltd v Persons Unknown* (unreported, 21 December 2020) case presented an opportunity to do so. It suggested that for the purposes of English law the *lex situs* of cryptocurrency is the place where the person or company who owns it is domiciled.[1] This approach was followed in *Fetch.ai Ltd and another v Persons Unknown Category A and others*[2] as part of the Court's consideration of whether to grant permission for the claimants to serve proceedings outside the jurisdiction. (In that case, the claimants were then able to obtain a worldwide freezing order and proprietary injunctive relief against unknown fraudsters, among other orders.)

Residency or domicile?

In the recent decision in *Tulip Trading Limited v Bitcoin Association for BSV*[3], in rejecting some ambitious legal arguments, English law appears to have adopted a different tack on the *lex situs* of a cryptoasset, preferring residency rather than domicile as the influencing factor.

The claimant (TTL, a Seychelles company owned by Dr Craig Wright, who claims to be the creator of the Bitcoin system) claimed to own Bitcoin worth ca. US$4.5 billion, which he accessed and controlled from his computer and network in England, facilitated by secure private keys. The keys were deleted by hackers who accessed Dr Wright's computer as a result of which Dr Wright lost access to the Bitcoin.

TTL claimed that the defendants, the developers who developed the relevant Bitcoin software owed a fiduciary, or alternatively a tortious, duty to TTL to enable it to re-access the Bitcoin. TTL sought a declaration that it owned the relevant assets and orders requiring the defendants to take reasonable steps to ensure that it had access to them, or for equitable compensation or damages, claiming that it would not be technically difficult for the defendants to write and implement a software "patch" enabling it to regain control of the lost cryptoassets. It obtained permission to serve the claim on the defendants out of the jurisdiction. Following service, some of the defendants challenged the English Court's jurisdiction.

When determining whether the English Court has jurisdiction, the Courts apply a three-limb test:

- whether there is a serious issue to be tried on the merits of the claim meaning that it must be demonstrated that there is a real, as opposed to a fanciful, prospect of

success;

- whether there is a good arguable case that the claims fell within one of the "gateways" under CPR PD 6B (good arguable case meaning, essentially, the better of the argument on the material available); and
- 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.*[4]*

The Court set aside a previous order permitting service of the proceedings on the developers out of the jurisdiction, as TTL had not established a serious issue to be tried on the merits (i.e. it failed on the first limb of the test). In reaching this conclusion, the Court held that cryptoassets systems and software developers did not owe a fiduciary or tortious duty to TTL (the cryptoasset owners) to permit or enable access to the assets where the owners had lost control over the assets following a hack.

A number of notable points arise from the judgment, reflecting the scope of the arguments deployed:

1. Fiduciary duty – The Court concluded that the defendants owed no fiduciary duty to TTL. In reaching that conclusion, the judge noted that an imbalance of power (and vulnerability to its abuse) is often a feature of fiduciary relationships, but it is not a sufficient condition for the existence of the duty. Cryptoasset owners cannot be described as entrusting their property to a fluctuating, and unidentified, body of developers of the software, and the defendants did not owe continuing obligations to remain as developers and make future updates whenever it might be in the interests of cryptoasset owners to do so. Further, TTL was seeking to require the defendants to take actions for TTL's benefit alone (to recover their property), and not for the benefit of all users (such as a systemic software change). This was not characteristic of a relationship of single-minded loyalty owed by the fiduciary to his principal, which is the distinguishing feature of a fiduciary relationship.

The Court did not entirely rule out the possibility of the existence of a fiduciary duty in certain circumstances, however. The judge observed that any holder of digital assets on the networks would have certain expectations, e.g. about the security of the networks and private keys, the efficacy of the "proof of work" processes and anonymity. Software changes that compromised these might create some cause for complaint (so this might be seen as an indication of bases for actions in the future) but this was not argued to be the case here.

1. Tortious duty – TTL said that the Court should recognise an actionable duty owed to owners of digital assets who have lost access to their private keys by developers who are able to assist them to regain control of their assets. This argument was rejected. The Court concluded that the required special relationship to found a duty of care could not be said to be an incremental extension of the existing law, and could not realistically be argued to be fair, just and reasonable.

2. Disclaimer in software notice – the defendants relied on a disclaimer of liability in the terms of the licence under which the relevant code was released, purporting to exclude liability for any claim, damages or other liability in contract, tort or otherwise arising from or in connection with the software or use or other dealings in the software. The Court accepted that the disclaimer was relevant to the question of the existence of a duty of care in tort, but its application to the facts was not sufficiently clear to make a difference to the outcome of the determination. The disclaimer was in broad terms, but it was not clear to the Court that it would reasonably be understood to mean that controllers of the network assumed no responsibility for any aspect of its operation.

3. Public policy considerations – TTL relied on various public policy considerations to support its case for the existence of a tortious duty. These arguments included that (i) there was no rationale for a person to be denied access to assets they own with the result that those assets are lost or become available to fraudsters, (ii) the defendants alone were able to remedy the situation, and (iii) widely held cryptoassets (such as Bitcoin) should not be amenable to manipulation by fraudsters, beyond the reach of law and the standard of accountability applied to those in control of these systems should reflect the significance of the services provided. The Court acknowledged that important issues were raised about the recourse that Bitcoin owners may have if private keys are lost. However, it found that there was no basis for imposing a duty which did not otherwise exist in law.

4. Good arguable case and forum conveniens – Having determined that there was no serious issue to be tried, the Court went on to consider, for completeness, the appropriate ground for service of the claim out of the jurisdiction. The key issue here concerned the *lex situs*, and whether the relevant Bitcoin was located in the jurisdiction, the parties having accepted that Bitcoin constituted property. They disagreed, however, as to the test to be applied to determining whether they were located in England & Wales.*[5]*

In determining the relevant test to apply, the Court considered *Ion Science*, which, as mentioned above, suggested that "*the lex situs of a cryptoasset is the place where the person or company who owns it is domiciled*". The Court concluded that it would have preferred the relevant test to be that of residency. Accordingly, whether the test for the *lex situs* of cryptoassets is domicile or residence remains a live issue to be determined in future cases. The Court also noted that the location of control of a digital asset, including by the storage of a private key, may be relevant to determining the *lex situs*, which could indicate that arguments based on the location of storage of private keys may also find favour in a future case.

On the final limb of the test, the issue of forum, the Court was satisfied that England would have been the appropriate forum for the trial of the dispute, and that the Court would likely have exercised its discretion to permit service of the proceedings out of the jurisdiction, had there been a serious issue to be tried. The factors that provided the relevant connection to England were: (i) TTL's and Dr Wright's presence in the jurisdiction, which was not ephemeral; Dr Wright has lived in the jurisdiction since 2015 and intended to apply for citizenship; (ii) TTL had the better argument that the cryptoassets were located in the jurisdiction and that damage has been or would be sustained in England; (iii) the claim was brought under English law; (iv) TTL's documents are generally located in England; (v) there was no other clear place where the "factual focus" will be, and the Seychelles was clearly not appropriate; (vi) the defendants were based in a number of different jurisdictions, but not one which had a closer link than England; (vii) there was no language difficulty and the relevant documents were in English.

We will be publishing the third (and final) instalment in this series which previews UK legal developments in the cryptoasset world shortly, and will continue to report on new trends and significant changes in the law and regulation of cryptoassets in the UK on Proskauer's Blockchain and the Law blog, so watch this space!

[1] A company's domicile is in the country under whose law it is incorporated.

[2] [2021] EWHC 2254 (Comm)

[3] [2022] EWHC 667 (Ch)

[4] For a summary of the principles and case law see [36]-[48] of *Tulip Trading*.

[5] TTL argued that its place of residence (England) was the key determining factor (being the place where its central management and control was exercised), while the defendants argued that domicile was the correct test, which would make the *lex situs* of the assets, being the Seychelles, where TTL is incorporated.

Related Professionals

- **Steven Baker**
  Partner
- **Julia Bihary**
  Pro Bono Counsel