# SOME HOT TOPICS IN CRYPTO CLAIMS

**Authored by: Zoe O'Sullivan KC (Barrister) - Serle Court**

Cryptocurrency frauds and cryptoexchange insolvencies have given crypto a bad reputation. Yet given that crypto has legitimate uses (making secure, cheap payment transfers is just one example), the law will need to evolve to address the special characteristics of cryptoassets. There are many current projects in different jurisdictions which aim to develop principles designed to facilitate transactions in digital assets, such as the Law Commission's report on Digital Assets, due to be published later in 2023. In the meantime, the common law courts have been showing their customary flexibility in adapting the law to the digital world and fashioning effective remedies for claimants whose cryptoassets have been hacked.

***Cryptoassets have been described as a "conglomeration of public data, private key and system rules"***

(see the Legal Statement on Cryptoassets and Smart Contracts published by the UK Jurisdiction Taskforce in November 2019). A fundamental question is whether cryptoassets are property. Why does this matter? Because property rights are rights against the whole world (save the bona fide purchaser for value), and the owner can assert a right to recover the asset itself, which might be important if it has increased in value, or if the asset is unique (as with an NFT).

An interference with property rights affords particular causes of action, such as a claim in constructive trust against the thief of an asset, now applied by analogy to hackers. Property rights are also critical in an insolvency: if the owner can show that the asset was held for it on trust, it can recover the asset and defeat claims of the unsecured creditors.

English law has traditionally recognised property of two kinds: tangible assets such as land or objects which can be physically possessed, and intangible assets or "things in action" such as debts, which can be enforced by legal action. Cryptoassets do not fall into either category. Nonetheless, in England, the courts have been willing to assume that it is at least arguable that cryptoassets are property. The issue has not yet been tested to the trial standard, as all the reported cases involve pre-trial applications for permission to serve out of the jurisdiction or interim relief. In reaching their conclusion, the courts have applied the definition of property set out by Lord Wilberforce in National Provincial Bank v Ainsworth [1965] AC 1175, where he said that before a right or interest can be admitted into the category of property, it must be definable, identifiable by third parties, capable in its nature of assumption by third parties, and have some degree of permanence and stability. The courts have also placed reliance on the discussion in the influential Legal Statement, above. The English cases with the fullest analysis are AA v Persons Unknown [2019] EWHC (Comm) and Ion Science v Persons Unknown (unreported, 21 December 2020). In Singapore, the Court of Appeal in Quoine v B2C2 [2020] SGCA(1)(02) has deliberately left the question open.

In New Zealand, the High Court has held to the trial standard in Ruscoe v Crytopia [2020] NZHC 728 that cryptoassets are property. Applying Lord Wilberforce's criteria, the court found that cryptoassets are definable by their unique private key, that they are identifiable by third parties because the controller of the private key has the ability to prevent others from dealing with the asset, that they are capable of being transferred again by use of the private key, and that they are sufficiently permanent and stable because their entire history is recorded on the blockchain. The court went on to hold that the remaining assets of the insolvent exchange were held on trust for the customers. By contrast, the New York bankruptcy court found in Re Celsius Network LLC, on a purely contractual analysis, that title to the assets had passed to the insolvent exchange, leaving the customers with worthless personal claims.

Cryptoassets are expressly designed to be decentralised, and thus cannot be said to be located in any particular place. This presents real challenges when determining whether the courts of a particular place have jurisdiction in a crypto dispute. Thus far, the English courts have addressed this question by holding that it is at least arguable that cryptoassets are located in the place where the person who controls the private key is resident, or domiciled, or carries on business, giving the courts of that place an arguable basis for asserting jurisdiction: see Tulip Trading Ltd v van der Laan [2022] EWHC 667 (Ch), not challenged on appeal.

This opens up a number of potential jurisdiction gateways under Practice Direction 6B which may be invoked where the claimant wants to serve a third party such as a cryptoexchange out of the jurisdiction. These include Gateway 11 (claims about property in the jurisdiction) and Gateway 15 (claim made against the defendant as constructive trustee arising out of acts committed in the jurisdiction or assets within the jurisdiction). There are unanswered questions as to whether the asset still has to be located in the jurisdiction at the time when the application for permission is made: see Osbourne v Persons Unknown [2023] EWHC 39 (KB). Where the private key has been used to misappropriate assets, there may be a claim for breach of confidence within Gateway 21: see Fetch AI Ltd v Persons Unknown [2021] EWHC 2254 (Comm). The landmark decision of the Court of Appeal in Tulip Trading v van der Laan [2023] EWCA Civ 83 also tells us that it is arguable that the software developers who control and run bitcoin networks owe fiduciary duties to the true owners of cryptoassets (and thus new Gateway 15B may apply).

Since the introduction of new Gateway 25 in October 2022, applications for information orders against cryptoexchanges have proliferated, making the exchanges the initial target of claims against "persons unknown". Although crypto transactions are anonymous, exchanges often hold KYC and AML information on their customers which is valuable for claimants seeking to trace hacked assets: see LMN v Bitflyer Holdings Inc [2022] EWHC 2954 (Comm).

***That case suggests that the major exchanges are increasingly willing to co-operate in providing such information (while not submitting to the jurisdiction): they appear to recognise that public confidence will be enhanced if the exchanges are seen to be assisting in the prevention of crime.***