XXIV OLD BUILDINGS

COMMERCIAL UPDATE ISSUE #1 FEBRUARY 2022

XXIV.CO.UK

Cryptocurrencies and Civil Fraud Practice – Questions in a Developing Area

Author / BEN WAISTELL

The use of cryptocurrency in commercial dealings and civil fraud has increasingly called upon the courts to consider how to fit these into existing legal concepts or how to adapt those concepts to fit these new problems. This update discusses a few recent cases involving different cryptocurrency issues, considers what they tell us about how the court analyses these assets, and identifies some questions they raise for future cases.

Status as Property

It is now established that cryptocurrencies are a species of property which it is possible to declare trusts over, obtain proprietary remedies in respect of, and – importantly – follow and trace in asset recovery exercises. It would have been deeply concerning had that not been the case, given cryptocurrencies' other attractions as instruments of fraud. However, cryptocurrencies remain a peculiar species of property and the consequences of that need to be carefully considered.

In *AA v Persons Unknown* [2020] 4 WLR 35, Bryan J granted proprietary injunctions over Bitcoin paid by the claimant to hackers in response to a ransom attack. Bryan J noted that cryptocurrencies did not neatly fit within a conventional proprietary analysis as either a chose in possession or a chose in action but held that they plainly had the characteristics of property and were thus capable of being subject to proprietary orders.

That decision has been repeatedly approved and relied upon in subsequent cases seeking to freeze cryptocurrencies (see for instance *Ion Science Limited & Anr v Persons Unknown* (21 December 2020, Butcher J), *Fetch.ai Ltd v Persons Unknown* [2021] 2254 (Comm), and *Wang v Darby* [2021] EWHC 3054 (Comm)). Perhaps unsurprisingly, many of these cases are brought against "persons unknown", however the decision in *Wang v Darby* followed a return date hearing on a freezing injunction at which both parties were represented. At paragraph 55, Stephen Houseman QC (sitting as a deputy high court judge) noted that it was common ground that cryptocurrencies constituted property[1]. Thus, the principle appears to be well established and reliable. The questions now turn to the detail of that analysis and its consequences.

Proprietary Practicalities

As cryptocurrencies have become more prevalent as business assets, the courts have had to consider how to engage with them in assessing interlocutory applications and the protection of each party's position pending resolution of the dispute.

In *Toma v Murray* [2020] 2295 (Ch), the Court

1 In that case the continuation of the proprietary injunction was declined on other grounds.

discharged a proprietary injunction over Bitcoin assets held through an online account on the basis that damages were not an adequate remedy in light of the volatility of Bitcoin. To some extent, the absence of a satisfactory cross-undertaking in damages made that result inevitable. However, the Deputy Judge made clear that an important part of his decision was the volatility of Bitcoin and the potentially vast sums in damages which could result if a defendant were not free to liquidate it as necessary.

A similar approach was taken in the very recent case of *Tulip Trading v Bitcoin Association for BSV & Ors* [2022] EWHC 141 (Ch), where Master Clark rejected an attempt by a claimant to rely upon cryptocurrency to meet a security for costs application. The total security amounted to £248,354.50. The claimant proposed an order whereby its solicitors would hold Bitcoin (either Bitcoin Satoshi Vision or Bitcoin Core) subject to an undertaking to transfer the same to meet any costs order in favour of the defendants. The Bitcoin was proposed to be held in a sum equivalent to the value of the ordered security plus a 10% 'buffer' to mitigate volatility risk. However, Master Clark held that as a result of the volatility of Bitcoin (notwithstanding the buffer), it did not meet the criteria to stand as security for costs. Rather, it would expose the claimants to a substantial risk that the value of the security would fall. It is likely that any further attempts to rely upon other cryptocurrencies in this way will meet the same fate, unless it can be established that they can provide equivalent security to a first-class bank guarantee. That gives rise to risks for any claimants who conduct their business or hold most of their assets in cryptocurrencies – they may need to liquidate these volatile assets at inopportune moments in order to meet a security for costs application and defendants may be able to time such applications in order to maximise the pain of the same.

These two cases show that dealing with cryptocurrency in the normal course of interlocutory applications requires an understanding of cryptocurrencies as distinct from traditional assets and a careful consideration of how they might be deployed or such deployment be made acceptable to the Court. It certainly seems that they will not suffice as security for costs and parties may need to consider whether a Court will need specialist evidence, or even fortification, on application for a proprietary injunction over such assets.

Location, Location, Location

One point of interest, particularly in light of the international nature of commercial fraud and asset recovery exercises, is where cryptocurrency assets should be located. Two decisions of the Commercial Court on this point (*Ion Science* and *Fetch.ai*) both proceeded on the basis that cryptocurrencies constitute intangible property and are located where the holder is domiciled[2]. It is fair to say that Butcher J in *Ion Science* was clear that he was adopting this analysis on the basis of the "serious issue to be tried" test in the context of an interlocutory application and not necessarily determining the legal issue. HHJ Pelling QC (sitting as a high court judge) in the more recent decision in *Fetch.ai* adopted and applied that conclusion and so the same qualification presumably applies.

The possibility of a different analysis appears to arise from the reasoning in the recent case of *DPP v Briedis* [2021] EWHC EWHC 3155 (Admin). This was an application under s. 254A of the Proceeds of Crime Act 2002 to obtain a property freezing order (PFO) as part of civil recovery

2 In the judgment and the academic work relied upon there seems scope to interpret this approach as leading to the usual place of business, at least insofar as the holder deals with cryptocurrency in the course of business.

proceedings in relation to property held by an associate of the criminal defendant. The assets in question included cryptocurrency wallets which had been discovered on various hard drives identified during a search of the respondent's UK address (the respondent himself was known to be outside the jurisdiction). The Court concluded (in reliance upon *AA v Persons Unknown*) that the cryptocurrency wallets were property capable of being subject to a PFO. At paragraph 9, Fordham J considered whether the target assets were within the jurisdiction. He held that although the respondent was known to be outside the UK, the target property itself was not. Paragraphs 9 and 11 describe the assets which were found at the UK house, including "*the hardware wallets containing the cryptocurrencies*".[3]

Depending on the further circumstances not mentioned in the judgment, it might be possible to construe this conclusion consistently with a domicile analysis but that was plainly not the approach Fordham J took – he considered the cryptocurrencies to be located within the UK because they were held as intangible assets within physical hard drives that was located within the UK. This is a peculiar characteristic of cryptocurrencies which leads to the famous stories of people forlornly searching landfill sites for discarded hard drives which hold Bitcoin wallets that are now worth many millions.[4] It is far from clear that this characteristic should be discarded in analysing where cryptocurrencies should be located.

On the current authorities, the more reliable argument is to locate cryptocurrencies with the holder's domicile (or, possibly, place of business) but the point remains open and there are good arguments for locating these unusual assets in the same place as any host physical hard drive.

The Dog Ate My Password

This peculiar nature of cryptocurrency led to an interesting issue in *Wang v Darby* [2021] EWHC 3125 (Comm)[5], where the defendant sought to increase the allowance for legal costs under a freezing injunction. One of the issues before the Court was the extent to which the defendant had access to other assets outside the frozen assets, through which such legal costs could be funded. On this issue, the defendant sought to dismiss substantial cryptocurrency he held, on the basis that he claimed to have forgotten the password to the relevant hard drive which enabled him to access his cryptocurrency wallets, rendering the cryptocurrency inaccessible.[6] Thus, the defendant was claiming that he was left in roughly the same place as the landfill-searchers: he knew where his cryptocurrency was but could not access it. Ultimately, the story in this case was disappointingly simple – the defendant was trying it on. The claimant instructed a cryptocurrency expert who was able to identify trading on the defendant's cryptocurrency wallet after the time he supposedly lost access. The defendant therefore ended up with a failed application and findings about his evidence on an interlocutory application which (notwithstanding

3 This is generally how cryptocurrencies are held. It is, of course, possible to hold indirect interests in cryptocurrencies or to hold them in an online wallet but this update focusses on the hard drive method.
4 See for example: Bitcoin: Newport man's pleas to find £210m hard drive in tip (https://www.bbc.co.uk/news/uk-wales-55658942)
5 Contrary to the neutral citation numbers, this decision predates the previously cited judgment from this litigation.
6 It is not entirely clear from the judgment whether this (or another) hard drive contained the cryptocurrency itself or just – as the judgment says – "*the access codes and other information required to access his various cryptocurrency wallets*".

the Judge's appropriate qualifications in paragraph 22) are tantamount to a finding of dishonesty.

It is, however, easy to see how another claimant (and court) might find itself unable to rebut such a claim by a defendant on an interlocutory application or even when giving final judgment for proprietary remedies. Since it is likely that proprietary rights to cryptocurrency assets would only involve the cryptocurrency wallet and not the host hard drive itself, claimants could find themselves in difficult positions. Presumably they would be able to obtain temporary control of the hard drive for the purposes of attempting to access the cryptocurrency but should they not be able to, the hard drive would likely remain the defendant's property and ultimately need to be restored (particularly if it contained other data beyond the wallet). A claimant would therefore be left to personal remedies in relation to the cryptocurrency (which might not be sufficient) and the risk that the defendant might subsequently 'remember' the password and access the relevant cryptocurrency. Claimants will need to be vigilant and think flexibly in order to address such a circumstance, which might require indefinite freezing injunctions and policing orders to continue post-judgment.

Conclusion

The courts, particularly the Commercial Court, are seeing an ever-increasing volume of cases involving cryptocurrencies and cryptocurrency transactions. This remains a rapidly developing area and existing legal concepts and analyses may have to be adapted to fit these peculiar assets. Their unique attributes need to be taken seriously by practitioners and raise issues as well as opportunities. In particular, the nature of cryptocurrencies as intangible property tethered to tangible hard drives raises some very interesting questions for civil fraud practitioners. An intriguing question will be how the Courts attempt to tackle defendants who seek to shield encrypted assets more successfully than the defendant in *Wang v Darby*.