Kingsley Napley

CRYPTOCURRENCY TALK FOR FRAUD LAWYERS ASSOCIATION

Intro

I am going to look into some of the issues relating to crypto-currencies and civil fraud, either where cryptocurrencies have been stolen, or the proceeds of a fraud have been converted into cryptocurrencies, and make some suggestions about how they might be overcome. I would like to name check and thank Sam Goodman from 20 Essex Street Chambers and my colleague Mary Young who have kindly assisted in the preparation of this talk.

I want first to ask you to remember a couple of key points about cryptocurrencies and the Blockchain. First, they are both totally anonymous and at the same time completely transparent. Anyone can see the public keys and there is a complete record of every transaction in the Blockchain, but it is impossible to see from the public keys anything about the identity of their owners.

Second a couple of points about the nature of crypto-currencies. There is some disagreement about whether they are currencies at all. A Texas Court said they were in a case involving a cryptocurrency Ponzi scheme in 2013. A Miami Court said exactly the opposite in 2016, also in the context of a prosecution. These may be differences in local laws, but there also seems to be some disagreement about this outside of the law. Mark Carney recently said in a talk to the inaugural Scottish Economics Conference at Edinburgh University that in his view cryptocurrencies were failing as currency, comparing their performance to Adam Smith's definition of money. He termed them crypto-assets as a result.

Jamie Dimon and other bankers have indicated they believe cryptocurrencies as a whole are a fraud and a Ponzi scheme (whilst at the same time working together to set up a private Blockchain). Some might say this was a bit rich from one of the senior bankers deeply involved in the causes of the financial crash in 2008.

It does appear to be in the nature of a currency as it is entries on ledgers, which is actually precisely what money is.

More interesting for this talk is whether cryptocurrencies can be described as property, particularly following the case of *Your Response Ltd v Datateam Business Media Ltd Court of Appeal (Civil Division), 14 March 2014*, in which the Court of Appeal suggested that information was not property. Information is effectively what cryptocurrency is.

On the other side of this argument can be found EU Carbon Credits – also electronic information, but held to be property in *Armstrong DLW GmbH v Winnington Networks Ltd [2012] EWHC 10 (Ch)* and the definition of property by Lord Wilberforce in *National Provincial Bank v Ainsworth* [1965] 3 WLR 1 at [1248].

This is worth quoting:

> *"Before a right or an interest can be admitted into the category of property, or of a right affecting property, it must be definable, identifiable by third parties, capable in its nature of assumption by third parties, and have some degree of permanence or stability."*

Cryptocurrencies generally fit into this definition, except maybe the last of the criteria, which perhaps only Bitcoin does, and perhaps not, because of its severe volatility.

Some other problems

A key difficulty I have identified in the context of trying to freeze and recover cryptocurrencies is jurisdiction of the claim, choice of law and of where the assets are located. There a large number of different possibilities, connecting to lots of different jurisdictions. I don't have an answer to this, as there is no authority yet on this which I have been able to find. It is worth noting the problems, though, as on any without notice application the court needs to be alerted to these difficulties in order for the applicant to properly comply with its duties of full and frank disclosure.

Some possible thoughts on jurisdiction:

- Is it where the issuing node is?
- Or the receiving node?
- Where the request for authorisation of the transaction is first received?
- Or where it is authorised?
- Or is it where the wallet is based?
- Or is it where the private key is located?
- Or the exchange is situated?

Freezing injunctions

Having identified a selection of problems a victim of a fraud involving cryptocurrencies might face, a recent case which did not involve cryptocurrencies at all, might provide some exciting developments which can be highly relevant to cryptocurrency fraud.

The case is *CMOC v Persons Unknown (2017) EWHC 3599 Comm.* It was a case involving a "CEO fraud" perpetrated on CMOC by way of a hack into its system and the hi-jacking of a senior executive's email account, which was then used to send payment instructions to the finance team. Large payments were made out of CMOC's account to accounts around the world. For obvious reasons the Applicants could not initially identify the perpetrators but could easily identify the accounts to which the money was paid.

The Court granted freezing orders against "persons unknown". This was billed as the first time this had happened. Apparently there is some doubt about this, but I certainly have not been able to find any other case in which it was. This jurisdiction has been around since 2003 when Harry Potter's publishers obtained an injunction against the individuals who had stolen copies of the book before its publication and were trying to sell it to newspapers. The key point identified by the court was to identify the defendants sufficiently that it was clear who was included and who was not. In CMOC the Court allowed the defendants to be identified as those who had perpetrated the fraud by reference to the transactions and/or those who were the legal or beneficial owners of the bank accounts into which the money was paid.

It is not too difficult to see how this might be translated to cryptocurrencies. Remember my first point about them. Both totally anonymous, making the identity of fraudsters difficult to ascertain, and completely transparent. The defendants can be identified as those who received the proceeds of a fraud as cryptocurrencies and are the holders of a certain public key.

Another very important point to come out of this case is that the Court granted a blanket order for service of the worldwide freezing order out of the jurisdiction, and made orders for alternative service, by electronic means. The latter point is not new, but the combination of orders is quite exciting in the context of cryptocurrencies. The Blockchain is essentially an open message system secured by cryptography. A transaction is no more than a message verified by the private key. Service could easily be effected by sending a message to the account holder, which would be verifiable, and evidence produced it had been received.

Disclosure orders

Another important development from CMOC was in relation to the disclosure order which was obtained against the foreign banks. Prior to CMOC it wasn't completely clear how extra-territorial disclosure orders could be obtained, as it was clear that Norwich Pharmacal orders could not be served out of the jurisdiction. In CMOC the applicant sought orders under the *Bankers Trust* jurisdiction and under CPR Part 25(1)(g). This was previously a little used jurisdiction and provides that the court can grant

> *"an order directing a party to provide information about the location of relevant property or assets or to provide information about relevant property or assets which are or may be the subject of an application for a freezing injunction."*

Two important points arise from this. First, that it allows the court to grant orders to provide information about both property and assets. Remember the other point I asked you to keep

in mind, and this is whether cryptocurrencies are "property" as defined by the common law. The fact that assets are also included means the applicant does not need to make what might be compelling points against itself in complying with its duty of full and frank disclosure, as the position is far from clear.

Second the Court can grant orders in relation to assets which are *or may be* the subject of an application for a freezing injunction. This clearly means that whilst you probably need to have the grounds for a freezer, you do not need to have obtained one before you seek information under this Part. The information obtained may make your application for a freezing injunction stronger or more targeted. It also covers assets which are in other jurisdictions.

The court had no hesitation in granting the order in CMOC under either or both grounds, and also allowed it to be served on the foreign banks.

In the context of cryptocurrencies you would seek such an order against cryptocurrency exchanges, or wallet holder providers. Exchanges are almost all in foreign jurisdictions. You are, however, reliant on whether those exchanges or wallet holders have adequate KYC procedures. Some might but others are equally likely not to have. Some even seek to create a level of anonymity between themselves and their users. It probably depends on the jurisdiction in which you find them, but as we heard from Jill it looks like many jurisdictions are moving in the direction of increased regulation around KYC.

Search orders/imaging orders

It is also worth mentioning the role that a search order, or related order might play in this. Search orders are extremely effective, and the main focus of them these days is the electronic devices and the information contained on them. This is even more the case in a situation involving cryptocurrencies, as the asset is the private key, which is a very small electronic file. A search order is, however, a very draconian order and the courts have been willing in the past to grant less draconian orders more readily, for instance the doorstep Pillar, not permitting a search but requiring immediate delivery up of specified information to the Applicant's solicitor on the doorstep. You can envisage a situation where you might seek a less invasive order to image devices, which the court might be more willing to grant.

As I thought about this I wondered if it would be possible to identify a private key from the image of a device. If you find the private key it gives you control over the asset, in much the same way as you serve a bank as well as the fraudster, as they cannot always be trusted to comply with orders.

Kingsley Napley

As I had no idea I asked a forensic IT expert we use, and I am not sure I am any the wiser, but this is what he said:

> *"In short maybe. [he did go on to elaborate…]*
>
> *A wallet is just an encryption key, so it's a lump of random data. Being a lump of random data we can probably identify it because it will have high entropy.*
>
> *Assuming it's not helpfully named, we might be able to identify it if it has a default file name known to be used by common cryptocurrency wallet applications. Failing that, we'd look at the broader context of the machine:*
>
> *What cryptocurrency software is installed?*
> *For each cryptocurrency software installed, what files has it read/written?*
>
> *In short, there's various forensicy things we'd do. I'd suggest a medium-to-high degree of confidence."*

A quick mention of Blockchain investigators

It is apparently very difficult when transacting using cryptocurrencies not to leave a trace of your IP address. It requires a high level of sophistication not to – even the creator of Silk Road made this mistake, which lead to his downfall. I am told that there are such things as Blockchain investigators, who can trace Blockchain transactions. As I am straying now a long way from any area I have any expertise in, I will leave it at having flagged up their existence.

Self-help remedies

A couple of thoughts from our own experience in acting for a client in a dispute over the ownership of a cryptocurrency account. We were dealing with a situation where at the first sign of the dispute the exchange had simply frozen the account, while the parties sorted it out. This caused a couple of problems as our client was also facing claims of huge losses as a result of this freeze, and we also had some difficulty in persuading the exchange to unfreeze the account in order for the parties to perform the settlement agreement.

If you are aware of an exchange being used, simply informing them about a dispute might be enough to temporarily freeze an account.

William Christopher
Partner
Kingsley Napley LLP
wchristopher@kingsleynapley.co.uk
+44 (0)20 7566 2967
+44 (0)7917 46249

LEGAL DISCLAIMER