THE INTERNATIONAL ACADEMY
OF FINANCIAL CRIME LITIGATORS

Bulletin

of The International Academy
of Financial Crime Litigators

LIN & JIAMIN

> "We have seen more instances of court tackling legal issuesrelating to cryptoassets and granting novel orders to keep up with the growing needs of crypto-related disputes."

– *Legal Tools*

ISSUE 2 | FALL 2023

Legal Tools

Available To Claimants Seeking To Recover Assets In Crypto-Related Disputes

WENDY LIN

LEOW JIAMIN

Introduction

Crypto-related fraud shows no signs of slowing down. The media have reported that crypto crime hit a record US $20 billion in 2022; cryptocurrency investment fraud tripled from 2021 to 2022; and losses to crypto fraud in the UK increased more than 40% from March 2022 to 2023.

Waves of insolvency have also hit the crypto industry, including the bankruptcy of FTX Trading Ltd, and cryptocurrency lender Celsius Network LLC. Litigation has been commenced by the United States Securities and Exchange Commission against various cryptocurrency exchanges.

It is therefore unsurprising that we have seen more instances of courts (in Singapore and other jurisdictions) tackling legal issues relating to cryptoassets and granting novel orders to keep up with the growing needs of crypto-related disputes.

We summarize some of these recent developments, focusing on the legal tools and options available to claimants seeking to recover cryptoassets in such fraud and disputes, including:

a. How can disclosure orders be served out of jurisdiction to seek information in respect of unknown fraudsters;

b. How freezing orders can be sought in a novel form in respect of cryptoassets;

c. How recovery of cryptoassets can be sought against crypto exchanges; and

d. How recovery of cryptoassets can be sought against blockchain developers.

SERVING DISCLOSURE ORDERS OUT OF JURISDICTION: SEEKING INFORMATION ABOUT UNKNOWN THIRD-PARTIES

The defendant in crypto fraud disputes is often unknown. A claimant would typically attempt to seek information from crypto exchanges to identify these fraudsters. Disclosure orders can be sought: (a) in support of injunctions (such as freezing or interim injunctions); (b) against non-parties to request documents to assist with a tracing claim where there is a *prima facie* case of fraud (*ie*, "*Bankers Trust* orders"); or (c) against non-parties who have become "mixed-up" in wrongdoing to provide information (*i.e.* "*Norwich Pharmacal* orders").

More often than not, the crypto exchanges would not be located in the same jurisdiction as the claimant. These crypto exchanges may also utilise opaque structures with numerous corporate entities situated across multiple jurisdictions, making it difficult for claimants to know which precise crypto exchange entity is involved or would hold useful information.

Traditionally, the UK Courts have found that it is more likely than not that a *Bankers Trust* order can be served against a party outside the jurisdiction "*in exceptional circumstances … includ*[ing] *cases of hot pursuit*" (*Ion Science Limited and or v Persons Unknown and ors No. CL-2020-000840* at [21]), but have not permitted *Norwich Pharmacal* orders to be served out of jurisdiction. To address this, the Practice Direction 6B of the UK Civil Procedure Rules 1998 had from 1 October 2022 included a new paragraph 3.1(25) to allow service of orders seeking information "regarding *(i) the true identity of a defendant or a potential defendant and/or (ii) what has become of the property of a claimant or applicant*" for commencement of proceedings in the UK.

In *LMN v Bitflyer Holdings Inc and ors* [2022] EWHC 2954 (Comm) ("*LMN*"), the English High Court thus permitted the orders to be served out of jurisdiction under paragraph 3.1(25). The English High Court explained that it "*would be impractical and contrary to the interests of justice to require a victim of fraud to make speculative applications in different jurisdictions to seek to locate the relevant exchange company and then to seek disclosure, probably in aid of foreign proceedings*". Instead, any concerns about national laws can be dealt with by ordering that no respondent is required to do anything contrary to local laws (*LMN* at [35]-[37]).

In Singapore, the Rules of Court 2021 that came into operation on 1 April 2022 also adopted an expanded approach in permitting service of orders out of jurisdiction. The Singapore Court would consider if there is a good arguable case that there is a sufficient nexus to Singapore (Paragraph 63(2)(a), Supreme Court Practice Directions 2021, "SCPD"), and would consider "*if the application is for the production of documents or information (i) to identify potential parties to proceedings before the commencement of those proceedings in Singapore; (ii) to enable tracing of property before the commencement of proceedings in Singapore relating to the property*" (Paragraph 63(3)(u), SCPD). While there have not been any reported judgments, the English position is likely to be adopted under this expanded gateway to permit the service of *Bankers Trust* orders and *Norwich Pharmacal* orders out of jurisdiction.

FREEZING ORDERS IN THE FORM OF NFTS: ENFORCING ORDERS AGAINST CRYPTOASSETS A CLAIMANT DOES NOT HAVE ACCESS TO

Obtaining a freezing order / injunction in respect of the cryptoassets and judgment against a fraudster is an important milestone for any claimant in a crypto-related dispute. However, it is only half the battle won in terms of asset recovery. How can the order / injunction / judgment be enforced if the claimant does not have access to the cryptoassets in question?

The transfer of and access to cryptoassets are controlled by a set of digital keys and addresses. While anyone is able to transfer cryptoassets to any public address, the recipient must have a unique private key to access the received cryptoassets. Private keys can be kept in custodial wallets (e.g., with a crypto exchange) or in non-custodial wallets (where one stores one's own private keys). Both types of wallets can be hot (connected to the internet) or cold (not connected to the internet).

As transfers of cryptoassets are recorded on the public blockchain ledger, it is possible to trace the last known location of the cryptoassets and whether they reside at an address associated with a custodial wallet (with a crypto exchange) or a non-custodial wallet (e.g., a cold wallet).

Where the defendant or the third party (or crypto exchange) in possession of the wallet is known, and a court order has been made over the cryptoassets which require keys to access, the private keys can be obtained through discovery procedures, *i.e.*, the claimant can seek disclosure of the private keys from the defendant or the third party (or crypto exchange) during enforcement. This would be largely analogous to traditional enforcement of orders against moneys held by a bank or financial institution. Claimants need to be aware that the third party / crypto exchange might not cooperate, and that they may have to adopt other strategies to pressure the platforms to voluntarily comply with such court orders.

Where cryptoassets are controlled by overseas exchanges, it is also possible for the court to order that they be transferred into the court's control in order to facilitate with future enforcement. This would allow the claimant to avoid issues concerning access to the private keys discussed above. In *Joseph Keen Shing Law v Persons Unknown & Huobi Global Limited* [2023] 1 WLUK 577 ("*Joseph Keen*"), the claimant had obtained a worldwide freezing order and a default judgment against the fraudsters. The London Circuit Commercial Court considered that while Huobi had not permitted the fraudsters to access the accounts (and Huobi had indicated an intention to cooperate with any order made by the English Court) that "*may not necessarily occur and continue to be the case, and of course the court has no control over any of the relevant defendants, all of whom are based exclusively outside the jurisdiction of this court.*" (*Joseph Keen* at [11]) The Court therefore found it appropriate to order the transfer the funds subject of the worldwide freezing order into jurisdiction, and for Huobi to convert the cryptoassets to fiat currency and credit them to the claimant's solicitors, or to credit the cryptoassets to the claimant's solicitors who will convert them into fiat currency (to be onwards transferred into the client account or to the court's office: *Joseph Keen* at [24]).

It is more challenging, however, where the cryptoasset is associated with keys kept in a cold wallet in the possession of an unknown party. However, not all is lost. Fraudsters may seek to extract value from cryptoassets by transferring them to other parties or by converting them to fiat currency, and such transactions would involve hot wallets, and become recorded on the public blockchain ledger and traceable. Claimants can then seek information and take action against the hot wallets and exchanges involved. It would nevertheless require more time and effort to monitor the movement of such cryptoassets.

In this regard, the Singapore High Court recently granted a worldwide freezing order in the form of an NFT (unreported). The order was tokenized and permanently attached to the cold wallets in question. While the NFT in itself does not stop transactions, the intention was for the NFT to serve as a warning to third parties that the wallets in question are subject of a hacking incident and the order. The party who obtained the order also designed a process to track funds leaving the wallets.

CLAIMS AGAINST CRYPTO EXCHANGES ON THE BASIS THAT THEY HOLD STOLEN CRYPTOASSETS IN TRUST

Constructive Trust

The Singapore High Court in *ByBit Fintech Ltd v Ho Kai Xin and ors* [2023] SGHC 199 recently held that cryptoassets are property in the eyes of the law, such that a wrongdoer can be found to be holding the cryptoassets on constructive trust for a claimant.

In that case, an employee of an external payroll company engaged by ByBit Fintech Ltd ("ByBit"), a crypto exchange, had wrongfully transferred, among other things, 4,209.720 USDT to four crypto addresses controlled by the employee. The Singapore High Court found that the wrongdoer employee held the USDT on institutional constructive trust for ByBit, and that institutional constructive trust arose by operation of the law as a result of unconscionability (such as fraud and profiting from a breach of fiduciary duty).

In the UK, claimants have attempted to apply similar arguments, not against the wrongdoer, but against crypto exchanges.

In *Piroozzadeh v Persons Unknown and ors* [2023] EWHC 1024 (Ch) ("*Piroozzadeh*"), a claimant traced stolen USDT to wallets in accounts registered with Binance. The claimant then obtained a without notice interim injunction against Binance on the basis that it held the stolen USDT on constructive trust for the claimant. Binance succeeded in having the without notice order set aside on the basis that the claimant failed to comply with its duty of full and frank disclosure:

a. The claimant omitted to inform the court that Binance could raise the defence that it was a bona fide purchaser of the transferred asset (as it was not involved in the fraud); and

b. The claimant failed to inform the court that Binance's practice was to transfer all cryptoassets it received into a pool. In other words, Binance mixed its customer's assets. The lack of segregation made tracing "essentially futile and close to impossible and possibly impossible exercise" (Piroozzadeh at [8]). The claimant was aware of this as Binance had raised this in its defence in separate but similar proceedings that the claimant had copies of (Piroozzadeh at [29], [38]-[39]).

While Binance succeeded in setting aside the without notice interim injunction, this does not mean that a claim in constructive trust against a crypto exchange is bound to fail.

Whether such a claim would succeed depends on the extent to which the crypto exchange was put on notice of the wrongdoing and how the cryptoassets are held by the crypto exchange. There have been more instances of crypto exchanges collapsing as a result of their own fraud. In such cases, it may be possible for claimants to contend that the wrongdoing on the part of the crypto exchange gives rise to a constructive trust in the claimant's favour.

Express trust

Conversely, if the crypto exchange was not put on notice of any wrongdoing, it might be able to raise the defence that it was a *bona fide* purchaser of the deposited asset (as in *Piroozzadeh*). Under common law, a *bona fide* purchaser for value of a property without notice of existing prior claims to the title would take good title to the property, even if the property was fraudulently obtained by the seller.

In a case of an insolvency where no fraud is involved, one may consider whether an express trust has been created in the claimant's favour when seeking to recover cryptoassets that have been deposited at addresses linked with wallets held by crypto exchanges. Under Singapore law, three certainties are required for the creation of an express trust:

> **"*Certainty of intention*** *requires proof that a trust was intended by the settlor. While no particular form of expression is necessary, there must be clear evidence of an intention to create a trust. Next, the trust must* ***define with sufficient certainty the assets*** *which are to be held on trust and the interest that the beneficiary is to take in*

> *them. Finally,* ***certainty of objects*** *requires clarity as to the intended beneficiaries so it is possible to ascertain those who have standing to enforce the trustee's duties under the trust.*" (*Cheng Ao v Yong Njo Siong* [2023] SGHC 22 at [35])

In cases involving cryptoassets involving crypto exchanges, certainty of intention is reflected from:

a. The terms governing the relationship between the customer and the exchange: Where the terms provided that customer deposits were held on trust by the exchange, an express trust can be found to exist (Ruscoe v Cryptopia Ltd (In Liquidation) [2020] NZHC 728, "Ruscoe"). On the other hand, if the terms contain clauses that provide for rights of ownership (such as the ability to pledge, hypothecate or lend) that can be exercised by the exchange, indicate the absence of a trust (In re Celsius Network LLC, 647 BR 631 (Bkrtcy SDNY 2023)); so would terms stating that the exchange did not take client fund safety measures (such as depositing client assets in a trust account) and that it would not be able to return customer assets in the event of bankruptcy (Quoine Pte Ltd v B2C2 Ltd [2020] 2 SLR 2020).

b. The behaviour of the exchange: The lack of segregation and the exchange's use of customer assets as though they belonged to the exchange would reflect a lack of intention to create a trust. How the exchange treats the assets in its financial accounts would also be considered. In Re Gatecoin Limited (in liquidation) [2023] HKCFI 941, the exchange included customer assets in its financial statements (which reflected a lack of intention to create a trust), whereas in Ruscoe, the exchange did not incorporate customer assets when filing its financial accounts and tax returns, and a trust was found to exist.

Turning back to Singapore, this issue may be less murky by next year. The Monetary Authority of Singapore has recently required all Singapore crypto service providers to deposit customer assets under a statutory trust before 2024. The aim is to mitigate the risk of loss or misuse of customers' assets and facilitate the recovery of customers' assets in the event of an insolvency.

BLOCKCHAIN DEVELOPERS MAY OWE FIDUCIARY / TORT-BASED DUTIES TO CLAIMANTS

In *Tulip Trading Limited (A Seychelles Company) v Bitcoin Association For BSV & Ors* [2023] EWCA Civ 83 ("*Tulip*"), the English Court of Appeal thought it arguable that cryptoasset software developers owed fiduciary and tort-based duties to owners of cryptoassets utilising their network. This was a preliminary determination and the matter would be decided at trial.

In that case, the private keys to US $4 billion worth of Bitcoin were lost in an apparent hack. The claimant contended that the 16 named software developers controlled and ran four Bitcoin networks and were able to secure the stolen Bitcoin by moving them to another address that the claimant could control. Unsurprisingly, the software developers contended that the Bitcoin networks were decentralized and "*part of a very large, and shifting, group of contributors without an organisation or structure*". Further, any change proposed would be ineffective as the miners would refuse to run it, and a disagreement would result in a "*fork*" (*ie*, the creation of additional networks) (*Tulip* at [33]). The English Court of Appeal eventually stated that this would be an issue to be resolved at trial (*Tulip* at [91]).

Each type of cryptoasset is created and issued within its own network. There are decentralized networks without any central network owner (like Bitcoin) and centralized networks where there is a central network owner.

In *Tulip*, the software developers were able to contest the claimant's argument that such duties existed by relying on the fact that the Bitcoin networks are *decentralized* and that they would not be able to implement the change requested by the claimant. However, where the cryptoasset network in question is *centralized* (*i.e.* where there is only one software developer controlling the entire network), it may well be that it is more likely that such duties would arise. As the English Court of Appeal noted in *Tulip*, "*developers are people who it is clearly arguable have undertaken a role which at least bears some relationship to the interests of other people*" and, in a cryptocurrency situation, have authority given to them by their control of access to the source code, and are "*in effect making decisions on behalf of all the participants in the relevant*" network. These features are common to fiduciary duties currently recognized by the law, and make it possible for developers of centralized networks to be found to owe fiduciary duties to claimants (*Tulip* at [70]-[76]).

AUTHORS

Wendy Lin

Wendy Lin is the Deputy Head of the Commercial & Corporate Disputes Practice, and a Partner in the International Arbitration Practice at WongPartnership LLP.

Leow Jiamin

Leow Jiamin is a Partner in the Commercial & Corporate Disputes Practice at WongPartnership LLP.

in Share This Read