Fraud and Asset Recovery: Cryptoassets

Guide to tracing, freezing and recovering stolen cryptoassets

Not one day goes by without cryptoassets being in the news. Cryptoassets are becoming the common target of fraud, be it ransomware demands made arising from cybersecurity breaches, scams, or thefts by hackers.

How can one trace, freeze and recover cryptoassets lost? How different is this from the recovery of traditional assets? We review the options available for victims of crypto fraud, and discuss the recent decision of the General Division of the Singapore High Court ("**High Court**") in *CLM v CLN & Ors* [2022] SGHC 46 ("***CLM***") and its implications.

INTRODUCTION

Cryptoassets refer to digital assets created using the blockchain (or distributed ledger technology). This technology is a type of database that contains electronic records shared and replicated across the network. The way the database is structured means that the records are irreversible and traceable, which makes the tracking of cryptoassets (mostly through transaction identifiers) relatively straightforward as compared to traditional assets.

Given the ease with which cryptoassets can be transferred, the tracing, freezing and recovery of cryptoassets is a race against time. Once the cryptoassets are traced to their last known location, necessary legal action should be taken as soon as possible. We discuss below the following interim relief that victims of crypto fraud may seek from the Singapore courts:

(a) *Mareva* injunctions;

(b) Interim proprietary injunctions;

(c) Disclosure orders in support of *Mareva* injunctions or interim injunctions; and

(d) Third-party / non-party disclosure orders (e.g., Bankers Trust orders and *Norwich Pharmacal* orders).

In seeking the above options, the predominant difficulty lies in identifying the persons behind the fraud, or the persons who are in control of the digital wallet containing the private keys to the stolen cryptoassets. This presents a few tricky issues: other than the crypto exchanges identified, how can one bring proceedings against the fraudsters, when their identity and location are almost always unknown? Even if one commences proceedings against unknown fraudsters, how can such proceedings be brought to their attention?

SEEKING A COURT INJUNCTION TO FREEZE CRYPTOASSETS

Commencing proceedings against unknown fraudsters

The High Court in *CLM* confirmed for the first time that the Singapore courts can grant orders against persons whose identities are unknown at the time of the application. This is because there is nothing in the Singapore Rules of Court ("**Rules**") that requires a defendant to be specifically named. Even if commencement of proceedings against persons unknown does contravene the Rules, this is a mere irregularity and will not nullify the proceedings, unless the court exercises its discretion to order a nullification.[1]

This is consistent with the position taken in the UK (where orders against persons unknown were granted even before cryptoassets were first created) and Malaysia.

What should be noted is that the description of unknown defendants must be sufficiently certain to identify those who are included and those who are not.[2] One can therefore describe "persons unknown" by referring to: (a) the actual transfers / fraudulent activities; (b) the digital wallets that had received the specific cryptoassets; (c) the cryptoassets themselves if they are unique, such as in the case of Non-Fungible Tokens ("**NFTs**"); or even (d) by email addresses or contact numbers (if there had been some communication in the case of ransomware demands or scams).

The need to be sufficiently certain has resulted in some interesting (and lengthy) ways defendants have been named or identified (for example, a defendant was recently named in US proceedings as "*Approximately 3879.16242937 bitcoin, seized from Bitcoin address bclq7rhc02dvhmlfu8smywr9mayhdph85jlpf6paqu*" [3], and a set of defendants were named in UK proceedings as "*Persons Unknown being the individuals or companies, describing themselves as being or connected to 'Neo Capital', some of whom gave the aliases Marilyn Black, Claire Jones, Robert Welsh, Carey Jones, Mia Davis and Grant Ford, who participated in a scheme to induce the Applicants to transfer Bitcoins between March-October 2020 in the belief that they were investing in Dimecoin and/or Ethereum and/or Uvexo and/or Oileum*[4]). This is testament to how the courts have sought to be flexible in order to keep up with technological developments.

Serving proceedings and orders on the unknown fraudsters

For the Singapore court to have jurisdiction to hear the dispute, proper service of the proceedings must be effected on the defendant, or the defendant must submit to the jurisdiction of the Singapore court.[5]

---

1 *CLM* at [28]-[29]; Order 2 rule 1 of the Rules of Court (Rev Ed 2014) ("**Rules of Court 2014**") (Order 3 rule 2 of the Rules of Court 2021, which will come into effect on 1 April 2021)

2 *CMOC v Persons Unknown* [2017] EWHC 3599 (Comm) at [2], citing *Bloomsbury v News Group Newspaper* [2003] EWHC 1205

3 Case Number '21CV2103 AJB JLB filed in the United States District Court Southern District of California

4 *Ion Science Limited and or v Persons Unknown and ors* No. CL-2020-000840

5 Section 16(1) of the Supreme Court Judicature Act

Under the Rules, proceedings must be served personally,[6] which means that they must be handed to an individual or left at the registered business address of a company.[7] If these methods are not successful after multiple attempts, the alternative would be to obtain permission from the court to effect substituted service, for example, by way of email (if it can be proven that the email address is still active and linked to the defendant), or by advertisement taken out in broadsheet papers.[8] If service overseas is necessary, permission must be obtained from the court before proceedings can be served overseas, and the mode of service must comply with the laws of that foreign jurisdiction.[9]

If it is clear at the outset (such as in the case of crypto fraud) that it would be "*impracticable for any reason to serve that document personally on that person*",[10] the court can grant substituted service at the get-go. This would be the case even if the unknown defendant is outside Singapore.[11]

That was the case in *CLM*. The High Court found that it was impractical to serve the proceedings on the fraudsters personally as their physical whereabouts were unknown. There was also evidence to show that the fraudsters had used virtual private networks to obscure their locations when accessing their crypto accounts, seemingly to avoid being located physically in the event their identities were uncovered.[12]

The High Court found that service by email instead would be effective and would bring the proceedings and orders to the unknown defendants' notice, as there was evidence to show that the email addresses were active (as they were used less than five months previously to register the crypto accounts). While the documents opening the said crypto accounts included a physical address, the High Court found that the onboarding process by the crypto exchanges did not include a verification of that physical address; instead, the operative contact was always through the email addresses.[13]

Besides email, substituted service *via* other forms of social media can be considered if it can be shown that they are effective ways of notifying a defendant of the proceedings. For instance, the High Court has allowed a claimant to effect substituted service through email, Skype, Facebook and an Internet message board.[14]

Types of injunctions that can be sought against cryptoassets

In traditional fraud and asset recovery litigation, it is common for claimants to seek:

(a) A worldwide or domestic freezing injunction to protect the claimant from the defendant's dissipation of assets, against which the claimant may enforce a judgment if the claimant is successful in the proceedings. This is known as a "*Mareva*" injunction.

---

6 Order 62 rule 1 of the Rules of Court 2014 (Order 7 rule 1 of the Rules of Court 2021)

7 Order 62 rules 3 and 4 of the Rules of Court 2014 (Order 7 rule 2 of the Rules of Court 2021)

8 Order 62 rule 5 of the Rules of Court 2014 (Order 7 rule 7 of the Rules of Court 2021)

9 Order 11 of the Rules of Court 2014 (Order 8 of the Rules of Court 2021)

10 Order 62 rule 5 of the Rules of Court 2014 (Order 7 rule 7 of the Rules of Court 2021)

11 *CLM* at [77]

12 *CLM* at [79]

13 *CLM* at [81]-[82]

14 *Storey, David Ian Andrew v Planet Arkadia Pte Ltd and ors* [2016] SGHCR 7

(b) A proprietary injunction to preserve the property over which a claimant has a proprietary claim. The purpose of the injunction is to allow the claimant to reclaim his ownership of the asset if the claimant is successful in the proceedings. This is an important consideration for cryptoassets, as the value of cryptoassets may have appreciated in the course of the proceedings. A proprietary claim would also extend to assets acquired through gains derived from the cryptoassets (if they were sold).[15]

Mareva injunction

To obtain a *Mareva* injunction, a key factor that the claimant would need to prove is actual or a risk of dissipation of assets by the defendant. It is generally insufficient to rely on allegations of dishonesty and fraud alone as proof of a risk of dissipation of assets.[16] A "*well-substantiated allegation that a defendant has acted dishonestly*", however, would be relevant and would be considered by the court.[17]

The court may additionally consider that, without more information as to who the fraudsters are, it may not be just and convenient to grant a worldwide *Mareva* injunction. This happened in a recent UK decision, where the UK court decided to stand over the *Mareva* injunction application until further information was obtained, so that the scope of the injunction could be restricted.[18]

In *CLM*, the High Court found that the fraudsters had acted dishonestly in misappropriating the stolen Bitcoin and Ethereum. A series of digital wallets appeared to have been created "*solely for the purpose of frustrating the* [claimant's] *tracing and recovery efforts, and which had either no or negligible transactions other than the deposit and withdrawal"* of the stolen Bitcoin and Ethereum. The High Court also found that the risk of dissipation "*is heightened by the nature of the cryptocurrency*".[19]

These point to the importance of tracing the assets immediately after the fraud has occurred. If the tracking efforts show that the stolen cryptoassets have changed hands quickly through digital wallets that seem to serve no other purpose but to disrupt recovery efforts, this is evidence that can be relied on in seeking a *Mareva* injunction. Further, if it is possible to identify the persons unknown with more precision, this may eliminate concerns that the *Mareva* injunction would be overly wide in scope.

Proprietary injunction

Whether a proprietary injunction can be granted depends on whether the cryptoasset is considered "property" in the eyes of the law, such that it can be the subject of proprietary claims (such as a breach of trust or breach of fiduciary duties) and be protected by a proprietary injunction.

---

15 *Choy Chee Keen Collin v Public Utilities Board* [1996] 3 SLR(R) 812 at [13]

16 *Bouvier, Yves Charles Edgar and anor v Accent Delight International Ltd and anor and anor appeal* [2015] SGCA 45 at [66]: "*it is incorrect for the court to treat allegations of dishonesty made at an interlocutory stage as if they have already been established. Such allegations may eventually be refuted. As a matter of principle therefore, the grant of Mareva relief should not generally be wholly founded upon an unproven allegation of dishonesty*."

17 *CLM* at [54]

18 *Lubin Betancourt Reyes and ors v Persons Unknown* [2021] EWHC 1938 (Comm) at [34]

19 *CLM* at [54]

Whether cryptoasset is "property" has not been conclusively resolved. The answer to this question also depends on the type of cryptoasset, which will be discussed below. For the purposes of the present analysis, we assume that the cryptoasset in question is Bitcoin (or similar cryptocurrencies).

Prior to the High Court's decision in *CLM*:

(a) The courts in the UK considered the question on a preliminary and *ex parte* basis, and either found, or assumed, that Bitcoin (and similar cryptocurrencies) are "property". The courts in most of the UK decisions considered that Bitcoin fell within the classic definition of property, that "*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*."[20]

(b) The New Zealand courts, upon an application made by liquidators seeking directions relating to the categorisation and distribution of assets of a crypto exchange in liquidation, similarly found that cryptocurrencies fell within the classic definition of property.[21]

In *CLM*, the High Court took a similar approach and found on a preliminary and *ex parte* basis that the stolen Bitcoin and Ethereum fell within the classic definition of property and were "*capable of giving rise to proprietary rights, which could be protected via a proprietary injunction*".[22] The High Court therefore granted the proprietary injunction over the stolen Bitcoin and Ethereum.

However, the High Court was also careful to add a caveat: "*the court does not engage in complex questions of law or fact at the interlocutory stage*", and all the claimants have to show in respect of this particular question at this stage is that they "*have a seriously arguable case that they [have] a proprietary interest*".[23]

Therefore, at present, claimants would (at least on an *ex parte* basis) likely be able to obtain a proprietary injunction and bring proprietary claims against fraudsters in respect of Bitcoin (or similar cryptocurrencies). This will likely be the case until a Singapore court (or common law court)[24] has decided after full argument or a full trial of the matter that Bitcoin (or similar cryptocurrencies) are not "property".

SEEKING ORDERS FOR INFORMATION

Similar to traditional fraud and asset recovery efforts, where information would be sought from a bank or financial institution as to who owns a certain account or where the monies or assets have been transferred to, crypto exchanges are a good source of information, even if the stolen cryptoassets are no longer with the exchange. As the UK High Court commented, some of the crypto exchanges operate on terms that

20 *National Provincial Bank Ltd v Ainsworth* [1965] AC 1175 at 1248

21 *Ruscoe v Cryptopia Limited (in liquidation)* [2020] NZHC 729 at [133]

22 *CLM* at [46]

23 *CLM* at [39]

24 Decisions from other Commonwealth Courts can be taken into consideration by the Singapore courts, where relevant.

their customers' personal data may be disclosed to "*comply with the laws … formulated by government authorities*".[25]

There are three options available in seeking information from crypto exchanges:

(a) Disclosure orders in support of a *Mareva* injunction or an interim injunction;

(b) Orders compelling non-parties to provide documents to assist with a tracing claim where there is a *prima facie* case of fraud, known as "Bankers Trust orders"; and

(c) Disclosure orders against non-parties who have become "mixed up" in wrongdoing to provide information, known as "*Norwich Pharmacal* orders".

In *CLM*, the claimant sought disclosure of:

(a) the current balances of the accounts which received the stolen Bitcoin and Ethereum;

(b) information and documents collected by the crypto exchanges in relation to the owners of the accounts; and

(c) details of all transactions of the accounts from the dates on which the stolen Bitcoin and Ethereum were credited.[26]

Disclosure orders in support of a Mareva injunction or proprietary injunction

The High Court found in *CLM* that the disclosure orders sought against the crypto exchanges were just and convenient, and granted them in support of the interim relief granted.[27] This is because the claimant required the information to understand what remained of the stolen cryptoassets and if they were transferred to other persons / accounts, and the whereabouts of the Bitcoin and Ethereum. The information would also help to identify the fraudsters, or persons who may have acted with the fraudsters.[28]

While the High Court referred to the court's power to grant ancillary disclosure orders in support of the *Mareva* injunction, it appears that the disclosure orders granted were both in support of the *Mareva* and the proprietary injunctions, as the scope of the orders went beyond that permitted solely in support of a *Mareva* injunction.

Disclosure orders granted to support a *Mareva* injunction would be those assisting:

(a) in determining the existence, nature and location of the defendant's assets (this is not limited to the stolen assets as the intention of the *Mareva* injunction is to freeze assets against which a money judgment can be satisfied if the plaintiff prevails);

---

25 *Fetch.ai Limited and ors v Persons Unknown Category A and ors* [2021] EWHC 2254 (Comm) ("***Fetch.ai***") at [35]-[37]

26 *CLM* at [57]

27 *CLM* at [58]

28 *CLM* at [60]

(b) clarifying questions of title concerning assets (as the *Mareva* injunction would not cover assets truly belonging to third parties); and

(c) identifying third parties to whom notice of the injunction should be given for the purpose of ensuring that they do not advertently or inadvertently assist the defendant in the removal or disposal of assets.[29]

The High Court's disclosure orders were not limited to those described in (a) and (b) above and included orders permitting the tracing of the Bitcoin and Ethereum (i.e., information as to whether the Bitcoin and Ethereum had been transferred to others and their whereabouts). Such a tracing disclosure order can only be granted in cases where there exists a proprietary claim. Thus, while not made explicit, it is likely that the tracing disclosure order granted was made in support of the proprietary injunction. After all, as the High Court noted, the court has wide powers to make ancillary orders in granting injunctions, i.e., "*either unconditionally or upon such terms and conditions as the court thinks just, in all cases in which it appears to the court to be just or convenient that such order should be made*".[30]

A claimant will thus likely be able to seek ancillary disclosure orders to assist with its recovery efforts if it is successful in obtaining a *Mareva* injunction and/or a proprietary injunction – the difference being in the scope of the orders that can or will be made.

Bankers Trust orders

The High Court declined to consider whether a Bankers Trust order should be granted, as the crypto exchanges were already parties to the proceedings, and therefore not non-parties.[31] This appears to be a departure from the position that the UK courts have taken, as the UK courts have been granting Bankers Trust orders against crypto exchanges even when they have been added as parties to the proceedings.[32]

This is not to say that a Bankers Trust order has no relevance in crypto fraud litigation. A Bankers Trust order remains a powerful tool by which information can be sought against non-parties. For instance, it may be more effective to seek a Bankers Trust order against additional parties uncovered subsequently, instead of attempting to add them as parties to the proceedings. Some possible factual scenarios where this may be applicable is if:

(a) Subsequent tracing efforts show that the cryptoassets have been moved to yet another cypto exchange.

(b) Further inquiry and investigations show that the crypto exchange initially named in the proceedings might not be the correct entity - an error arising from the fact that the way crypto exchanges are structured is often unknown and information as to which precise entity is involved is often opaque.[33]

---

29 *Singapore Civil Procedure 2021* at [21/1/69]; *Sun Electric and ors v Menrva Solutions Pte Ltd and ors* [2020] SGHC 18 at [102]

30 Section 4(10) of the Civil Law Act; *CLM* at [59]

31 *CLM* at [59]

32 For example, in *Fetch.ai*

33 See a discussion by the UK Court in *Fetch.ai* at [26] as to the structure of the Binance Group

It is also of note that 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 (i.e., outside the UK) "*in exceptional circumstances … includ*[ing] *cases of hot pursuit*"[34], unlike *Norwich Pharmacal* orders (which we discuss briefly next).

It remains to be seen whether the Singapore courts will adopt a similar approach and permit Bankers Trust orders to be served against a party outside the jurisdiction. In this regard, it should be noted that the upcoming revision of the Rules has broadened the grounds on which the Singapore court can permit service out of Singapore, and claimants are no longer restricted by the limited prescribed grounds under the old Rules.[35] The Bankers Trust order therefore still remains an option that claimants should consider in crypto fraud litigation.

Norwich Pharmacal orders

The High Court in *CLM* did not need to consider whether a *Norwich Pharmacal* order should be granted, as the claimant did not seek one. Nonetheless, it is likely that the court would find that a *Norwich Pharmacal* order can only be granted against non-parties / third parties. This is because *a Norwich Pharmacal* order can only be granted "*before the commencement of proceedings*" or against "*a person who is not a party to the proceedings*".[36]

As mentioned above, the UK courts have taken the position that *Norwich Pharmacal* orders cannot be served on parties outside its jurisdiction (i.e., outside the UK) as they do not satisfy the grounds permitting service out of jurisdiction under UK law. They have instead granted *Norwich Pharmacal* orders against crypto exchanges within the same jurisdiction (i.e., in the UK).[37] It remains to be seen whether the High Court would adopt a similar approach and restrict such orders to parties within the jurisdiction (i.e., in Singapore), given the broadening of the grounds on which the Singapore courts may permit service out of Singapore under the new Rules.

STEPS AFTER ORDERS ARE GRANTED

Obtaining the abovementioned orders from the court is just the start to recovering stolen cryptoassets. If the cryptoassets are still with the crypto exchanges, it would be a matter of urgency to request that the crypto exchanges comply with the injunctions to freeze or block the digital wallets in question, to ensure that the fraudsters are prevented from moving the cryptoassets again.

---

34 *Ion Science Limited and or v Persons Unknown and ors* No. CL-2020-000840 at [21]; *Fetch.ai* at [14]

35 Order 8 rule 1 of the Rules of Court 2021, read with paragraph 63 of the Supreme Court Practice Directions 2021 (both coming into effect on 1 April 2022)

36 *Liberty Sky Investments Ltd v Oversea-Chinese Banking Corp Ltd and anor* [2017] SGHC 20 at [19]; Order 24 rule 6(5) of the Rules of Court 2014 (Order 11 rule 11 of the Rules of Court 2021)

37 *Fetch.ai* at [39]-[43], and it is of note that the crypto exchanges (against whom the *Norwich Pharmacal* orders were issued) were added as parties to the proceedings there.

While most reputable exchanges may willingly comply with orders of court, it is equally possible for others to refuse, especially if they are not within or do not operate within the jurisdiction which granted the court order. It is therefore important to consider steps that may have to be taken in other countries. For instance, it may be necessary to seek enforcement of a Singapore court order in another country where the crypto exchange can be located.

In this regard, a worldwide *Mareva* injunction is usually granted by the Singapore court on the claimant's undertaking that it will seek permission before: (a) enforcing that injunction in any other country,[38] or (b) starting proceedings against the defendant in any other country.[39] All the relevant circumstances and options would be considered by the Singapore court in determining whether permission ought to be granted, and the claimant would have to show that it is just and convenient for the purposes of ensuring the effectiveness of the worldwide *Mareva* injunction, and not oppressive to the parties in the Singapore proceedings or to third parties who may be joined to the foreign proceedings.[40]

It may also be necessary to rely on documents obtained in the primary litigation in Singapore in foreign ancillary proceedings. Claimants would need to be aware that documents obtained pursuant to disclosure orders granted by the Singapore court are produced under compulsion, and would be subject to an implied undertaking given by the claimant to the Singapore court that the document obtained will not be used otherwise than in that action, or for any ulterior or alien purposes.[41] Documents obtained pursuant to disclosure orders granted in support of the *Mareva* injunction may be subject to a further undertaking from the claimant that they are not to be used in any other jurisdiction (whether for civil or criminal proceedings) unless permission is granted by the court.[42] Therefore, in order for such documents to be used in foreign ancillary proceedings, one would have to seek permission from the Singapore court and explain that the court's processes have not been and will not be abused.[43] It is therefore important to consider as a matter of timing (as any legal step is a race against time) when would be appropriate to seek such permission.

It will also likely be necessary to seek additional orders, or enforcement of orders after information is received from the crypto exchanges identifying more parties involved in the fraud. This is what happened in *CLM*, where after further investigations and disclosures made by the crypto exchanges, two additional persons were identified who were joined to the proceedings.[44]

---

38 Paragraph 10 of Schedule 1 to Form 7 to Supreme Court Practice Directions (Form 25 of Supreme Court Practice Directions 2012)

39 Paragraph 9 of Schedule 1 to Form 7 to Supreme Court Practice Directions (Form 25 of Supreme Court Practice Directions 2012)

40 *Bouvier, Yves Charles Edgar and anor v Accent Delight International Ltd and anor and anor appeal* [2015] 5 SLR 558 at [131]; *Dadourian Group International Inc v Simms* [2006] 1 WLR 2499 at [24]-[25] sets out 9 guidelines.

41 *Riddick v Thames Board Mills Ltd* [1977] QB 881; *ED&F Man Capital Markets Ltd v Straits (Singapore) Pte Ltd* [2020] 2 SLR 695 at [66]

42 Paragraph 9 of Schedule 1 to Form 7 to Supreme Court Practice Directions (Form 25 of Supreme Court Practice Directions 2012)

43 *Ong Jane Rebecca v Lim Lie Hoa and ors appeals and ors matters* [2021] 2 SLR 584 at [148]-[149]

44 *CLM* at [61]-[63]

Once the cryptoassets are frozen and the fraudsters identified, the proceedings against the fraudsters (i.e., the proprietary claims or any other claims made) would have to be tried in full by the court, before final judgment will be granted.

In some circumstances where the stolen cryptoassets have ended up in the hands of possibly innocent third parties, the fact that injunctions have been granted over the assets may pave the way to negotiations and an eventual settlement of the matter.[45]

FUTURE DEVELOPMENTS

Why is it still uncertain if Bitcoin (or cryptocurrencies) are "property"?

We mentioned above that whether a cryptoasset is "property" has not been concretely resolved. The uncertainty boils down to the fact that in the eyes of the law, it has been long regarded that there are principally two categories of property: (a) a "chose in possession" (referring to physical assets, which cryptoassets, including Bitcoin, are not); and (b) a "chose in action".[46]

To simplify the legal jargon, we consider a hypothetical example of you wanting to deposit monies in a bank account. Before monies are deposited with the bank, the monies exist in the form of cash, which is a "chose in possession" as they exist physically. Once you deposit the monies with the bank, they no longer have a physical presence. Such monies deposited with the bank are therefore considered a "chose in action", and your property right arises from the fact that you can take action against the bank to enforce your rights in the monies deposited.

Unlike monies deposited with a bank, cryptocurrency resides on the blockchain (which are pockets of data replicated across the network). Further, in the case of Bitcoin (and other decentralised cryptocurrencies), there is no particular issuer (i.e., there is no equivalent of a central bank) as it is a decentralised network. Strictly speaking, therefore, there is no one against whom an action can be taken to enforce the rights in the Bitcoin. This is the same for other cryptocurrencies similar to Bitcoin.

One may then ask: what about the digital wallets opened with crypto exchanges? Do they not operate similarly to banks?

What resides in the digital wallet, however, is not the Bitcoin itself, but the private keys allowing one to access or control the Bitcoin that resides on the blockchain. Further, not all Bitcoin are stored with crypto exchanges; many choose to create cold wallets (i.e., devices that are disconnected from the Internet) for added security.

In the event the court finds that cryptoassets are not "property", that would preclude claimants from seeking a proprietary injunction over the cryptoassets and bringing proprietary claims against the

---

[45] It was reported that in *AA v Persons Unknown who demanded Bitcoin on 10th and 11th October 2019 and ors* [2019] EWHC 3556 (Comm), the defence raised was that the defendant was a good faith purchaser of the Bitcoin in question, and the matter was eventually settled by way of negotiations.

[46] *Colonial Bank v Whinney* [1885] 30 ChD 261 (per Fry LJ): "*All personal things are either in possession or action. The law knows no tertium quid between the two.*"

cryptoassets (i.e., claims as to ownership of the property in the hands of someone else). As we mentioned above, this has serious implications:

(a) It is critical that a proprietary injunction is obtained over the cryptoasset if that is the only known asset held by the fraudster (thus the only asset that one can recover).

(b) The value of cryptoassets may have appreciated in the course of the proceedings, and without a proprietary claim, a claimant would not be able to recover the cryptoassets themselves. In that event, the claimant may be left with seeking compensation of the losses arising as at the date of the fraud, which may fall far short of the value of the cryptoassets if the claimant was able to recover ownership of them.

(c) If the cryptoassets have unfortunately been sold, a claimant would not be able to assert a claim over assets bought with those gains if he / she is unable to assert a proprietary claim over the cryptoassets.

The courts, however, are starting to recognise that the law needs to keep up with the developments in crypto. The New Zealand courts have opined that while it has long been regarded that there are two categories of property (arising out of a dissenting English Judge's finding made in 1885), that in itself is a matter of categorisation and does not limit what can be recognised as "property", and the categorisation itself would not lead a court to conclude that cryptocurrencies are not property.[47] The UK courts have also commented that it would be "*fallacious to proceed on the basis that the English law of property recognises no forms of property other than choses in possession and choses in action*".[48] Indeed, it may be time for the law to consider if a statement of law from 1885 ought to be applied strictly 137 years on.

What about other types of cryptoassets?

There are various types of common cryptoassets, which categorisation can be simplified based on their function:

(a) Cryptocurrency or crypto coins, like Bitcoin, is a medium of exchange widely understood to function like a digital currency. These coins can be used to exchange for products or service, trade, or simply function as a store of value.

(b) NFTs refer to tokens that are each unique and irreplaceable. NFTs are most commonly created to certify the ownership of real-world assets (for example, one may own an NFT which certifies that one is the owner of an artwork).

(c) Security tokens are tokens in a project, such as an initial coin offering (ICO) or initial token offering (ITO), which allow the issuer to raise funds. Such security tokens are often coupled with other benefits, such as the right to vote, or the right to dividends.

---

47 *Ruscoe v Cryptopia Limited (in liquidation)* [2020] NZHC 729 at [123]-[124]

48 *AA v Persons Unknown who demanded Bitcoin on 10th and 11th October 2019 and ors* [2019] EWHC 3556 (Comm) at [58]

(d) Utility tokens are tokens providing a particular function to its holder, such as access to a specific product or service by the issuer. The use of such utility tokens is usually limited within the network they are issued.

Notably, all of the reported decisions in the Commonwealth have dealt only with Bitcoin (or similar cryptocurrencies like Ethereum). This is not surprising, given that Bitcoin, Ethereum, and cryptocurrencies are fungible and valuable, and hence a popular target for fraudsters. Tokens, however, are becoming increasingly important. For instance, it has been reported that NFTs have a combined value of US$16 billion.[49] While this is still a fraction of the US$2 trillion crypto ecosystem, it is still of significant value.

Interestingly, if tokens (such as NFTs, security tokens, or utility tokens) are created / issued on a closed network by an issuer that is identifiable, it may be relatively easier to argue that these should be considered "property" in the eyes of the law. This is because there exists an identified party against whom a holder of the token can take action to enforce his/her rights in that token (hence a "chose in action").

Therefore, while it may be uncertain whether Bitcoin (or cryptocurrencies) can be considered "property", that may not be the case for tokens, which means that the same options and principles outlined above, can and should be extended to crypto litigation involving tokens.

If you would like information or assistance on the above or any other area of law, you may wish to contact the Partner at WongPartnership whom you normally work with or any of the following Partners:

Wendy LIN
Partner – Commercial & Corporate Disputes
d: +65 6416 8181
e: wendy.lin@wongpartnership.com
Click here to view Wendy's CV.

LEOW Jiamin
Partner – Commercial & Corporate Disputes
d: +65 6416 8136
e: jiamin.leow@wongpartnership.com
Click here to view Jiamin's CV.

Connect with WongPartnership.

[49] *Bloomberg* (11 February 2022) "Seemingly Ubiquitous NFTs Make Up Only 1% of Crypto Universe" accessible at https://www.bloomberg.com/news/articles/2022-02-10/seemingly-ubiquitous-nfts-make-up-only-1-of-crypto-universe (accessed on 10 March 2022)

WPG MEMBERS AND OFFICES

- contactus@wongpartnership.com

SINGAPORE

-
WongPartnership LLP
12 Marina Boulevard Level 28
Marina Bay Financial Centre Tower 3
Singapore 018982
t +65 6416 8000
f +65 6532 5711/5722

CHINA

-
WongPartnership LLP
Shanghai Representative Office
Unit 1015 Link Square 1
222 Hubin Road
Shanghai 200021, PRC
t +86 21 6340 3131
f +86 21 6340 3315

MYANMAR

-
WongPartnership Myanmar Ltd.
Junction City Tower, #09-03
Bogyoke Aung San Road
Pabedan Township, Yangon
Myanmar
t +95 1 925 3737
f +95 1 925 3742

INDONESIA

-
Makes & Partners Law Firm
Menara Batavia, 7th Floor
Jl. KH. Mas Mansyur Kav. 126
Jakarta 10220, Indonesia
t +62 21 574 7181
f +62 21 574 7180
w makeslaw.com

MALAYSIA

-
Foong & Partners
Advocates & Solicitors
13-1, Menara 1MK, Kompleks 1 Mont' Kiara
No 1 Jalan Kiara, Mont' Kiara
50480 Kuala Lumpur, Malaysia
t +60 3 6419 0822
f +60 3 6419 0823
w foongpartners.com

MIDDLE EAST

-
Al Aidarous Advocates and Legal Consultants
Abdullah Al Mulla Building, Mezzanine Suite 02
39 Hameem Street (side street of Al Murroor Street)
Al Nahyan Camp Area
P.O. Box No. 71284
Abu Dhabi, UAE
t +971 2 6439 222
f +971 2 6349 229
w aidarous.com

-
Al Aidarous Advocates and Legal Consultants
Oberoi Centre, 13th Floor, Marasi Drive, Business Bay
P.O. Box No. 33299
Dubai, UAE
t +971 4 2828 000
f +971 4 2828 011

PHILIPPINES

-
ZGLaw
27/F 88 Corporate Center
141 Sedeño Street, Salcedo Village
Makati City 1227, Philippines
t +63 2 889 6060
f +63 2 889 6066
w zglaw.com/~zglaw

wongpartnership.com