Fraud, Asset Recovery & Investigations

How the Courts are Dealing with Crypto Disputes – Recent Developments in Crypto Asset Litigation across Jurisdictions

Introduction

The crypto market has been through a tumultuous past year. Within months, the market went from all-time highs to the coldest crypto winter as Three Arrows Capital cratered, spreading a contagion that consumed the likes of Celsius, Voyage, TerraLuna and FTX amongst others. Meanwhile, the industry continues to be ravaged by crypto crime, with Chainalysis reporting crypto scam 'revenue' at US$5.9 billion in 2022 led by 'investment'-type scams.[1] These developments have led to an uptick in crypto litigation.

In this Update, we explore the notable crypto litigation developments in the past year, taking a closer look at significant cases from Singapore, the UK, and the US. We examine how the courts are dealing with key issues in crypto disputes, including issues of jurisdiction, service of court documents, and the duties of blockchain developers and crypto exchanges.

A refinement of the jurisdictional gateways for invoking the court's jurisdiction?

Given the frequently cross-border nature of crypto hacks / scams, victims seeking their local courts' assistance to aid in the recovery of their stolen assets against unknown fraudsters or crypto exchanges based overseas must first demonstrate a good arguable case for invoking the court's jurisdiction over the foreign parties.

Several frequently invoked jurisdictional 'gateways' are based on the stolen crypto asset being located within the local courts' jurisdiction. Until recently, the English courts have generally accepted that there is a good arguable case that the location of intangible crypto assets is deemed to be its *rightful* owner's place of domicile, and therefore based within the jurisdiction of the English courts if the owner is domiciled there. This means the question of whether the crypto assets are located within the local courts' jurisdiction is determined at the time before the assets were stolen from the *rightful* owner and transferred out of jurisdiction.

[1] https://blog.chainalysis.com/reports/2022-crypto-scam-revenue/

Fraud, Asset Recovery & Investigations

In *Osbourne v Persons Unknown* [2023] EWHC 39 ("***Osbourne***"), the purported victim of a hacked MetaMask wallet based in England and Wales sought permission from the English High Court to serve the claim documents abroad on a person in South Africa, whose wallet she had traced her 'stolen' NFT to. She invoked the jurisdictional gateway based on her NFT being located within the Court's jurisdiction. The Court was not inclined to grant permission for service of the claim documents out of jurisdiction under this gateway (though it did so on other grounds), questioning whether the victim was still the NFT owner at the time of the application, as the NFT had at that point already been transferred to the wallet of the person in South Africa and the victim was no longer able to exercise control over the NFT.

This decision in *Osbourne* represents a departure from other decisions made by the English courts. For example:

- In *Fetch.ai Ltd v Persons Unknown* [2021] EWHC 2254, the claimant – an English registered company whose cryptocurrencies had been stolen – sought permission from the English High Court to serve court documents out of jurisdiction on the fraudsters and Binance. The Court granted permission via several jurisdictional gateways grounded on the finding that "*it is at least realistically arguable*" that the claimant's stolen cryptocurrency is located in England. The Court held that the "*test for whether assets are within the jurisdiction … must focus on where the assets were located before the justiciable act occurred*".

- In *D'Aloia v Persons Unknown* [2022] EWHC 1723, the claimant – an English-domiciled individual who had been scammed of his Tether ("**USDT**") and USD Coin ("**USDC**") cryptocurrencies – sought permission from the English High Court to serve court documents out of jurisdiction on the fraudsters and Binance. Similarly, the Court granted permission via several jurisdictional gateways grounded on the finding that "*there is a good arguable case … that the situs of the asset is England*" because "*[t]he evidence is that the claimant was at all material times domiciled in England, and, as such, the USDT and USDC of which he was deprived by the fraudulent misrepresentation of … the persons unknown, was located in England*".

The development in *Osbourne* now present victims with an additional obstacle to secure their stolen assets, which will typically be dissipated to wallets or exchanges based abroad in seconds.

It remains to be seen whether the Singapore courts will adopt the English High Court's approach in determining the stolen crypto asset's location for the purpose of establishing jurisdiction. This issue has not arisen squarely for consideration yet. Instead, the Singapore courts have typically assumed jurisdiction on other bases:

- In *CLM v CLN* [2022] SGHC 46, the Singapore High Court granted the victim of stolen crypto assets permission to serve court documents out of jurisdiction on crypto exchanges and payment service companies on the grounds that they carry on business in Singapore or have assets situated in Singapore (being shares in Singapore-incorporated subsidiaries). Read more about this landmark case that our Fraud, Asset Recovery & Investigations team successfully argued here.

- In *Janesh s/o Rajkumar v Unknown Person* [2022] SGHC 264, the Singapore High Court granted the victim of a stolen NFT permission to serve court documents out of jurisdiction on the unknown wrongdoer based on the "*primary connecting factor*" that the "*claimant was located in Singapore, and carried on his business here*" Read more about this case here.

These alternative jurisdictional gateways that are separate from the location of the stolen crypto assets remain viable options notwithstanding the developments in *Osbourne.*

Service of court documents via NFT airdrop

In litigation, courts generally require claimants to serve court documents on respondents. This is to ensure that respondents are notified of the claim or court order against them and given a chance to respond. Specifically, originating process (*ie*, the claim documents that initiate the litigation) must be served on respondents personally. Where personal service of documents on the respondents is not possible or practicable, for example, where respondents take steps to evade personal service, the courts may permit alternative forms of service, *eg*, via post, advertisement in traditional media, email, direct messaging through social media (Facebook, Instagram etc.) and through messaging apps (WhatsApp, Telegram etc.).

In court proceedings to recover 'stolen' crypto assets, it can be notoriously difficult (or impossible) to serve court documents on the wrongdoers. The nature of crypto 'theft' cases and the obscurity of the blockchain mean the wrongdoers are typically unknown or would evade service, since they would not be interested to engage in the court proceedings.

Courts have recently adopted an innovative solution to address this problem – *Service of court documents via NFT airdrop*:

- In *LCX AG v John Doe Nos. 1-25* (Docket No. 154644/2022), the New York Supreme Court allowed LCX – a crypto exchange victim of a US$8 million hack – to serve the claim documents and injunction orders on the unknown hackers by airdropping a NFT (containing a link to the court documents) to the wallets that the bulk of the stolen assets were traced to. In permitting service via NFT airdrop, the Court noted that "*[c]ommunication through the account using the Service Token is effectively the digital terrain favored by the Doe Defendants*" and "*using a blockchain transaction to communicate with the Doe Defendants is the only available manner of communication*".

- In *D'Aloia v Persons Unknown* [2022] EWHC 1723, the English High Court allowed the victim of a US$2.3 million scam to serve claim documents and injunction orders on the unknown fraudsters by airdropping a NFT to the wallets that the victim had been induced to transfer his USDT and USDC to. The Court noted that permitting service by NFT airdrop "*is likely to lead to*

a greater prospect of those who are behind the [scam] being put on notice of the making of this order, and the commencement of these proceedings".

- In *Jones v Persons Unknown* [2022] EWCH 2543, the English High Court allowed the victim of a £1.5 million "*large scale cyber fraud*" to serve a summary judgment order on the unknown fraudsters and the crypto exchange, Huobi, by airdropping a NFT to the Huobi wallets that Mr Jones had been induced to transfer his Bitcoin ("**BTC**") to. In permitting service by NFT airdrop, the Court noted that these "*are the means most likely to bring the proceedings and this order to the attention of the … defendants and therefore meet the justice of this application*" and "*is appropriate because it is important that the order comes to the attention of the defendants quickly, not least because [the BTC] could be dissipated at any moment simply at the flick of a mouse*".

- In *Benjamin Arthur Bowen v Xingzhao Li* (Case No. 23-cv-20399), the Florida District Court allowed the victim of a US$2.2 million "*sophisticated global internet cryptocurrency fraud and conversion scheme*" to serve claim documents on the known fraudster by airdropping a NFT (containing a notice of the action and a link to a website containing the court documents) to the wallets that the plaintiff had traced his crypto assets to. The Court noted that "*the Defendants conducted their scheme … using cryptocurrency blockchain ledger technology*" and the NFT is "*reasonably calculated to give notice to [the] Defendants*" of the action.

These developments are illustrative of the courts' innovation to combat crypto-related wrongdoing by equipping litigants with faster and surer means of serving documents. It remains to be seen whether the Singapore courts will permit this novel form of service of court documents though we expect this issue to arise for consideration soon.

Blockchain developers may owe token holders fiduciary and tortious duties

In the English case of *Tulip Trading Ltd v Van der Laan* [2023] EWCA Civ 83, Mr Craig White of self-proclaimed 'Satoshi Nakamoto' fame (a.k.a the creator of Bitcoin) sued the developers of various Bitcoin networks through his company, Tulip. Tulip claimed to own around £3 billion worth of BTC but had lost the private keys to the two wallets holding the BTC in a hack, without which it could not access the BTC. Tulip also claimed "*it would be a simple matter*" for the developers of the Bitcoin networks to move Tulips' BTC to another address which Tulip could control. Tulip contended the developers owed Tulip fiduciary and tortious duties in relation to the BTC in the two wallets, which obliged them to introduce new code to transfer the BTC in the two wallets (to which the private keys had been lost) to a new address that Tulip could access or provide a patch to issue replacement private keys for the two wallets to Tulip.

In a preliminary decision determining that English courts are the appropriate forum to determine the dispute, the English Court of Appeal held there was a "*realistic argument*" that network developers are

fiduciaries and owed fiduciary duties to cryptocurrency owners including a duty of single-minded loyalty to the users of the Bitcoin software. This duty may oblige developers to not act in their own self interest and to introduce code so that an owner's bitcoin can be transferred to safety in the circumstances that Tulip alleged.

The English Court of Appeal's findings are tentative and remain to be conclusively determined at the trial of Tulip's claims slated to take place in 2024. The outcome of this case should be watched closely as it concerns the fundamental nature of blockchain, and will have significant implications for the crypto and web3 industry. Developers would do well to review the terms and conditions for their token issuances and tighten the exclusionary clauses in the meantime.

Crypto exchange found to be constructive trustee of stolen crypto assets

In *Jones v Persons Unknown* [2022] EWHC 2543, the victim of a £1.5 million "*large scale cyber fraud*" – sought an order against the crypto exchange, Huobi, for the delivery up of his stolen BTC that had been traced to a wallet controlled by the exchange. In granting the victim summary judgment, the English High Court found that Huobi held the BTC on constructive trust for the victim given that it controlled the wallet that received the BTC, and there was no claim by Huobi or any other party to the BTC that may override the victim's interest in the BTC. On that basis, the Court ordered Huobi to deliver up the BTC to the victim.

This case is the first reported instance of a court imposing a constructive trust on a third party to the fraud (in this case, a crypto exchange) and ordering the third party to deliver up the stolen crypto assets to the victim. These developments are significant for:

- victims of crypto fraud / hacks, who now have clearer recourse against crypto exchanges and potentially other third parties to recover their crypto assets; and

- crypto exchanges and other custodians of crypto assets, not just in terms of liability to return the tainted crypto assets to the victims but possibly exposure for other duties as constructive trustee, for example, to account for profits made using the tainted crypto assets.

Invoking the doctrine of illegality to resist enforcement of peer-to-peer cryptocurrency sale and purchase agreement

One of the grounds to resist enforcement of a contract is illegality, for example, where the contract itself is illegal or where the contract itself is not illegal but has an illegal objective, such that it would be contrary to law and public policy to enforce the performance of the contract.

In the Singapore High Court case of *Rio Christofle v Malcolm Tan Chun Chuen* [2023] SGHC 66, the plaintiff (through his company) and the defendant (through his company) entered into a peer-to-peer ("**PTP**") agreement for the plaintiff's company (the "**Seller**") to sell BTC to the defendant's company (the "**Intermediary**"). The Intermediary would in turn on-sell the acquired BTC to an ultimate buyer ("**Buyer**") via a separate PTP BTC sale and purchase agreement and receive an administration fee for facilitating the transaction.

Following the transfer of the BTC, a dispute arose amongst the parties. The Seller transferred the BTC to the Intermediary, which in turn transferred the BTC to the Buyer. However, the Buyer claimed to not have received the BTC from the Intermediary and therefore declined to pay the purchase price to the Intermediary, who in turn did not pay the same to the Seller. The Plaintiff sued the Defendant for recovery of the purchase price. To resist enforcement of the sale and purchase agreement, the Defendant argued that the agreement was void for illegality as the Plaintiff and his company were not licenced to operate as a payment service provider under section 5 of the Payment Services Act ("**PSA**"), which prohibits the carrying on of business of providing payment services in Singapore without a licence.

As a starting point, the Court found that: (a) BTC and other similar cryptocurrencies constituted digital payment tokens under the PSA; (b) the sale and purchase of cryptocurrencies in return for money or other cryptocurrencies constituted digital payment token services under the PSA; and (c) the carrying on of business of selling and purchasing of BTC without the requisite licence would be a breach of the PSA.

Nonetheless, the Court rejected the Intermediary's argument on the facts. The Court found that the sale and purchase agreement itself was not illegal as it was not prohibited by the PSA. The Court also found that the Seller was not carrying on a business of providing digital payment services – the Seller was merely selling BTC in its possession to the Intermediary. Crucially, the Seller was not acting as an intermediary itself, which the Court regarded as "*an important factor that distinguishes bona fide trading in cryptocurrencies from providing an unlicensed digital payment token service which would expose one to criminal liability under s 5 of the PSA*". Therefore, the sale and purchase agreement between the Seller and the Intermediary did not have an illegal object.

This case is significant as it is the first reported decision in Singapore where crypto actors have sought to have a sale and purchase agreement for crypto assets voided for illegality and made enforceable by claiming the agreement breaches the PSA. While the argument failed on the facts, the case illustrates that Singapore courts accept such arguments in-principle and may affirmatively apply in the appropriate future case.

Concluding words

Crypto disputes, having come into more recent prominence, are the source of much developing law. Across jurisdictions, courts are assessing how best to manage the various unique issues associated with crypto disputes, including issues of civil procedure, enforceability, and the duties of the parties

involved. While the decisions highlighted above demonstrate the ingenuity and flexibility of the courts, they also show that the law in this regard is still in the process of development. Parties to crypto arrangements should thus be aware of the emerging law and how it may affect their rights and obligations.

For further queries, please feel free to contact our team below.

Contacts

Jansen Chow
Co-Head, Fraud, Asset Recovery & Investigations
Commercial Litigation

T +65 6232 0624

jansen.chow@rajahtann.com

Foo Xian Fong
Senior Associate,
Commercial Litigation

T +65 6232 0232

xian.fong.foo@rajahtann.com

Please feel free to also contact Knowledge and Risk Management at eOASIS@rajahtann.com

Regional Contacts

R&T SOK & HENG | *Cambodia*
R&T Sok & Heng Law Office
T +855 23 963 112 / 113
F +855 23 963 116
kh.rajahtannasia.com

RAJAH & TANN 立杰上海
SHANGHAI REPRESENTATIVE OFFICE | *China*
Rajah & Tann Singapore LLP
Shanghai Representative Office
T +86 21 6120 8818
F +86 21 6120 8820
cn.rajahtannasia.com

ASSEGAF HAMZAH & PARTNERS | *Indonesia*
Assegaf Hamzah & Partners

Jakarta Office
T +62 21 2555 7800
F +62 21 2555 7899

Surabaya Office
T +62 31 5116 4550
F +62 31 5116 4560
www.ahp.co.id

RAJAH & TANN | *Lao PDR*
Rajah & Tann (Laos) Co., Ltd.
T +856 21 454 239
F +856 21 285 261
la.rajahtannasia.com

CHRISTOPHER & LEE ONG | *Malaysia*
Christopher & Lee Ong
T +60 3 2273 1919
F +60 3 2273 8310
www.christopherleeong.com

RAJAH & TANN | *Myanmar*
Rajah & Tann Myanmar Company Limited
T +95 1 9345 343 / +95 1 9345 346
F +95 1 9345 348
mm.rajahtannasia.com

GATMAYTAN YAP PATACSIL GUTIERREZ & PROTACIO (C&G LAW) | *Philippines*
Gatmaytan Yap Patacsil Gutierrez & Protacio (C&G Law)
T +632 8894 0377 to 79 / +632 8894 4931 to 32
F +632 8552 1977 to 78
www.cagatlaw.com

RAJAH & TANN | *Singapore*
Rajah & Tann Singapore LLP
T +65 6535 3600
sg.rajahtannasia.com

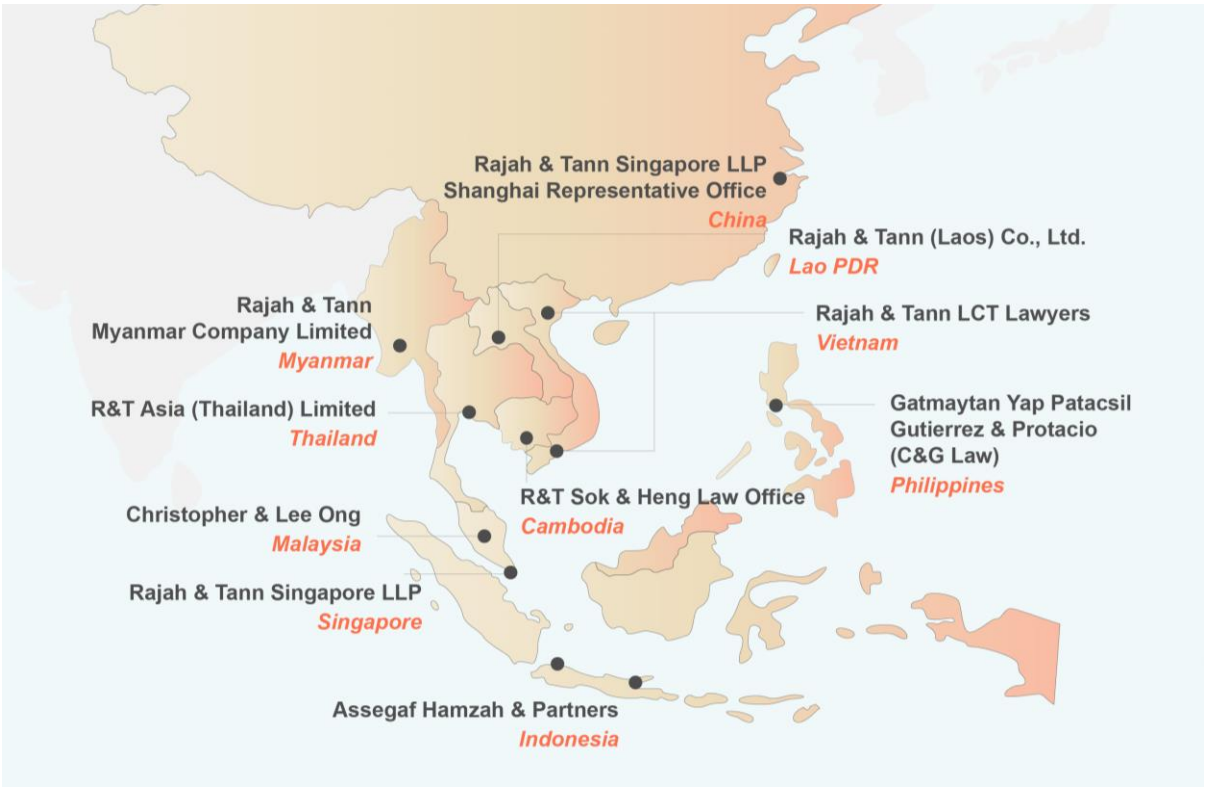
RAJAH & TANN | *Thailand*
R&T Asia (Thailand) Limited
T +66 2 656 1991
F +66 2 656 0833
th.rajahtannasia.com

RAJAH & TANN LCT LAWYERS | *Vietnam*
Rajah & Tann LCT Lawyers

Ho Chi Minh City Office
T +84 28 3821 2382 / +84 28 3821 2673
F +84 28 3520 8206

Hanoi Office
T +84 24 3267 6127
F +84 24 3267 6128
www.rajahtannlct.com

Our Regional Presence



Rajah & Tann Singapore LLP is one of the largest full-service law firms in Singapore, providing high quality advice to an impressive list of clients. We place strong emphasis on promptness, accessibility and reliability in dealing with clients. At the same time, the firm strives towards a practical yet creative approach in dealing with business and commercial problems. As the Singapore member firm of the Lex Mundi Network, we are able to offer access to excellent legal expertise in more than 100 countries.

Rajah & Tann Singapore LLP is part of Rajah & Tann Asia, a network of local law firms in Cambodia, China, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam. Our Asian network also includes regional desks focused on Brunei, Japan and South Asia.