Navigating the Complexities of Cryptocurrency Fraud: Recovery of Stolen Assets in respect of USDT (Tether)

Lionel Chan
Partner, Litigation & Dispute Resolution

Navigating the Complexities of Cryptocurrency Fraud: Recovery of Stolen Assets in respect of USDT (Tether)

Recovering stolen cryptocurrency is challenging due to the decentralized nature of many cryptocurrency assets, the irreversible nature of such transactions, and the pseudonymity aspect. This makes it difficult to identify the fraudsters and to trace and reverse cryptocurrency transactions.

Victims of these cryptocurrency frauds will often need to wait for the assets to be moved by the fraudsters to centralized cryptocurrency exchanges or Virtual Assets Service Providers ("**VASPs**") to freeze and recover the stolen assets. However, and even then, lack of regulation, slow legal processes, and challenges in cross-jurisdictional issues can delay recovery. Additionally, fraudsters use techniques like mixers, tumblers, and privacy coins to obscure the source and movement of stolen funds. These elements make recovering stolen cryptocurrency difficult.

Increasingly, there has been a surge in the use of stablecoins, and in particular, USDT (Tether).

When it comes to the tracing and recovery of the USDT, its features provide several unique advantages in the recovery of stolen cryptocurrency compared to other decentralized cryptocurrencies like Bitcoin (BTC) or Ethereum (ETH). These stem from USDT's centralized nature and specific features designed to enhance traceability and control, as will be explored in this article.

1. How Centralised Cryptocurrency Exchanges / VASPs Assist in Recovering Stolen Cryptocurrency

Centralized VASPs collect and retain Know Your Customer ("**KYC**") information and have powers over the cryptocurrency wallets in their custody. This allows them to freeze cryptocurrency wallets in their custody and to provide information regarding their customers.

These powers are contractually stipulated in the user agreements and generally include a discretion for the centralized VASPs to freeze funds in the wallets in their custody on their own volition.

2. Fraud and Asset Recovery in Law

Laundering processes include mixing stolen assets with "clean" cryptocurrency, which are designed to distance the funds from their source and make them difficult to trace. When fraudsters are satisfied with how "clean" the stolen funds appear—or with how muddied the transaction trail has become—they will "cash out" by passing the stolen funds through a VASP, converting them into fiat currency (e.g. US dollars) to preserve their value.

The legal process for recovering stolen crypto assets can be broken down into the following stages:

(a) Stage One: Identify and Trace

When it has been determined that cryptocurrency has been misappropriated by fraudsters, it is crucial to act swiftly—first to identify the stolen assets and determine their latest whereabouts. This is typically done with the assistance of specialized crypto-tracing firms using blockchain analysis and forensic investigation techniques.

(b) Stage Two: Obtain Court Orders to Freeze Assets and Obtain Disclosure

In Singapore, the High Court in *ByBit Fintech Ltd v Ho Kai Xin* [2023] 5 SLR 1748 confirmed that proprietary injunctions can be made to claim ownership over stolen cryptocurrency. Therefore, once the stolen cryptocurrency is identified and traced to a VASP, the next step is to secure the funds quickly. This includes obtaining freezing injunctions against the crypto wallets held with recipient VASPs.

Disclosure orders should also be sought against the VASPs to obtain information about the identities of the customers and to further trace the movement of the stolen funds.

These court orders should be pursued soonest to prevent further transfers or dissipation, to aid in the further tracing of the funds, and to identify the fraudsters.

A common challenge in such proceedings is the fact that the fraudsters are persons whose identities are unknown. In Singapore, in *CLM v CLN and others [2022] SGHC 46* ("***CLM v CLN***") it was held that it is not a contravention of the Singapore Rules of Court 2021 to grant injunctive relief, including ancillary disclosure orders against "persons unknown". The Singapore Courts do not require the defendant to be specifically named in crypto fraud proceedings. However, the description of the defendant must be sufficiently certain to identify both those who are included and those who are not.

(c) Stage Three: Enforcement of Court Orders

Service of court orders on the VASPs may be challenging if they are located out of jurisdiction as there will be the added hurdle of seeking recognition and enforcement of the orders in the relevant foreign court. This will necessarily involve additional time, costs, and legal complexity, especially in jurisdictions with stricter rules on recognition of foreign-issued orders, or where the legal framework around virtual assets is still developing. VASPs may be based in different legal systems and are therefore subject to varying compliance standards. Some exchanges are more accommodating than others.

In practice, many of the crypto exchanges and VASPs—particularly those with global reputations or substantial market capitalization—have demonstrated a willingness to comply with court orders voluntarily, sometimes even without the need for formal recognition proceedings. Where the likelihood of voluntary compliance by a VASP is high, it is important to engage them in negotiations proactively with the force of court orders to encourage compliance and cooperation in returning the funds.

3. The Reasons for The Popularity of Stablecoins

(a) Value-Retaining Cryptocurrency

Stablecoins have become an increasingly attractive option for users looking for stability and liquidity. Unlike other cryptocurrencies, stablecoins are designed to be pegged to fiat currencies, typically the US dollar. They are also designed to maintain consistent value, providing a safeguard against market volatility that characterizes traditional cryptocurrencies like BTC or ETH. While BTC and ETH are subject to significant price fluctuations, stablecoins offer a comparatively more reliable alternative (albeit there are also risks of depegging), making them particularly appealing to users who wish to avoid depreciation and ensure that the value of their assets is preserved.

(b) Liquidity

Compared to other cryptocurrencies, stablecoins offer high liquidity and are generally easily convertible to fiat currency across a wide range of platforms, including the major cryptocurrency exchanges. Its widespread acceptance ensures that users can quickly transfer funds across borders, avoiding the limitations of less widely accepted cryptocurrencies. For users, this liquidity makes stablecoins the preferred choice for transactions that require efficiency, stability, and global usability.

4. How Fraudsters Abuse These Features

While stablecoins offer clear benefits for users, these very same features also make them attractive tools for fraudsters. According to a United Nations Report on Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat (2024), USDT is the preferred asset of money laundering and organized crime in East and Southeast Asia.

(a) Preserves Value of Stolen Assets

Fraudsters often convert the stolen assets into stablecoins to preserve their value. Stablecoins provide a way for criminals to "lock in" the value of stolen funds without being exposed to price fluctuations common to other cryptocurrencies.

(b) Obfuscation

Due to its high liquidity, stablecoins have increasingly become a crucial instrument in layering and obfuscation techniques. Stablecoins, and in particular USDT, can be traded with relative ease across a range of centralized and decentralized platforms, including exchanges with less robust KYC enforcement. Criminals may transfer stolen funds through multiple wallets and decentralized finance ("**DeFi**") platforms, engaging in cross-chain transactions to muddy the transaction trail. This makes tracing more resource-intensive and increases the chances that the funds will be successfully laundered before law enforcement or victims can intervene.

5. Unique Advantages for Recovery of USDT

(a) Backdoor Programming

USDT, like certain other centralised stablecoins, offers a unique advantage to victims of crypto fraud. Unlike traditional decentralised cryptocurrencies, where victims often must wait for stolen assets to reach exchanges before initiating recovery, USDT incorporates an internally programmed "backdoor" feature that enables early intervention.

(b) Correction at Wallet-level

Tether can freeze, burn, and/or reissue the USDT back to its rightful owner directly at the wallet level. This "backdoor" mechanism circumvents the uncertain and sometimes lengthy wait for fraudsters to move the assets into an exchange. As a result, USDT provides victims with an additional recovery route and increases the likelihood of recovering stolen assets swiftly. By freezing a wallet, Tether (the issuer of USDT) disables the "send USDT" function, thereby preventing further dissipation and dilution of the stolen funds until the freeze is lifted.

In their October 2023 Press Release, Tether reported that it had assisted 31 agencies globally in investigations spanning 19 jurisdictions, leading to the freezing of a total of US$835 million, primarily linked to theft. More recently, in May 2024, it was also reported that Tether had frozen US$5.2 million worth of USDT due to its connection to phishing scams, demonstrating its willingness to cooperate with the authorities. Given their willingness to cooperate with the authorities, it is likely that Tether will comply with freezing and disclosure orders issued by the Court.

6. Conclusion

The centralized nature of USDT, combined with Tether's control mechanisms, enhanced traceability, and demonstrated cooperation with the authorities, offers significant advantages in the recovery of stolen cryptocurrency. These features allow for an additional and faster recovery process compared to other decentralized cryptocurrencies, and which should therefore be considered and discussed in seeking to recover stolen cryptocurrency.

This article was authored by our Partner Lionel Chan. The author thanks Legal Trainee Nicolle Cheung for her assistance with the article.

Oon & Bazul LLP is a leading crypto law firm in Singapore, specializing in crypto fraud and asset recovery, restructuring, and dispute resolution. Our experienced cryptocurrency lawyers in Singapore provide strategic guidance on regulatory, insolvency, and tax challenges, ensuring compliance and asset protection.

As a trusted blockchain law firm, our team of crypto lawyers, including crypto litigation lawyers and crypto recovery lawyers, are skilled in mediation, arbitration, and litigation, offering effective solutions to protect our clients' interests in this rapidly evolving sector.

You may visit our Blockchain & Cryptocurrency page to learn more about our practice: ***https://oonbazul.com/blockchain-cryptocurrency-disputes/***

If you require any legal advice on related matters, please do not hesitate to get in touch with us.