DIGITAL ASSET FRAUD AND ASSET TRACING: AN UPDATE FROM THE BRITISH VIRGIN ISLANDS

Authored by: Christopher Pease, Megan Elms – Harneys and James Drury - Kalo

The BVI is a popular jurisdiction for companies providing services relating to cryptocurrencies and digital assets. It is home to various exchanges, token issuers, blockchain projects and crypto funds. Inevitably, there are an increasing number of related disputes with a BVI nexus.

While the nature of these disputes can be wide-ranging, a common theme is beginning to emerge: smart contracts are being exploited by hackers and used to misappropriate tokens; stolen tokens are transferred through numerous wallets, in a series of transactions, to disguise their origin. The use of decentralised 'mixer' protocols often play an important role in this process.

The recent case of ChainSwap v Persons Unknown is a prime example of how blockchain analysis can be combined with well-established asset tracing and recovery tools and court remedies to meet the challenges thrown up in this relatively new arena. Harneys and Kalo acted for ChainSwap, the successful claimant.

An increasingly familiar tale

The facts in the ChainSwap case demonstrate how tokens can be stolen pursuant to the hacking or exploitation of smart contracts that are used to provide blockchain services.

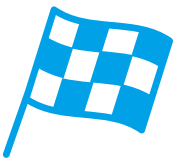
In this case, a smart contract allowed ChainSwap's users to transfer tokens across blockchains (known as a cross-chain bridge). The smart contract would receive the tokens to be 'transferred' and would send them to a 'vault wallet' where they would be locked away or 'burned', following which an equivalent token would be minted on the 'receiving' blockchain and deposited into the user's designated wallet. As is typical for smart contracts, the code underpinning it was open- source and could be viewed publicly.

The smart contract was exploited on two separate occasions, roughly a week apart, in July 2021.

Following the first hack, tokens received by the smart contract were sent to a wallet designated by the hacker(s) rather than the vault wallet. Tokens were then drawn into the smart contract from user wallets that had been pre-authorised to interact with the bridge, without the users' authorisation. The result was that the hacker(s) diverted tokens from user wallets into his/her own wallet.

As part of the second hack, the smart contract's requirement for tokens received into the vault wallet to tally with those being minted was removed. This allowed the hacker(s) to mint substantial numbers of tokens and direct them into their own wallet (the initial transfers were sent to the same wallet that had been used as part of the first hack, but the majority were sent to a second wallet owned by the hacker(s)).

Affected users and projects were compensated, leaving ChainSwap seeking to recover the loss from an unknown wrongdoer or wrongdoers.



The starting point

As is the case for the most widely used blockchains, the transactions pursuant to which tokens had been stolen by the hackers were recorded permanently and could be viewed publicly.

With the use of blockchain explorers, such as Etherscan, it was possible to identify that the hacker(s)had exchanged many of the stolen tokens for stablecoins (a digital token designed to be pegged at a fixed rate to fiat currency), which had then been transferred to other wallets and exchanges.

This preliminary analysis informed what further steps could be taken to trace and recover the tokens or their equivalent value.

Token functionality

One type of stablecoin that the hacker(s) acquired with the stolen tokens, and which therefore became the proceeds of the wrongdoing, could be 'burned' (i.e. permanently locked or disabled) by the token issuer, wherever held. This meant that the token issuer could reissue the same number of tokens to another wallet.

This function was used effectively in this case: ChainSwap satisfied the token issuer that the hacker(s) was not the rightful owner of the tokens in question (because they could be traced back to the hacks) and provided appropriate assurances to allow the token issuer to burn the tokens in the hands of the hacker(s) and re-issue tokens to ChainSwap. It provided an effective and efficient method of remedying (in part) the loss caused by the hacking.

Tracing through a mixer

Further blockchain analysis revealed that a significant portion of the remaining proceeds from the hacks had been routed through Tornado Cash, which provides a mixing service (also known simply as a 'mixer' or 'tumbler').

Tornado Cash describes itself as a fully decentralised protocol for private transactions. Users transfer tokens to the Tornado Cash smart contract by sending them to a receiving wallet, which mixes the tokens with those belonging to other users. Upon transferring tokens, users receive a code. When the user elects to withdraw the tokens they provide the code and nominate a different wallet into which a new token can be sent. The paying or outgoing Tornado Cash wallet will then pay out the tokens, less a small proportion of the tokens which are sent to different wallet as a 'relay fee'. The intended effect is to break the link in transactions of tokens and obfuscate the origin of the tokens exiting Tornado Cash.

While not inherently improper, mixers provide hackers and fraudsters with a useful tool for laundering the proceeds of their wrongdoing. Their decentralised nature (they run purely on algorithms) and the ease with which they can be accessed means that they are a common hurdle to overcome when tracing the proceeds of hacks.

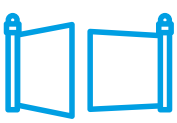
One would be forgiven for losing hope of tracing and recovering digital assets that pass through mixers. The common perception is that they are impenetrable. However, the permanent ledger of all transactions in and out of Tornado Cash is an important counter-balance and one that can be used highly effectively with the right forensic tools.

ChainSwap's legal advisors, Harneys, teamed up with Kalo, who boast a deep knowledge of digital assets and blockchain data analytics, with a view to proving that it was possible to trace assets through a mixer.

Using bespoke software and forensic analysis, Kalo identified transfers out of Tornado Cash that very closely matched the numerous transfers that the hacker(s) had made in (via numerous wallets).

Kalo set out their findings in a comprehensive forensic investigative report detailing the web of transactions, transaction hashes and wallet addresses used.

It concluded that, given the number and size of payments in and out of Tornado Cash and the time between them, it was more likely than not that the transfers out to a separate wallet were related to the payments in from the wallets that were known to be associated with the hacker(s).



Identifying the gateway

The ability to identify the new wallet, which received the tokens from Tornado Cash, as likely belonging to the hacker(s) meant that subsequent transactions could be analysed. These included transactions with a centralised exchange based in Croatia. Whilst the exchange was unable to provide material information voluntarily, it was clear that it would be required to hold information that would reveal the identity of those using its services, as well as details of any bank accounts into which payments had been received from a sale of digital tokens..

It is unsurprising that the hacker(s) sought to use a centralised exchange at some point during the chain of transactions.

Exchanges continue to be the primary avenue for the exchange of fiat currency and digital assets – whether purchasing crypto (on-ramping) or selling crypto in exchange for fiat currency (off-ramping).

They provide the necessary gateways for entering and exiting the self-contained blockchain universe.

These gateways, and the information they hold, will often provide the key to unlocking crypto recovery cases.

Familiar tools in a brave new world

Having identified that a wallet belonging to the hacker(s) had interacted with the Croatian exchange, ChainSwap commenced legal proceedings against the unknown hacker(s)in the BVI seeking compensation for tortious wrongs and/or restitution of unlawful gains.

In addition to the main underlying claim, ChainSwap applied to freeze the assets of the unknown hacker(s), particularly anything held in the hacker'swallets.

ChainSwap also sought disclosure of information from the Croatian exchange via a letter of request from the BVI Court, which would reveal the identity of the hacker and any bank accounts used to receive fiat currency. Whilst other courts have recently been willing to grant third party disclosure orders directly against entities out of the jurisdiction, there was doubt as to whether the exchange would comply with such an order in this instance.

ChainSwap also commenced other investigations and proceedings, including in other jurisdictions, to obtain further information and with a view to speeding up the recovery process.

Pursuing "persons unknown"

Legal proceedings can be commenced, and interim relief sought, against unknown persons. However, to do so a claimant must define the defendant(s) in a way that:

1 Makes it possible to determine those that fall within the class of persons and those that fall outside of it; and

2 Allows the defendant(s) to be served with the claim or application.

In this case the categories of persons being pursued were: (i) those responsible the initial hacking or exploits of the smart contract; (ii) those that had received the tokens diverted pursuant to the hacking; and (iii) those that had received, dissipated and attempted to launder the proceeds of the hacks. In reality, the same person or people were likely to make up all three categories.

ChainSwap had been able to obtain an email address that was believed to be associated with category (i). Those in categories (ii) and (iii) could be identified by reference to digital wallet addresses and their interaction with the Croatian exchange. Accordingly, the defendants in this case were sufficiently identifiable.

Interim relief

The BVI Commercial Court was persuaded that this was an appropriate case in which to grant a freezing order and to issue a letter of request to the Croatian authorities seeking information from the Croatian exchange. It granted the relief ex parte and on an urgent basis (within a day of the application having been filed).

Importantly, the BVI Court also permitted the claim and other documents to be served on the hacker(s) via: (i) the email address; and (ii) the Croatian exchange, on the basis that the exchange was believed to hold contact information for the hacker(s).

Despite the hacker(s) acknowledging that they had received the served documents, they did not appear at the return date for the continuation of the freezing order. The court's judgment in respect of the return date hearing is available here.

The importance of identifying pseudonymous actors

Through its various legal actions, ChainSwap was closing in on uncovering the identity of the hacker(s).

The pseudonymous nature of crypto ownership means that whilst bad actors can hide behind obscurity, if and when their real identity is revealed, all transactions associated with them will be laid bare. This should be of particular concern to those that have carried out numerous hacking attacks that appear to be unconnected: once exchange accounts and digital wallets are revealed to belong to a hacker, blockchain records can be analysed to determine where else tokens have come from. Obscurity can be a hacker's greatest asset; revealing their identity their greatest weakness. There is also a question as to who else might be exposed in what might be a wider network of wrongdoing.

It is unsurprising then that with the walls closing in the hacker(s) made contact and sought to settle the claim on condition of remaining anonymous, demonstrating the leverage to be gained by obtaining (or even just seeking) information.

Conclusion

As the use of digital assets continue to increase worldwide, the BVI's nexus to multiple exchanges, token issuers and projects suggests it will be a key jurisdiction for disputes in the sector.

The ChainSwap matter, which is a landmark case in the BVI, is a welcome decision which demonstrates that the BVI, including its courts, are on top of the issues posed by digital asset fraud and offers a variety of tools to overcome them.

There are of course key variables in any crypto recovery case and every case is likely to differ in terms of complexity of the tracing exercise and the practical and legal steps that should be taken to achieve recovery, The methods used by wrongdoers to obfuscate transfers of digital assets and obstruct tracing exercises are becoming far more sophisticated. Legal advisors and forensic experts need to adapt their tracing and recovery tools and techniques to keep pace.