



 DREW & NAPIER

Legal Update

*Blocked on the blockchain? -
Hacking of Digital Assets and
Enforcement Actions*

3 December 2021

**LEGAL
UPDATE**

In this Update

As of October 2021, the market capitalisation of the digital assets market stood at over US\$2.74 trillion, with Bitcoin reclaiming its US\$1 trillion market value in October 2021. As digital assets rise in prominence as a new asset class, it has become the target of several high-profile hacks.

Given the limited insurance coverage available (if any at all) for theft or loss of digital assets, this article explores the technologies enabling these hacks, and the legal and practical enforcement difficulties with the recovery of stolen cryptocurrency and other digital assets (except non-fungible tokens) from such bad actors in Singapore and around the world.

03
INTRODUCTION

03
TECHNICAL ISSUES WITH TRACING DIGITAL ASSETS

04
APPLICABILITY OF LEGAL REMEDIES – INJUNCTIONS

06
TECHNICAL AND NON-LEGAL REMEDIES

07
CONCLUSION

INTRODUCTION

KEYPOINT

This article discusses the potential legal issues to be considered when seeking to recover stolen digital assets (excluding non-fungible tokens) under Singapore law.

Successful digital assets hacks have made the headlines several times in recent months. It is estimated that in 2020, over US\$1.9 billion worth of digital assets was stolen by bad actors. In August 2021, hackers successfully hacked decentralised finance platform Poly Network, making off with US\$600 million worth of digital assets. Whilst the stolen funds were eventually returned by the hacker, the fact that the vulnerability could have been and was indeed exploited highlights the very real risk users are taking on when they invest in digital assets. In the same month, one of the largest digital asset exchanges in the world, Binance, was ordered by a UK High Court judge to take steps to identify hackers and freeze their accounts following a hack of a user's account.

This has led to an increased spotlight on the practicalities of retrieving such stolen digital assets, as well as the effectiveness of available legal remedies.

TECHNICAL ISSUES WITH TRACING DIGITAL ASSETS

One of the primary difficulties with recovering stolen digital assets (except non-fungible tokens) lies in successfully tracing the stolen assets.

Bitcoin, as the classic example of cryptocurrency, is, at its essence, computer code that records transactions between users. There is no fixed data set with non-fungible information for each coin, but rather a record of inputs and outputs for every transaction. As no personal information is recorded on addresses, and users are encouraged to generate a new address with every transaction, the number of addresses involved multiply exponentially as the number of transactions increase. More addresses mean more time, effort and possibly costs are required to trace the digital assets. The use of exchanges also complicates the matter, as they generally consolidate transactions into a single transaction with multiple inputs and outputs netted off.

Given the speed at which digital assets can be dispersed, time is usually of crucial importance when tracing stolen digital assets. For example, time is spent identifying the hacked wallet addresses, blacklisting the hacker's wallet address and subsequently broadcasting such information to other exchanges, which are steps that may provide some assistance in limiting the movement and cashing out of such stolen funds. Unfortunately, in the hack on the Liquid exchange in August this year, the hackers were able to get these funds out faster than the exchanges were able to react.

However, the law (even while still developing) may assist in preventing and tracing such hacks.

APPLICABILITY OF LEGAL REMEDIES – INJUNCTIONS

Where a bad actor has made away with stolen property, the first legal remedy is typically an interim injunction. In Singapore, a freezing injunction or order (also known as a Mareva injunction) is often the first port of call. In simple terms, it is a court order which freezes a person's assets and seeks to prevent the dissipation of funds and assets which could frustrate an anticipated judgment. In addition, proprietary injunctions may also be sought to restrain a party from dealing with assets which are alleged not to belong to the party, so that he cannot dispose of them to defeat a claim against him.

Applying these injunctions to the context of digital assets will require consideration of various issues. For example, a prerequisite for obtaining a proprietary injunction is to establish a proprietary claim. The nature of cryptocurrency and whether it is a type of property has yet to be definitively affirmed in many jurisdictions. In Singapore, the Singapore International Commercial Court (“**SICC**”) in *B2C2 Ltd v Quoine Pte Ltd* [2019] SGHC(I) 03 found at first instance that cryptocurrency satisfied the traditional definition of a property right as established in *National Provincial Bank v Ainsworth* [1965] 1 AC 1175, that is, it is identifiable and definable by third parties, capable in its nature of assumption by third parties and has some degree of permanence or stability. On appeal, the Singapore Court of Appeal (“**SGCA**”) appeared to incline towards the SICC's finding on the nature of cryptocurrency as property, but eventually found that based on the present case, it was not necessary for the SGCA to come to a final position as to whether cryptocurrency constituted property, and if so, the type of property involved. Hence, while the SGCA's statement is encouraging, until the above is tested in the Singapore courts, it is difficult to definitively assert that a proprietary injunction can be granted over digital assets like cryptocurrency in Singapore.

There are also potential difficulties with satisfying the jurisdictional requirements for injunctions. As transactions of digital assets like cryptocurrency are often cross-border in nature, questions arise as to whether it is necessary to seek leave out of jurisdiction, and how a court may establish its jurisdiction over the parties. While Singapore jurisprudence continues to develop, we may seek guidance from foreign decisions. In *Ion Science Ltd v Persons Unknown* (UK, unreported, 21 December 2020), where injunctions were sought by claimants who had allegedly been induced by unknown persons to transfer Bitcoin to invest in legitimate cryptocurrency products, the UK High Court applied the traditional approach that (i) there must be a serious issue to be tried; (ii) there should be a good arguable case; and (iii) whether the UK was the appropriate forum for the dispute. With reference to the issue of the forum, in the absence of clarity on the *lex situs* of the crypto assets, the judge held that the UK was the appropriate forum as the UK was the place where the damage had occurred:

- (i) The account that funded the Bitcoin was from the UK.
- (ii) The assets were taken from the claimants' control in the UK.
- (iii) The Bitcoin was located in the UK, as the place where the claimants were domiciled.
- (iv) The computer used to purchase the alleged cryptocurrency products was in the UK.

Perhaps an additional difficulty is ascertaining the person against whom the injunction can be filed, given the high degree of anonymity in the cryptocurrency industry. That said, this difficulty is surmountable and courts in other jurisdictions have applied a pragmatic approach when handling matters relating to hacked or stolen digital assets like cryptocurrencies. As an example, the court in *Fetch.ai Ltd and another v Persons Unknown Category A and others* [2021] EWHC 2254 ("**Fetch.ai**"), which involved a cryptocurrency fraud over trades on the Binance cryptocurrency exchange platform, recognised that the material generated by the Binance group of companies concerning which entities conduct what business was "opaque". Fortunately, this did not prevent disclosure orders from being granted by the UK court against Binance Holdings Limited (a Cayman Island entity) and Binance Markets Limited (a UK entity) which might be able to assist with tracing claims and identification of the wrongdoers. Additionally, the court decided that freezing orders against Binance were also appropriate because Binance had indicated that, in the absence of such orders, it might not maintain the freezing arrangement it had already provided an account that held some of the proceeds of the fraud. The court's willingness to grant the relevant disclosure orders

against the Binance entities would be an important step towards allowing the plaintiff to identify the unknown fraudsters.

In the same decision, the UK court also issued injunctions against categories of “persons unknown”, in recognition of the difficulty of identifying the bad actors in digital asset fraud. The concept of issuing injunctions against “persons unknown” has gained traction in the UK in recent years. Singapore has not invoked the concept of a “persons unknown” injunction yet, but it appears that existing legislation is at least not closed to the possibility – there is no express requirement in Singapore’s civil procedure rules that a defendant be identified before the high court grants an interim injunction. Whether the Singapore courts are willing to accept writs or originating summonses without a named defendant given the circumstances of the case, or to elect to cure any deemed procedural defect relating to the identity (or lack thereof) of the defendants, is yet to be tested in court. That said, other common law jurisdictions such as Hong Kong and Malaysia have also granted injunctive relief against “persons unknown”, and Singapore courts may elect to take guidance from developments in these jurisdictions when the opportunity arises to decide on such a matter.

Even then, a “persons unknown” injunction (if granted) is only a stopgap measure as actual defendants will need to be named by the time the trial commences. That said, getting such an injunction may still play a pivotal role as one of the first steps to be taken in stakeholders’ overall strategy, when it comes to identifying fraudsters and preventing and reducing the dissipation of assets. While not a panacea for digital asset hacks, it is one more tool in victims’ and stakeholders’ arsenals. Thus far, judicial statements inclining towards recognising cryptocurrency or other digital assets as property, and the willingness to utilise relatively newer forms of injunctions such as the “persons unknown” injunction in the UK, are indeed encouraging signs that the traditional legal tools against fraud may also develop and serve as effective and accessible tools in the context of hacks of digital assets regionally and in Singapore.

TECHNICAL AND NON-LEGAL REMEDIES

In addition to applying legal remedies, perhaps the most immediate step when notified of a hack is to call upon the industry to band against these bad actors. Poly Network, following the historic hack, immediately published a list of addresses to which the stolen funds had been transferred and called on exchanges and miners to “blacklist” transactions and tokens coming from the addresses. In response, the issuer of Tether (USDT), used a build-in failsafe to freeze US\$33 million worth of stolen USDT. There is indeed a reasonable probability that exchanges and issuers that wish to engender trust and establish their legitimacy are likely to react

favourably to such calls to take temporary action to freeze assets or block transactions from certain addresses, in the interests of their own reputation. The effectiveness of such measures, however, is nonetheless heavily dependent on the speed of reaction and the concerted cooperation of industry actors.

At the same time, it is also this same ability to identify and place a “red flag” on certain suspect addresses that prevents successful hackers from transferring the stolen digital assets, or liquidating them for fiat. It is a tight race of time and technology – whether the hackers are able to mix and transfer the stolen digital assets quickly enough before industry actors around the world can be alerted to and take action to halt the further dispersion of the digital assets. Another “self-help” remedy which victims of stolen assets could employ may be to “fork” a privately operated blockchain to render the stolen tokens useless while ensuring that other legitimate tokens on the blockchain continue to operate normally.

CONCLUSION

Against the backdrop of these immediate actions taken by affected industry actors, the legal remedies add to the arsenal of tools available to victims of digital asset hacks. It lends legitimacy and force to the victims’ appeals for wallets to be frozen or addresses to be “blacklisted”, such as in *Fetch.ai*, when the UK High Court ordered Binance, one of the largest centralised cryptocurrency exchanges, to identify hackers and freeze their addresses at the request of a hack victim.

The application of the law to digital asset hacks as well as industry protocols and technical safeguards against such hacks is likely to develop rapidly in the near future, jointly building a more robust ecosystem for the safekeeping and security of digital assets.

The content of this article does not constitute legal advice and should not be relied on as such. Specific advice should be sought about your specific circumstances. Copyright in this publication is owned by Drew & Napier LLC. This publication may not be reproduced or transmitted in any form or by any means, in whole or in part, without prior written approval

If you have any questions or comments on this article, please contact:



Chua Tju Liang

Director, Corporate & Finance
Head, Blockchain & Digital Assets

T: +65 6531 4101

E: tjuliang.chua@drewnapier.com




Rakesh Kirpalani

Director, Dispute Resolution &
Information Technology
Chief Technology Officer

T: +65 6531 2521

E: rakesh.kirpalani@drewnapier.com

 **DREW & NAPIER**

Drew & Napier LLC

10 Collyer Quay

#10-01 Ocean Financial Centre

Singapore 049315

www.drewnapier.com

T : +65 6535 0733

T : +65 9726 0573 (After Hours)

F : +65 6535 4906