mourant

GUIDE

Cryptocurrency: Speculative Risks

Last reviewed: May 2022

Speculative risks

Given the economic uncertainty experienced over recent years, Bitcoin itself having been created in reaction to the 2008 financial crisis and the failure of centralized stores of wealth, investors have naturally turned their attention to alternative sources of investment; cryptocurrency and digital assets being an example of this. Accordingly, cryptocurrencies have grown in popularity since the establishment of Bitcoin in January 2009, with an initial market capitalisation of zero, and a current market capitalisation of almost US$800 billion. Other widely adopted cryptocurrencies, such as Ethereum, have seen similar dramatic increases in market capitalisation, and the global daily trading volume of cryptocurrency generally is estimated to be more than US$275 billion, across more than 400 platforms.[1] The market's adoption of cryptocurrencies (along with other forms of digital asset, and the supporting and associated infrastructure) has therefore been rapid.

The adoption and implementation of concomitant regulation has, in various jurisdictions, historically lagged behind this rapid pace. Various jurisdictions have also taken differing approaches to the adoption and regulation of cryptocurrencies. Indeed, in a recent article, Thomson Reuters note:[2] '*Thus far, the regulatory response is best described as ad-hoc, rhetorical or driven by enforcement in some instances. The challenge in such a new and disruptive area will likely take years to finalize. Adding to the challenge is the ambiguous nature of digital assets themselves and the lack of standardized definitions, thus creating questions of overlap and jurisdiction*'.

Investing in cryptocurrency or other digital assets is not without its risks, not least because of this changing and patchy regulatory space, but also the fundamental nature of the asset class, which leaves it, to some extent, vulnerable to attack. Accordingly, in this article, we set out some practical ways to help protect such investments from the outset. We also provide an update as to how cryptocurrency is viewed by the courts and the associated rights and remedies available to investors when it is misappropriated.

What can I do to protect my investment – before the event

As noted, above, regulation surrounding cryptocurrencies and other digital assets is developing at varying rates across different jurisdictions. Given this, along with the manner in which digital assets are commonly held and traded, this can leave investors open to fraud, theft and other forms of cyber-attack. As Forbes recently noted, '*cryptocurrency fraud is on the rise. The Federal Trade Commission (FTC) received 7,000 reports of crypto theft, with a combined value of more than $80 million, between October 2020 and March 2021. That's a 12-fold increase in cases and a 1,000% jump in cash amount compared to the same period a year prior*'.[3] Below are some practical tips for trying to reduce such risks, at the outset of an investment:

[1] Cryptocurrency regulations by country, Thomson Reuters, 2022 (Thomson Reuters 2022).

[2] Thomson Reuters, 2022.

[3] https://www.forbes.com/advisor/investing/cryptocurrency/bitcoin-scams-fraud/.

1. Use a secure wallet (also termed a 'cold' wallet): In order to deal in cryptocurrency it is necessary to have the use of the associated public and private keys. Using a cold wallet essentially means that the necessary keys are not stored on or connected to the internet, thereby reducing their vulnerability to online attack or seizure. As such, one must be in physical possession of, or at least be able to physically access, the cold wallet. The downside is that if the cold wallet is lost, so is access to the cryptocurrency. There are a number of cautionary tales on this subject.
2. Passwords: Separate public and private keys and use complex passwords and multi-device authentication. Change passwords often. Do not share them or use the same passwords across multiple accounts.
3. Due Diligence: For those investing through an exchange, it is advisable to research each exchange's security processes before creating an account or investing through that medium. For instance, in order to minimise risk, use a well-known platform with an established history and developed security protocols. Some exchange platforms, such as Coinbase, also offer insurance, which may give peace of mind.
4. Security: If using your laptop or mobile phone, install security software to help reduce the risks from malware and other cyber-attacks. Be wary of phishing messages from text messages, social media, online dating platforms and unresponsive calls.

What can I do to protect my investment – after the event

In the event of fraud or theft of cryptocurrency, one option is to look to the remedies available from the courts, for instance with a view to freezing misappropriated assets, or obtaining information necessary to track the wrongdoer and trace the assets. This is necessarily a developing area of law, given the relatively fledgling and changing nature of the asset class and its underpinning technology. With that said, in our view, the offshore courts and the courts of England & Wales (whose decisions are highly persuasive in other common law jurisdictions, such as the Cayman Islands and the British Virgin Islands) have risen to the challenge well. Some recent examples of this are described below:

1. In recent cases such as *AA v Persons Unknown and Ors* [2019] EWHC 3556 (Comm) (see here for our recent article on this case), cryptoassets have been recognised as 'property' within English law. Such a finding is significant and opens up the remedies available to the injured party, who is able to pursue hackers using proprietary remedies such as proprietary injunctions, for instance.
2. In *CLM v CLN* [2022] SGHC 46, relying on the Singapore Court of Appeal decision in *Quoine Pte Ltd v B2C2 Ltd* [2020] 2 SLR 20 and the New Zealand decision of *Ruscoe v Cryptopia Ltd (in liq)* [2020] 2 NZL, the General Division of the High Court in Singapore similarly ruled that cryptocurrency could be classified as 'property' and therefore be protected by proprietary remedies.
3. The courts have also been willing to make orders such as proprietary freezing injunctions against 'persons unknown' when the defrauded investor is unable to establish the identities of the wrongdoers (as is often the case). This was the case in the recent English decision in *Danisz v (1) Persons Unknown (2) Huobi Global Ltd (Trading as Huobi)* [2022] EWHC 280 (QB), whereby stolen Bitcoin was tracked to a wallet under the control of the Huobi exchange. That wallet was frozen by order of the English High Court. The Court also ruled that it had jurisdiction to grant the injunction as the claimant was domiciled in England and the asset was purchased through an English bank account. Similar orders were also recently made by the BVI court in the case of *ChainSwap v Persons Unknown*, where unknown hackers stole large quantities of tokens from ChainSwap's users, and exchanged them for stablecoins which were then sent on to a centralised exchange in Croatia.
4. Another weapon in the lawyer's arsenal is to issue an application for a *Norwich Pharmacal* order against a third party, such as an exchange, in order to retrieve identification information about the suspected wrongdoers. Exchanges often have, and in many cases are mandated to obtain, 'Know Your Client' information about their users, meaning that valuable information necessary to bring a claim may be retained about wrongdoers. Access to this information is a primary perquisite for defrauded investors to track their misappropriated assets. Indeed, this occurred in the *ChainSwap* case, where the exchange in Croatia, to which the fraudulently obtained stablecoins were sent, was ordered by the BVI court to provide disclosure in relation to the suspected wrongdoers.
5. Bankers Trust disclosure orders may also be sought from the court, as in the aforementioned case of *Danisz*. These orders are available in narrower circumstances compared to *Norwich Pharmacal* orders, and are made where there is a clear case of fraud and the claimant seeks disclosure from the

respondent (typically a financial institution) in order to trace assets over which they have a proprietary interest.

In the case of suspected fraud or misappropriation of cryptocurrency or other digital assets, it is important to act quickly, not least given the ability to move and mix assets almost instantly and with pseudonymity. Legal practitioners should be brought on board at the earliest opportunity who, together with the necessary forensic investigators, can help to track the assets and take the necessary court action to pursue the wrongdoers.

Mourant has a wealth of cross-jurisdictional experience, both in the litigation and regulatory spheres, in relation to such matters, and is well-placed to service such needs.

Contacts

A full list of contacts specialising in Fintech law can be found here.

2021934/83576035/1