MAY 2022

UPDATE

Cryptocurrency: Gold Mine or Minefield

Update prepared by Abel Lyall (Guernsey)

This update addresses the regulators and Court's approach to combatting the difficulties associated with crypto in order to encourage innovation whilst protecting consumers and investors.

This update forms part of our series on cryptocurrency. Our previous article on speculative risks can be found here.

Gold Mine or Minefield

Blockchain is re-shaping the way in which business transacts across the globe; being applied to achieve real time processing of transactions, minimise the risk of loss of data and reduce costs through eliminating intermediaries. From smart contracts through to securitisation; blockchain promises to change how we interact, the speed at which we interact and how trust is formed.

However, where there is opportunity, there is risk – this article explores the difficulties associated with crypto together with regulators and Court's approach to combat these in order to continue to encourage innovation whilst protecting consumers and investors. Finally, it provides food for thought on why directors and trustees may wish to expand their knowledge in this area to manage any possible reputational risk to their business but also to ensure they are exercising their duties and powers with eyes wide open.

With every innovative digital advancement there is an equally innovative fraudster

You may have seen our previous articles on this subject which provide an introduction to cryptocurrency and the fundamental risks of investing in blockchain ecosystems, including our publications on speculative and operational risks. It will be no surprise that one of the fourth categories of risk faced by those purchasing and trading in cryptocurrencies and assets described by the US Commodity Futures Trade Commission is 'Fraud and Manipulation Risk'.

Headlines describing crypto scams which resulted in severe investor losses (such as disappearing custodians or scam currency such as SQUID) or hackers using the distributed ledger technology (DLT) to effectively 'clean' proceeds of crime received in Bitcoin by layering transactions and ultimately converting them into regulated currencies are becoming part of monthly routine. Although John Glen Secretary to the Treasury in the UK says "Above all, we want to position the UK as a pro-innovation jurisdiction... which is attractive to inward investment, and to firms who don't yet have a settled base."[1] it remains an incredibly volatile investment option - Just last month the price of bitcoin plunged to its lowest point since 2020[2] causing significant investor loss. On top of this, with £318bn wiped out by the collapses of Terra Luna and TerraUSD it appears that not even stablecoins can provide a safe-haven[3].

Volatility aside, why is there such a hype about fraud in connection with crypto over general financial services?

[1] Keynote Speech by John Glen, Economic Secretary to the Treasury at the Innovative Finance Global Summit (April 2022) (here)
[2] NY Times: "Cryptocurrencies Melt Down in a 'Perfect Storm' of Fear and Panic" dated 12 May 2022 (here)
[3] BBC Newx, 'Cryptocrash: 'I was arrested for knocking on Luna boss's door' dated 24 May 2022 (here)

As you will know, blockchain is a shared, decentralised, digitally distributed, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network, the technology which is often referred to as DLT. One of the reasons why perhaps fraud is more prevalent in this sector might be the lack of KYC protocols – due to the decentralised nature, there are no real safeguards to say who is a good actor and who is a bad one.

Added to this is the lack of regulation. The financial services industry is heavily legislated and regulated – there are reasons why this is the case, but pertinently, they aim to prevent financial crime, money laundering and terrorist financing and to protect consumers and investors from becoming the victim of those. Whilst the application of DLT to financial services has transformed this sector, one of the main issues is that this innovation has outpaced regulation. At the outset, one difficulty has been understanding the technology sufficiently well to find a new home for these services within the current regulatory framework - how do you regulate technology that is constantly changing and is not yet fully understood? Legal issues range from IP ownership, data safety, fraud to jurisdiction and enforcement.

It does not stop there - if you are the subject of a fraud or theft for example, you will first have to overcome a number of hurdles in order to bring a claim. As you could be transacting from anywhere in the world and are doing so anonymously in the knowledge that your transactions, once made, cannot be undone, you will need to ask yourself:

(1) How do I identify the fraud/theft?

(2) What losses have I suffered and can these be quantified?

(3) Who am I going to sue for my losses?

(4) Where do I sue them?

What is the regulatory landscape?

For many years regulators across various jurisdictions have attempted to grapple with how to encourage innovation whilst protecting the integrity of the financial system and thereby its users from financial crime. The joint HM Treasury, Financial Conduct Authority and Bank of England Cryptoassets Taskforce report sets out the UK's approach to cryptoassets and DLT in financial services[4], and also summarises some of the steps taken to manage this developing sector. These include for example the creation of the FCA Regulatory Sandbox the Bank of England Fintech Hub. When looking specifically at fraud and money laundering prevention, the focus has been on bringing Crypto into the scope of AML legislation and finding ways to assist the court in categorising crypto assets in order to give affected parties a possible civil recovery route.

The Courts' approach is discussed in more detail below. However, the position on regulation in Guernsey is that the GFSC is keen to continue to encourage and support innovation whilst ensuring protection to consumers and investors. Its commitment is demonstrated in the launch of the first crypto fund last year[5] in which they reiterated that they are keen to help new financial services businesses understand the regulatory framework. Although they state that they will continue to take a cautious and considered approach to review each application on its own merits, they will focus particularly on safeguards and the criteria applied i.e. to custody, liquidity, valuation of assets and KYC. To assist with the process, the GFSC established the Innovation Soundbox, a hub created by the regulator to assist prospective innovation or start-up financial services businesses who are considering applying for a regulatory licence or registration.

Court's approach

Whilst the GFSC has made its position clear, there has not been much opportunity to date for the Royal Court to test cases surrounding crypto. However, across the globe, some examples of the Court's approach are emerging which may provide some clarity for those wishing to be compensated if they were the subject of a fraud.

Endorsing much of the UK Jurisdiction Taskforce's legal statement on crytpoassets and smart contracts, the English High Court held that Bitcoins are "property"[6]. This case arose from a ransomware attack, where hackers accessed the computer system of the claimant and installed malware which encrypted the system.

---

[4] Cryptoassets Taskforce: Final Report (2018)
[5] GFSC, "Consideration of Crypto Fund" October 2021 (here)
[6] *AA v Persons Unknown* [2019] EWHC 3556 (Comm)

The hackers then demanded a ransom for the encryption key. Bitcoins worth approx. US$950,000 were transferred to the hackers who then send the decryption software to allow the company to continue its day to day business.

ChainSwap[7] is another good example of hackers exploiting vulnerabilities to redirect tokens to other wallets. As set out above, due to the way in which DLT works, it is not easy to trace the culprits or indeed to undo the fraud. This then raises the question - who do you sue if you do not know who you are suing or in which jurisdiction they are based? You can read more about the case here, however in short, *ChainSwap* was the victim of cryptoasset fraud and brought a claim against "persons unknown" for losses they suffered and also applied for a freezing injunction to secure the assets which the BVI Court's granted. These types of applications against unknown defendants are becoming commonplace in the cryptosphere.

In *Danisz v Persons Unknown* and Huobi Global, the High Court granted the claimant (a Bitcoin-holder) an interim proprietary *injunction* against persons unknown and a cryptocurrency exchange, a worldwide freezing order against persons unknown, and a banker's trust order against the cryptocurrency exchange, following a suspected cryptocurrency fraud. This demonstrates the Court's willingness to provide swift injunctive relief to combat cryptocurrency fraud.

Two key point to take away are – if you do want to act, 1) take decisive action on which jurisdiction you want to sue in and attempt to avoid a jurisdiction battle; 2) act quickly in order to increase your chances of securing assets before they are dissipated – this principle is amplified by the fact that the identity of your potential defendant is unknown.

Why you should be vigilant

As is evident from global developments, crypto is here to stay and the application of DLT is only going to increase. Whilst this presents a raft of opportunities (from investment in technology through to investing in cryptoassets and currencies themselves) the above demonstrates that there are some significant risks. The scope for criminal activity is wide – hacking of digital wallets, fake ICOs, Ponzi schemes resulting in the misappropriation of tokens, fake or unregulated brokers, ransom payments, etc. Cyber scams are often very similar to those of a legitimate transaction involving a digital asset which makes it even more difficult to spot. Whilst these gaps in regulation remain, fraudsters will continue to exploit them and vigilance is required.

Whether you decide to invest, trade, facilitate trade or host platform that do so, or you are a trustee who is responsible for managing trust crypto assets, you too will need to understand the regulatory framework within your jurisdiction and how this might affect your statutory or fiduciary duties. You will also need to be alive to the global nature of any potential fraud in that a claim could be brought not only where you are based, but where your fraudster may be based of the theft occurred which is often unknown or could be in multiple jurisdictions.

As you can see this is a vast topic with constant development. It will be integral to businesses and trust companies and their reputations moving forward to understand the regulatory landscape they are or might become subject to through transactions or ownership of assets within structures and to have a "crisis management" plan in place to deal with the fall out if they do become subjected to fraud in order to manage any possible reputational damage.

[7] *ChainSwap Limited v Persons Unknown* [2022] BVIHC (COM)

Contacts

Abel Lyall
Partner I Advocate
Mourant Ozannes (Guernsey) LLP
+44 1481 739 364
abel.lyall@mourant.com

2021934/83733801/2