CRYPTO TRANSACTIONS AND DISPUTES: THE RISKS AND REGULATORY ISSUES

Authored by: Noor Kadhim (Consultant), Mark Pearce (Private Wealth Consultant), and Emily Drake (Legal Director) - Gateley Legal

The rapidly evolving digital asset market offers exciting opportunities for investors. Digital assets are more accessible than traditional financial investments and can present returns that are uncorrelated to the market. Their reward potential is, therefore, often much higher.

These advantages also come with risks, particularly for unsophisticated investors. The volatility and rapid fluctuation of cryptocurrency value can result in significant losses, as can the inherent risks of electronic storage and transfer. The market's susceptibility to fraud and money laundering, due to less stringent regulation, transactions that are often not transparent, and difficulty tracing assets once they are stolen or removed, is also already well documented.

Although the UK, EU, and USA – among others – are developing new regulations to protect investors, including the introduction in many jurisdictions of Virtual Asset Service Provider (of "VASP") legislation, the risks detailed above present a significant barrier to the wider adoption of digital assets. This article seeks to address these risks, outline how to achieve redress in the event of fraud, and discuss the regulatory forecast in certain key jurisdictions.

Practical risks for potential claimants

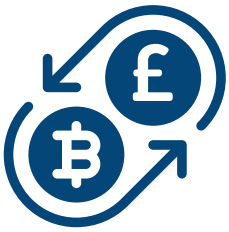
Following economic loss in a crypto dispute, a potential claimant must consider two issues: whether there is a right of action in law against the alleged fraudster, and whether pursuing said fraudster is likely to achieve redress.

A significant hurdle in both cases is tracing the stolen assets and, ultimately, identifying the fraudster(s). While the blockchain technology on which crypto transactions are based provides data that can be used for tracing, this is often negated by the privacy and pseudo anonymity such digital transactions can afford to wallet holders. This is complicated by exchanges or 'mixers', a common feature of jurisdictions such as North Korea and Russia, which are designed to obfuscate the flow of funds or assets. Enhanced privacy is even a mark of distinction for some cryptocurrencies. Monero and Zcash, for example, use advanced cryptographic techniques to obscure transaction details. This means that, even if a claimant successfully traces assets to a wallet, they are unlikely to uncover the fraudster's details.

Conducting transactions on exchange platforms can provide a safety net, as will be discussed in more detail below, but platforms are not always obliged to disclose wallet holder details unless forced by a Norwich Pharmacal Order, Bankers Trust Order or their equivalents in jurisdictions outside the UK. A platform's location will also have an important bearing on their willingness to cooperate when unmasking fraudsters and tracing assets. It is easier, for example, to obtain disclosures from Las Vegas-headquartered Bitcoin than it is Tether, which is based in Hong Kong and less accepting of foreign court orders or cryptocurrencies.

Even unmasking the trail of a stolen asset is no guarantee of that asset's recovery. Without fast intervention such as freezing, assets can be dissipated or converted into fiat currency.

At this point, they become as difficult to trace as traditional bank transfers, particularly if the recipient's chosen monetary platform is outside the claimant's jurisdiction.



Are exchange platforms a better target for redress?

With individual fraudsters proving difficult to trace and target, the intermediary platforms that hold wallets through which digital assets are transferred are becoming an increasingly popular alternative route to redress. Established, reputable platforms will usually owe a contractual obligation or duty of care, making them a more straightforward route for the courts to impel disclosure of information and enforce against assets.

From a UK perspective, the potentially pivotal case of Tulip Trading Ltd v van der Laan provides a useful example of a claimant using a platform's capabilities and obligations to achieve redress.

According to the Court of Appeal: "It is indeed conceivable that relevant individuals, when they are acting in the role of developers, should be held to owe a duty in law to Bitcoin owners".

In this case, the duty extended to the platform varying the blockchain's underlying source code to retrieve approximately $4.5bn of Bitcoin that hackers had deleted. It remains to be seen, however, how a court may enforce orders against developers to rewrite source code to bring about the appropriate redress (e.g. access to wallets without knowing the private key)."

Crypto regulation – what is coming?

A legal route against the exchange platforms is not always available. It will depend largely on a platform's credibility and liability, and its contractual and tortious obligations towards its customers. As such, it does not provide a complete remedy for the absence of effective 'policing' by global regulators.

Regulation is finally starting to gather pace, particularly in the wake of several high-profile company collapses and international scams within the crypto asset market, such as FTX.

In the UK, such regulation could come into force within the next year. A bill containing amendments to the Financial Services and Markets Act (FSMA 2) is expected to tighten rules around crypto promotions, which would impact firms, influencers, or celebrities being able to promote currencies, and equate them with high-risk investments. Non-compliance, therefore, will be a criminal offence. Digital assets will also be included within the FSMA's section 21 financial promotion restrictions and the regulated activities regime under section 22.

Cryptocurrency regulations passed in the EU in April 2023 will also take effect in 2024. Emphasising consumer protection, environmental safeguards, and traceability, they will cover digital assets not already within the remit of existing financial services legislation. These regulations are expected to be among the most wide-ranging legislation applicable to cryptocurrency.

The USA remains less consistent in its approach across agency, state, and federal level. While cryptocurrencies are now classed as securities rather than commodities and therefore fall under the extensive enforcement and regulatory powers of the Securities and Exchange Commission (SEC), general digital assets are considered commodities. This makes them subject to the Commodity Futures Trading Commission (CFTC), which can enforce, but not regulate.

What does the future hold?

Clarity around operating rules in the crypto space is likely to be welcomed by the digital community. Government regulation could also provide the safeguards required to make digital assets more attractive to investors. Until such measures are established, however, investors should limit exposure to fraud by keeping within the transaction limits imposed by multinational banks and only undertaking transactions via reputable platforms established within jurisdictions with solid legal frameworks.

Given that digital assets were originally intended as a decentralised financial system free from government control, there must be a balance between maintaining the advantages of an open, egalitarian financial system, and protecting consumers from unlawful exploitation. It remains to be seen how state regulation and justice systems will achieve this over the coming years.