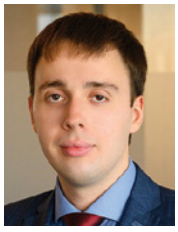
Crypto Fraud: Potential for Recovery

James RAMSDEN QC
is a partner at Astraea Group (London)

Nicholas CONNON
is CEO at Quintel Intelligence (London)



Ivan KOVALENKO
is a senior associate at Hillmont Partners (London)

It has a market value of around USD 2 trillion and it is not gambling or some forbidden business. This article is about the cryptocurrency market, whose value topped USD 2 trillion in April 2021.

It is undoubtedly true that this market involves the risk of illegal actions like fraud or theft.

In April 2021 investors in Turkey lost their funds in the amount of almost USD 2 billion due to alleged fraud on the Thodex cryptocurrency exchange platform. Following the pre-trial investigation, the Central Bank of Turkey decided to explicitly ban the use of cryptocurrencies in Turkey and introduced the Regulation on the Disuse of Crypto Assets in Payments. It is a vivid example when a state attempts to regulate relations after criminals have already taken advantage of a gap in legislation.

Definition

The current features of the cryptocurrency market are the high price volatility of crypto assets, absence of Central Bank backing and limited acceptance among retailers. There are several definitions currently used around the world: virtual currencies, cryptocurrencies, digital currencies, crypto assets (CC).

The Financial Action Task Force (FATF) has issued the most comprehensive explanation to date, where it approached cryptocurrencies (crypto assets) as a subset of virtual currencies (VCs), which it defines as "a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e. when tendered to a creditor, it is a valid and legal offer of payment) in any jurisdiction".

The current features of the cryptocurrency market are the high price volatility of crypto assets, absence of Central Bank backing and limited acceptance among retailers

This definition is the broadest as the FATF admits that VCs may possess some (or all) of the main functions of money (a store of value, a medium of exchange and a unit of account), which were established by economic theory.

The last published changes to the Recommendations of the FATF (October 2018) make it clear that jurisdictions should ensure that the providers of VCs are subject to AML/CFT regulations. For example, conducting customer due diligence including ongoing monitoring, record-keeping and the reporting of suspicious transactions. They should be licensed or registered and subject to monitoring in order to ensure compliance.

It is important to note that current regulatory oversight, such as that by the Financial Conduct Authority in the UK, does not provide protection for investor should they become a victim of fraud.

Types of cryptocurrency fraud

Ponzi schemes

Crypto assets may be used in traditional Ponzi schemes (that attract investors and pay profits to earlier investors with funds from more recent investors). The most vivid example of such a scheme using cryptocurrencies is the Bitcoin Savings & Trust case (BS&T). Investors in BS&T were promised returns as high as 7% per week, but what really happened is that more than 265,000 Bitcoins were stolen via fraud and at least 48 out of 100 investors lost all or part of their investments.

Theft

Criminals can merely hack crypto wallets and steal CCs from investors. According to data researched by Trading Platforms UK, the value of cryptocurrency hacks and thefts between 2019 and 2020 increased by 38.38% from USD 370.7 million to USD 513 million. The most recent example is the theft committed of cryptocurrency platform Roll, where hackers stole about USD 5.7 million from one of the user's wallets. Hillmont Partners also recently assisted in a matter where a user of one well-known English exchange platform lost CCs from his wallet despite using Two-Factor Authentication (2FA). Quintel and Astraea are currently instructed on a large fraud where assets have been dissipated across the globe, layered through unidentified wallets, resulting in a large-scale international recovery case.

Scams

Criminals attempt to use the lack of reliable information which potential investors sometimes may face and create fake exchange platforms. These usually resemble a legitimate business/its website, application. For instance, Bitcoin Gold is a legitimate platform. However, scammers created a legitimate-looking website (mybtgwallet.co), which offered new users the opportunity to create Bitcoin gold wallets. There was a requirement to submit one's private wallet keys to use a gold wallet. Thus, criminals were able to fraudulently acquire more than USD 3 million.

Another example is BitKRX, which was a completely fake South Korean Bitcoin exchange. The exchange claimed it was a branch of the legitimately existing Korea Exchange, which allowed scammers to defraud hundreds of investors.

A recent example in Ukraine is the Swisscoin case. A group of individuals conspired to launch the "Swisscoin Ukraine project", which resembles the Swisscoin exchange platform that ultimately does not have a Ukrainian branch. The purpose was the same as in other similar cases: to attract investors and embezzle their funds.

> With a lack of AMF/KYC requirements from some exchange platforms, crypto assets may be used as a new tool for tax avoidance, money-laundering, and bribery

Financial crimes

Similar to the conventional financial arena there are characteristics of the movement of digital funds which indicate that there may be suspicion as to their legitimacy. A leader in identifying these characteristics is Chainalysis, a US-based company that provides software to a number of law-enforcement bodies across the globe, including the Department of Justice (US), Europol, FBI and the NCA amongst others. Chainalysis reported in early 2021 that "illicit activity made up 0.34% of all cryptocurrency transaction volume", a percentage which may surprise some observers.

However, with the increase in adoption we expect to see a significant increase in the quantum of fraud and financial crime in the digital currency market place. With a lack of AMF/KYC requirements from some exchange platforms, crypto assets may be used as a new tool for tax avoidance, money-laundering, and bribery, which is reflected in the hesitance of most national banks to adopt digital stable coins.

Crypto Fraud protection and choice in action

England and Wales

There is currently no legislation directly governing crypto assets. Moreover, there is no single description/definition of CCs. However, as is usually the case with English law, the substantive case law assists in eliminating some gaps in statutory provisions.

In *Vorotyntseva v Money-4 Ltd (t/a Nebeus.com) [2018] EWHC 2596 (Ch)* the claimant applied for a freezing order against a company to which she had given a substantial quantity of cryptocurrency (worth around £1.5 million). James Ramsden QC of Astraea Group made submissions on behalf of the claimant in relation to the risk of dissipation of crypto assets. Eventually, Birss J granted a freezing injunction against the defendants where CCs were treated as a form of property.

Bryan J in *AA v Persons Unknown [2019] EWHC 3556 (Comm)* confirmed the position that crypto assets are to be considered as property "...as being definable, identifiable by third parties, capable in their nature of assumption by third parties, and having some degree of permanence".

Supperstone J, in his judgment in *United States v Panovas [2018] EWHC 921 (Admin); [2018] 4 WLUK 160* saw the court allow the USA's appeal against the granting of bail to a Lithuanian national whom it wished to extradite on the grounds of evidence relating to his ownership of 200 Bitcoin (worth around USD 2 million). Thus, the court treated crypto assets as a store of value.

In *R v West* Bitcoin seized from a hacker became compensation for victims, proving that the court recognizes crypto assets as a store of value.

In Binance v Persons Unknown, a case before the Grand Court of the Cayman Islands on 25 June, 2020, the Cayman Grand Court issued a world-wide freezing and disclosure order against defendants, both known and unknown in Egypt, and in multiple other jurisdictions. The claim concerned a hack into the algorithmic trading platform operated by Binance. The persons unknown were identified only by mobile phone numbers or IP addresses. The court broadly followed the English decisions narrated above. James Ramsden QC acted for Binance.

Finally, on 22 December, 2020 in Ion Science Limited v Duncan Johns and Persons Unknown, the English Commercial Court joined all these dots together making disclosure (and subsequent freezing orders) in relation to an allegedly fraudulent Initial Coin Offering. The orders were made, as in Binance, against known and unknown defendants.

What are the implications of the above in practice?

If virtual currency (or cryptocurrency, crypto asset) is property, then it could be legally purchased or disposed of. These, in turn, provide grounds to apply laws and statutes that may protect investors. For instance, Chapter 3 of the Consumer Rights Act 2015 sets out protections for consumers who purchase digital content. This includes provisions in relation to the method of refund for faulty content. Where the consumer uses cryptocurrency to pay for digital content, the trader can (and must, unless the consumer agrees) make the appropriate refund in the digital currency (CRA 2015 s. 44(5)).

The tracing of CC can be straight forward, though often is not. The public ledger offers investigators great visibility on the movement of assets, but it is not absolute. Where complexities arise is understanding real world entities and how to access the information they hold. Each fraudster needs an "offramp" to release their looting. These offramps have to be CC to fiat brokers as these fiat brokers, as official and legitimate entities, hold information to real world identities which are needed for enforcement. Courts (criminal and civil) in the UK are becoming more comfortable with disclosure applications which, providing they are suitably resourced through forensic investigation, are applied in the digital currency sphere. In turn, Quintel's experience in these applications has shown that cryptocurrency entities are becoming far more dynamic in responding to these requests.

There is currently no substantive legislation regulating crypto assets in Ukraine

Ukraine

There is currently no substantive legislation regulating crypto assets in Ukraine. However, there are provisions that attempt to regulate use of CCs from the AML/CFT/tax evasion perspective.

Following the October 2018 changes to the Recommendations of the FATF, already in October 2019 Ukraine adopted amendments in the Law of Ukraine *On Prevention of Corruption*, providing a new term, "cryptocurrency" (though it does not define it). CCs are treated as intangible assets that are subject to declaration by PEPs. On the other hand, the National Agency on Prevention of Corruption issued guidelines which clarify that cryptocurrencies are types of virtual assets and not a digital form of fiat money.

Furthermore, Ukraine is actively working on creating fully-fledged cryptocurrency regulations. The Ministry of Digital Transformation prepared the Draft Law *On Virtual Assets*. The Draft Law is designed to determine the legal status of virtual assets, their use and circulation on the market of Ukraine, the establishment of legal relations in the market of virtual assets, regulation of procedures for the issue of virtual assets.

Analysis of domestic case law shows no theory development, as is so in England and Wales. The courts there do not recognise CCs as a form of property, asset, or form of money. For instance, criminal case law has some references to cryptocurrencies ("CC wallet", "PC system unit used for mining") but ultimate objects of court orders (arrest, seizure) are sale proceeds from CCs and not CCs themselves.

Neither does civil case law support crypto assets being a form of property because "...virtual currency does not have any collateral and legally related persons and is not controlled by the state authorities of any country. Thus, Bitcoin is a monetary surrogate that has no reality..." However, this position contradicts a recent family dispute where a court accepted CCs as intangible assets owned by the defendant.

What are the implications of the above in practice?

The implications are controversial. While the legislature imposed some obligations on PEPs in relation to declaring CCs, they do not provide any legal protection to other individuals against any types of Crypto Fraud.

Ukrainian contract law and subsequent case law provide that despite the fact that crypto assets themselves cannot be a medium of exchange, unit of account or store of value, parties may execute agreements where CCs are pegged to fiat money.

Thus, Ukrainian law does not currently provide any protection to investors. Therefore, any transaction involving crypto assets in Ukraine is risky. The only viable option is to draft contracts where CCs are pegged to fiat money, though such contracts will protect only fiat money, not cryptocurrencies. However, English law provides substantial grounds to enforce contractual rights and recover crypto assets lost due to fraudulent activities.

END