HARNEYS

Article

Cryptocurrencies: risk and recovery

Although cryptocurrencies are not 'new', it is only in recent years that ownership of digital assets has become widespread. Given the increased interest and value in the crypto market, it is unsurprising that fraudsters have sought to capitalise on the lack of regulation and investors' fear of missing out on potentially life-changing returns.

One of the supposed advantages of crypto is that the blockchain technology that underpins it is secure, transparent and more resilient to fraudulent misuse. It is therefore ironic that a vast number of scams have emerged in parallel with this growing market. The risk of falling victim to fraud, along with the highly volatile prices, have given crypto a reputation for being a precarious investment. Is that reputation fair?

The unique characteristics of cryptocurrencies and their resilience to fraud

Blockchain technology and the cryptocurrencies that use it are supposed to be more resilient to fraudulent misuse because of the decentralisation of processes used to verify and broadcast transactions. Simply put, cryptocurrencies with sufficiently large networks should be resistant to having transaction data changed, forged or otherwise corrupted because every transaction is verified by a large number of unrelated computers, by reference to all previous transactions, and majority consensus is required before the transaction is recognised as having been effective. Once verified, the transaction will be broadcast to a much wider network of users, which prevents a minority of users being able to pass off inaccurate information as genuine.

The permanent nature of the data recorded within each blockchain should ensure that fraudsters are unable to falsify information relating to assets. Whilst all cryptocurrencies are different, they are all based upon blockchain technology that consists of a single unbroken record of all past transactions. Having a comprehensive and indelible ledger makes it straightforward to audit the movements of the currency and trace its ultimate destination.

The transparency of ownership of crypto may appear paradoxical: whilst crypto is transferred from one 'public' address to another, those addresses present only as a long string of letters and numbers and it will not normally be obvious who owns the currency held at an address. In fact, these 'addresses' are public keys denoting the ownership of the cryptocurrency which, when paired with the owner's private key, allow the owner to deal with the cryptocurrency associated with the public key. If a public address or key can ever be linked to an owner then one can generally infer that all transactions linked to that address were undertaken by that same owner. It is for this reason that ownership of cryptocurrencies is referred to as 'pseudonymous'.

In terms of how an owner can be identified, most cryptocurrency exchanges will require personal information from the user before enabling them to operate an account for trading purposes. Exchanges are required to collect personal information in accordance with anti-money laundering regulations – the specific regulations will vary depending upon the countries in which they operate and the services offered by the exchange. For example, there are differing KYC requirements for exchanges that offer crypto-fiat exchange to those that allow only crypto-crypto exchange. There are some exchanges that boast not to require any form of KYC verification. However, most of these exchanges will limit the amount of currency that can be withdrawn by users who have not provided KYC information or will only facilitate crypto-crypto trades.

One other distinguishing feature of cryptocurrencies is the speed at which transactions can take place. Removing intermediaries from the transaction process significantly shortens the time it takes to complete transfers. Consequently, cryptocurrency transactions are normally cheaper too.

Despite the undoubted benefits that blockchain technology provides, it has unfortunately not stopped crypto (or something purporting to be crypto) being used in numerous scams and frauds. The pseudonymous nature of ownership, and the ease and speed of trading, has also resulted in crypto becoming the currency of choice for transmitting and concealing proceeds of wrongdoing by fraudsters. The portrayal of cryptocurrencies as inherently risky or susceptible to fraud, however, is unfair given the inbuilt safeguards and ability to trace transactions. Whilst the crypto market has been identified as fertile ground for

fraudsters to deceive unwitting investors, this is no more an issue for crypto than it is for any evolving product or marketplace, especially where investors are inclined to take more risks because of the potential gains.

How can cryptocurrencies be misused?

Whilst one can find many reports of cryptocurrencies being used fraudulently or improperly, the primary ways in which crypto has been and can be misused fall into three categories: (i) cases where the underlying blockchain technology itself is used or altered fraudulently; (ii) cases where crypto or its wider market is used as the catalyst or 'bait' in a fraudulent scheme; and (iii) cases where crypto represents the by-product or proceeds of fraud or other wrongdoing.

(i) Fraudulent use of blockchain technology

Although blockchain technology is more resilient to fraud it is not entirely impervious to it. There are ways (albeit for some cryptocurrencies only hypothetically) in which data stored on the blockchain can be tampered with or abused so as to facilitate double spending or even deleting and/or rewriting parts of the blockchain. This can happen where one person or organisation is able to control the process for verifying transactions on the blockchain by holding at least 51 per cent of the verification power. Although such attacks have been relatively rare, they have the effect of entirely defeating the purpose and all the inherent advantages of blockchain technology – by broadcasting as verified a fraudulent transaction and using the wider network to log that information as genuine. Where '51 per cent attacks' have occurred it has significantly reduced the price of the affected cryptocurrency.

Various technological solutions have been introduced to prevent 51 per cent attacks (or at least to make them much more difficult or uneconomical) but it remains a risk, particularly to smaller cryptocurrencies.

The resilience of a particular cryptocurrency to a '51 per cent attack' will depend on the method used to verify new transactions.

For those cryptocurrencies using the 'proof of work' concept (such as Bitcoin) carrying out a 51 per cent attack would require a person to control 51 per cent of the computing power required to verify transactions, which would generally require a lot of power and would be expensive in terms of electrical cost. It also becomes much harder to perform the larger the network becomes, which means a cryptocurrency such as Bitcoin is often regarded as being at no risk of such an attack.

For those cryptocurrencies using the 'proof of stake' concept whereby transactions are verified by user depending on the amount of the cryptocurrency they hold, such an attack would require substantial holdings in that currency (and the logic is that if you hold more than 51 per cent of a currency it would not be in your interest to undermine confidence in it and thereby lower the price).

(ii) Cryptocurrencies being used as bait for fraudulent schemes

Perhaps the most high-profile instances of fraud concerning cryptocurrencies is, ironically, where they are not used at all; fraudsters have attracted huge amounts of investment for so-called cryptocurrencies or products related to the crypto market where there is no such product, or they have used the investment for entirely different purposes.

For example, fraudsters have launched sham cryptocurrencies or initial coin offerings (ICOs) that are not based on genuine blockchain technology or are otherwise designed purely to swindle investors out of their money. Many take the form of traditional Ponzi schemes: early investors are led to believe that the tokens or coins they have purchased or earned have significantly increased in value, so they not only acquire more themselves but also encourage friends and family to follow suit. Ultimately, however, investors may be unable to convert their tokens/coins into fiat or a more reputable cryptocurrency if they cannot be traded on exchanges, or sales are to new investors entering the fray in the expectation of similarly large gains. When it becomes apparent that there is no genuine blockchain technology underpinning the currency and that the price has been propped up purely by speculative investment, the fraud is uncovered and the price of the investments inevitably crashes with the rogue 'founder' often having walked away with much of the investment.

In circumstances where many people have made huge (and very real) profits, it becomes difficult to gauge whether projected profits are unrealistic or simply in line with the boom cycle of this fledgling market. The sheer number of cryptocurrencies that have emerged in the past few years and the fact that hitherto unknown personalities are responsible for creating some of the most successful variations in this market has made it difficult for an uninformed investor to separate the wheat from the chaff.

Even well-informed and sophisticated investors have been caught out. An investment fund that sold itself to investors on the basis that it would generate profit by arbitraging from the minor price differentials across numerous cryptocurrency exchanges attracted almost US$100million of investment. However, the fund manager had no such technology and used the

investments for an entirely different purpose (reportedly to fund his own lavish lifestyle). Whilst this scenario could arise regardless of the investment type, those investing in funds will tend to go by the investment manager's track record and reputation. In a market that is still young, there is only a relatively limited timeframe over which to adjudge the bona fides of investment managers running crypto-specialised funds.

(iii) Cryptocurrencies used as proceeds of fraud or other wrongdoing

The final category of misuse is where cryptocurrencies represent the proceeds of wrongdoing. For example, where hackers demand a ransom in cryptocurrency that is ultimately paid, or where a fraudster deceives a person into sending them a quantity of cryptocurrency to which they are not entitled. It is in these scenarios where asset recovery specialists will most likely step in to assist with the identification, tracing and recovery of the ill-gotten cryptocurrency or its proceeds.

It may not come as a shock that cryptocurrencies are being used in this way given the 'pseudonymity' attached to the ownership of cryptocurrencies and the speed with which ownership can change and its value converted into other currencies (whether crypto or fiat).

However, because blockchain technology provides a permanent and unbroken record of transactions, it should be possible to identify what has happened to the proceeds of the wrongdoing, at least until it is converted back into fiat currency (even where an owner's private key is held offline – in a 'cold wallet' – it remains possible to determine the public address or key that owns the cryptocurrency).

Tracing, preserving and recovering cryptocurrencies

Where cryptocurrencies are used to dissipate, conceal and/or launder the proceeds of wrongdoing, those assets are liable to be traced and recovered by the victim of the wrongdoing.

As with any asset-tracing and recovery exercise, it will be necessary to ascertain where the assets are located, ensure that they are not dissipated and then reverse the harmful transaction or compel the fraudster to return their ill-gotten gains to the victim or otherwise compensate them. When recovering crypto it will often be necessary to confront the additional complications of: (i) not knowing the identity of the fraudster; (ii) potentially having to unravel numerous transactions by which the tainted cryptocurrency has been moved across different accounts or by which it has been converted into another form of currency; and (iii) determining the relevant governing law.

Publicly available information should reveal the address that has been used to receive the ill-gotten cryptocurrency and whether the cryptocurrency is still held there and, if not, the address to which it was transferred.

In many instances it should be possible, in principle, for victims to obtain injunctive relief, either in the form of a proprietary injunction or a worldwide freezing injunction, to prevent the wrongdoer moving or dealing with their ill-gotten assets whilst steps are taken to identify the wrongdoer and recover the assets in question. Whether injunctive relief will be available in a particular case will depend on the law that governs the cryptocurrency in question. The position adopted by the courts in England & Wales (most recently in *AA v Persons Unknown* [2019] EWHC 3556 (Comm)) is that cryptocurrencies are a form of property such that injunctive relief can be obtained to prevent the cryptocurrency being dealt with. That is an approach which is likely to be followed (to the extent it hasn't already) in other parts of the Commonwealth and in overseas territories. The *sui generis* nature of cryptocurrency means it can be difficult to ascertain the relevant governing law. Fortunately, the interim basis on which injunctive relief will generally be sought means that an applicant will only need to present a prima facie case that the court is applying the correct law and that it has the necessary jurisdiction to grant the relief sought.

Even in circumstances where the identity of the wrongdoer holding the cryptocurrency is unknown at the time of obtaining injunctive relief, where the currency is held within or moved to a hot wallet (i.e. an account that is accessed online) an injunction brought to the attention of the third-party custodian that manages that wallet should ensure the assets cannot be dealt with by the wrongdoer (the custodian will hold the private key).

Disclosure orders can be used against the exchange to which any relevant addresses are linked to compel production of information that will reveal the identity of the owner of the address, assuming the exchange holds know your customer (KYC) information. If the exchange does not hold such information, then chances are that the owner will be limited in terms of the currency that can be withdrawn in a single transaction or the type of asset they can receive in exchange. Disclosure orders can also be sought against the unknown wrongdoer directly – these have become known as 'Spartacus orders' – albeit they will only be effective if the wrongdoer is sufficiently concerned about being in contempt of court so as to comply with the order.

At this juncture it is important to bear in mind that because most exchanges limit the extent to which crypto can be exchanged for fiat currencies unless the account holder has provided KYC information, in most cases this will mean that the wrongdoer has either retained the proceeds of wrongdoing in crypto, which should be easily traceable, or they have converted those proceeds into fiat currency, in which case they will likely have used an account with an exchange for which they would have had to provide KYC information revealing their identity and residential address. Consequently, the victim can ultimately, subject to the applicable governing law, seek to recover ill-gotten gains using traditional asset recovery actions. Where available, actions may entail restitutionary claims in unjust enrichment (aimed at disgorging profits made by the wrongdoer) or tortious claims based in deceit (aimed at compensating the victim for any loss suffered).

In circumstances where it has not been possible to act in time to prevent the wrongdoer converting the ill-gotten cryptocurrency into fiat currency (or other traditional asset classes) asset recovery lawyers will be on familiar ground. Whilst the use of cryptocurrencies may have given the wrongdoer a head-start in their concealment/laundering efforts due to the speed of transactions, the process of tracing the proceeds of wrongdoing should be relatively straightforward given the comprehensive records of transactions stored on blockchains and the ability to associate trading accounts with real names (at least those accounts used to trade in or out of fiat currencies).

A condensed version of this article first appeared on Fraud Intelligence (counter-fraud.com).

Christopher Pease
+1 284 852 4385
christopher.pease@harneys.com
British Virgin Islands

For more information and key contacts please visit **harneys.com**