Cryptocurrency

THE DAYS OF A "WILD WEST" CRYPTOCURRENCY MARKET ARE DRAWING TO A CLOSE

Inside:

Concerns about security, price volatility and secrecy have attracted lawmakers who have pledged to take a much tougher stance in 2019.

AUTHORED BY:

ALEX HODGSON AND
BERNARD REGAN

btvk advisory

INTRO

Financial investigators are becoming more skilled at tracing assets and shining a light on some of the shady corners of the cryptoasset market.

CONTENTS

2 Bitcoin and Other Cryptocurrencies

4 Bitcoin – An Overview

6 Keys and Padlocks

8 Mining and the Blockchain

10 Putting An Investigation Team Together

12 Interrogation of Devices and Seizures of Digital Artifacts

14 Identifying the Entry and Exit Points

16 The Importance of the Bitcoin Exchange

18 Seizing Assets

20 Structure of Work

Introduction

The days of a “Wild West” cryptocurrency market are drawing to a close. The cryptoasset market has been described more than once as the “Wild West” because of concerns about security, price volatility and secrecy, and the tempting environment that those factors create for criminals. The portrayal of the crypto world as a lawless one has attracted the attention of lawmakers who have pledged to take a much tougher stance in 2019. Meanwhile, financial investigators are becoming more skilled at tracing assets and shining a light on some of the shady corners of the cryptoasset market.

A UK Treasury Committee report in September 2018 called for regulation of the “Wild West” cryptoasset market. In October 2018 the UK’s Cryptoassets Taskforce – made up of HM Treasury, the FCA and the Bank of England – published a report detailing the current state of the UK’s regulatory perimeter and its applicability to cryptoassets, as well as setting out its plan, to be carried out throughout 2019, to develop the UK’s regulatory environment so as to prevent the use of cryptoassets for illicit activity; to guard against future threats to financial stability and to encourage responsible development of cryptoasset-related activity.

In January 2019 the FCA took the first step in that plan by publishing a Consultation Paper, aimed at providing guidance to interested parties as to where the regulatory perimeter sits with regard to different types of cryptoassets, to be followed by a consultation period lasting until 5 April 2019; with final guidance to be published by Summer 2019.

On a wider scale, by the end of 2019 jurisdictions across the EU will be required to transpose the provisions of the Fifth Anti Money Laundering Directive (“5AMLD”) into national law, which substantially updates existing regulations to deal with the illicit use of cryptocurrencies and other cryptoassets. The UK Government has committed to going significantly beyond the requirements set out in 5AMLD, to provide one of the most comprehensive responses to the illicit use of cryptoassets in the world.

As with any regulatory system, the regulations are only of value if they are enforceable. In the case of the illicit use of cryptocurrencies, such enforcement relies upon the ability to uncover the facts, reconstruct money flows, trace assets, and successfully achieve restitution; through the courts or otherwise.

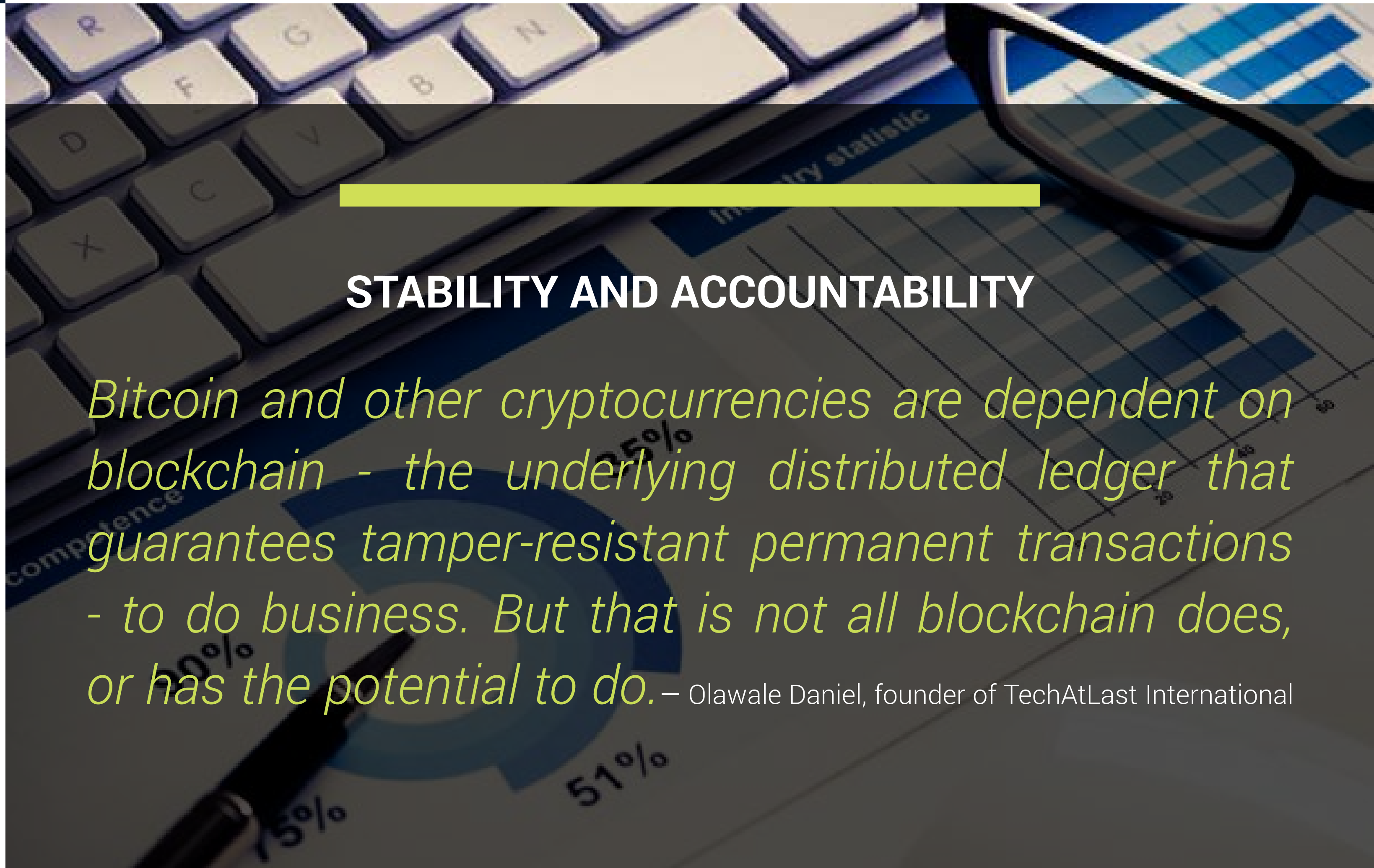
✓ Bitcoin is a decentralised, peer-to-peer cryptocurrency that operates using a complex encryption/decryption process involving public and private keys

✓ The blockchain acts as a publicly-accessible ledger of Bitcoin transactions, which helps ensure Bitcoin ownership and allows .investigators to trace payments

✓ Because of both its popularity and volatility, Bitcoin markets could soon be policed more closely as lawmakers look to develop .new regulations and policies

Bitcoin and other cryptocurrencies

At the time of writing there are more than 2,000 cryptocurrencies in circulation. It would be impractical to write a manual that deals with asset tracing in every cryptocurrency – it would doubtless be outdated long before it was completed. However, many cryptocurrencies, such as Bitcoin and Litecoin, are closely related to each other. Others, such as Ethereum, have more noticeable differences, while still others, such as Monero, have additional anonymising techniques hard-wired into them. Such currencies are substantially more resistant to investigation. In this paper, we concentrate on the most widely-used and well-known cryptocurrency: Bitcoin. We highlight at the outset that the contents of this paper may be more or less applicable to other cryptocurrencies, and that the ability of the investigator to generate useful results may depend partially upon which cryptocurrency is under investigation.



STABILITY AND ACCOUNTABILITY

Bitcoin and other cryptocurrencies are dependent on blockchain - the underlying distributed ledger that guarantees tamper-resistant permanent transactions - to do business. But that is not all blockchain does, or has the potential to do. – Olawale Daniel, founder of TechAtLast International

Bitcoin – an overview

Bitcoin is a decentralised, peer-to-peer cryptocurrency that has been trading since 2009 and is the first widespread non-fiat "currency". The use of the word "currency" is itself a contentious issue. Bitcoin has many features of a currency and is often described as such. However, many international regulatory authorities, including the Bank of England, do not recognise it as money. In a March 2018 speech entitled "The Future of Money", Bank of England governor Mark Carney expressed the view that cryptocurrencies should not be treated as currencies, on the grounds that they are too volatile to be a useful store of value, they are inefficient media of exchange due to the lack of vendors willing to accept them and technical capacity constraints; and they are not used as units of account. Elsewhere in the world, the Securities and Exchange Commission in the USA likewise refuses to recognise cryptocurrencies as currencies. A recent legal case that garnered widespread attention in the USA was that of *HashFast Technologies LLC v Lowe*, in which the judge disappointed many observers by not making a 'cutting-edge ruling' about whether Bitcoin should be considered a commodity or a currency. However, the worldwide trade in foreign currency is a useful analogy for some (but not all) features of Bitcoin. To reflect this uncertainty, this paper will refer to Bitcoin as a "currency", using speech marks throughout.

Understanding the principles of Bitcoin investigations necessitates an understanding of some key issues.

Keys and padlocks

The principle of asymmetric cryptography is that everyone has a public key and a private key. The public key is visible to everyone, and the private key is kept secret. The keys work together such that the public key can encrypt a message, which can then only be decrypted by the private key. However, it is not possible to work out a user's private key from the public key. It may be helpful to think of the public key as a padlock, and a private key as the padlock key.

Let us suppose that Alice wishes to send a private message to Bob. She possesses one of Bob's padlocks, because they are available to anyone who wants one. She signs the message, puts it in a strongbox and locks it using Bob's padlock (encrypts it using Bob's public key). She then sends the message to Bob. Everyone else can see that a message is being sent, but no-one can read it, because no-one else has Bob's private key. The message reaches Bob, who can tell that it came from Alice (because she has signed it with her private key, although not so as to allow Bob to reconstruct it), and can unlock it using his private key.

Bitcoin works analogously. If Bob is a Bitcoin user, his public key is his "Bitcoin address". In reality, Bob is likely to have many Bitcoin addresses, as most Bitcoin users do. Alice may send bitcoins to one of Bob's addresses by encrypting a transaction. Once this has been done, nobody but Bob, not even Alice herself, may decrypt it.

Most users have user interfaces (known as wallets) that carry out the mechanics of the encryption and decryption. The wallet software typically generates the private keys, and corresponding public keys, on behalf of the user, often from a "master" or a "seed" key, reducing the risk of keys being lost.

Crucially, the private keys must be kept private at all costs. It is functionally as good as impossible to work out a user's private key from their public key, even though they are intrinsically linked, because the encryption is asymmetric. However, the private key is by itself sufficient to authorise the transfer of bitcoins away from an associated address. Therefore, if the user lets a private key slip, any bitcoins in the related address can be stolen.

The pitfalls of losing a private key are neatly encapsulated by the tribulations of Quadriga CX, Canada's largest cryptocurrency

1998 - 2009

The early years – pre-Bitcoin

Although Bitcoin was the first established cryptocurrency, there had been previous attempts at creating online currencies with ledgers secured by encryption. Two examples of these were B-Money and Bit Gold, which were formulated but never fully developed.

2009

Bitcoin begins

The Bitcoin software is made available to the public for the first time and mining – the process through which new Bitcoins are created and transactions are recorded and verified on the blockchain – begins.

2010

Bitcoin is valued for the first time

As it had never been traded, only mined, it was impossible to assign a monetary value to the units of the emerging cryptocurrency. In 2010, someone decided to sell theirs for the first time – swapping 10,000 of them for two pizzas. If the buyer had hung onto those Bitcoins, at today's prices they would have been worth more than $70 million.

2011

Rivals emerge on the market

As Bitcoin increases in popularity and the idea of decentralized and encrypted currencies catch on, the first alternative cryptocurrencies appear. These are sometimes known as altcoin and generally try to improve on the original Bitcoin design by offering greater speed, anonymity or some other advantage. Among the first to emerge were Namecoin and Litecoin. Currently there are over 2,000 cryptocurrencies in circulation with new ones frequently appearing.

2013

Bitcoin price crashes

Shortly after the price of one Bitcoin reaches $1,000 for the first time, the price quickly begins to decline. Many who invested money at this point will have suffered losses as the price plummeted to around $300 – it would be more than two years before it reached $1,000 again.

2014

Scams and theft

Perhaps unsurprisingly for a currency designed with anonymity and lack of control in mind, Bitcoin has proven to be an attractive and lucrative target for criminals. In January 2014, the world's largest Bitcoin exchange Mt.Gox went offline, and the owners of 850,000 Bitcoins never saw them again. Investigations are still trying to get to the bottom of exactly what happened but whatever the story, someone dishonestly got their hands on a haul which at the time was valued at $450 million dollars. At today's prices, those missing coins would be worth $4.4 billion.

2016

Ethereum and ICOs

One cryptocurrency came close to stealing Bitcoin's thunder this year, as enthusiasm grew around the Ethereum platform. This platform uses cryptocurrency known as Ether to facilitate blockchain-based smart contracts and apps. Ethereum's arrival was marked by the emergence of Initial Coin Offerings (ICOs). These are fundraising platforms which offer investors the chance to trade what are often essentially stocks or shares in startup ventures, in the same manner that they can invest and trade cryptocurrencies. In the US the SEC warned investors that due to the lack of oversight ICOs could easily be scams or ponzi schemes disguised as legitimate investments. The Chinese government went one further, by banning them outright.

2017 - 2019

Bitcoin continues to grow

After a huge price spike in late 2017 and subsequent collapse, Bitcoin prices declined throughout 2018 as investors remained cautious. However, with the promise of better regulation across the world's major economies, and increasing mainstream investor attention, prices tripled in the first half of 2019, and the market cap of all cryptocurrencies rose from $11bn to its current height of over $300bn. Banks including Barclays, Citi, and Deutsche Bank have said they are investigating ways to work with Bitcoin, and the tech giant Facebook has announced the launch of Libra, its own cryptocurrency. Meanwhile the distributed ledger technology behind Bitcoin – blockchain – has sparked a revolution in the FinTech industry (and beyond) which is only just getting started.

> Whatever your opinion on Bitcoin and cryptocurrency – and educated commenters have described them as everything from the future of money to an outright scam – it seems they are here to stay. Will it succeed in doing what many early adopters and evangelists claim it is destined to – replace government-controlled, centralised money with a distributed and decentralized alternative, controlled by nothing besides market forces? Well, this year may yield some clues but we are unlikely to know the answer for some time yet.

https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/#199ccfad3f27

PITFALLS

The pitfalls of losing a private key are neatly encapsulated by the tribulations of Quadriga CX, Canada's largest cryptocurrency exchange. It held the equivalent of £145 million in Bitcoin and other cryptocurrency reserves in a "cold wallet" (broadly analogous to a savings account at a bank, as opposed to a "hot wallet" current account) accessed by a private key known only to its chief executive, Gerald Cotton. Tragically, it was announced in January 2019 that Mr. Cotton had died. It appears that any knowledge of the relevant private key died with him (although the investigation continues, and some reports suggest that at the time of Mr. Cotton's reported death, Quadriga's holdings may in fact have been lower than previously believed). There is no Bitcoin Central Bank or court of appeal. If the private key to a cryptocurrency account is lost, the cryptoassets in that account are forever unavailable.

As a result of Mr. Cotton's death, it appears that Quadriga (and its customers) have permanently lost their funds. The company has filed for creditor protection in Canada, but it appears doubtful that it can survive.

Mining and the blockchain

Returning to Bob and Alice, thanks to asymmetric encryption Bob knows that the bitcoins he has received originated from Alice. However, he must also be sure that Alice had those bitcoins to spend. Bitcoin provides this assurance with blockchain technology. A blockchain is a publicly-accessible ledger in which every previous transaction is recorded, so that the contents of any Bitcoin address can be checked at a glance. The system outsources the laborious task of checking every new transaction against the blockchain to Bitcoin users known as "miners".

A blockchain is a series of blocks, each of which contains a megabyte's worth of transactions that have been checked against the blockchain for legitimacy by the miner that built it. Once the block has been added, it becomes part of the blockchain and therefore part of the publicly-accessible record. Each block also contains a cryptographic hash of all of the data in the previous block, so the blocks form a chain. On average, a new block is created approximately every ten minutes. The reward for the miner is the transaction fees that accompanied each transaction in the block, and a number (currently 12.5) of freshly-minted bitcoins that are released to the miner. Becoming a miner involves setting a computer to checking transactions, building a block, and racing against other prospective miners to solve a complex and time-consuming mathematical "proof-of-work" problem (to regulate the speed at which new blocks can be created) to be allowed to add the block to the system.

The entire transaction history of every Bitcoin address is also publicly available. The transaction history includes:

- The sending address or addresses;
- The receiving address or addresses;
- The date and time of the transaction, accurate to the second; and
- The amount transferred to each recipient.

The determined user can utilise services such as coin mixing and CoinJoin to disguise their transactions to a degree, and opinion is divided on the efficacy of such devices. However, without such additional efforts, which many users do not attempt, the entire transaction history of any and every Bitcoin address is freely and immediately available to all.

The key issue for the investigator, therefore, is not traceability: it is attribution.

Putting an investigation team together

It is in the nature of a cryptocurrency asset tracing assignment that it can be as much an IT exercise as an accounting one. Therefore, it is crucial that an investigation team should have access to forensic technology expertise as well as accounting and investigative expertise at an early stage, particularly given the fragility and volatility of some computer-based evidence.

Additionally, the legal and regulatory framework that applies to cryptocurrencies is evolving as governments and regulators scramble to update existing regulatory systems that pre-date, and which therefore were not designed to deal with, cryptocurrencies. Against such a backdrop, early access to specialist legal counsel may be crucial to the success of an investigation and any subsequent court action.

Of course, in many of the cases in which a cryptocurrency asset tracing assignment might be required – fraud, money laundering, contentious litigation, etc. – the need for legal counsel will already be apparent to the parties involved.

The investigation itself may include, inter alia:

- Blockchain analysis;
- Seizure and interrogation of electronic devices;
- Examination and analysis of bank records;
- Physical searches of home and office addresses;
- Interviews with witnesses, parties to litigation, suspected co-conspirators and/or primary suspects;
- Applications for disclosure orders to be served on banks, exchanges or wallet providers; and
- Review and analysis of complicated and extensive transaction data.

Therefore, a robust mixture of accounting, technical, investigative, data analytic and legal skills is a critical factor in the success of an investigation.

Interrogation of devices and seizure of digital artefacts

If the circumstances are such that forensic examination of devices is lawful and practical, the investigator is potentially in a position to gather crucial information. Any device with an internet connection may contain essential data. As with most investigations, forensic images of the device's hard drive and RAM should be taken at the time of appropriation.

To exchange and transact with Bitcoins the user ordinarily downloads wallet software. As with any other software, this entails local storage of program and user data. Successful interrogation of the wallet software may yield information including the user's transactions, the wallet's default keys, reserve keys, accounts, and addresses.

Additionally, wider interrogation of computer files and correspondence records may provide further valuable evidence linking addresses to individuals. A Bitcoin address is a string of 26-35 characters encoded in Base 58. The string will generally begin with 1, 3, or "bc1", and most users have many such addresses. It is highly unlikely that any Bitcoin user will retain them mentally, or on scraps of paper. Bitcoin transactions will therefore generate electronic records (probably through a wallet provider) and/or electronic correspondence with counterparties.

This has implications for device and communication archive searches. It is straightforward to code a search algorithm that searches for 26-35 character strings of letters and numbers in Base 58, as well as for some of the other distinctive keywords that indicate Bitcoin use.

There are a number of other ways in which a Bitcoin address could be attributed to a person.

"Encoded in Base 58" means that each 'digit' of an address can be one of 58 characters, being the numerals 1-9, the 25 lower case letters excluding l (lower-case L, because it resembles the number 1), and the 24 upper case letters excluding I and O (because they resemble the numbers 1 and 0).

Public advertisement

Occasionally, Bitcoin addresses are published on social media. The document archive and disclosure website WikiLeaks, for example, periodically advertises a Bitcoin address via Twitter to solicit donations. Users of online forums occasionally post their Bitcoin addresses, often while asking for community help or advice. The question in such cases becomes one of attributing the social media account, rather than the Bitcoin address, to the individual.

Real-world purchases

Some merchants accept purchases in Bitcoin. Expedia was previously one such merchant, who allowed hotel rooms (but not flights) to be booked using Bitcoin between 2014 and 2018. As at January 2019, there were between 500 and 600 retailers in the UK that accepted Bitcoin as a means of payment. Any such retailer may hold information (such as shipping addresses for goods) that can assist in de-anonymising the Bitcoin user.

Internet service providers

Bitcoin transactions occur over the internet, and as each transaction occurs it leaves a trail of information that may lead back to the user. As with any other internet traffic, a user's activity is linked to an IP address. Internet Service Providers ("ISPs") analyse the traffic going through their networks and use it to identify users. To counter this deanonymisation threat, many online forums and Bitcoin user guides encourage Bitcoin users to use Virtual Personal Networks to disguise their IP address. The ISP's ability to identify the user may depend on the extent to which the user follows this advice.

Wallet closure

For two different addresses to be used as inputs to the same transaction, the owners of those addresses must know each other's private keys. It is very unlikely, for reasons discussed above, that different users would reveal their private keys to each other. It has therefore been suggested that, if two addresses are used as inputs to the same transaction, it may be concluded that they belong to the same person, which may aid the investigator once a single address has been attributed to a subject.

Identifying the entry and exit points

Crucial to the tracing of cryptocurrency assets is the matter of identifying the point at which the assets entered and, if applicable, exited the blockchain. Often, an investigation can begin with the routine examination of bank statements, which can reveal a transaction to a recognisable Bitcoin exchange.

The blockchain will contain a record of the counterpart to this transaction, i.e. a flow of bitcoins from the exchange to the user. If this transaction can be isolated with a sufficient degree of certainty, the recipient address can be attributed to the user. However, at the time of writing there have been over three hundred and fifty million Bitcoin transactions, which is added to at a current rate of several hundred thousand per day, which makes it difficult to isolate the relevant transaction.

However, subject to the provisos set out below, a record such as a bank statement will give the investigator two crucial pieces of information: the size of the transaction, and the date and time of the transaction. Often, a bank statement will list the time of the transaction to the minute. Historical bitcoin exchange rates are readily available online, and many Bitcoin exchanges have websites that are trading platforms analogous to foreign currency exchanges, which detail factors such as bid-ask spread, other transaction fees or commissions. The size of the transaction in bitcoin may therefore theoretically be calculated, at least to the extent to which the investigator can develop a value range and a date and time range.

At this point the blockchain may be usefully interrogated. If there is only one transaction of the appropriate size at the appropriate time, the recipient address of that transaction may be attributed to the user. If the blockchain informs us that the sending address was involved in several thousand other transactions in that month, we may take further comfort in our attribution, as this is likely to be an exchange. If an open source search on the sending address reveals that the address belongs to the exchange named on the bank statement, yet further comfort may be achieved.

However, there are real-world issues that may render calculations of both value and time inaccurate. In respect of time, the bank statement may be inaccurate, due to processing times or bank error. Additionally, the subject may have charged their exchange account with the cash, but not immediately converted it to bitcoins.

Inaccuracies may also arise due to the workings of the exchange. Some exchanges "bunch" transactions together, paying multiple recipients in the same transaction. The time it takes to gather together a suitable number of recipients may be of such a duration as to invalidate the information from the bank. A small timing difference may move the target transaction outside of the investigator's search range, or bring too many other similar transactions within it, or render the value calculation misleading due to exchange rate fluctuations.

There are additional problems with calculating the transaction size. Not all databases of historic exchange rates agree with each other, and even minute-by-minute historical data may mask exchange rate variances, given Bitcoin's volatility.

As a general rule, the more transactions that can be identified, and the less common the amounts involved, the greater the prospect of identifying the transactions on the blockchain. One transaction of £100 may be nearly impossible. Six transactions to the same address over a five-month period, each of £30,000, may be significantly easier.

The importance of the Bitcoin exchange

Significant information about any such transactions should be available from the Bitcoin exchange itself, which, depending on local jurisdiction, may be required to collect Know Your Customer information from its customers, which may be accessible via disclosure orders.

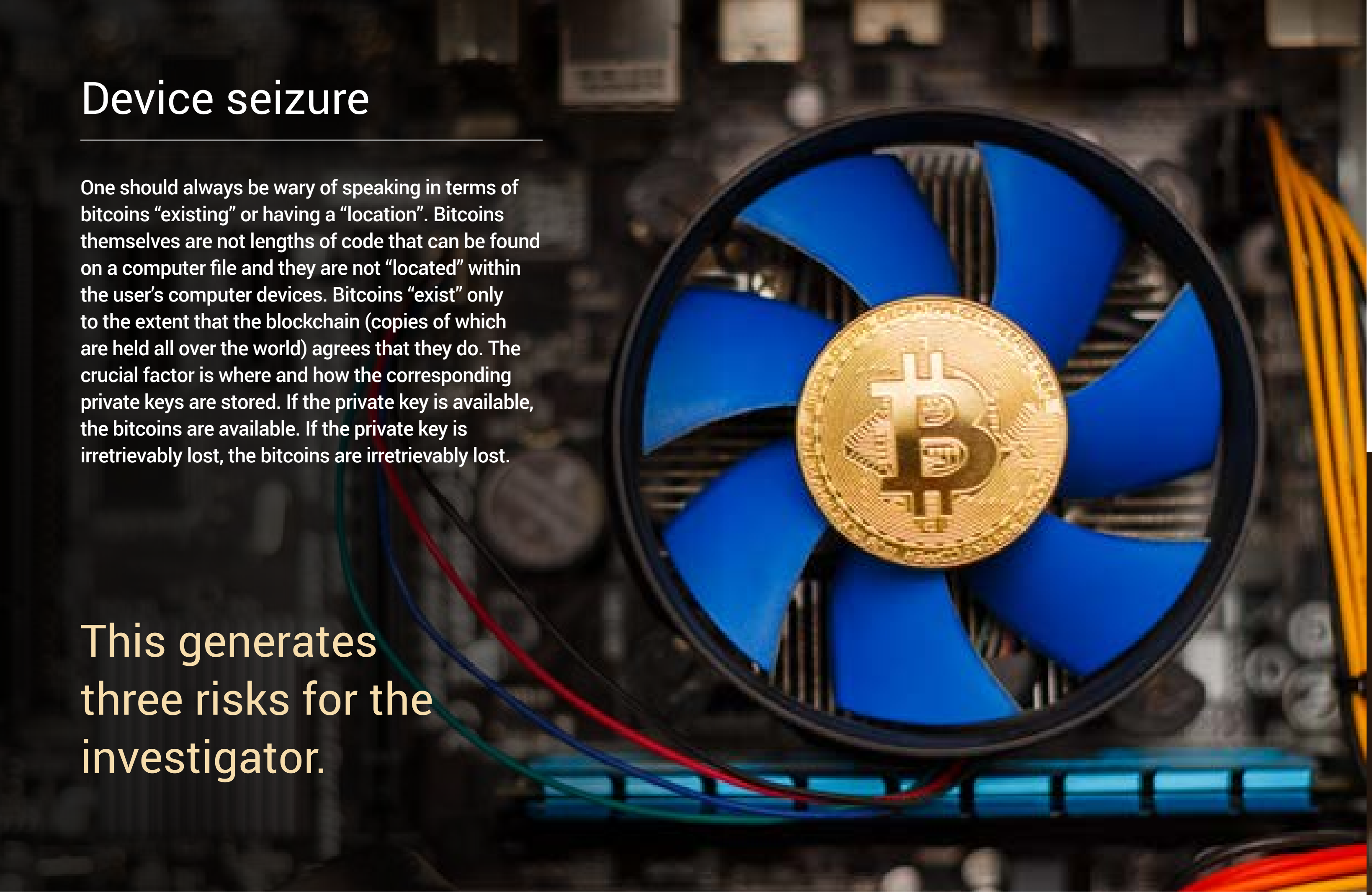
Not all Bitcoin conversions are handled by exchanges, and it is possible for a subject to sell bitcoins privately to another individual, in exchange for cash or a bank transfer. However, in the event that a Bitcoin exchange can be identified as having been used, a successful approach could yield information including:

- **Evidence that links the subject to one or more Bitcoin addresses;**
- **Other cryptocurrency transactions involving the subject; and**
- **The location of assets, including previously-undiscovered bank accounts.**

Additionally, and as referenced earlier in this paper, EU member states have until 10 January 2020 to transpose the Fifth Anti Money Laundering Directive ("5AMLD") into their national laws. 5AMLD is the EU's first attempt expressly to regulate cryptocurrency exchanges and wallet providers. This directive has the potential to improve the quality and the accessibility of information from such organisations. Although the UK may leave the EU in the near future, its government has made a welcome commitment to matching and, indeed, exceeding the provisions of 5AMLD.

Seizing assets

Once Bitcoin assets have been identified, there are a number of other issues that must be considered.



Device seizure

One should always be wary of speaking in terms of bitcoins “existing” or having a “location”. Bitcoins themselves are not lengths of code that can be found on a computer file and they are not “located” within the user’s computer devices. Bitcoins “exist” only to the extent that the blockchain (copies of which are held all over the world) agrees that they do. The crucial factor is where and how the corresponding private keys are stored. If the private key is available, the bitcoins are available. If the private key is irretrievably lost, the bitcoins are irretrievably lost.

This generates three risks for the investigator.

1

If a seized device contains a private key that is not otherwise known, and cannot be reconstructed, then that device is the only gateway to whatever “currency” is at the command of that key. The “value” of the device itself, in such circumstances, may be colossal, so enhanced security procedures may be required.

2

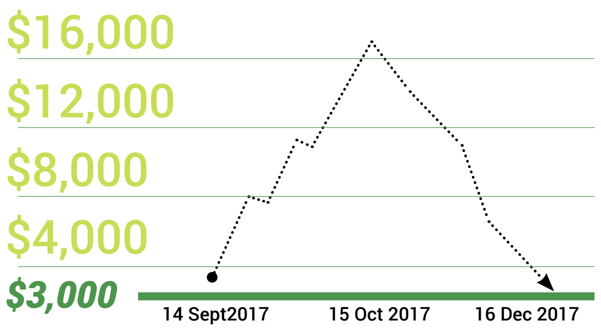
The investigator must not assume that, because a device in which a private key is stored has been seized, the bitcoins are secure. If the device’s owner has also recorded the key elsewhere, or can reconstruct it from a seed key or otherwise, that person may still be able to move the “currency” beyond reach even without the device. In circumstances where this possibility is suspected, the investigator may consider the audacious step of pre-emptively moving the “currency” to a new, secure address, and must balance the evidential and liability risk of doing so with the risk of leaving the “currency” insecure.

3

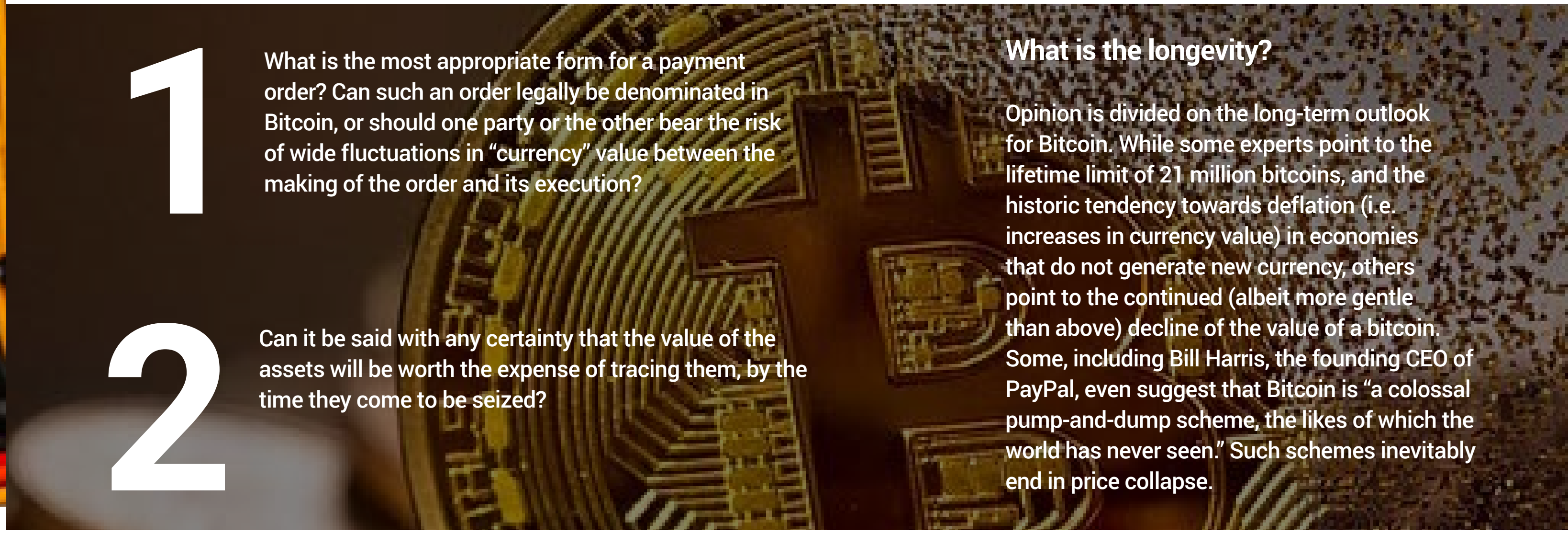
In the event that ownership of cryptocurrency assets is proved, a risk arises that their owner may, in court proceedings, claim to have lost his or her private key, such that no payment order can be complied with, until after the case has settled, whereupon the key is “re-discovered”. Should possibilities related to seizure and examination of devices be exhausted, one novel possibility, as used in the HashFast case referenced above, is a freezing order on a Bitcoin address. However, there may be significant legal and practical obstacles to overcome in the enforcement of any such order.

“Currency” volatility

Between 14 September 2017 and 16 December 2017 the value of a bitcoin rose from $3,320 to $16,499, before slumping back just over $3,000 by 16 December 2017. Novelty, intense speculative activity and the lack of a Alex Hodgson is a forensic accountant & former Metropolitan Police detective who now specializes in fraud and related investigative assignments. He is the author of a series of blogs on cryptocurrencies, which are available to read at btvkadvisory.com/blog central bank conspire to make the value of a bitcoin unpredictable.



This raises two issues, one legal and one investigative:



1

What is the most appropriate form for a payment order? Can such an order legally be denominated in Bitcoin, or should one party or the other bear the risk of wide fluctuations in “currency” value between the making of the order and its execution?

2

Can it be said with any certainty that the value of the assets will be worth the expense of tracing them, by the time they come to be seized?

What is the longevity?

Opinion is divided on the long-term outlook for Bitcoin. While some experts point to the lifetime limit of 21 million bitcoins, and the historic tendency towards deflation (i.e. increases in currency value) in economies that do not generate new currency, others point to the continued (albeit more gentle than above) decline of the value of a bitcoin. Some, including Bill Harris, the founding CEO of PayPal, even suggest that Bitcoin is “a colossal pump-and-dump scheme, the likes of which the world has never seen.” Such schemes inevitably end in price collapse.

Structure of work

To mitigate the investigative risk, we would not ordinarily expect to be instructed to undertake a full-scale asset-tracing assignment without a preliminary fact-finding stage. In this stage, we would conduct a review of the information at hand, including some preliminary searches, to determine what evidence might be present, and answer the following questions in high level terms:

- Is there evidence that the subject has or had possession of cryptocurrency?
- Can such assets be identified and traced?
- If not, can we identify entities that may be able to provide further information?
- Are disclosure orders a viable possibility?
- Can we identify any cryptocurrency exchanges involved?
- If so, what information can we expect to be available from them?
- Can we give a preliminary estimate of the value of any assets that we can identify?

If there are devices available for interrogation, we would seek to identify and locate any wallet software. For any devices that do not contain such software, we would secure the device’s RAM and hard drive, and review web history for online wallet management, residual files and transactions, and user information.

The purpose of this stage would be to provide an indication of whether a full-scale asset recovery process would be feasible and worthwhile, without incurring excessive fees. If a reasonable prospect of success could be established, we would set out how we would identify, locate and seize the assets.

> *We would seek to identify and locate any wallet software. For any devices that do not contain such software, we would secure the device’s RAM and hard drive, and review web history for online wallet management, residual files and transactions, and user information.*

Cryptocurrency transactions do not exist in a vacuum: the transactions that underlie them also generate computer data, correspondence and other ancillary records. The success of an asset tracing assignment will depend on the investigator's ability to uncover and interpret those records.

Conclusion

Bitcoin affords an opportunity to develop a keen understanding of the difference between traceability and attribution. It is often said, erroneously, that transactions that take place via Bitcoin are not traceable. In fact, Bitcoin transactions are among the most minutely traceable in world finance. The blockchain works such that every transaction that has ever taken place is freely available to everyone who wants to know, so it should never be assumed that cryptocurrency presents an immediate dead end to the investigator. Cryptocurrency transactions do not exist in a vacuum: the transactions that underlie them also generate computer data, correspondence and other ancillary records. The success of an asset tracing assignment will depend on the investigator's ability to uncover and interpret those records.

If cryptocurrency markets were like the "Wild West" in their early years, that period may be coming to a close as lawmakers look to toughen up the way in which markets are policed. In the meantime, it would be wrong to assume that investigators are powerless in the world of virtual currencies. They have many tools, old and new, at their disposal which mean that cryptocurrency markets should not be seen as a safe hiding place.

Alex Hodgson, BA (Oxon), is a forensic accountant and former Metropolitan Police detective who now specializes in fraud and related investigative assignments. He is the author of a series of blogs on cryptocurrencies,which are available to read at btvkadvisory.com/blog.

Bernard Regan, MSc, MBCS, is a director of forensic technology. He specialises in the application and management of computer forensic processes, including cybersecurity, digital forensics, data analytics and e-discovery.

CONNECT WITH US:

BTVK Advisory

btvkadvisory.com

btvk advisory