LLOYD'S

Emerging Risk Report – 2015
Innovation Series

TECHNOLOGY

Bitcoin

Risk factors for insurance

Disclaimer

Key contacts

Nick Beecroft – Manager, Emerging Risks & Research
+44 (0)20 7327 5605 nick.beecroft@lloyds.com

For general enquiries about this report and Lloyd's work on emerging risks, please contact emergingrisks@lloyds.com

Contents

Executive summary

This report presents two expert contributions which investigate the key risk factors for the insurance of Bitcoin operations. Their findings suggest that the technology, procedures and practices that underpin Bitcoin are maturing. Nevertheless, legitimate concerns remain over security risk and the potential for criminal exploitation. The report does not, therefore, endorse the insurance of Bitcoin operations, but rather aims to contribute to the assessment of these risks for insurance purposes.

Bitcoin risk has been brought into sharp focus by high-profile losses such as that suffered by the original Bitcoin Exchange, Mt. Gox, in 2014. Furthermore, Bitcoin losses from fraud and theft in 2014 represented a much higher share of the overall volume of transactions compared with credit card fraud. These factors, when combined with the intangible and novel nature of Bitcoin, have served to generate a high degree of uncertainty over its security and credibility as a store of value.

Benefits of Bitcoin

In essence, Bitcoin offers a low-cost, relatively fast means to transfer value anywhere in the world; the only real constraint is the availability of an internet connection. As such it offers a lower-cost alternative to established banking and money transfer systems, which require a bank account and/or the payment of fees. These benefits could be very significant for a wide range of users around the world.

Security risk

Bitcoin is both a digital asset and a network, and both are exposed to the potential for cyber attacks. The particular characteristics of Bitcoin make it an attractive target for cyber attack because the stolen data has instant value, and transactions are not reversible. These vulnerabilities can be managed through effective security encompassing not only cyber security, but also well-established physical and personal measures used to protect other valuable assets that share these characteristics. Nevertheless, Bitcoin (like all financial services entities) faces a dynamic threat, and the security risk will never be reduced to zero. The establishment of recognised security standards for cold (offline) and hot (online) bitcoin storage would greatly assist risk management and the provision of insurance.

Forms of attack against Bitcoin

A variety of tactics have been developed for the theft of bitcoins, and this report classifies these as 'local' – those designed to steal specific bitcoins – and 'global' – those which manipulate the network to steal bitcoins. Technical and procedural mitigations are developing, but a number of vulnerabilities remain. As with any system of security, measures must evolve with the threat, and their effectiveness will rely on routine and robust application.

Exploitation by criminals

There are legitimate concerns that the absence of regulation and potential anonymity of transactions in the Bitcoin network could afford real advantages for criminals. Nevertheless, it should be remembered that a Bitcoin transaction does leave a digital trail. It is essential for the long-term viability of Bitcoin that it does not become synonymous with crime, and the Bitcoin community should co-operate with law enforcement agencies to prevent exploitation by criminal networks.

Innovation

The short history of Bitcoin has been punctuated by high-profile security incidents and substantial price volatility. Challenges such as these have characterised many emerging technologies, and there are signs that the technology, together with the procedures and professional capabilities of practitioners, are maturing. Insurance can be a component of responsible risk management to enable the next phase of Bitcoin's evolution.

Introduction: insurance of Bitcoin operations

The growing volume of Bitcoin transactions is generating demand for insurance cover for Bitcoin operations and this report was commissioned to investigate the risks that insurers should consider in designing risk transfer.

Jerry Brito and Peter Van Valkenburgh (Coin Center) describe a classification of 'local attacks' – i.e. those designed to steal specific bitcoin assets – and 'global attacks' that seek to steal bitcoins by manipulating the Bitcoin network as a whole. Their analysis investigates the capabilities and intent underlying the threat of both forms of attack.

Garrick Hileman (London School of Economics) and Satyaki Dhar provide a wider perspective and examine sources of risk including market volatility and regulatory uncertainty. These sources of risk are unlikely to be directly transferred in an insurance policy, but they are important in shaping the overall risk profile of Bitcoin operations, and therefore provide relevant insights for insurers.

Bitcoin offers the promise of major benefits – for example through bringing global payment technology to populations unable to access or afford conventional banking methods – but it is subject to security risk and legitimate concerns over its potential to be exploited by criminals.

Many of the features of Bitcoin are novel and can be difficult to comprehend for non-specialists. However, the essential components of risk bear similarity with other more established insurable assets. By way of illustration, Bitcoin is a digital asset that provides instant value, a level of anonymity and is not reversible. As such it is fundamentally different to other forms of valuable data, but has many similarities to cash. The security measures required for Bitcoin should therefore be informed equally by the physical and personal protection measures routinely applied for cash, as by the cyber security measures required for sensitive data. A private Bitcoin key kept offline on removable media or recorded on paper should be protected just as if it were a large sum of cash or consignment of gold.

One area of development that would arguably greatly assist risk management, and the provision of insurance, would be the establishment of recognised security standards for cold and hot storage. While this might run against the decentralised ethos of the Bitcoin network, compliance with agreed security standards could be expected greatly to enhance insurers' insight and confidence in the nature of the risk.

The potential for Bitcoin to be exploited by criminals is a legitimate concern. Nevertheless, it should be remembered that Bitcoin transactions, while anonymous, do leave a digital trace that could assist law enforcement. It is imperative for the long-term viability of Bitcoin that is does not become synonymous with criminality, and the Bitcoin community has a responsibility to co-operate in the prevention of crime. Criminal exploitation is a major challenge for the entire banking system, and risk management will need to evolve in line with the tactics and techniques used by criminal networks.

Price volatility and high-profile losses, notably that suffered by Mt. Gox, have generated understandable scepticism over the long-term future of Bitcoin, and this report is not designed to establish its commercial viability. But the challenges that are described in this report should be viewed as symptomatic of an emerging, innovative technology, rather than evidence of underlying critical flaws. There are signs that the technology, together with the skill and professionalism of practitioners, are maturing. With responsible and innovative risk management, insurance can be a key component of the future of Bitcoin.

The following Lloyd's underwriters provided valuable input to the report: Andrew Banks (Ace), Madeleine Bradnam (MR Underwriting), Ross Louden (Novae), Andrew Pearson (Barbican), Jason Roe (Ace).

Operational risks faced by Bitcoin companies

Jerry Brito & Peter Van Valkenburgh

COIN CENTER

Introduction

The February 2014 bankruptcy of Mt. Gox, the original and for three years running largest Bitcoin exchange[1], *may* have been precipitated by a grand digital heist. Mt. Gox announced a "high possibility" that $600 million in bitcoins had been stolen because of a security vulnerability, what CEO Mark Karpelès described as "a bug" in the Bitcoin protocol itself[2]. That claim has come under intense scrutiny[3], and with lessons still waiting to be learned from Mt. Gox, the landscape of risks that surround Bitcoin remains very much *terra incognita*. Before that continent can be explored, some schema must be developed to categorise any potential discoveries. This report aims to create that schema and begin to offer data, primarily in the form of case studies, on the potential risks posed by Bitcoin.

No systemic risk from the emergence of Bitcoin

As a technology poised to disrupt existing financial industries and currencies, Bitcoin may one day pose systemic risks to the economy at large. For the near future, however, it is important to keep these risks in perspective. At present, the scale of the Bitcoin economy is minuscule by global standards. As of January 2015, Bitcoin's total market capitalisation was around $2.5 billion, less than the price tag of Santiago Calatrava's new train station in Manhattan[4]. While Bitcoin's design currently limits transaction volume to seven transactions per second[5], Visa's network is designed to handle peak volumes of 47,000 transactions per second[6]. Should the scale of Bitcoin adoption grow substantially, economy-wide risks may emerge, but this would not be expected to happen in the short to medium term or without warning.

Understanding operational risks

Risks to those within the Bitcoin industry should broadly be divided into price or volatility risk, regulatory risk, and theft or loss risk. The final element of this trio is where Bitcoin sparks particular confusion owing to its technological novelty. The remainder of this report will focus exclusively on those eccentricities and how they can increase or mitigate the theft or loss risks facing a Bitcoin or other cryptocurrency business.

To understand how something might be stolen we need to understand what it is. For traditional assets this perfunctory matter can be taken as writ: a car is a car and usually you can drive it away. For Bitcoin it is the exotic "what is it?" enquiry that occupies the bulk of a risk assessment. The following is a high-level overview of what bitcoins are and how they might be lost or stolen.

Background and classification of threats

Bitcoin is both a network protocol – Bitcoin – and an emerging asset – bitcoin(s).

Bitcoin protocol

As a network protocol, Bitcoin is an open tool for provably sending value between any computers connected to the internet, just as the Hypertext Transfer Protocol (HTTP) is an open tool for sending text and pictures. HTTP is accessed with software that is run by network participants: web browsers (e.g. Google Chrome) and web servers (e.g. Apache Tomcat). The Bitcoin protocol is also accessed with software: bitcoin wallets[7] (e.g. Electrum[8]) and bitcoin mining clients (e.g. bfgminer[9]). Bitcoin is "open" because, unlike a credit card network or a wire transfer service, a user hoping to send or receive value via bitcoins need not apply to an institution for approval or access. She need only download and run free software on her computer.

Bitcoin software is not produced by a single individual or institution. Instead, there is an open-source reference client developed and maintained by a group of "core developers" who have access to a public software code repository on GitHub[10]. Other clients are developed by individuals and institutions building on this reference client. These alternative clients are developed for various reasons: to make the reference client software compatible with different types of hardware or operating systems (e.g. desktop computers vs. smartphones, or Windows vs. Mac) or to offer particular features to end users, such as the design of the client's user interface[11].

Incompatibility would result from altering so-called *consensus rules* found within the reference client. These consensus rules are particular software rules that reject attempts to create fraud on the Bitcoin network by either (A) attempting to spend coins from an address whose keys you do not control, or (B) attempting to "double-spend" coins (i.e. send someone coins that you have already spent elsewhere in a previous transaction). Therefore, even if a malicious software developer was to attempt to alter an independently developed Bitcoin client in order to commit fraud, this attack would be fruitless because other nodes in the network would ignore any actions of the client that violate these fraud-preventing consensus rules[12].

All notable software for accessing the Bitcoin network is open source. Closed-source clients may be developed and are not precluded by the copyright licence under which the Bitcoin reference client is released[13], but the community of Bitcoin users is culturally biased against the creation or use of closed-source clients because it is more difficult to independently audit such software for back-doors that might weaken the network or steal user credentials[14].

Bitcoin asset

There are no physical bitcoins, nor are bitcoins software files like .mp3 music files or Word documents. Instead, a bitcoin, or some fraction of a bitcoin, is a chain of digital signatures stored in a public ledger called the blockchain. The final digital signature in a given chain will be that of the current holder of a bitcoin amount and she will be recognised by the network by a random but unique string of characters, the user's public address. Possession and control over a particular bitcoin holding is synonymous with having knowledge of one or more private keys that are mathematically linked to one or more public addresses. If those addresses have been sent some quantity of bitcoin in the past, as noted by the public record, the user holding the private keys is the only person capable of sending them on to another address.

By signing a transaction message with her private key, the transferor asks bitcoin miners to add a new digital signature, identifying the transferee's public address, to the chain of signatures that proves provenance back to the original creation of a bitcoin or bitcoins. Bitcoins are created when miners solve difficult mathematical problems and faithfully update the blockchain, recording valid transactions across the network that occurred within a ten-minute interval.

The Bitcoin network is not, therefore, a tool for transmitting actual bitcoins. It is a tool for building an authoritative public record that records the chain of title for any current bitcoin holdings, and prevents individuals from creating fraudulent entries in that record by attempting to double-spend their bitcoins or spend some other user's bitcoin. Owning a bitcoin is perhaps most similar to owning land. The *conditio sine qua non* of land ownership is identification in the most recent deed within a chain of title found in a public record. The *conditio sine qua non* of bitcoin ownership is holding the private key that links to the most recent recipient public address within a chain of title found in the blockchain.

Bitcoin businesses

Many Bitcoin users do not choose to directly access the Bitcoin network, relying instead on an intermediary who runs Bitcoin software and, potentially, secures the private keys that constitute a customer's bitcoin ownership. Users may choose to keep their bitcoins with an intermediary, because running Bitcoin software can be technically complicated and leave the user open to theft if she does not properly secure her computer, or loss if she does not make backup copies of her keys[15].

Intermediaries that run Bitcoin software and secure the user's keys are referred to as *cloud wallet* or *hosted wallet* providers; Coinbase[16] and Circle[17] are notable examples. Intermediaries that run software but do not secure keys, leaving them in the user's possession, are referred to as *hybrid wallet* providers; Blockchain.info[18] is a notable example. By contrast, a user who is running her own software and securing her own private keys is running a *software wallet*.

In addition to wallet providers, there are also Bitcoin exchanges (e.g. Bitstamp[19] and the now defunct Mt. Gox[20]) and Bitcoin merchant service providers (e.g. BitPay[21]). These intermediaries will hold keys and run Bitcoin software in order to provide traders or merchants with access to the Bitcoin network.

Classification of operational risks in running a Bitcoin business

This simplified though accurate picture of Bitcoin reveals that all theft and loss risk emerges from two threat vectors: (1) an institution holding bitcoins may suffer a *local attack,* where the thief obtains the institution's private key(s) in order to gain control of bitcoins in the matched public addresses, or (2) a *global attack*, where the thief seeks to manipulate the network in order to create fraudulent transactions within the blockchain that benefit herself or cause harm to her targets.

Local attacks

Capability
To the extent that there is ever a "thing" to be stolen in a local attack, that "thing" is the string of characters that make up a private key[22]. Safeguarding that string is a challenge identical to the safekeeping of any digitised secret such as banking credentials, intellectual property, or private photographs. Where Bitcoin differs most from ordinary digital secret keeping is in the intent or incentives that motivate attackers, and certain methods of preventing attacks.

Intent
While the capability of malefactors to steal keys is identical to that of any digital secret, the incentives that drive thieves are different in three significant ways.

1. **Instant gratification and irreversibility**
   Before Bitcoin, network breaches only allowed

attackers to acquire information, not excludable assets. This means that, in order to ultimately profit from an attack, an attacker must "fence" the data they gather. For example, stolen credit card numbers or traditional financial credentials must be either sold on black markets or used to purchase real goods before the theft is discovered and the credentials invalidated. Stolen bitcoins, by contrast, grant the thief their full value immediately, and no steps can be taken to recover or mitigate this lost value after the thief has used the private key to move the funds to a different public address. Acquiring the bitcoin is essentially acquiring money. This creates an instant gratification incentive not previously present in network breaches, and because there is no intermediary in the Bitcoin network, there is no possibility that the transaction can be reversed by a third party.

Irreversibility is, in fact, a good thing for the network. Recall that claims to bitcoins are recognised as authoritative because the entire chain of title is publicly displayed on the blockchain. This record is constructed via deterministic rules that generate network consensus: transfer requests will only be recorded if they are signed with the private key linked to the transferor's address and if the transferor had sufficient funds (previous transfers into their address) to send the amount they are announcing. The result of this system is that a Bitcoin user must only trust that a majority of the Bitcoin network is behaving honestly, rather than placing her trust in some particular third party. Selectively granting some party the authority to reverse previously recorded transactions erodes the certainty of this system. Who should have this authority and who should not? How is authority limited? What if the secret passkey enabling any balance on the ledger to be changed is leaked to criminals? What if those entrusted with such power fall victim to their own greed?

Moreover, any discussion as to how the protocol might be altered to enable reversibility would be met with resistance from existing participants. Changes in the protocol would need to be adopted by the majority of network participants, many of whom would believe such a change to be antithetical to the purpose of Bitcoin.

2. **Immobility and publicity**
Despite the instant gratification and irreversibility of a Bitcoin theft, the benefits of a heist may be surprisingly difficult to transmute into actual material well-being without inadvertently triggering one's identification and capture. Recall that all transactions are recorded on the blockchain. This recordation necessarily extends to all thefts. When a thief obtains the private key to an address holding bitcoins at least two persons now have full control over the coins: the rightful holder and the thief. To truly steal the coins the thief must request a transfer of the funds to an address she alone controls. The network will validate that transfer because network participants have no way of distinguishing between a rightful holder and a thief. Miners only look for proof that the initiator of the request has the private key.

With the theft transaction recorded, the subsequent movement of the funds can be tracked from address to address until there is an attempt to convert the bitcoins to a fiat currency or real goods[23]. Exchanges and merchants can be asked to deny such cash-out transactions or take steps to identify the individual by reference to credentials submitted for the cash-out (e.g. a bank account if the thief is trying to exchange the coins, or an IP address if the thief is trying to buy real goods on a e-commerce website that logs user data).

The thief may attempt to make tracing the stolen bitcoins more difficult by using a coin *mixing* service. These services take funds from a large number of individuals seeking greater anonymity and scatter transactions across many new Bitcoin addresses. The coins you put in are not the same as those you get out. These services can make it harder to trace stolen coins but they come with several liabilities for the thief: (1) she must trust the mixing service to not run off with the coins, (2) she must trust the service to not keep records of whose coins went to who, and (3) she must pay fees for the service[24]. Even more problematic for major heists is the fact that coin mixing only works if one is trying to anonymise a quantity of bitcoin that is relatively small as compared with the total volume of the mixing service. If a thief is seeking to hide $1 million in coins she must find a service with sufficient volume provided by other, non-criminal participants so that her participation is not a significant portion of the mix. Otherwise she'd be unable to receive as many untainted coins as she put in.

3. **'Insider' theft**
A further consideration for assessing the intent of hostile actors with respect to a local attack is the opportunity for an insider to steal bitcoins. This arises because of the difficulty inherent in discriminating between thefts from outside criminal actors and those that originate from dishonest employees within the company. As discussed, Bitcoin transfers occur without the use of a business intermediary, meaning that embezzlement could occur from within a Bitcoin company without

the need for a conspiracy involving other parties. Embezzling Bitcoin is akin to walking out of your own bank with cash from the vault. Any individual within the company who has knowledge of the private keys related to public addresses can be a vector for such embezzlement. That individual could blame the lost funds on other parties in the bank who had knowledge of the same key, or on outside hackers. As will be discussed in the following section on mitigation, the best defence against an inside job is dividing control of keys among a number of control persons in the bank, all of whom would need to collude to defraud the organisation.

Mitigation

Four common ways that the risk of a local attack can be mitigated are robust *server-side security, cold-storage, multi-signature wallets*, or by leaving custody of private keys with the customer (i.e. offering *hybrid wallets*).

1. **Server-side security**
   Maintaining server-side security is essential to a Bitcoin business, but the techniques are no different from those necessary for securing any other secret on internet-connected computers. Should a company choose to secure their own servers, their techniques should be compared with industry standards. A promising alternative, particularly for capital-constrained start-ups, is to outsource storage and computing needs to a cloud services provider with a known track record for top-notch security[25].

2. **Cold storage**
   Cold storage involves placing the majority of an institution's private keys in offline media, either disconnected computer memory such as a thumb-drive, paper, or as memorised passphrases – a so-called "brain bank". If keys are not stored on internet-connected servers, then they can only be accessed by compromising either the individual with access to the key or the physical security surrounding the key. The attack surface could thus be minimised by limiting the number of employees with knowledge of or access to offline key storage, and storing the offline drives or slips of paper in safe deposit boxes or guarded premises. Cold storage necessarily makes transactions slower because keys must be recovered from their off-network storage location before any transaction can be signed. The bulk of an institution's funds, however, can be kept in cold storage addresses, while sufficient funds for day-to-day liquidity can be kept in a handful of vulnerable but small online "hot" wallets.

3. **Multi-sig and control persons**
   Multi-signature wallets involve assigning bitcoins to public addresses that are linked to multiple private keys, each separately stored, some majority of which are needed to effectuate any transfer. Think of it like the keys to a hypothetical safe deposit box at a bank: you have one key, your banker has the other, and both are required to open the box. Bitcoin addresses can be mathematically linked so that some number (M) of the total linked keys (N) are required to move funds out of an address. This is what is referred to as "M of N transactions"[26] or, more simply, "Multi-sig". Different officers in a company could retain keys to these addresses so that a majority of control persons would need to approve any transfer out of a wallet. If one control person was compromised, either because her devices had been hacked or she, herself, was no longer trustworthy, then her key alone would not be sufficient to move funds.

   Institutions may also rely on a vendor that specialises in protecting funds using multi-signature technology combined with external transaction monitoring and policy rules. One such service is BitGo, recently chosen by Bitstamp to help secure its funds in the aftermath of the January 2015 hack[27]. BitGo's co-founder and Chief Product Officer describes how BitGo monitors a multi-sig wallet that they have created for a client and what motivates their decision to sign off or refuse to sign off on a requested transfer:

   Before deciding to co-sign, BitGo applies security policy checks on the wallet, such as enforcing velocity limits, address target whitelists, IP restrictions, and so on. If the transaction passes the security checks, BitGo issues the second signature on the transaction using its key, and submits it to the network. If not, then BitGo may either reject the transaction, or hold it for additional approval from another administrator on the wallet. The final (backup) key does not come into play during normal operation. It is a cold-storage key which is for disaster recovery, and also allows the customer to retain ultimate custody of the bitcoin[28].

   These technical aspects of the Bitcoin protocol may offer protections substantially more effective than those available for a holder of large sums of cash or credit: multi-sig Bitcoin holdings cannot be spent unless an external security firm signs off or seeks additional confirmation from a high-level employee, and the bulk of reserve funds cannot be accessed without stepping out of the virtual world and into a series of real life vaults or safe deposit rooms.

4. **Hybrid wallets**
   Finally, an institution could avoid losing keys by choosing never to hold them in the first place.

Blockchain.info, for example, is an online service that helps users secure their bitcoins. However, Blockchain.info never actually learns or holds the keys that its customers utilise to prove their control over Bitcoin holdings[29].

Blockchain.info builds and continually updates a software wallet program that can be used by a customer to store keys. They help the user configure this software and allow the user to generate Bitcoin addresses (for receiving funds) matched to private keys. The generation of these keys occurs on the user's local computer and, afterwards, the wallet program along with its new keys is encrypted so that it is unreadable. This encrypted file is stored on Blockchain.info's servers as a back-up in case the user's computer is lost or damaged. Because of encryption, at no point can Blockchain.info employees or any unauthorised parties lurking on their servers see the keys unencrypted. By never handling unencrypted customer keys, the risk of key loss is mitigated. As we will see in the next section, however, other risks may remain.

Global threats

These attacks may be called global because they target not the particular servers of the exchange or anything onsite, but, instead, the protocol and ledger with which any exchange must interact. This analysis focuses on six key modes of global attack: flawed key generation; transaction malleability; 51% attacks; "Sybil" attacks; distributed denial of service attacks; and "consensus" or "fork" risk.

Capability

1. **Flawed key generation**
   All Bitcoin holdings are associated with public addresses on the blockchain, each with a corresponding private key. Think of the private key as a password required to spend the funds in the address. Both the key and the public address appear as highly random, uncorrelated and unique strings of characters. For example, here are two linked keys generated using an Elliptic Curve Digital Signature Algorithm (ECDSA)[30]:

   Private Key:
   e6edcf30220499bd034a7f4ebbadd4d62c8995c0115
   7067983b4f1f26b58111

   Public Key:
   0488ff723a55ae8f46d9decf66c10a249adb59ac9119
   5adee879ecb5944ea7f5098dd9e193c2172047e6ea
   cb6ddd524c77ee5669b2f69bbfb27fc03d717d657195

   The two strings are, in fact, provably linked by the mathematical formula used to generate them. It is probabilistically impossible to guess a private key by simply knowing the corresponding public key, but it is trivially easy for a computer to check that two keys are, in fact, linked. This is known in computer science as a one-way function, a broad class of technical tools that form the basis for all secure communications technology.

   These mathematical properties allow for digital signatures and verifiable messaging online. To send such a message, a person would first publicly announce her public key. Then she would take the private key and run it through a mathematical operation called a *hash function* along with the message she wishes to sign. The output of that hash is called a digital signature. Anyone who sees the output can know with certainty that only the person with both the public and private keys could have signed the message. The observer, however, does not learn the private key throughout this process of validation; therefore she can verify but not forge the identity of the sender.

   A Bitcoin public address is an ECDSA public key that has been mathematically transformed with hash functions in order to provide a shorter string of characters to which network participants can send funds[31]. The particular operation of equations involved in this set-up is beyond the scope of this report. Suffice it to say, however, that ECDSA and the associated hash functions are industry state-of-the-art tools for key generation and message encryption across the internet[32].

   One can, however, fail to implement these tools correctly when generating keys and addresses. If there is a faulty implementation, the keys generated may not be sufficiently random and, given the public address, a malicious party could be able to guess the private key, at which point they would be able to sign transactions and transfer funds out of the public address.

   This happened in December 2014 to hybrid wallet provider Blockchain.info[33]. A mistake was made during a software update, and when an affected user generated a new key pair on her local machine using Blockchain's software (recall that as a *hybrid wallet* provider Blockchain.info does not know its customers' keys, but rather gives them software to generate those keys locally and stores encrypted versions in the cloud), inputs to the ECDSA algorithm were not sufficiently random so as to generate an effective one-way function. As a result,

a thief could use software to determine the user's private key merely by looking at the public address.

Only a very small fraction (0.0002%) of users were affected, and the issue was detected and resolved within two-and-a-half hours[34]. Even given this short time frame, individuals outside of Blockchain.info observed the vulnerability. As a result, some bitcoins were stolen. Again, the public character of the Bitcoin ledger is the reason for this quickness.

Individuals can, and do, watch addresses as they appear on the public ledger in real time. They can build computer programs that sit and wait for observable weaknesses in address generation, and even steal funds as soon as those weaknesses are detected. In Blockchain.info's case, the "thief" turned out to be a German computer science researcher, and frequent contributor to Bitcoin community online discussion forums, where he is known as Johoe. Johoe returned the funds and helped point out the implementation weaknesses that caused the hack[35].

2. **Transaction malleability**
In a transaction malleability attack the thief tricks her target into believing that a transaction has failed. The thief then asks for the transaction to be repeated. In this manner a thief who was already owed X bitcoins could fraudulently obtain twice the amount[36].

The deception is created by altering a transaction request as it is sent through the peer-to-peer Bitcoin network. Some malformed transaction messages can be corrected by intermediary parties in the chain of peer-to-peer message exchange. That change may make the transaction difficult to recognise, even to the original sender, and she may, instead, think that the message failed to go through. If a targeted institution is careless about how it verifies that a transaction has either succeeded or failed to be recorded in the blockchain, it may unwittingly send a second transaction when the thief claims that the first transaction did not go through. The thief will have doubled her money.

To be clear, this particular attack relies on social engineering, not mere technological manipulation. An individual at the institution must be contacted and persuaded to re-send funds that allegedly failed to be transferred in an initial request.

Mt. Gox blamed its insolvency on this particular attack, but this has been challenged by many in the Bitcoin community as the scale of theft would have required hackers to repeatedly convince customer service personnel at Mt. Gox that their transactions had failed and needed to be reinitiated. Moreover, by careful monitoring of the transaction messages and tracing the outputs of a transaction, all with publicly available information on the blockchain, the attack is avoidable[37].

Blockchain technologies can also be employed to improve internal accounting and auditing. Accounting software can be run by the business as an integrated part of the business's consumer-facing applications. It can be programmed to interact with the Bitcoin protocol, placing limits on any suspicious requests that could indicate a transaction malleability hack or some other wrong-doing. The software can also be programmed to automatically generate human-readable double-entry accounting records or other visualisation tools in real time, so that the institution can always have a good sense of which transactions have succeeded, which have failed, and what is the general state of the business.

3. **Fifty-one per cent attack**
A 51% attack involves manipulation of the blockchain itself rather than the protocol that facilitates communication between users and miners. Each block added to the blockchain describes the transactions verified in roughly the previous 10 minutes. Miners compete for the privilege to write the next block and receive a mining reward of new bitcoins. To fraudulently manipulate the blockchain, an attacker would need to consistently out-compete all other miners by wielding a majority of the global computing power spent mining bitcoins.

The prospect of a single individual or small group of individuals obtaining such mining power is highly remote because the cost would grossly exceed the likely benefits of such an attack. The recent advent of large mining pools increases the likelihood that an organised group of miners could maintain a majority of computing power long enough to manipulate the blockchain[38]. However, it is not considered likely that a 51% attack would pose a major risk of loss or theft.

A successful 51% attack could prevent a targeted actor from engaging in new transactions, might allow the dishonest miners to demand exorbitant transaction fees, or allow them to shut down the network entirely by processing no new transactions. Attackers, however, would never be able to rewrite the blockchain's history in order to steal funds already listed in a target actor's public addresses. If a 51% attack were to be successfully carried out, it would be a significant blow to consumer confidence in the stability and trustworthiness of Bitcoin.

Institutions holding Bitcoin would suffer real losses from any collateral drop in Bitcoin prices, but nominal Bitcoin holdings themselves would remain unthreatened.

Additionally, the evidence of such an attack would be manifest – newly mined blocks would not include requested transactions – and steps could be taken to adjust the Bitcoin protocol so as to ignore the blocks mined by the attacker and return the network to normal operation sufficiently quickly that the chance of collateral consequences, like loss of faith in the currency, could hopefully be minimised[39].

4. **Sybil attacks**
Bitcoin, as discussed previously, is a peer-to-peer network. Rather than seeking to attack the entire network, as with a 51% attack, a sybil attacker seeks to target one node on the network, say a particular Bitcoin company's known connection point to the network. The sybil attacker creates a sufficient number of Bitcoin nodes adjacent to the target node to become the victim's only means of connecting to the network as a whole. In other words, the attacker surrounds the victim with malicious peers. It may appear to the victim that they are still accessing the network through many different individual computers owned by various, honest individuals, but in reality their access is limited to a handful of peers that are all under the control of the attacker.

Once the attacker has her victim surrounded, she can refuse to relay the victim's transactions, effectively disconnecting the victim from financial access. Alternatively, the attacker can feed the victim mis-information about the state of the network as a whole. Let us say the victim is an exchange and the attacker is a putative customer of that exchange. The attacker could claim that it transferred bitcoins to the victim exchange hoping to trade those coins for dollars. To validate this transfer, the victim expects the network to send it up-to-date versions of the blockchain, the record of all valid transactions. The attacker can send fraudulent versions of this record. The fraudulent version could indicate that the attacker has paid the victim even if there is no such record on the genuine blockchain of the larger network. The victim believes they hold new bitcoins and therefore credits the bank account of the attacker (presumably opened under a fraudulent name). If the attacker can continue to deceive the victim for long enough, they may be able to withdraw from their bank account and walk away with cash before either the exchange or the bank is aware of the deception.

The Bitcoin network, however, is inherently resilient against these attacks. In order to keep up the deception, the attacker would need to continuously feed the victim new fraudulent blocks that make it appear as though the network is functioning as normal. Each block, even a bogus block, is difficult to create, depending, as it must, upon the exertion of scarce computing resources. An attacker with only 10% of the computing power of the entire network (still a massive amount of power for any individual participant) would only be able to generate bogus blocks at 10% of the normal speed. A would-be victim could monitor for such an attack by looking for notable decreases in the frequency of new block generation. Should the network computing power, referred to as the hash-rate, appear to drop precipitously, the victim can be on guard that they may be under attack. At this point the victim can block the current nodes to which they connect and seek other, honest nodes within the peer-to-peer Bitcoin network. The extreme difficulty of deceiving one's victim in a sybil attack has led many in the development community, including lead developer Gavin Andresen, to label the attack "theoretically worrisome, but practically not a high priority."[40] Exchanges and other large Bitcoin businesses should, nonetheless, take reasonable steps to mitigate against such an attack. Automated processes should be developed, if they have not been already, to monitor for unusual network states, as when hash rate declines precipitously because of a sybil attack.

5. **Distributed denial of service attacks**
As with any network, Bitcoin is potentially vulnerable to distributed denial of service ("DDoS") attacks. Simply put, a DDoS attack is an effort to make a network resource unavailable by overwhelming it with service requests. Given that Bitcoin is a peer-to-peer network, the resources on that network (e.g. transaction relaying or validation) depend on the availability of peers. For the purposes of this network service, there are two classes of node on the Bitcoin peer-to-peer network: those that accept incoming Transmission Control Protocol ("TCP") connections, and all others. When a Bitcoin wallet or Bitcoin node is attempting to connect to the network, it must contact one or more remote nodes that receive incoming connections from outsiders.

There is no accepted technical term for these nodes, but we can refer to them as "acceptor" nodes. Acceptor nodes are the linchpin of the network. There may be 100,000+ nodes out there with copies of the blockchain. Without acceptor nodes, however, there is no network to relay copies of the blockchain to users. Estimates on acceptor node count are under 7,000, and falling[41]. A malicious

party could spam these nodes with phony requests, overwhelming their ability to respond to legitimate requests from the network at large. This could make the network slow or unresponsive for the duration of the attack.

The resources necessary to sustain such an attack would likely be costly. Nevertheless, it is widely believed that those costs are substantially less than the costs involved in a 51% attack[42].

To be clear, a DDoS attack would not threaten existing Bitcoin holdings or enable theft. It would simply make the network unavailable to process new transactions. A prolonged attack would, however, significantly undermine confidence in the value of the currency, potentially leading to a large-scale sell-off once transactions resume.

6. **Consensus or fork risk**

Another global risk is consensus or fork risk. In this context, "consensus" means the Bitcoin network's ability to agree upon an authoritative ledger, or blockchain, that lists all current Bitcoin holdings. Miners continuously add to this chain by generating new blocks at a rate of roughly one block every ten minutes, network-wide. All miner software is pre-programmed to add blocks only to the largest currently broadcast chain. A "fork" occurs when some miners work on one chain while others work on another. The danger of a fork is that it presents Bitcoin users with two alternative states of the transaction record. One state has new blocks that could suggest that a transaction has occurred, while the other has blocks that could deny that fact or even record that a different transaction, using the same funds but paying another party, has occurred. Users are left wondering whether money has, or has not, in fact changed hands. And malicious users could purport to send the same money to two different people on two different prongs of the fork.

Brief forks are normal, and one or two block forks happen on the network every day. These forks are quickly resolved as the network actively and automatically seeks to identify the prong of the fork that has the most computing effort dedicated to it, i.e. to reach consensus. Once that prong is clearly and certainly identified, the new blocks in the rejected prong will be abandoned. Because these forks only last some two blocks, transactions can only be lost or double spent within a short (~20 minute) window. As the network returns to consensus, these discrepancies will be resolved, and after an hour any transactions included in the now unified and authoritative blockchain can be presumed trustworthy. Therefore, as with transaction malleability risk, losses can be avoided by refusing to take an action (e.g. credit an account, or resend a purportedly lost transaction) until the relevant transaction has been confirmed by some five or six blocks (i.e. existed in the blockchain for roughly an hour).

However, should a long-standing fork occur, the damage to Bitcoin as a whole could be severe. In this situation, merchants and businesses cannot be certain which fork is accurate. The same bitcoins may be double-spent on each fork, violating the core Bitcoin security promise[43]. Such a fork would be instantly recognisable by Bitcoin users and observers owing to the public nature of the blockchain. An insurer, faced with this event, might well consider limiting insurable assets to those on the books before the fork. In such a circumstance, all responsible, aware Bitcoin parties would stop processing transactions beyond the fork, and until the fork is resolved, to avoid being defrauded.

Until that resolution is reached, all Bitcoin payments stop. Bitcoin is essentially shut down, as one cannot trust any bitcoins received. The longer this divergent state of affairs continues, the greater the likely erosion of faith in Bitcoin as money. This

creates added incentive amongst invested parties to resolve the fork. This larger risk is less relevant for the purposes of insurance so long as insured assets are limited to those on the books before a fork and/or businesses decline to transact during a long-standing fork. Nonetheless, this is a profound risk to Bitcoin as a whole, given that an unresolved fork could lead to a massive decline in the price of Bitcoin.

Intent

The incentives driving a global attack are similar to those behind a local attack, with one exception. Particularly far-reaching attacks that would be perceived as destabilising the entire network – such as in the 51% attack, but not with transaction malleability or flawed key generation – would be observed in real time. The alarm generated by such an event would likely severely lower the price of bitcoins. An attacker would have invested heavily in bitcoin-specific infrastructure only to erode the value of that which she sought to steal or control.

This self-righting incentive has only been accentuated in recent times by the proliferation of new mining hardware known as Application Specific Integrated Circuits[44] (ASICs). This new hardware is vastly more efficient at mining Bitcoin than previous tools because it is purpose-built to solve Bitcoin hash functions alone. As a consequence, however, the hardware is useless for any activity other than mining Bitcoins. A malevolent miner hoping to commit a 51% attack would need to purchase large volumes of these ASIC machines, incurring significant costs, in order to be successful. The attack, however, could very well render that costly hardware useless if the network was abandoned or forked in a way that broke compatibility with the attacker's hardware in order to repair the damage.

This self-righting incentive does not, however, apply to individuals who wish only to destabilise or destroy the Bitcoin network, rather than profit from it. Moreover, a widespread DDoS attack, as discussed, could immobilise the network and destroy faith in Bitcoin as money without requiring costly investment in bitcoin-specific hardware. Governments, for example, may at some point have the intent to destroy Bitcoin, whether because of the perceived illegality of transactions, the funding of terror, a fear of capital flight, or widespread tax evasion. Should a government wish to do so, DDoS attacks may be a cost-efficient means of bringing the network down. At present, however, these risks and any potential efforts at mitigation[45] are considered highly speculative.

Conclusion

Quantifying risk is difficult within the Bitcoin industry. The technology is new, early entrepreneurs show wide-ranging skill, caution and capability, and best practices are still being determined and implemented. Even before Mt. Gox's insolvency, the exchange industry had a worrisome track record. Computer scientists Tyler Moore and Nicolas Christin found that of some forty Bitcoin exchanges established in a three-year period, eighteen closed, many taking consumer balances with them[46]. Some have called the spate of failures a sign of a shake-out or changing of the guard: under-qualified or downright criminal amateurs are exiting an industry that has outgrown them. Others, however, question this analysis, arguing that too many technically savvy and reasonable persons have suffered losses[47]. In this analysis, the underlying cause was the weaknesses of the technology's early iterations and the slow adoption of newer techniques for safeguarding funds. Those newer technologies have been discussed throughout this report: multi-sig, cold storage and hybrid wallets. Rather than quantifying risk from past performance, Coin Center advises that insurers and industry observers keep tabs on whether a business is employing these new controls.

References

1. Historic exchange market share can be visualised at *http://bit.ly/1oYFCbF*

2. See Mt. Gox. Addressing Transaction Malleability. Mt. Gox, *https://xrptalk.org/topic/1258-mtgox-press-release-addressing-transaction-malleability/*

3. For example, Decker and Wattenhofer have conducted a technical analysis of the Blockchain and conclude that only some "386 bitcoins [of the total 850,000] could have been stolen using malleability attacks," the particular protocol vulnerability cited by Mt. Gox. *See http://bit.ly/1ojBa7U*

4. David Dunlap, How Cost of Train Station at World Trade Center Swelled to $4 Billion, NY Times (Dec. 2, 2014) *http://www.nytimes.com/2014/12/03/nyregion/the-4-billion-train-station-at-the-world-trade-center.html*

5. Bitcoin Wiki, Scalability, *https://en.bitcoin.it/wiki/Scalability*

6. Visa, Merchants Rack Up $7.8 Billion in Online Sales on US-issued Visa Cards in Just Five Days, VISA Viewpoints, *http://www.visa.com/blogarchives/us/category/visanet-2/index.html*

7. A wallet is used to store the keys to one's bitcoins, allowing the user to prove that they hold bitcoins and giving them an interface from which to send transaction messages to the network.

8. *Electrum, https://electrum.org/*

9. BFGMiner, *http://bfgminer.org/*

10. GitHub is a software repository on the internet: *https://github.com/*. The Bitcoin repository on GitHub is located at *https://github.com/bitcoin/bitcoin*

11. Independently developed clients may also include some adjustments to the code that determines how the software speaks with the network, called policy rules, so long as those adjustments do not make the client incompatible with the reference client.

12. Unless the malicious client was adopted by a majority of participants in the network, an unlikely state of the network unless the malicious code was hidden and undiscoverable by all network participants.

13. Bitcoin is released under the MIT open source software licence. See Satoshi Nakamoto, Re: Switch to GPL, Bitcointalk (Sep. 12, 2010). The MIT licence is permissive meaning future original works that borrow from the underlying code can be, themselves, copyrighted and closed source.

14. See ibid. (Satoshi Nakamoto, the pseudonymous inventor of Bitcoin, stresses the importance of open source software for his/her project). See, e.g., Nick ODell, Suggestion: Closed-source cryptocurrencies should be off topic. Bitcoin Meta Stack Exchange (Oct. 22, 2014).

15. For example, in 2013 Mr James Howells of Wales lost 7,500 bitcoins when he threw away his hard drive. At that point the holdings were worth around £500,000. Mr Howells never recovered the drive and those coins are lost to this day. Without a private key, they simply can never be transferred to a new address. Alex Hern, Missing: hard drive containing Bitcoins worth £4m in Newport landfill site, The Guardian (Nov. 2013) *http://www.theguardian.com/technology/2013/nov/27/hard-drive-bitcoin-landfill-site*

16. *Coinbase, https://www.coinbase.com/*

17. *Circle, https://www.circle.com/en*

18. *Blockchain.info, http://blockchain.info/*

19. *Bitstamp, https://www.bitstamp.net/*

20. Robert McMillan, The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster, Wired (Mar. 3, 2014) *http://www.wired.com/2014/03/bitcoin-exchange/*

21. *Bitpay, https://bitpay.com/*

22. This is what a private key looks like: 5HpHagT65TZzG1PH3CSu63k8DbpvD8s5ip4nEB3kEsreAbuatmU. That particular key is matched to this public address on the Bitcoin network: 1MsHWS1BnwMc3tLE8G35UXsS58fKipzB7a. Bitcoins can be sent to this address; however, anyone who has read this footnote knows that matched private key and can, therefore, spend them.

23. See, for example, how individuals utilising publicly available tools tracked the early transactions from the $5 million BitStamp breach. Michael Carney, With the stolen BitStamp bitcoins on the move, Reddit flies into detective mode, Pandodaily (Jan. 2015) http://pando.com/2015/01/08/with-the-stolen-bitstamp-bitcoins-on-the-move-reddit-flies-into-detective- mode/

24. Tracking Bitcoin transactions and linking them to identities has proven easier than many initially expected. See Alex Biryukov, et al. "Deanonymisation of clients in Bitcoin P2P network" eprint arXiv: 1405.7418 (May 2014) available at http://arxiv.org/pdf/1405.7418v3.pdf; Elli Androulaki, et al. "Evaluating User Privacy in Bitcoin" 7859 Financial Cryptography and Data Security Lecture Notes in Computer Science 34 (2013); Philip Koshy, et al. "Analysis of Anonymity in Bitcoin Using P2P Network Traffic" (Doctoral dissertation, Pennsylvania State University) (2013) available at *http://ifca.ai/fc14/*

papers/fc14_submission_71.pdf; Sarah Meiklejohn, et al. "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names" Proceedings of the 2013 conference on Internet measurement conference (ACM, 2013) available at http://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf

25. For example, after suffering $5 million in losses from a local attack wherein private keys were compromised, prominent Bitcoin exchange Bitstamp rebuilt its platform utilising Amazon Web Services for storage and computing.

26. See Gavin Andresen, BIP 0011, https://github.com/bitcoin/bips/blob/master/bip-0011.mediawiki

27. Bitstamp, Bitstamp is open for business - Better than ever! (Jan, 2015).

28. Ben Davenport, No Sleep till Multi-Sig, Medium.com (Jan. 2015) https://medium.com/@bendavenport/no-sleep-till-multi-sig-7db367998bc7

29. See Blockchain.info, http://blockchain.info/

30. The ECDSA algorithm can be tested at this site: http://kjur.github.io/jsrsasign/sample-ecdsa.html Key pairs can be generated and signing of documents tested out.

31. See Bitcoin Wiki, Technical background of version 1 Bitcoin addresses https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses

32. See Certicom, An Introduction to the Uses of ECC-based Certificates https://www.certicom.com/index.php/an-introduction-to-the-uses-of-ecc-based-certificates

33. Giulio Prisco, Gentleman Hacker Returns Stolen Bitcoins to Blockchain.info, Cryptocoinsnews (Dec 2014) https://www.cryptocoinsnews.com/gentleman-hacker-returns-stolen-bitcoins-blockchain-info/

34. Alyson Margaret, Blockchain.info Security Disclosure, Blockchain Blog (Dec 2014) ("When making a scheduled software update overnight to our web-wallet, our development team inadvertently affected a part of our software that ensures private keys are generated in a strong and secure manner. The issue was present for a brief period of time between the hours of 12:00am and 2:30am GMT on December the 8th 2014. The issue was detected quickly and immediately resolved. In total, this issue affected less than 0.0002% of our user base and was limited to a few hundred addresses.")

35. Ibid, note 33.

36. Christian Decker and Roger Wattenhofer, Bitcoin Transaction Malleability and MtGox, arXiv:1403.6676 (Mar. 2014) http://arxiv.org/abs/1403.6676

37. Ibid, note 36.

38. The mining pool GHash.io has crossed the 51% mark for brief periods although no exploitation of this power has been authoritatively observed. GHash.io has promised to abstain from achieving such disproportionate power in the future. See http://bit.ly/1gMDDGb

39. Gavin Andresen, Neutralizing a 51% attack, GavinTech (May 2012) http://gavintech.blogspot.com/2012/05/neutralizing-51-attack.html

40. Gavin Andresen, "What's the plan about the sybil attack?" BitcoinTalk.org (Comment #3, May 12, 2011) https://bitcointalk.org/index.php?topic=8051.msg117573#msg117573

41. See Daniel Cawrey, "What are Bitcoin Nodes and Why do we Need Them?" CoinDesk (May 2014) http://www.coindesk.com/bitcoin-nodes-need/

42. See David Bradbury, "Bitcoin network recovering from DDoS attack" CoinDesk (June 2013) http://www.coindesk.com/bitcoin-network-recovering-from-ddos-attack/ (Bitcoin core developer Jeff Garzik explains, "Operationally, network attacks are far cheaper. Any smart attacker is going to look for a cheaper way to attack Bitcoin. Network attacks are one of the big worries right now.").

43. See Gavin Andresen, "BIP 50: March 2013 Chain Fork Post-Mortem" GitHub (Mar 2013) https://github.com/bitcoin/bips/blob/master/bip-0050.mediawiki

44. See Ian Cutress, The Rush to Bitcoin ASICs: Ravi Iyengar launches CoinTerra, AnandTech (Aug 2013) http://www.anandtech.com/show/7246/the-rush-to-bitcoin-asics-ravi-iyengar-launches-cointerra

45. The vulnerability of the network to a large scale DDoS attack at the hands of a state or other large entity could, in theory, be minimised by increasing the number of acceptor nodes (thereby increasing the number of nodes that must be spammed) or by enhancing existing protocol protections against spammy connections.

46. Tyler Moore and Nicolas Christin, Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk, 6859 Financial Cryptography and Data Security Lecture Notes in Computer Science 25 (2013).

47. Vitalik Buterin, Multisig: The Future of Bitcoin, Bitcoin Magazine (Mar 2014) https://bitcoinmagazine.com/11108/multisig-future-bitcoin/

Strategic risks to Bitcoin operations

Garrick Hileman (London School of Economics) & Satyaki Dhar

What is Bitcoin? Why do people use it? What makes it different from other currencies and transaction networks?

Financial and monetary systems rarely experience paradigm shifts. Indeed, the operating principles that guide commercial and central banks have remained largely similar to the era when Walter Bagehot's *Lombard Street* was first published in 1873. Today, however, many believe that cryptocurrencies such as Bitcoin have the potential to revolutionise the way we transact, store and account for value.

Cryptocurrencies can be considered as a type of peer-to-peer (P2P) value transfer system. In contrast to other P2P payment networks like PayPal, which orchestrate the movement of currencies such as the US dollar, cryptocurrencies incorporate both their own currency unit (often referred to as "bitcoin" with a little "b") and payment network (often referred to as "Bitcoin" with a capital "B"). The advantages that cryptocurrencies offer over existing payment networks include:

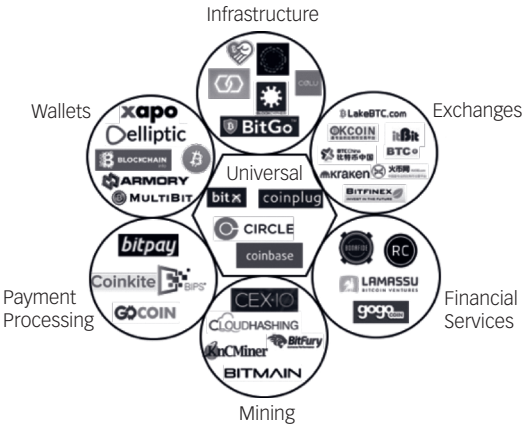
- Low cost, speedy transactions: Bitcoin can be faster and significantly less expensive than other types of transactions, such as credit card and international remittances.
- Ease and flexibility of use: Bitcoin enables micro transactions of up to eight decimal places; also the widespread implementation of image scanning technology (such as Quick Response codes for identifying/tracking items) could enable cryptocurrency adoption.
- New approaches to privacy and transparency: pseudonymous accounts limit identity theft risk; all transactions publicly registered on a 'blockchain'.
- Decentralised structure: thousands of different network nodes mitigate single point of failure risk.
- Open access: no need to apply for an account – anyone can use bitcoin.

Bitcoin is far from the only cryptocurrency: as of March 2015 there were approximately 600 known cryptocurrencies available to users[1]. Nevertheless, Bitcoin has a dominant market share, representing 84% of the USD 4.2 billion in total market capitalisation for all cryptocurrencies as of 23 March 2015. For this reason the report will primarily focus on and refer to Bitcoin, although many of the issues discussed in the report are applicable to other cryptocurrencies.

Bitcoin has now been operating for over six years[2]. However, the system is still considered to be in its infancy with many still referring to Bitcoin as a "beta technology"[3]. Beta technologies, and the still maturing ecosystem of companies and processes which surround them (Figure 1) often feature a greater number of risks than more established systems.

This report examines three dimensions of the risk attached to Bitcoin: security and technology risk, through hacks and other technical breaches; market risk, through exchange rate and liquidity risk; and regulatory risk, through the impact of policy uncertainty.

Figure 1: The Bitcoin start-up ecosystem – seven different Bitcoin company types



Source: State of Bitcoin Report 2015, CoinDesk
http://www.coindesk.com/research/state-of-bitcoin-2015/

Security and technology risk

Bitcoin security risk arises from deliberate targeting by malicious actors for theft or other purposes, while technology risk is associated with the design of the Bitcoin software protocol.

Security risk

Bitcoin's pseudonymous nature, the fact that bitcoins are fungible, the network's fast transaction execution and the irreversibility of transactions are a few of the reasons why the cryptocurrency can be an attractive target for theft. Many justice systems are also still just learning about Bitcoin and are either unwilling or unsure how best to pursue loss claims. The rapid rise in Bitcoin's value, coupled with the discovery of vulnerabilities, has attracted the attention of cyber-criminals, leaving Bitcoin institutions and users susceptible to material losses.

The largest Bitcoin loss to date stems from the well-publicised February 2014 collapse and insolvency of the Bitcoin exchange Mt. Gox, where an estimated $500 million worth of bitcoins went missing[4]. While no other cryptocurrency-related loss comes anywhere close to the size of Mt. Gox, other notable losses include the

January 2015 hack of another leading Bitcoin exchange's "hot wallet", which resulted in a loss of $5 million[5].

While such larger thefts receive the lion's share of the media headlines, it is important to note that Bitcoin losses are by no means isolated to large-scale events. Based on recently published research that examined smaller Bitcoin losses (i.e. excluding larger multi-million dollar losses like those at Mt. Gox and Bitstamp) it has been estimated that approximately $11 million has been lost by about 13,000 victims in close to 200 smaller-scale Bitcoin scams over the past few years[6]. The majority of these Bitcoin losses have been realised in the last year, during which time Bitcoin's value increased substantially, as shown in Figure 2 below.

Three primary categories of Bitcoin scams have been identified:

- "Ponzi schemes": investors are promised lucrative returns, which are in turn used to attract new investors.
- Mining scams: a form of advanced-fee fraud that exploits people's interest in Bitcoin mining by promising a way to profitably mine Bitcoin without making large up-front investments in expensive hardware.
- Scam wallets and exchanges: thieves provide sought-after services, such as "mixing" coins at a seemingly affordable price, only to steal incoming transfers from customers. Fraudulent exchanges and escrow services have also employed similar tactics.

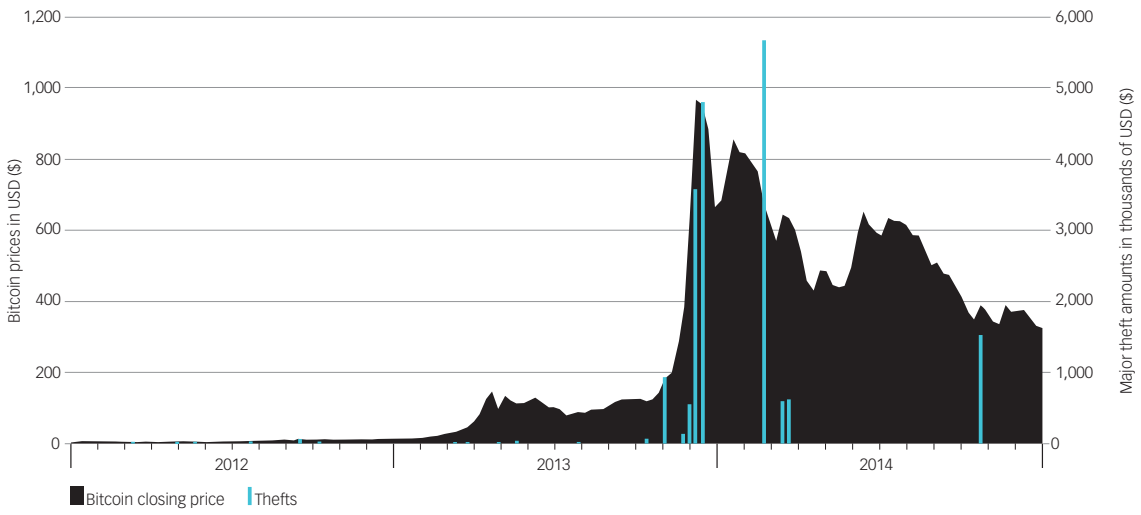
How do Bitcoin losses compare to other types of financial services losses? The total estimated losses due to UK credit card fraud in 2013 were $675 million, a figure not far off from total Bitcoin losses for 2014[8]. However, it is worth noting that credit card transactions in the UK in 2014 totalled approximately $240 billion (£160 billion), or over ten times larger than the $22 billion in total worldwide bitcoin transactions over the last 12 months[9]. In other words, losses related to Bitcoin scams and fraud in the last year have, given the amount of underlying economic activity, been an order of magnitude larger than credit card fraud.

Technology risk

Most of the security risk associated with Bitcoin tends to be focused on service providers such as wallets and exchanges, and Bitcoin security has arguably come a long way in recent months with the further adoption of additional security measures, such as the wider use of multi-signature (third-party transaction approval) and "cold storage" (offline) wallets. However, a recent study of wallet services and their ability to survive an attack designed to exploit the Bitcoin protocol's long-known transaction malleability problem (where elements of a Bitcoin transaction are performed in a way that undermines the integrity of the transaction's data) revealed that problems still exist at nearly all major Bitcoin wallets. The test conducted by Andrychowicz et al found that all the wallets in their study except Xapo and Bitcoin Core failed at least one aspect of their transaction malleability test, as shown in Figure 3:

Figure 2: Major Bitcoin thefts coincide with Bitcoin weekly price spikes

Note: The highest peak is the Mt. Gox loss and has been scaled down by a factor of 100



Sources: Weekly average Bitcoin price source: https://www.quandl.com/BCHARTS/BITSTAMPUSD-Bitcoin-Markets-bitstampUSD and top 25 major thefts source: https://bitcointalk.org/index.php?topic=576337#post_t2013_fork

Figure 3: Summary of results of malleability tests on leading Bitcoin wallets (• denotes problem)*

Wallet name	Type	(a)	(b)	(c)	when the problem disappears
Bitcoin core	Desktop				-
Xapo	Web				-
Armory	Desktop	•			never
Green Address	Desktop	•			never
Blockchain.info	Web	•	•		after six blocks without confirmation
Coinkite	Web	•	•		after several blocks without confirmation
Coinbase	Web	•	•		after several hours
Electrum	Desktop	•	•		after application test
MultiBit	Desktop	•	•		after "Reset block chain and transactions" procedure
Bitcoin Wallet	Mobile	•	•		after "reset block chain" procedure
KnC Wallet	Mobile	•	•	•	after "Wallet reset" procedure
Hive	Desktop	•	•	•	after restoring the wallet from backup
BitGo	Web	•	•		never
Mycelium	Mobile	•	•		never

*Notes from study authors:
(1) Three malleability tests were performed: (a) the wallet incorrectly computes the balance, (b) the wallet is unable to make an outgoing transaction because it assumes that some transaction will be confirmed in the future (which in fact will never happen), (c) the application crashes.
(2) All the tests took place in October 2014 and hence may not correspond to the current software version.

Source: Andrychowicz, Dziembowski, Malinowski, Mazurek, On the Malleability of Bitcoin Transactions
http://fc15.ifca.ai/preproceedings/bitcoin/paper_9.pdf

One widely discussed technical risk associated with the core Bitcoin software protocol is the "51% attack", whereby an individual or entity controls at least a majority (over 50%) of the Bitcoin network's "hashing" (computer) power. This level of control would enable a number of malicious activities, including spending the same bitcoin more than once ("double-spending") and preventing certain Bitcoin transactions from being added to the blockchain[10]. The 51% vulnerability is inherent to Bitcoin core software protocol, meaning this risk will remain unless a change to the protocol can be devised and implemented.

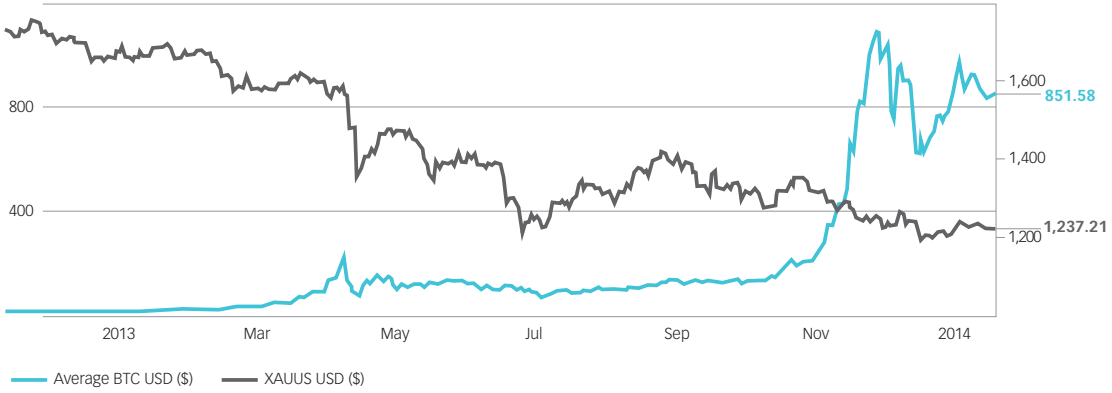
While at least one pool of miners has already garnered over 50% of the Bitcoin's hashing power, a 51% attack has yet to take place[11]. Indeed, there are considerable economic disincentives in place for many of those who would have the resources to carry out such an attack[12]. For these and other reasons, many believe it is highly unlikely that a 51% attack will ever occur. However, the history of hacking has demonstrated that many hackers are often motivated for non-economic reasons. Indeed, hacker motivation often tends to resemble something akin to Mallory's famous quip to the question of why climb Everest ("because it is there"). Like a famous but still unsolved mathematical puzzle, executing a successful 51% attack may represent a tantalising trophy for some hackers or other actors with incentives to steal or damage Bitcoin. It is unclear how much damage a 51% attack would do to Bitcoin's prospects for adoption in the longer run, but in the short run a material decline in Bitcoin's price, disruptions to transactions and reputational damage could be anticipated.

In sum, Bitcoin security and technology risk is considered unlikely to go away in the near future regardless of whether Bitcoin companies further adopt enhanced security practices. In the words of the US Federal Bureau of Investigation, "As long as there is a means of converting bitcoins into real money, criminal actors will have an incentive to steal them."[13]

Market risk

Market risk stems from the volatility in Bitcoin's price and can be examined in two principal ways – exchange rate risk and liquidity risk.

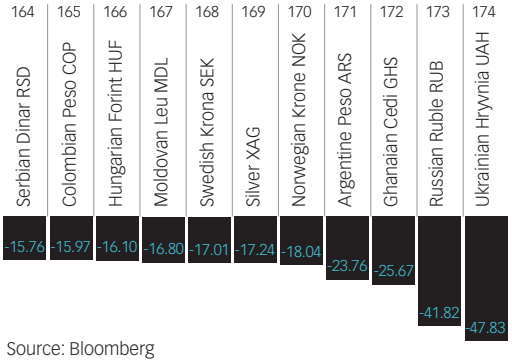
Figure 4: Bitcoin price vs. gold price in USD, 2013–2014



Data Source: https://www.bigterminal.com/chart/averageBTCUSD/?from_goldnet=1

Bitcoin's value, like other freely traded assets, is ultimately a function of supply and demand. As a relatively new asset class, Bitcoin lacks the historical track record of other commodities (such as gold) that can guide its valuation. It has been claimed that the main drivers of Bitcoin's price volatility have been interest in Bitcoin (measured through Google Trends data) and the number of Bitcoin transactions[14]. In addition, unlike national currencies such as the dollar and pound, Bitcoin's price is not backed by a central bank with the capacity to guide the currency's exchange rate.

Figure 5: 2014's worst performing national currencies



Source: Bloomberg

It has been claimed that Bitcoin was 2014's "worst performing currency" with an annual price decline of 67%, significantly worse than both the Russian ruble and the Ukrainian hryvnia (Figure 5)[15]. Nevertheless, weekly Bitcoin price volatility, although still considerably greater than other asset classes, has been on a downward trend over the past year (Figure 6a). The weekly Bitcoin price volatility displayed in Figure 6a has been calculated in three different ways:

- Weekly Volatility – Method 1: Standard deviation of daily returns over a week.
- Weekly Volatility – Method 2: Weekly high minus weekly low divided by weekly low.
- Weekly Volatility – Method 3: Magnitude of Sunday night closing price minus previous Monday night closing price divided by the previous Monday night closing price.

Figure 6b: Bitcoin volatility methods comparison

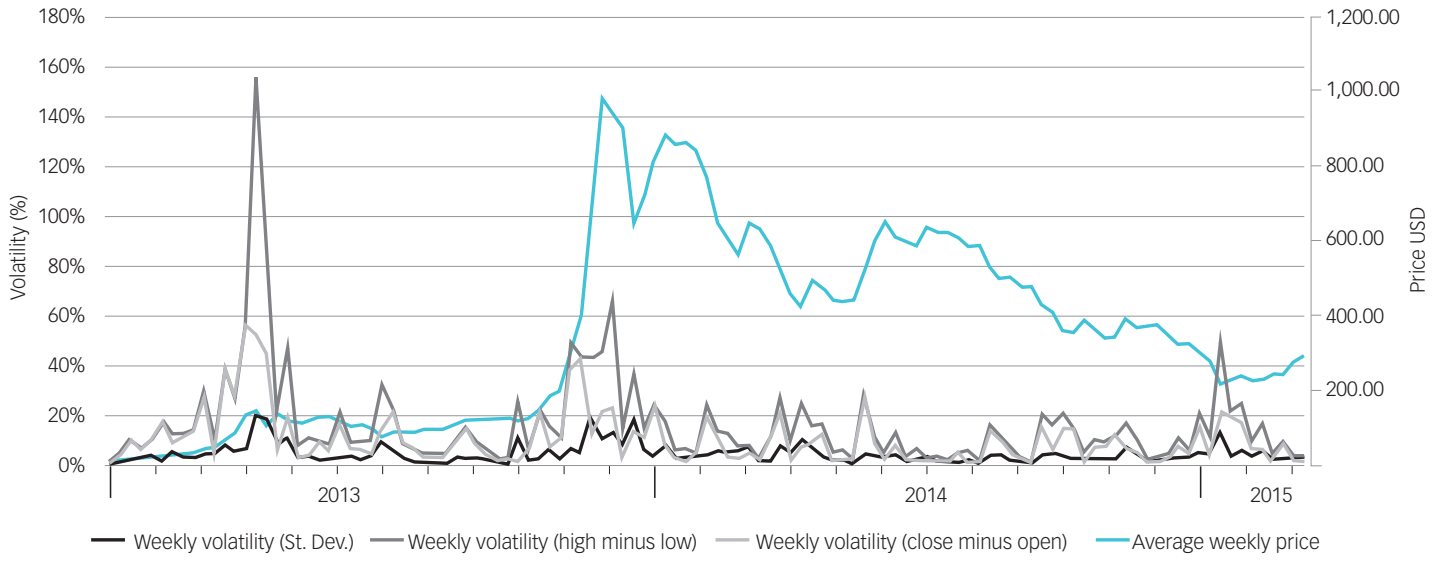
	Average	St. Dev.
Weekly Volatility – Method 1	4.37%	3.82%
Weekly Volatility – Method 2	16.33%	19.36%
Weekly Volatility – Method 3	10.08%	10.92%

Method 1 is a standard measure for volatility and under the same measure the average of the volatility of gold (In USD) was 0.93% for the same period, whereas Bitcoin's is 4.37%, or ~500% greater than gold[17].

Liquidity risk

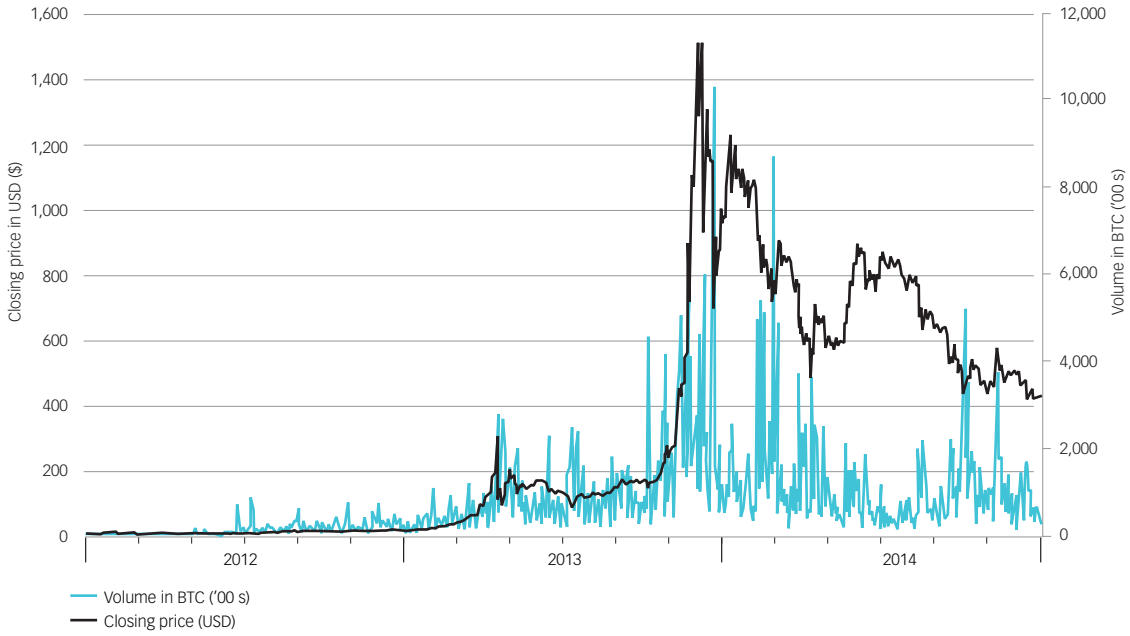
Liquidity risk can result in not being able to exchange bitcoins quickly enough to prevent a loss, and it is currently one of the main drivers of Bitcoin price volatility. Bitcoin liquidity risk stems primarily from the limited number of market participants and lack of

Figure 6a: Bitcoin weekly price volatility



Data Source: http://www.coindesk.com/price/

Figure 7: Bitcoin price (USD) and trading volume (in 100 BTC units), December 2011 – December 2014



Data Source: http://bitcoincharts.com/

market depth. Bitcoin's comparatively small market capitalisation makes it particularly vulnerable to large swings in value from relatively small transactions[18]: as of March 2015, Bitcoin had a relatively small total market capitalisation of approximately $3 billion, compared with the total value of all gold estimated at approximately $6.5 trillion[19]. Daily turnover of Bitcoin is also relatively small at 0.01% of total market capitalisation, as compared with 2–6% for other liquid asset classes such as gold, US Treasuries and Japanese Government Bonds[20].

The liquidity risk attached to Bitcoin is illustrated in Figure 7, which shows the volatile nature of trading volume. We can see that trading volume peaks often follow sudden spikes and declines in Bitcoin's price. This can also be taken as evidence of the speculative nature of transactions that drive Bitcoin trading volume at present.

Both greater liquidity and lower volatility could come about through greater adoption of bitcoin. For example, it is estimated that less than 50% of all bitcoins in circulation are used in transactions, and greater acceptance by merchants would mean more demand for conversion, and hence more liquidity[21]. Over 88,000 merchants now accept bitcoin, including a number of Fortune 100 companies such as Microsoft and Dell (Figure 8). While bitcoin has proven attractive for merchants to adopt due to its lower fees, no chargebacks, and other factors, consumers have yet to show much interest in paying for goods and services with bitcoin. Barriers to wider consumer adoption of bitcoin include the previously noted concerns over theft and price volatility, as well as the fact that bitcoins are still relatively difficult to use and acquire for many consumers.

Figure 8: Ten largest retailers that accept bitcoin (annual revenue)

Rank	Company	2013 annual revenue ($B)
1	Microsoft	86.80
2	Dell	56.90
3	Dish Network	13.90
4	Expedia	5.00
5	Intuit	4.50
6	Monprix*	4.30
7	Time Inc.	3.40
8	NewEgg	2.80
9	Overstock	1.30
10	TigerDirect*	1.00
		Total $179.90

*Note: Monprix is a private company and most recent revenue data is from 2005. TigerDirect estimate provided by parent company investor relations. Other divisions that are part of a larger parent organisation, but do not break out individual divisional revenues, are excluded.

Source: State of Bitcoin Report 2015, CoinDesk http://www.coindesk.com/research/state-of-bitcoin-2015/

Regulatory risk

Legal and regulatory concerns
Government-imposed restrictions could result in a fall in Bitcoin's value or the suspension of Bitcoin operations for those involved in the Bitcoin economy. To date, the actions and statements about Bitcoin by government agencies around the world reveal three primary areas of concern:

1. **Money laundering and illegal trade.** The unregulated and decentralised nature of Bitcoin means that it could be attractive for money laundering and other illegal activities, such as trade in illicit goods and tax evasion[22]. Bitcoin has been prominently associated with online black markets such as the original Silk Road, which was shut down in autumn 2013. Technological developments designed to offer additional layers of anonymity protection, such as the 'Dark Wallet' app, combined with cryptocurrency mixing services (which make bitcoin ownership more difficult to trace) have led to further concerns over the potential for Bitcoin to be exploited by criminals[23].

2. **Consumer protection.** Bitcoin is a decentralised money transfer system and there is no recourse available for users to reverse transactions or enjoy other safeguards offered by traditional and more centrally managed financial services, such as fraudulent transaction protection and deposit insurance.

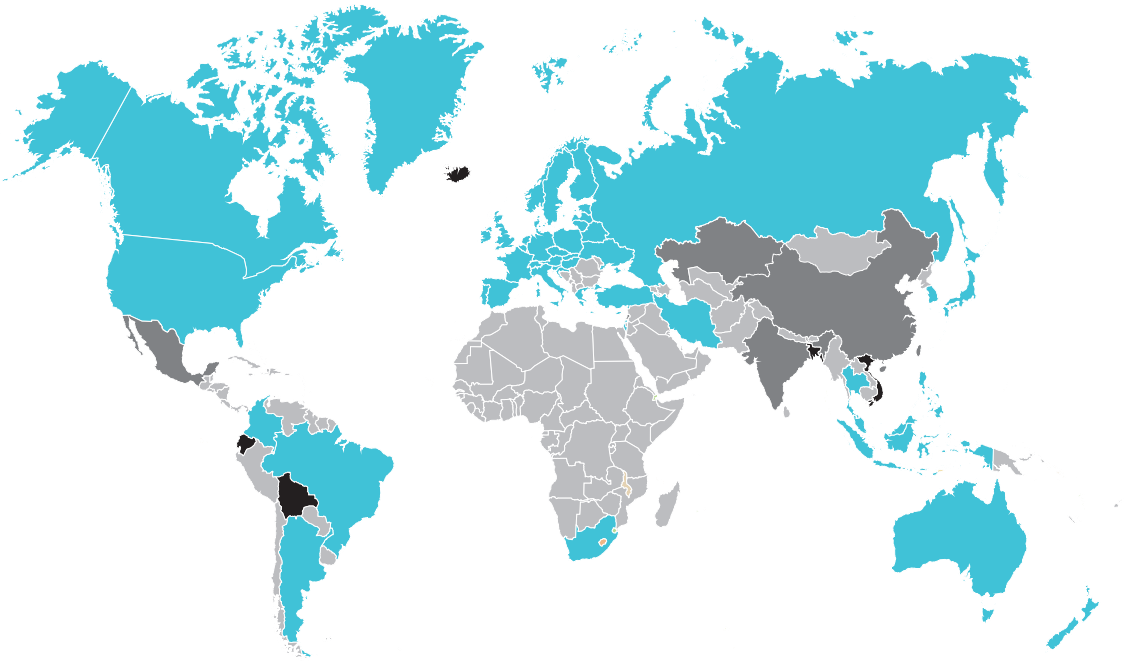
3. **Avoidance of capital controls.** Bitcoin can enable the avoidance of regulations designed to restrict the international movement of funds or limit ownership of foreign financial instruments[24].

Some regulatory authorities have also published reports that identify cryptocurrencies as posing a systemic risk to the financial system in the medium to long term[25]. However, barring a significant increase in Bitcoin adoption, and/or a macroeconomic crisis, it is unlikely that such systemic concerns will affect Bitcoin regulation in the near future.

Worldwide approaches to Bitcoin regulation
To date over 60 countries have officially issued some form of regulatory guidance or regulation relating to Bitcoin or alternative currencies more generally. The Bitcoin regulatory map in Figure 9 shows a rough approximation of the countries where the use of bitcoin is legal (blue), subject to some restrictions (dark grey), and banned or severely restricted (black). Countries coloured light grey have not yet issued any regulatory guidance on Bitcoin.

Overall, the map highlights how the vast majority of countries have neither banned nor severely restricted bitcoin's use. The map also highlights how few African

Figure 9: Legal status of Bitcoin by country



Source: Wikipedia https://en.wikipedia.org/wiki/Legal_status_of_Bitcoin

countries have issued any regulatory guidance on Bitcoin. It is important to note that the regulatory map is rather simplistic. For example, while bitcoin has not been banned in Europe, the authorities have discouraged banks from transacting with bitcoin or interacting with the Bitcoin companies[26]. This in turn has limited the ability of Bitcoin businesses to connect with the broader financial system and grow.

Given both the high number of Bitcoin operations based in the US, and the position of the US in the global economy and financial system, regulation in the US will probably have a significant influence on the development of global Bitcoin regulation. In July 2014 the US Securities and Exchange Commission issued an investor alert on cryptocurrencies[27]. Subsequently, the New York State Department of Financial Services proposed specific regulation for Bitcoin businesses and operators called "BitLicenses"[28]. In March 2014 the Internal Revenue Service classified bitcoin as a property and suggested that all bitcoin transactions could be subject to individual capital gains taxes. Perhaps on a more positive note, the US Marshals' auctioning of millions of dollars of bitcoins seized in the Silk Road drug marketplace raid has been viewed as a *de facto* legalisation of bitcoin at the federal level of the US government given that the government will not auction any seized goods that are deemed illegal (e.g. cocaine). While a unified regulatory policy has yet to emerge, further examination of Bitcoin by US state and federal authorities is expected.

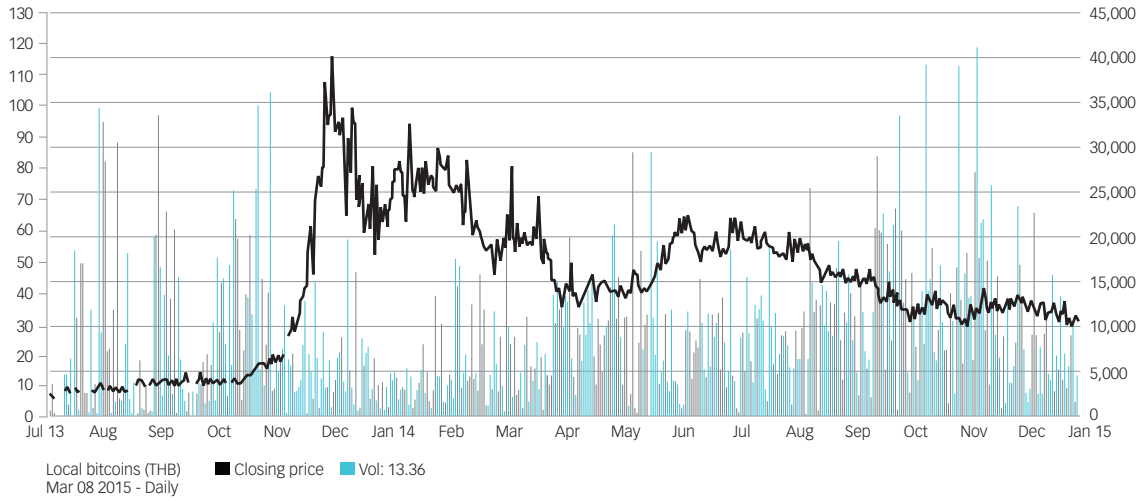
Impacts of varying approaches to Bitcoin regulation

The different Bitcoin regulations that have been applied and the resultant impact are illustrated in the following three mini regulatory case studies. While they diverge in approach, all three cases demonstrate the potential that regulation has to impact bitcoin's market value:

1. **Prohibition.** Citing security issues, the possibility of enabling tax evasion, and clashes with its monetary policy, the central bank of Bolivia issued a resolution banning all cryptocurrency-related activity[29]. The ban covers conversion and quoting of prices in bitcoin, amounting to an indirect ban on transactions. Since implementing the ban in May 2014 there has been a gradual decline in the bitcoin/boliviana (BOB) exchange rate at a rate faster than the bitcoin/USD exchange rate. Bitcoin/BOB exchange rates have fallen by about 66% since the ban was implemented.

2. **Partial restrictions.** In Thailand, exchanges are allowed to legally convert Thai bahts to bitcoins but are banned from converting bitcoins for other currencies. The Thai government initially banned Bitcoin altogether before moving to this more relaxed stance[30]. On 29 July 2013, Bitcoin Co. posted a notice saying it was suspending all activity due to a directive from the Bank of Thailand, resulting in a 15% decline in the value of bitcoin (Figure 10). It remained at that level until December 2014, after which it recovered and stabilised.

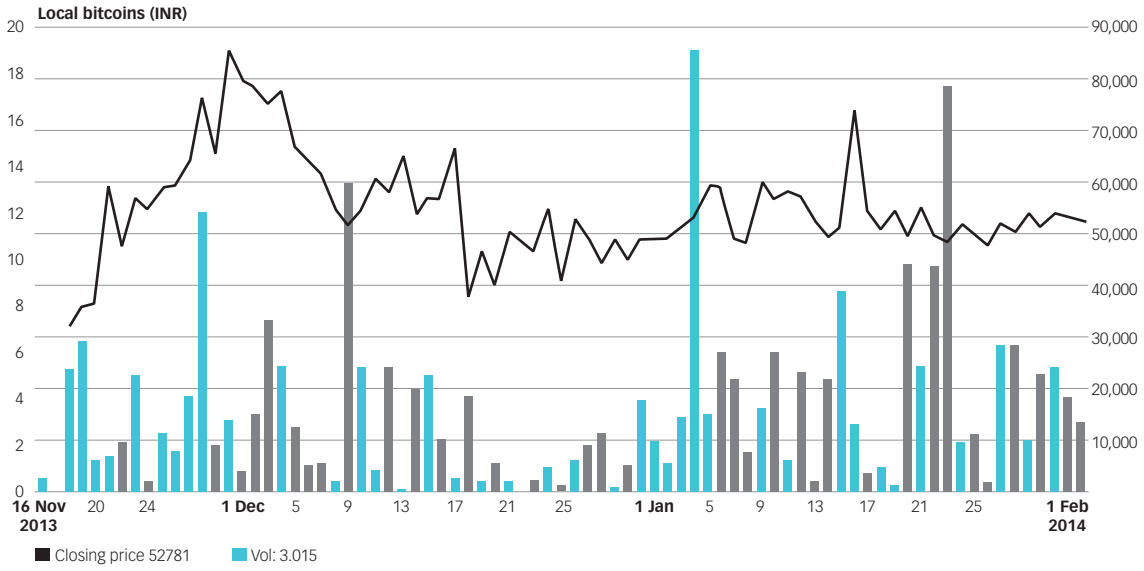
Figure 10: Bitcoin value against Thai baht, July 2013 – September 2014



Data Source: http://bitcoincharts.com/charts localbtcTHB#czsg2013-07-01zeg2015-01-01ztgCzm1g10zm2g25zv

3. **Regulatory warning.** The Reserve Bank of India has indicated that it has no plans to regulate Bitcoin, but on 24 December 2013 it issued a public notice warning citizens about the dangers of virtual currencies[31]. In the weeks leading up to the notice the value of bitcoin fell by almost 40% against the Indian rupee (Figure 11). The warning coincided with a steep fall in the value of bitcoin against the Indian rupee, including a 27% fall in a single day. Volume can also be seen to dip sharply in the week the notice was released.

Figure 11: Bitcoin/Indian rupee closing prices for a month before and after the RBI notice (24 December 2013)



Data Source: http://bitcoincharts.com/charts/localbtcINR#tgCzm1g10zm2g25zv

Conclusion

Cryptocurrencies such as Bitcoin could play an important role in transforming financial services and other industries that many feel are ripe for disruption. Investment in the Bitcoin ecosystem of start-ups to date totals over $660 million, which is roughly on par with the level of early stage investments in internet start-ups[32]. This strong showing of support from the venture capital community indicates the very significant economic potential seen for cryptocurrencies.

However, there are no clear solutions on the horizon for some Bitcoin risks, such as the currency's price volatility or technical vulnerabilities like a 51% attack. Individuals and institutions that are seeking to participate in the Bitcoin economy must take into consideration a wide range of risk factors that come with Bitcoin's innovative but still maturing ecosystem.

References

1. *http://coinmarketcap.com/all/views/all/*

2. Bitcoin creator Satoshi Nakamoto first published his paper describing Bitcoin on 31 October 2008 and then mined the first bitcoins on 3 January 2009 http://historyofbitcoin.org/

3. Reflecting this status the current Bitcoin Core protocol is Version 0.10.0 *https://bitcoin.org/en/download*

4. At the time of writing this report, the vast majority of the approximately 800,000 bitcoins originally reported missing have yet to be fully accounted for or recovered *http://www.nytimes.com/2014/02/25/business/apparent-theft-at-mt-gox-shakes-bitcoin-world.html?_r=0*

5. *http://www.coindesk.com/bitstamp-claims-roughly-19000-btc-lost-hot-wallet-hack/*

6. Moore and Vasek, There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams *http://fc15.ifca.ai/preproceedings/paper_75.pdf*

7. Only confirmed thefts are included i.e. all cases of bitcoin loss from the list have been omitted from the graph. The Silk Road seizure by the FBI has also been omitted.

8. Financial Fraud Action UK *http://www.theukcardsassociation.org.uk/news/EOYFFfor2013.asp*

9. Bitcoin USD transaction value obtained from *https://blockchain.info/charts/estimated-transaction-volume-usd UK credit card data obtained from http://uk.creditcards.com/credit-card-news/uk-britain-credit-debit-card-statistics-international.php*

10. *https://en.bitcoin.it/wiki/Attacks#Attacker_has_a_lot_of_computing_power*
    Note: transaction censorship is something that could take place without 51% control of the Bitcoin network. All that is required is that the current mining block award winners collude to exclude certain transactions from inclusion in the blockchain.

11. *http://www.theguardian.com/technology/2014/jun/16/bitcoin-currency-destroyed-51-attack-ghash-io*

12. *http://www.bitcoinx.com/bitcoin-developer-gavin-andresen-weighs-in-on-centralized-mining-and-the-ghash-situation/*

13. *http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf*

14. Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry, Polasik et al *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2516754*

15. *http://www.bloombergview.com/articles/2014-12-23/and-2014s-worst-currency-wasbitcoin*

16. Calculated using data from World Gold Council: *http://www.gold.org/*

17. Method 2 (and to an extent Method 1) is a reliable measure in liquid markets to gauge the trend as a widening measure would imply that the trend is likely to be reversed.

18. See for the example the October 2014 price impact of a sale of 30,000 bitcoins on Bitstamp by an early bitcoin adopter (pp. 7–8) *http://panteracapital.com/wp-content/uploads/Pantera-Bitcoin-Letter-November-2014-1.pdf*

19. 171,300 tonnes of gold have been mined throughout 2011 according to the Minerals Handbook published by the USGS (*http://minerals.usgs.gov/minerals/pubs/commodity/gold/myb1-2011-gold.pdf*) and 462 tonnes were mined in 2012 and 2013 according to USGS (*http://minerals.usgs.gov/minerals/pubs/mcs/2014/mcs2014.pdf*). The price of gold was taken as $38 per gram.

20. *http://www.gold.org/sites/default/files/documents/gold-investment-research/liquidity_in_the_global_gold_market.pdf*

21. Bitcoin: Technical Background and Data Analysis, Anton et al *http://www.federalreserve.gov/econresdata/feds/2014/files/2014104pap.pdf*

22. See for example Danton Dryans, Bitcoin and Money Laundering: Mining for an Effective Solution, *Indiana Law Journal* - *http://ilj.law.indiana.edu/articles/19-Bryans.pdf*

23. See "Hiding Currency in the Dark Wallet", BBC *http://www.bbc.co.uk/news/technology-29283124* and "Dark Wallet' Is About to Make Bitcoin Money Laundering Easier Than Ever" WIRED, *http://www.wired.com/2014/04/dark-wallet/*

24. G. Hileman, Bitcoin Market Potential Index *http://www.bitcoiniq.info/*

25. For example, see "The Economics of Digital Currencies" by Ali et al *http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesbitcoin2.pdf* and "Risks to financial stability and payment system stability" *http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf and "Impact of innovations in retail payments on monetary system" http://www.bis.org/cpmi/publ/d102.pdf*

26. EBA Opinion on Virtual Currencies *http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf*

27. Investor Alert: Bitcoin and Other Virtual Currency-Related Investments, SEC *http://investor.gov/news-alerts/investor-alerts/investor-alert-bitcoin-other-virtual-currency-related-investments#.VNKXomjkdcR*

28. In the matter of virtual currency exchanges, DFS NY *http://www.dfs.ny.gov/about/po_vc_03112014.pdf*

29. Resolution from El Banco Central de Bolivia *http://www.bcb.gob.bo/webdocs/2014/Normativa/Resoluciones/044%202014.PDF*

30. Bitcoin Ban Fear Fades in Thailand With Exchange Launch *http://www.coindesk.com/bitcoin-ban-fear-fades-thailand-exchange-launch/*

31. RBI cautions users of Virtual Currencies against Risks *http://rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=30247*

32. *http://www.coindesk.com/bitcoin-venture-capital/ and http://www.coindesk.com/research/state-of-bitcoin-2015/*


FIDENTIA