Bitcoin: Its Risks, Opportunities, and Developments in Audit and Regulation

Rosanne Lai

June 29, 2015

Executive Summary

Bitcoin has been a public fascination since its emergence in 2009. Despite its popularity in the media and notoriety following the collapse of the Mt. Gox exchange, the technical background of Bitcoin is still unknown to many. Bitcoin is essentially an electronic ledger that is publically maintained by its network of users. All transactions, accounts, and balances are public yet pseudo-anonymous as there are no names, addresses, or other personally identifying data. Bitcoin transactions are sent peer to peer through the network, and verified by users. The verification process uses a cryptographic hash that can only be solved by inputting random number guesses. The first user to solve the hash is awarded newly created bitcoins by the system as a reward for helping to maintain the system, known as “mining”.

There are a number of incentives to using Bitcoin. The first is that it is decentralized, so that customer accounts cannot be seized, confiscated, or frozen. Inflation will never be a problem as the supply of Bitcoin is fixed. The system is completely transparent so that every single transaction is publically viewable. And yet, Bitcoin is also pseudo-anonymous as none of the transactions can be traced back to private identities. The code is also open sourced so that anyone can review the software. The most attractive benefit of Bitcoin to the average consumer and business is its cost savings. While traditional payment processes such as Visa, MasterCard and PayPal charge around 3% per transaction, Bitcoin only costs 1% per transaction and no base fees.

As Bitcoin continues to grow, there has been an increasing demand from consumers for audits on Bitcoin exchanges. In light of the Mt. Gox’s collapse, customers now want assurance from independent third-parties that their bitcoins are safe. Bitcoin’s largest exchanges, such Bitstamp and Kraken, have already paved the path for the first Bitcoin audits in history. However, there still remains to be much improvement that could be made to these audits, which opens up an entirely new market for audit service providers.

For Bitcoin to truly become a universally accepted currency, its best chance of success is to embrace regulation and integration with the traditional financial system. Getting the average consumer on board will require the backing of trusted institutions and government authorities. Should Bitcoin be able to achieve this, we should expect it to become a permanent player in our economy into the future.

Table of Contents

1. Introduction

Bitcoin is the world's first decentralized digital currency. While the concept of digital currencies is not new, Bitcoin has proven itself to be a game-changer via its widespread adoption and survivorship. The genius that sets Bitcoin apart lies it its design which enables it to function without the need for a central authority or third-party intermediary. This appeals to users as Bitcoin is cheaper to transact with, is anonymous, and cannot be seized. However, Bitcoin's existence has not been without road bumps; most notably, the bankruptcy of the Mt. Gox exchange - which handled 70% of all bitcoin transactions at its peak[1]. As a result of these events, Bitcoin companies and exchanges have opened up a new market for audit service providers.

2. Bitcoin: A Technical Overview

Prior to Bitcoin, there were several early iterations of digital currencies that were issued by companies for the exclusive redemption of its own products and services, such as Microsoft points. It was not this concept of virtual currency for the exchange of goods and services online that made Bitcoin unique. The problem with a truly decentralized digital currency is that, like any other electronic file, it does not get deleted when sent and can be used multiple times. Without a central authority keeping an independent ledger, it would be impossible to prevent people from double-spending. For example, online transactions would have to go through a third party intermediary such as PayPal, which keeps a ledger with user account balances. PayPal deducts the amount of the transaction from the sender's account and adds the same balance to the receiver's account so that all of PayPal's accounts nets to 0 at the end of the day. In 2008, Satoshi Nakamoto published a paper online that proposed an eloquent solution to this double-spend problem, without the need for a third-party intermediary[2]. He named this solution Bitcoin, and went on to code and release the first Bitcoin software in 2009.[3]

Bitcoin is essentially an electronic ledger that is public and maintained by its network of users, rather than by a single entity. All transactions, accounts, and balances are public yet pseudo-anonymous, as there are no names, addresses or other personally identifying data. The technical breakthrough that makes Bitcoin possible is that, by maintaining its ledger across all users, the double spend problem can be mitigated by allowing the network itself to verify transactions[4]. Bitcoin transactions are sent through messages requiring a digital signature from the owner of the bitcoins. This digital signature is generated using a mathematical algorithm with the transaction message and the owner's private key as inputs. Any small change to the transaction message will result in an entirely different digital signature, preventing

1 Vigna, P. (2014, 02 25). 5 Things about Mt. Gox's crisis. Retrieved 06 27, 2015, from the Wall Street Journal: http://blogs.wsj.com/briefly/2014/02/25/5-things-about-mt-goxs-crisis/
2 Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved 06 27, 2015, from https://bitcoin.org/bitcoin.pdf
3 Davis, J. The Crypto-Currency: Bitcoin and Its Mysterious Inventor. Retrieved 06 27, 2015 from The New Yorker: http://www.newyorker.com/magazine/2011/10/10/the-crypto-currency
4 Driscoll, S. (2014, 09 26). The Essence of How Bitcoin Works (Non-technical). Retrieved 06 27, 2015, from http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

others from making unauthorized modifications[5]. Therefore, each transaction produces a completely different digital signature. It is important that the private key never be revealed to the network as anyone who has access to a private key will have access to the bitcoins in possession by the owner of that private key. The transaction message, digital signature, and public key addresses of the owner and the recipient are then sent to the Bitcoin network and transferred peer to peer to every computer in the network.

Each computer receives the transaction message and updates its copy of the ledger before passing it on to the next computer in the network. Users on the network can verify that the owner of the bitcoins sent the transaction by using the transaction message, digital signature, and the sender's public key using another mathematical algorithm[6]. These algorithms are provided on the network so that anyone can participate in the verification process. Due to the peer to peer distribution of transaction messages, the timing and order of transactions received by each computer varies[7]. Transactions that are received at the same time are grouped and ordered into a block that awaits confirmation. To prevent the double-spending problem, the network needs to collectively decide on the order in which transactions are to be processed so that no one can send two transactions using the same bitcoins to fraudulently double their use. Users will run their version of these blocks of unconfirmed transactions, along with the hash reference of the most recently processed block and a random number guess into a cryptographic hash. The user who solves the hash first below a certain value confirms their version of the transaction block as the next to be processed along the block chain[8]. The transactions contained in block are then completed so that the ledger updates to show a deduction in the sender's balance and increase in the recipient's balance.

On average, it takes 10 minutes for someone in the network to solve the cryptographic hash confirming the block of transactions[9]. The hash can only be solved using random number guesses by virtue of trial-and-error. Therefore, the process is similar to partaking in a random lottery. This democratizes the system so that a single user cannot control the ordering of transactions. Every 2 weeks, the Bitcoin software recalibrates the difficulty of solving the hash to target 10 minutes[10]. Similar to the digital signature, the hash output changes entirely if any small change is made to the block of transactions. This prevents users from switching the order of the transactions at a later date. The user who solves the hash is compensated with newly-created bitcoins. The creation of bitcoins is designed as an inherent incentive in the system to reward users for helping to maintaining the ledger and preventing the double-spend problem. This process of confirming transactions and receiving bitcoins is known as "mining". Every four years, the system readjusts so that only half of the remaining bitcoins can be mined. The Bitcoin system

5 Discoll, S. (2013, 07 14). How Bitcoin Works Under the Hood. Retrieved 06 27, 2015, from http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html
6 Ibid.
7 Ibid.
8 Ibid.
9 Ibid.
10 Ibid.

was designed so that a fixed supply of only 21 million bitcoins can ever be created. Therefore, by the year 2140, no more bitcoins will be issued and small transaction fees will replace mined bitcoins as the incentive for users to perpetuate the maintenance of the system[11].

3. Bitcoin: Its Risks and Opportunities

No single institution owns or controls the issuance or management of bitcoin transactions. Unlike with cash and credit, in which users place their trust in banks and third-party intermediaries, Bitcoin is designed so that trust is not needed. Instead, Bitcoin is regulated collectively by the Bitcoin network. However, therein lies one major disadvantage to decentralization. Unlike when dealing with banks or Visa/MasterCard, there is no insurance for Bitcoin or opportunity to sue if something goes wrong. For example, 2600 bitcoins were lost forever in 2011 due to a malformed address for a single batch[12]. User mistakes, such as misplaced private keys and hard drive crashes, can easily result in the loss of bitcoins to both the owner and the Bitcoin economy overall. Bitcoins are also non-refundable once they've been sent.

Like any other fiat currency, Bitcoin only has value because people believe that it has value and trust that other people share in this belief. It will only work if people are willing to trade goods and services for a higher value of bitcoins next to their account. The infrastructure of Bitcoin requires marketplace exchanges to get traditional fiat monies into Bitcoin, payment processors to spend bitcoin, and digital wallets to hold bitcoins. Should any of these infrastructure components malfunction, the perceived value of Bitcoin will fall.

Bitcoin is pseudo-anonymous so that transactions and ownership cannot be traced back to individuals despite their public keys and balances being public. If the user wishes to further protect their personal identity, they can choose to access Bitcoin using the TOR network to hide their IP address, and generate a new public key for every bitcoin transaction[13]. Unfortunately, the anonymity that Bitcoin offers has led to its association with the black market. In particular, the media has often linked Bitcoin to Silk Road, an online black marketplace known for selling drugs that has since been shut down.

Despite these risks, Bitcoin offers many advantages over traditional currencies and payment methods. Since the supply of Bitcoin is limited, inflation resulting from the printing of excess money will never be a problem. Instead, it is more likely that Bitcoin will eventually become a deflationary currency due to the inevitability of lost bitcoins due to user error. As there is no government authority regulating Bitcoin, amounts cannot be seized, confiscated, or frozen. Bitcoin is also less susceptible to political pressure, as was demonstrated in 2010 when Bitcoin continued to process donations to WikiLeaks while PayPal, Visa,

11 Ibid.
12 Brown, A. (2015). Bitcoin Thefts. Retrieved 06 27, 2015, from https://bitcointhefts.com/
13 CoinDesk. (2014, 02 20). Why Use Bitcoin? Retrieved 06 27, 2015, from CoinDesk: http://www.coindesk.com/information/why-use-bitcoin/

and MasterCard dropped. Bitcoin is completely transparent, from its most recent transactions to the very first Bitcoin transaction in history. Furthermore, the Bitcoin software code is open source so that anyone can review the code.

Bitcoin is a platform for innovation. As it is open source, anyone can create a start up to build new technologies to add on to its network, such as wallets, mobile apps, exchanges, and more. This open innovation will, in turn, make Bitcoin more accessible to the average layperson and perpetuate user adoption. Thus, an entirely new industry has been created by Bitcoin. The current market cap for Bitcoin is currently $3.5B USD[14]. As evidence of Bitcoin's allure, Coinbase - the first U.S. bitcoin exchange - is set to open later this year with $106M USD of funding from the New York Stock Exchange, banks, and venture-capital firms[15].

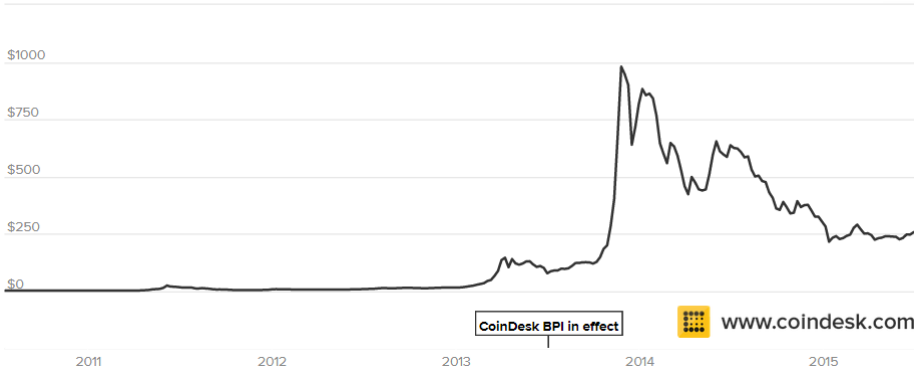
The most attractive advantage of using Bitcoin to the average layperson is its cost savings. Anyone can set up a Bitcoin address on the network for no fee, given that they have access to a computer and internet connection. There is also no limit on the size of transactions. Bitcoin offers significant cost savings compared to the traditional forms of online payment such as Visa, MasterCard, and PayPal. Currently Visa and MasterCard charge 2.7% in fees, while PayPal charges 2.9%, and American Express charges 3.1%[16]. Using a Bitcoin exchange like Coinbase only results in charges of 1%. If a company's profit margin is 5%, switching to Bitcoin represents approximately 40% of cost savings on its bottom line. Both merchants and consumers will benefit as cost savings are passed on to customers. For example, Subway offers a 10% discount to customers who pay in bitcoins. Bitcoin is currently accepted by over 30,000 online retailers including Dell, Newegg, and Overstock.com[17]. In addition to percentage fees, traditional forms of online payment also charge a fixed base fee per transaction. The micro transaction market is currently non-existent given that a 5 cent transaction will cost at least a base fee of 20 cents to process. In the case of charities, a significant portion of small denominations of donations are lost to these base transaction fees. By switching to Bitcoin, a nominal amount of the donation is forfeited to third party payment processors. Lastly, remittances from the developed to the developing world now represent a $582B USD market.[18] While Western Union charges 10% on remittances, Bitcoin would represent 9% of cost savings to people transferring their hard-earned money back home to their friends and family in need.

14 CoinDesk. (2015, 06 27). Bitcoin Price Index. Retrieved 06 27, 2015, from CoinDesk: http://www.coindesk.com/price/
15 Bensinger, G. (2015, 01 25). First U.S. Bitcoin Exchange Set to Open. Retrieved 06 27, 2015, from The Wall Street Journal: http://www.wsj.com/articles/first-u-s-bitcoin-exchange-set-to-open-1422221641
16 PwC. (2014, 02 07). Digital Disruptor: How Bitcoin is Driving Digital Innovation in Entertainment, Media, and Communications. Retrieved 06 27, 2015, from http://www.pwc.com/en_SG/sg/tmt/assets/tmtnews201402/digital_disruptor.pdf
17 CoinDesk. (2015, 02 17). What Can You Buy with Bitcoin? Retrieved 06 27, 2015, from CoinDesk: http://www.coindesk.com/information/what-can-you-buy-with-bitcoins/
18 Graillot, F. (2015, 05 25). Bitcoin Might Be The Next Big Thing In The Remittance Market. Retrieved 06 27, 2015, from TechCrunch: http://techcrunch.com/2015/05/25/bitcoin-might-be-the-next-big-thing-in-the-remittance-market/

4. Volatility and Mt. Gox

The history of Bitcoin prices has experienced ups and downs. A bitcoin today is worth approximately $248 USD, while its lowest price in the trailing twelve months was $117 USD (see Appendix 1 below). At its peak in November 2013, one bitcoin was worth $1,216.73 USD.

Appendix 1: Bitcoin Historical Price Index[19]



Around this time, Mt. Gox was the largest Bitcoin exchange in the world - handling over 70% of all Bitcoin transactions. Its customers had recently begun experiencing difficulty withdrawing their funds from Mt. Gox. Amongst increasing concerns that the exchange was insolvent, more and more customers began trying to withdraw from the exchange. It was reported that customers were experiencing delays of weeks to months in having their withdrawals processed, which Mt. Gox attributed to technical problems[20]. In February of 2014, Mt. Gox officially suspended trading, closed its website, and filed for bankruptcy protection due to insolvency. It was revealed that a total of 850,000 bitcoins had been stolen from the Mt. Gox's reserves, an amount that was equivalent in value to $460M USD at the time.[21] Only 200,000 bitcoins were later recovered. Upon the collapse of Mt. Gox, Bitcoin's value fell close to 23% to $418[22]. It had been in decline for the half year prior. According to an investigation of the collapse, Mt. Gox's bitcoins were likely stolen beginning in 2011 with most of them gone by May 2013[23]. Mt. Gox had therefore been operating on a fractional reserve for months, if not years. Whether or not Mt. Gox was aware of this, an audit could have prevented a situation like this from being undiscovered by the public for so long.

5. Post-Mt. Gox: The First Bitcoin Audits

In the wake of the Mt. Gox downfall, Bitcoin exchanges began voluntarily submitting themselves to be audited. Bitstamp, the largest Bitcoin exchange by volume post-Mt. Gox, engaged one of the first Bitcoin

19 CoinDesk. (2015, 06 27). Bitcoin Price Index. Retrieved 06 27, 2015, from CoinDesk: http://www.coindesk.com/price/
20 Wong, J. I. (2014, 02 04). Poll: Are you having Mt. Gox Withdrawal Issues? Retrieved 06 27, 2015, from CoinDesk: http://www.coindesk.com/poll-mt-gox-withdrawal-issues/
21 McMillan, R. (2014, 03 03). The Inside Story of Mt. Gox's $460 Million Disaster. Retrieved 06 27, 2015, from Wired: http://www.wired.com/2014/03/bitcoin-exchange/
22 Ibid.
23 Southurst, J. (2015, 04 29). Most Mt Gox Bitcoins Were Gone by May 2013, Report Claims. Retrieved 06 27, 2015, from CoinDesk: http://www.coindesk.com/most-mt-gox-bitcoins-were-gone-by-may-2013-report-claims/

audits conducted by Firestartr.co[24]. While it is common for banks to operate on fractional reserves with most of deposits going towards investments and loans, this is a problem should all customers decide to withdraw their funds at the same time. This was the case for Mt. Gox, as more and more customers rushed to cash out and the true insolvency of the exchange was revealed. Despite all Bitcoin transactions being public and transparent, the transactions of exchanges are kept "off-chain" once bitcoins are sent to the exchange until they are withdrawn[25]. Transactions within the exchange are thus not recorded in the public bitcoin block chain, but only in the exchange's proprietary transaction system. To provide customers with comfort that the exchange wasn't backed by only fractional reserves, Kraken created the largest single Bitcoin wallet and transaction in history - worth $147M USD[26]. Following the audit's success, Bitstamp committed itself to future quarterly audits. This set the precedence for other Bitcoin companies to also engage audits to reassure customers that they did not have to worry about suffering the same fate as Mt. Gox's customers.

Kraken, another prominent Bitcoin exchange, engaged Stefan Thomas (Chief Technical Offer at Ripple Laps – a company that developed its own payment protocol and exchange network) to perform its audit[27]. Similar to Bitstamp, Kraken wanted to reassure customers that it wasn't operating a fractional reserve. In addition, it requested that Thomas criticize the process at Kraken and suggest improvements. Kraken tagged this engagement as a "proof-of-reserves" audit, given its nature as neither a typical financial statement audit nor a controls audit[28].

Rather than create a massive transaction of the sum of Kraken's reserves, Thomas sought to reconcile the exchange's assets with its liabilities. The balance of bitcoins held in reserve in Kraken's public key address were the assets of the exchange, while the total sum of bitcoins tied to the set of public key addresses belonging to customer accounts were the liabilities of the exchange. Each bitcoin tied to a customer account represented a bitcoin that the exchange would have to eventually pay out when the customer decided to cash out.

To compute the total balance of bitcoins belonging to Kraken, Thomas extracted all transactions from the block chain associated with the public key address of the exchange. These transactions were hashed together, and the results of these hashes hashed together until every transaction block had been combined together into a single hash. This hashing approach is known as the Merkle tree, with the final

24 Firestartr.co. (2014, 03 06). Letter for Bitstamp. Retrieved 06 27, 2015, from https://www.bitstamp.net/s/documents/Firestartr_DD_Letter_for_Bitstamp.pdf
25 Discoll, S. (2013, 07 14). How Bitcoin Works Under the Hood. Retrieved 06 27, 2015, from http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html
26 Rizzo, P. (2014, 03 06). Bitstamp Audit Proves it was Behind $147 Million Mystery Bitcoin Wallet. Retrieved 06 27, 2015, from CoinDesk: http://www.coindesk.com/bitstamp-audit-proves-behind-147m-mystery-bitcoin-wallet/
27 Bradbury, D. (2014, 05 02). What Really Happens Inside a Bitcoin Audit. Retrieved 06 27, 2015, from CoinDesk: http://www.coindesk.com/what-happens-inside-bitcoin-audit/
28 Kraken. (2014). Kraken Proof-of-Reserves Audit Process. Retrieved 06 27, 2015, from https://www.kraken.com/security/audit

hash known as the Merkle root.[29] The Merkle root effectively hashes together all transactions in the tree into a single, small hash. From an audit respective, the creation of the Merkle root allows for evidence of existence of bitcoins held by the exchange. The same was done for customer balances. The total balance of the Merkle root for Kraken's reserves was checked against the balance of the Merkle root for the customer accounts to prove the exchange's solvency[30].

Following this, Thomas still had to check that Kraken indeed had all of its customer accounts included on the list that it provided. For auditors, this would be known as a completeness check. An exchange could under report the customer accounts to look like it owed less than it did. The solution to this problem was proposed by Gregory Maxwell (Bitcoin core developer and co-founder of Blockstream)[31]. Kraken simply published the Merkle root to the public, as well as all the transactions of bitcoins belonging to their account and their account balance from the point in time of the audit. They also disclosed the hashing algorithm used to generate the Merkle root. This allowed customers to run the hash themselves to check that their transactions of bitcoins were included in the audit's Merkle root. While it was on the onus of users to verify that their balances had been included, each confirmed check decreased the probability that the exchange omitted any customer accounts exponentially.

6. The Future for Bitcoin Audits

However, some problems still exist in the current audit process. For example, the audit does not prove that the exchange has not borrowed bitcoins for the purposes of the audit. It also does not prove that the exchange has not misappropriated its private key – meaning that the exchange may not have exclusive access to its own Bitcoin wallet and may have compromised the integrity of its private key by exposing it to other parties[32]. Andreas Antonopoulos (Chief Security Officer at Blockchain), conducted a similar engagement for Coinbase, one of the largest Bitcoin exchanges and wallets on the market. He has since vouched for more comprehensive and rigorous audits to be implemented going forward.[33] According to Antonopoulos, Bitcoin exchange audits of the future should require audits of the exchange's fiat operations and security as well, beyond just an audit of the exchange's Bitcoin reserves. An audit of fiat operations would ensure that the exchange is not simply buying more bitcoins to cover customer accounts with its fiat currency, and then exchanging it back once the audit is over. Therefore, the entirety of the exchange's assets on both the regular fiat currency side and the Bitcoin side should be audited. An audit of the exchange's cybersecurity systems is also important to ensure that the exchange has not been visibly hacked. These three pillars of an audit would ideally be inspected as both a snapshot of the present, as well as on an ongoing basis as future governance. This would involve looking at the controls

29 Bradbury, D. (2014, 05 02). What Really Happens Inside a Bitcoin Audit. Retrieved 06 27, 2015, from CoinDesk: http://www.coindesk.com/what-happens-inside-bitcoin-audit/
30 Ibid.
31 Ibid.
32 Kraken. (2014). Kraken Proof-of-Reserves Audit Process. Retrieved 06 27, 2015, from https://www.kraken.com/security/audit
33 Bradbury, D. (2014, 05 06). Why Bitcoin Exchange Audits Don't Go Far Enough. Retrieved 06 27, 2015, from CoinDesk: http://www.coindesk.com/exchanges-must-still-prove-themselves-customers/

that are in place to prevent future hacks, shifting of fiat reserves to bitcoins, and misappropriation of Bitcoin reserves.

A general challenge for Bitcoin audits is recruiting auditors who are technically capable for the job. The users and customers of the exchange must believe in the auditor's reputation and capabilities for the audit to be of value. Given the heavily technical coding and mathematics behind the Bitcoin software, the future auditors of Bitcoin must be technical themselves - which is not typically a skill set that is required of auditors. Currently, there is not much of an overlap between Bitcoin experts and accountants. A team of auditors would likely be required to achieve expertise across multiple disciplines, including "CPAs and financial auditors, security auditors for infosecurity, and experts in cryptographic currencies" [34]. Lastly, auditors must be trustworthy and have adequate security measures in place to ensure that none of the exchange's confidential data is compromised. In 2011, a hacker allegedly was able to fraudulently transfer bitcoins to himself after gaining access to credentials from an auditor's compromised computer[35]. User privacy is a large concern given that exchanges keep records of public key addresses, account balances, and other user data that may be commercially sensitive.

Going forward, Bitcoin exchanges have voiced their intention to perform regular audits on an ongoing basis, using different auditors to maintain independence. As it stands, the audit methodology employed for the Bitstamp and Kraken audits are proofs-of-solvency at a snapshot in time. The more dated these snapshots become, the less relevant they are. Repeat audits are needed to continue validating the exchange to assure customers that their funds are still safe. To make these repeat audits possible, customers would have to do their part to check that their balances had been included in the audit as described above. Third-party software has emerged to independently complete this check in a user-friendly interface, such as Chinese startup Bifubao[36]. Exchanges have also invited feedback and suggestions from the Bitcoin community to improve the audit process. It is now the collective goal of the Bitcoin industry to develop basic standards, scalable tools, and comprehensive manuals for others to follow and standardize their audits.

7. Standardization of Bitcoin Audits

Recently, Netagio became the first Bitcoin exchange to receive International Standard on Engagement (ISAE) 3000 certification on its Bitcoin storage[37]. The review was performed by public accounting firm BDO LLP. The ISAE 3000 is a standard issued by the International Auditing and Assurance Standard Board (IAASB) for assurance engagements other than audits or review of historical financial information.

34 Ibid.
35 Nilsson, A. (2014, 02 12). The Troublesome History of the Bitcoin Exchange Mt. Gox. Retrieved 06 27, 2015, from https://anders.io/the-troublesome-history-of-the-bitcoin-exchange-mtgox/
36 Southurst, J. (2014, 03 18). With Bifubao's Wallet, Users Can Prove Funds via Cryptography. Retrieved 06 27, 2015, from CoinDesk: http://www.coindesk.com/bifubaos-wallet-users-can-prove-funds-via-cryptography/
37 Shanafelt, S. (2014, 09 22). UK-based gold and bitcoin exchange Netagio passes ISAE 3000 audit. Retrieved 06 27, 2015, from BitcoinX: http://www.bitcoinx.com/uk-based-gold-and-bitcoin-exchange-netagio-passes-isae-3000-audit/

This standard addresses IAASB requirements for the quality of assurance work, report verification, internal compliance, corporate governance, and other areas of corporate responsibility required for special engagements. The procedures performed by BDO sought to first understand the setup of the Bitcoin storage environment, followed by tests over the design and operational effectiveness of Netagio's control objectives as at May 2014[38]. The results of the review were that Netagio had adequate control mechanisms in place that ensured the security of the bitcoins in its possession. Furthermore, BDO found that Negatio's bitcoin, gold and sterling exchange had been designed to meet the highest compliance requirements and standards of other registered financial exchanges. It reported that Netagio was in adherence to the stringent anti-money laundering (AML) rules and customer on-boarding checks required by the European Payment Services Directive, as well as continuous exchange and trade monitoring surveillance.[39] Bitstock, another Bitcoin exchange, has since also obtained an ISAE 3000 certification as well as an opinion from PwC that its customer account balances and accounting records reconcile in all material aspects[40]. Both Netagio and Bitstock have led the way for the industry to achieve compliance with international standards. As was stated by Netagio's CEO Simon Hamblin, "any steps that can be taken to achieve internationally recognized standards will give further credibility to Bitcoin in both financial and retail industries."[41]

Compared to the proof-of-solvency audits commissioned by Bitstamp and Kraken, the ISAE 3000 audit offers customers more assurance beyond the amount of reserves held by the exchange. The proof-of-solvency audits are simply confirmations that the claimed number of bitcoins were controlled by the exchange's set of public addresses, and provided no insight into how much the address or other data were being protected. The ISAE 3000 framework allows customers, particularly financial investors, to understand that the controls of the exchange are functioning to certain standard upheld by the IAASB. Other potential standards that may be applicable to Bitcoin audits in the future are the ISO 27000 series of standards specifically reserved for information security matters, as well as the COBIT 5 framework for governance of enterprise IT.

Due to the increasing number of Bitcoin companies, in conjunction with the increasing demand from customers for these companies to submit themselves to audits, Bitcoin may present itself as a lucrative new market opportunity for audit service providers. Each of these clients would likely require regular audits going forward on a quarterly and annual basis. As the scope of these audits expand, auditors will be required to perform more procedures over the controls and other assets of clients. Should the ISAE 3000 become a competitive standard in the Bitcoin industry, this will represent more work and hours

38 Netagio: The First Bitcoin Exchange To Attain ISEA 3000. (2014, 09 22). Retrieved 06 27, 2015, from cryptocoinsnews: https://www.cryptocoinsnews.com/netagio-the-first-bitcoin-exchange-to-attain-isea-3000/
39 Hajdarbegovic, N. (2014, 09 22). Netagio Becomes First UK Bitcoin Company to Meet Auditing Standard. Retrieved 06 27, 2015, from CoinDesk: http://www.coindesk.com/netagio-becomes-first-uk-bitcoin-company-meet-auditing-standard/
40 Bitstock. (2014). Audit by PricewaterhouseCoopers company. Retrieved 06 27, 2015, from Bitstock: https://www.bitstock.com/en/info/audit
41 Millet, J. (2014, 09 22). Netagio Receives Assurance of Bitcoin Holdings Under ISAE 3000 Standards. Retrieved 06 27, 2015, from NewsBTC Bitcoin News Service: http://www.newsbtc.com/2014/09/22/netagio-receives-assurance-bitcoin-holdings-isae-3000-standards/

required by the auditor. To grab a share of this new market, accounting firms will need to acquaint themselves with Bitcoin technology and the services that it can offer to meet the unique needs of these companies.

8. Bitcoin Regulation

As Bitcoin attracts more and more institutional and overall users, it is not unlikely that it may be brought to the same standards and regulations as banks. The New York State Department of Financial Services have proposed "Bitlicense" regulations requiring licensees to submit audited annual financial statements in the future.[42] If such regulations were to be passed, this would set precedence for other jurisdictions to set equivalent or similar standards. In its current state, regulation of digital currencies is inconsistent across countries. In the U.S., digital currencies are regulated by FinCEN under the Bank Secrecy Act[43]. In the U.K., digital currencies are unregulated but a "Call for Information" has been issued by the Treasury to set the process in motion. Other countries are adopting a "wait-and-see" approach for developing regulation. Some countries, including Russia, have banned the use of digital currencies entirely – while others have heavily restricted the use of digital currencies.

From a user perspective, new tax regulations have recently been implemented in the U.S. by the Internal Revenue Service (IRS) that Bitcoins are to be classified as property for federal income tax services[44]. Therefore, not reporting Bitcoins will now have tax avoidance consequences. The Financial Accounting Standards Board (FASB) has not yet offered any guidance on the classification of Bitcoin for financial reporting purposes.[45] Organizations that hold a balance in bitcoins have a choice of whether or not to hold their bitcoins or to convert them at the time of the audit. This will have implications on the financial reporting disclosures and audit procedures required for that company.

For Bitcoin to become truly universally accepted, there are several key obstacles that it needs to overcome. The first is that it needs to appeal to the average business. While lower transaction costs are a good incentive to use Bitcoin, the average user also needs to trust that the currency will hold its value. Part of this will involve overcoming the media's portrayal of Bitcoin as a make-believe currency, with negative associations to the black market. Bitcoin can repair and build its public goodwill by embracing regulation. Users will see compliance with regulation as a stamp of approval from government authorities that Bitcoin is safe. Regulation of Bitcoin will be necessary to get the average consumer to become onboard with using it. As Bitcoin grows, it will continue to go after bigger markets. This will not be possible without engaging the government, regulators, and banks. In order to go mainstream, Bitcoin will have to

42 Haque, M. (n.d.). Why would a Bitcoin audit be required? Retrieved 06 27, 2015, from MAH Chartered Accountants: http://www.mah.uk.com/bitcoin-audit/
43 BDO. (2015, 02 04). What to Expect from Digital Currencies in 2015. Retrieved 06 27, 2015, from BDO: http://www.bdo.co.uk/talk-shop/what-to-expect-from-digital-currencies-in-2015
44 Feinsmith, S. (2014, 10 22). Bitcoin in the Charitable Sector – Part One: Three Big Questions. Retrieved 06 27, 2015, from BDO Non Profit: http://nonprofitblog.bdo.com/index.php/2014/10/22/bitcoin-in-the-charitable-sector-part-one-three-big-questions/
45 Ibid.

effectively integrate itself into the traditional financial system. It is through regulation that Bitcoin stands its best chance at achieving global recognition as a legitimate currency.

9. Conclusion

The continuing adoption and growth of Bitcoin has led it back to a need for regulation and audits. While decentralization was the very feature that made Bitcoin unique, an increasing portion of users are now demanding that some regulation be applied to Bitcoin to prevent a repeat failure of Mt. Gox. This call for increased regulation and audits of Bitcoin companies has presented itself as a considerable opportunity for audit service providers. As user confidence in Bitcoin increases with regulation, more growth opportunities will be available to the Bitcoin industry as a universally recognized new form of currency.

References

BDO. (2015, 02 04). *What to Expect from Digital Currencies in 2015*. Retrieved 06 27, 2015, from BDO: http://www.bdo.co.uk/talk-shop/what-to-expect-from-digital-currencies-in-2015

BDO LLP. (2014, 10 20). *What Investors Should Know About Bitcoin*. Retrieved 06 27, 2015, from http://www.bdoblog.com/techandmediawatch/Pages/What-investors-should-know-about-Bitcoin.aspx

Bensinger, G. (2015, 01 25). *First U.S. Bitcoin Exchange Set to Open*. Retrieved 06 27, 2015, from The Wall Street Journal: http://www.wsj.com/articles/first-u-s-bitcoin-exchange-set-to-open-1422221641

BitStock. (2014). *Audit by PricewaterhouseCoopers company*. Retrieved 06 27, 2015, from BitStock: https://www.bitstock.com/en/info/audit

Bradbury, D. (2014, 05 02). *What Really Happens Inside a Bitcoin Audit*. Retrieved 06 27, 2015, from CoinDesk: http://www.coindesk.com/what-happens-inside-bitcoin-audit/

Bradbury, D. (2014, 05 06). *Why Bitcoin Exchange Audits Don't Go Far Enough*. Retrieved 06 27, 2015, from CoinDesk: http://www.coindesk.com/exchanges-must-still-prove-themselves-customers/

Brown, A. (2015). *Bitcoin Thefts.* Retrieved 06 27, 2015, from https://bitcointhefts.com/

CoinDesk. (2014, 02 20). *Why Use Bitcoin?* Retrieved 06 27, 2015, from CoinDesk: http://www.coindesk.com/information/why-use-bitcoin/

CoinDesk. (2015, 06 27). *Bitcoin Price Index*. Retrieved 06 27, 2015, from CoinDesk: http://www.coindesk.com/price/

CoinDesk. (2015, 03 20). *How to Sell Bitcoin*. Retrieved 27 2015, 06, from CoinDesk: http://www.coindesk.com/information/sell-bitcoin/

CoinDesk. (2015, 02 17). *What Can You Buy with Bitcoin?* Retrieved 06 27, 2015, from CoinDesk: http://www.coindesk.com/information/what-can-you-buy-with-bitcoins/

Davis, J. *The Crypto-Currency: Bitcoin and Its Mysterious Inventor*. Retrieved 06 27, 2015 from The New Yorker: http://www.newyorker.com/magazine/2011/10/10/the-crypto-currency

Deloitte. (n.d.). *Bitcoin 101: Back to Basics*. Retrieved 06 27, 2015, from Deloitte: http://www2.deloitte.com/nz/en/pages/forensic-focus/articles/bitcoin-101-back-to-basics.html

Discoll, S. (2013, 07 14). *How Bitcoin Works Under the Hood*. Retrieved 06 27, 2015, from http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

Driscoll, S. (2014, 09 26). *The Essence of How Bitcoin Works (Non-technical)*. Retrieved 06 27, 2015, from http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

Feinsmith, S. (2014, 10 22). *Bitcoin in the Charitable Sector – Part One: Three Big Questions*. Retrieved 06 27, 2015, from BDO Non Profit: http://nonprofitblog.bdo.com/index.php/2014/10/22/bitcoin-in-the-charitable-sector-part-one-three-big-questions/

Firestartr.co. (2014, 03 06). *Letter for Bitstamp*. Retrieved 06 27, 2015, from https://www.bitstamp.net/s/documents/Firestartr_DD_Letter_for_Bitstamp.pdf

Graillot, F. (2015, 05 25). *Bitcoin Might Be The Next Big Thing In The Remittance Market*. Retrieved 06 27, 2015, from Techcrunch: http://techcrunch.com/2015/05/25/bitcoin-might-be-the-next-big-thing-in-the-remittance-market/

Hajdarbegovic, N. (2014, 09 22). *Netagio Becomes First UK Bitcoin Company to Meet Auditing Standard*. Retrieved 06 27, 2015, from CoinDesk: http://www.coindesk.com/netagio-becomes-first-uk-bitcoin-company-meet-auditing-standard/

Haque, M. (n.d.). *Why would a Bitcoin audit be required?* Retrieved 06 27, 2015, from MAH Chartered Accountants: http://www.mah.uk.com/bitcoin-audit/

KPMG. (n.d.). *Cutting through concepts: virtual currencies get real* . Retrieved 06 27, 2015, from KPMG: http://www.kpmg.com/global/en/issuesandinsights/articlespublications/frontiers-in-finance/pages/virtual-currencies-get-real-fs.aspx

Kraken. (2014). *Kraken Proof-of-Reserves Audit Process*. Retrieved 06 27, 2015, from https://www.kraken.com/security/audit

McMillan, R. (2014, 03 03). *The Inside Story of Mt. Gox's $460 Million Disaster*. Retrieved 06 27, 2015, from Wired: http://www.wired.com/2014/03/bitcoin-exchange/

Millet, J. (2014, 09 22). *Netagio Receives Assurance of Bitcoin Holdings Under ISAE 3000 Standards*. Retrieved 06 27, 2015, from NewsBTC Bitcoin News Service: http://www.newsbtc.com/2014/09/22/netagio-receives-assurance-bitcoin-holdings-isae-3000-standards/

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved 06 27, 2015, from https://bitcoin.org/bitcoin.pdf

Netagio: The First Bitcoin Exchange To Attain ISEA 3000. (2014, 09 22). Retrieved 06 27, 2015, from cryptocoinsnews: https://www.cryptocoinsnews.com/netagio-the-first-bitcoin-exchange-to-attain-isea-3000/

Nilsson, A. (2014, 02 12). *The Troublesome History of the Bitcoin Exchange Mt. Gox*. Retrieved 06 27, 2015, from https://anders.io/the-troublesome-history-of-the-bitcoin-exchange-mtgox/

PwC. (2014, 02 07). *Digital Disruptor: How Bitcoin is Driving Digital Innovation in Entertainment, Media, and Communications*. Retrieved 06 27, 2015, from http://www.pwc.com/en_SG/sg/tmt/assets/tmtnews201402/digital_disruptor.pdf

Rizzo, P. (2014, 03 06). *Bitstamp Audit Proves it was Behind $147 Million Mystery Bitcoin Wallet*. Retrieved 06 27, 2015, from CoinDesk: http://www.coindesk.com/bitstamp-audit-proves-behind-147m-mystery-bitcoin-wallet/

Shanafelt, S. (2014, 09 22). *UK-based gold and bitcoin exchange Netagio passes ISAE 3000 audit*. Retrieved 06 27, 2015, from BitcoinX: http://www.bitcoinx.com/uk-based-gold-and-bitcoin-exchange-netagio-passes-isae-3000-audit/

Southurst, J. (2014, 03 18). *With Bifubao's Wallet, Users Can Prove Funds via Cryptography*. Retrieved 06 27, 2015, from CoinDesk: http://www.coindesk.com/bifubaos-wallet-users-can-prove-funds-via-cryptography/

Southurst, J. (2015, 04 29). *Most Mt Gox Bitcoins Were Gone by May 2013, Report Claims*. Retrieved 06 27, 2015, from CoinDesk: http://www.coindesk.com/most-mt-gox-bitcoins-were-gone-by-may-2013-report-claims/

Vigna, P. (2014, 02 25). *5 Things about Mt. Gox's crisis.* Retrieved 06 27, 2015, from the Wall Street Journal: http://blogs.wsj.com/briefly/2014/02/25/5-things-about-mt-goxs-crisis/

Wong, J. I. (2014, 02 04). *Poll: Are you having Mt. Gox Withdrawal Issues?* Retrieved 06 27, 2015, from CoinDesk: http://www.coindesk.com/poll-mt-gox-withdrawal-issues/