Journal of International Technology and Information Management

Volume 24 | Issue 3 Article 2

2015

The State of Cryptocurrencies, Their Issues and Policy Interactions

Ramesh Subramanian
Quinnipiac University

Theo Chino

The State of Cryptocurrencies, Their Issues and Policy Interactions

Ramesh Subramanian
Quinnipiac University
USA

Theo Chino
Bitcoin Entrepreneur
New York, NY
USA

ABSTRACT

This paper focuses on the evolution of cryptocurrencies. It traces the history of early cryptography, the 'cypherpunk' movement, and how the work of some cyber libertarians and cryptographers enabled the emergence of popular cryptocurrencies. The paper then focuses on Bitcoin. It delves into the technology behind the Bitcoin architecture and shows how exactly this technology works. The paper then does an analysis of security and regulatory considerations that affect the growth of Bitcoin-based businesses. The paper concludes with some suggestions for future work in the area.

Keywords: cryptocurrency, cryptography, Bitcoin, security, IT policy, regulation.

INTRODUCTION

The concept of a completely anonymous and untraceable "digital cash" has existed for over two decades. In this paper we trace the evolution of cryptocurrencies, primarily focusing on Bitcoin. We then consider some of the security considerations that have been brought to the fore by cryptocurrencies. Cryptocurrencies have also come under scrutiny by governmental agencies as they can, and have enabled nefarious activities to take place by successfully hiding those transactions from the law. Given the increasing acceptance of Bitcoin, we then consider some of the policy issues and attempts that have been made to regulate cryptocurrencies. We discuss the implications of such policies, both negative and positive. We then conclude by discussing the future of cryptocurrencies, the challenges and issues and possible remedies.

Background: Early work on cryptography

As noted by William E. Burr, until the early 1970s, there was little commercial or academic expertise in cryptography (Burr, 2001). Cryptography and encryption were generally the preserve of defense establishments such as the military and the espionage agencies. Public awareness of cryptography in the US came with the publication of the Digital Encryption Standard (DES) on March 17, 1975 in the *Federal Register* (Leech & Chinworth, 2001). The origins of DES can be traced to 1971, when IBM researcher Horst Feistel, working on a project codenamed *Project Lucifer,* filed a patent application for a 48-bit block cipher cryptographic system (also known as the Lucifer cipher) (Feistel, 1974). The project was commissioned by Lloyds Bank for encrypting ATM transactions. In 1972, the National Bureau of Standards (NBS) identified the need for an

  ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

encryption standard for encrypting unclassified but sensitive government documents, and in May 1973, solicited proposal for such a system. The NBS then chose, with the approval of the National Security Agency (NSA), a modified version of IBM's algorithm (IBM, 2012). The original algorithm was strengthened to a 56-bit block cipher by a team led by Walter Tuchman and aided by Carl Meyer (Bamford, 1982). Other members of the team were Don Coppersmith, Alan Konheim, Roy Adler, Edna Grossman, Bill Notz, Lynn Smith and Bryant Tuckerman. On January 15, 1977, DES was adopted as a standard for unclassified government documents.

The publication of DES did led to many discussions and debates in the academic community and civil society. Some academics such as Martin Hellman and Whitfield Diffie at Stanford University felt that the original 56-bit block cipher was altered by IBM at NSA's behest to provide that NSA a backdoor into the cryptographic system. They also felt that the 56-bit cipher was not secure enough and could be broken with appropriate computing power – presumably available to the NSA, again enabling it to capture and decrypt messages (Blight, 2013). The controversy made the DES standard one of the most scrutinized cryptographic systems. Diffie and Hellman conducted a comprehensive analysis of the DES in 1977 (W. Diffie & Hellman, 1977). However, DES became very popular and was soon adopted internationally as the encryption standard. This period also saw further developments in cryptographic systems. In 1976 Ralph Merkle developed a paradigm based on the concept of a "puzzle" to accomplish secure communications over insecure channels (Merkle, 1978), and at around the same time, Diffie and Hellman proposed a system they called "Public Key Cryptography" and thus developed public key encryption (Whitfield Diffie & Hellman, 1976).

The early controversy pertaining to DES serves to illustrate the sense of unease that the academic community and civil society had over the possibility of its misuse by the government to surveil citizens. This unease led some people to conceptualize the development of anonymous means of communications and anonymous methods of financial transactions. Developments in this sphere also occurred in conjunction with developments in networked computing in the 1970s and 1980s, the advent of the Web in 1991 and the ensuing surge in web-based commerce. Along with this came the realization that a person's online activities could be easily tracked by various entities (Narayanan, 2013a). This gave impetus to the emergence of cryptocurrencies – digital currencies whose movements could not be tracked easily (Narayanan, 2013a). Interest in creating alternate exchanges that are anonymous, fast, allowed direct peer-to-peer transactions without any intermediary grew. An autonomous digital currency that is not connected to any government or other intermediary such as a bank is appealing because of the anonymity and liberty that it affords. Transfer of money across geographic regions both domestic and international can be easily and quickly accomplished without worrying about governmental regulations.

These ideas coalesced into the *Cypherpunk* movement that "formally" emerged in the early 1990s. The cypherpunk movement (not to be confused with the *cyberpunk* movement) is an activist movement whose participants seek to engineer social and political change and subvert the status-quo by enhancing security and privacy through cryptographic techniques. The founders of the cypherpunk group were Eric Hughes, a UC Berkeley mathematician, Timothy C. May, a former chief scientist at Intel, and John Gilmore, one of the early employees (the fifth employee) at Sun

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

Microsystems and founder of Cygnus Support as well as the Electronic Frontier Foundation. All three were wealthy, and shared a strong libertarian streak. The group started with a meeting in 1992 in the Bay area of San Francisco. They started the cypherpunk mailing list in 1992 and within two years, the mailing list garnered over 600 subscribers.

An important technology enabler to this movement is David Chaum, a cryptologist who got his doctoral degree from the University of California Berkeley. As a doctoral student in the 1980s, Chaum explored several concepts and developed several methods focusing on anonymous communication and anonymous financial transactions. In 1981 Chaum published the article "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms" which described a method, using public key cryptography, to hide the identity of a participant in an email communication, as well as the contents themselves. He explained one of its uses - in elections where an examiner could verify that all the ballots have been correctly counted without revealing the identity of the voters (Chaum, 1981). His 1982 doctoral dissertation titled "Computer Systems Established, Maintained and Trusted by Mutually Suspicious Groups" (Chaum, 1982) and his 1983 paper on "Blind signatures for untraceable payments" (Chaum, 1983) laid the foundations for the creation of an anonymous currency. As early as 1985 he stated that "Computerization is robbing individuals of the ability to monitor and control the ways information about them is used. As organizations in both the private and the public sectors routinely exchange such information, individuals have no way of knowing if the information is inaccurate, obsolete, or otherwise inappropriate." He proposed an approach using which surveillance of electronic transactions could be rendered "obsolete (Chaum, 1985)." Chaum went on to create a digital currency based on cryptography that he called E-Cash, and in 1990 founded a company called DigiCash, an electronic money corporation. The world's first electronic cash payment took place in May 1, 1994. However, most attempts at creating a workable cryptocurrency have failed to gain consumer acceptance. DigiCash filed for Chapter 11 bankruptcy on November 4, 1998. Since then, several new attempts have been made to create digital cryptocurrencies. Examples are Peppercoin – a company founded by Ronald Rivest and Silvio Micali that uses a cryptographic system for processing micropayments (Micali & Rivest, 2002); the NetBill, another system for micropayments for information goods from researchers at Carnegie Mellon University (Cox, Tygar, & Sirbu, 1995); Wai Dai's B-Money which was a precursor to Bitcoin (Vigna & Casey, 2015, page 319, Note 51) and Nick Szabo's Bit Gold (Szabo, 2008).

Despite this renewed activity, by 2013, many analysts had written off any future for these types of currencies. Arvind Narayanan and Jonathan Zittrain separately note the following points that make cryptocurrencies unusable in the long run (Narayanan, 2013a; Narayanan, 2013b; Zittrain, 2012):

1. They are extremely complicated for the common person to understand and use – the lay user may not have the technological familiarity to download and operate the necessary software and implement the necessary security measures required for cryptocurrencies.

2. Maintaining absolute privacy may not work economically in a world where collecting, aggregating and selectively disseminating personal data is a technique used by almost

all businesses – many businesses are able to provide "free" services to users only because they can collect, categorize and sell users' information to advertisers or other aggregators.

3. The concept of trust without any government to back it might be unpalatable to many people – the lay person still accepts the authority of the government and the government's guarantee on currency.

4. Many existing laws and legal restrictions such as the Digital Millennium Copyright Act (DMCA) will undermine such digital currencies – some of the proposed currencies could be stopped if they are found to violate the copyrights of other software.

BITCOIN

One cryptographic currency that has nevertheless gained non-trivial acceptance is Bitcoin, announced in 2008 by its mysterious developer, Satoshi Nakamoto. The name, however, is widely considered to be a pseudonym, and the real identity of the inventor of Bitcoin continues to remain a mystery seven years after it was announced. Over the last six years, Bitcoin has emerged as the most successful cryptographic currency in history. In just two years after its quiet launch, Bitcoin grew to comprise several billions of dollars of economic value (Bonneau et al., 2015). At the time of writing this, over 14 million Bitcoins are in circulation. Each Bitcoin has a market price of around US $ 241.44. During the 24-hour period between June 25 and June 26, 2015 the estimated transaction volume of Bitcoins was US $ 50,780,376.25 (blockchain.info, 2015). Indeed, the growing success of Bitcoin has caused further interest in identifying the real Bitcoin inventor – spurring a small army of researchers and journalists (Davis, 2011). Many academic researchers have also started studying the inner workings of Bitcoin.

Introduction to the workings of Bitcoin

The outlines of Bitcoin's specifications were posted by Nakamoto in the *Cryptography Mailing List* on November 1, 2008 (Nakamoto, 2008b). The details of how exactly Bitcoin works are difficult to comprehend from the posting or from Nakamoto's original paper describing Bitcoin (Nakamoto, 2008a). The following description of the inner workings of Bitcoin therefore draws from a variety of sources, including the original Nakamoto paper. There are three fundamental constructs associated with Bitcoin: *Transactions*, the *block-chain*, and the *peer-to-peer network*.

Transactions

Basically, Bitcoin can be considered to be a sequence of transactions rather than a single digital object such as a file. Each transaction consists of one or more inputs and outputs: Each transaction is used to transfer a certain number of units of Bitcoin currency directly from one entity to another, say, Alice to Bob. Bitcoin units come into a designated address (say, representing Alice), and these units can then be transferred to another address (representing Bob) in part or whole. A Bitcoin *address* can be created using a Bitcoin client software, also known as a Bitcoin wallet. There are

  ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

currently many Bitcoin wallets that one can choose from. The Bitcoin client generates the public and private keys for a user. The public key is the user's, say Alice's address. The private key is used by Alice to sign a transaction and transfer some Bitcoin units to Bob (using Bob's public key).

Bitcoin units are called '*satoshis'*, and there are 10^8 *satoshis* in one Bitcoin, which is commonly denoted as BTC. Thus very small units of the currency can be transferred between Alice and Bob. Obviously, if Alice wants to transfer Bitcoin units to Bob, Alice needs to know the Bitcoin address of Bob (i.e. Bob's public key). Alice should also include as part of the transaction her own Bitcoin address, so that Bob can verify that it was indeed Alice who made the transfer, and that Alice was entitled to make such a transfer (i.e. Alice legitimately owned the Bitcoin units that were transferred – which means that Alice previously legitimately received the Bitcoin units earlier though another transaction). This record of Alice's receipt of the currency on some past date is included in the transfer transaction to Bob. This record is also available in a *block-chain* of transactions. The block-chain consists of all verified transactions and is a "general ledger" of sorts. Thus, Bob can verify the authenticity of Alice's Bitcoins which she is transferring to his address. (Construction of the *Bitcoin block-chain* is explained below under "Bitcoin Mining.")

Once Bob receives the transfer and makes the appropriate verifications (that Alice was entitled to send the Bitcoin units), Bob can transfer part of or the whole currency amount to another entity (say, Charlie) using the same process as above. Bob's transfer to Charlie will include proof that he legitimately received the Bitcoin units from Alice, and also the proof that Alice legitimately received her Bitcoin units form another person. Thus, a complete chain of transactions is passed from person to person along with each transaction. The veracity of the chain of transactions is verified by the Bitcoin *P2P network.*

P2P network

Once Alice transfers some funds to Bob, Bob has to wait until the transaction is verified and adjudged to be correct, and then successfully added into a *block-chain.* This process is known as *mining* (explained in detail in the next section). The actual transfer from Alice to Bob takes place through the Bitcoin peer-to-peer network. When Alice creates a transaction - i.e. to transfer some funds to Bob, she propagates the transaction into the P2P network. Alice does this by connecting to another node on the P2P network and making a simple transfer of the transaction data. It is assumed that Bob is also part of this P2P network. The transaction eventually propagates to Bob. But before Bob can begin using the transferred funds, the transaction itself has to be verified for legitimacy. The actual process of verification is accomplished though a complex process using public key cryptography, hashing, digital signing and code scripts which do the necessary checks to verify that each transaction is legitimate, and that there is no duplicate transaction using the same Bitcoin. The verification is done by certain members of the P2P network who are Bitcoin miners, who get compensated for their efforts. After the verification, the transaction is grouped with other verified transactions and the group is posted on an open ledger. Once a transaction appears on the ledger, that confirms that the transaction is legitimate and not duplicated (i.e. that the same Bitcoin unit is not used to buy two different items by the same owner). Once the

transaction is added to the ledger it can be seen by everybody on the P2P network, and now the recipient Bob can use his Bitcoin units to create new transactions.

Bitcoin mining

A Bitcoin miner has two roles: (1) Examine each transaction and makes sure that it meets certain conditions or rules; (2) To group a set of transactions and create a block-chain of the transactions. Examples of the conditions for (1) are: "Is the syntax correct?" "Are the input and output lists non-empty?" "Are the sum of input values greater than the sum of output values?" etc. A list of rules for a successful transaction is given in the *Protocol Rules* (en.bitcoin.it, 2014). The miner then appends this transaction to with other transactions to form a block-chain, as noted in (2). The process of creating an acceptable block-chain is purposely designed to be complicated and competitive. It is designed to ensure that a lot of computing power (also known as *proof-of-work*) is expended to achieve an acceptable block-chain. The process is as follows: First a block is created. The block contains the hash of the previous (accepted) block in the block-chain; a hash of a bunch of transactions to be added to the block-chain, called the *Merkle Root;* a *nonce* (a random seed). A new hash (using the double SHA-256 hash function) is created. Please see Appendix A for a diagram of a block. A successful hash is one that is smaller than a *target hash.* The target is continuously varied so that the difficulty of achieving the result – a hash that is smaller than the target always remains high and thus requires substantial computing power. (An example of a target hash could be one where the leading zeros in the hash is at least thirteen in number.) The target hash is calibrated continuously and dynamically so that a new block-chain is successfully created about ten minutes after a transaction is released into the P2P network, and that all the miners have the same (long) odds of computing a successful hash. If a resulting hash is unsuccessful, the computation is repeated with a new nonce. Once a miner achieves a successful hash, the result is easily verified by other miners. In this process, there is always the possibility that a miner may include a transaction that is not valid. If that happens, then the other nodes are able to notice that, and invalidate the miner's claim. The successful miner gets a reward of 25 Bitcoins (at present). In addition, the miner is also awarded a small number of Bitcoin units for every transaction successfully processed and verified.

This completes our description of how the Bitcoin currency works, and how Bitcoins are mined. We now move to the interpretive and analytic part of the paper. Our focus turns to the current state of cryptocurrencies, issues and challenges.

Analysis

In the world of cryptocurrencies, Bitcoin holds a lot of promise. An important point to note is that Bitcoin is an open-source project. Its code is available for anyone to tinker with, and is posted on the open-source online community, GitHub. There are currently five core developers in the Bitcoin project: Gavin Andresen, Jeff Garzik, Mike Hearn, Matt Corallo, and Pieter Wiuelle. Andresen is considered to be the "Linus Torvalds" of Bitcoin, the unofficial leader. There is an official mailing list and an IRC chat that are used for communication among themselves and the worldwide Bitcoin community (Liu, 2013b).

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

BITCOIN STRENGTHS

Hedge against economic downturn

As can be seen from the above discussion, the concepts behind Bitcoin operation and mining are very complex and not very easy to grasp. But it is truly a triumph of cryptography and its application to the world of finance and banking. The fact that it has survived major challenges, technical as well as political, and continues to grow in acceptance, show that cryptography has not failed, as asserted by Narayanan et al (Narayanan, 2013a,b). In fact, over the years, Bitcoin has been boosted as a hedge against government issued currencies in tough financial times. For instance, Bitcoin came to the forefront during the 2012-2013 financial crisis in Cyprus. The crisis itself was a result of a domino effect stemming from the sub-prime mortgage crisis in the US in 2007-2008, which resulted in negative consequences in the EU. The economy of Cyprus went into recession in 2009. Cyprus's economy was largely supported by the tourism industry and offshore banking, but bad loans caused severe financial pressure on the banks. Facing financial collapse, the government of Cyprus announced a plan that would allow it to directly withdraw money from the citizens' savings accounts. This led to an upsurge in Cypriot as well as Spanish citizens buying Bitcoin as a hedge against government actions (Liu, 2013a).

BITCOIN WEAKNESSES

Security Issues

Bitcoin currency has also been used for nefarious purposes. In October, 2013, the FBI announced that it had seized a collection of 144,000 Bitcoins, worth $ 28.5 million from Ross Ulbricht, who ran an underground web site called "The Silk Road" and operated under the pseudonym "Dread Pirate Roberts". The Silk Road was a popular drug-selling site which dealt only with Bitcoins (Greenberg, 2013).

This action suddenly brought the attention of the US Congress to the potentials for misuse of the virtual currency by criminals. The FBI saw Bitcoin as a "haven for money-laundering and other criminal activity – including as a tool for hackers to rip off fellow Bitcoin users (Zetter, 2012)." Analysts have recently suggested that the terror organizations are increasingly beginning to see the potential of Bitcoin in funding their activities (Higgins, 2014).

BITCOIN THREATS

Hacking Bitcoins

One particular threat to Bitcoin owners is that Bitcoins, despite the security they offer, can still be stolen by hackers. This can happen if the virtual locations used for storing Bitcoins become compromised, and some private keys of users are stolen. While the process of stealing Bitcoins requires strong technical skills, it is not immune from hacking. Another potential threat to Bitcoins is the possibility of a *denial of service* attack. This can be done by a defect or bug called *"Transaction Malleability* (Felten, 2104)." Ritchie King notes that a transaction that is being routed to the P2P network (to be validated and mined by the miners) can be hacked in a minor way so that the hash is changed just a little. This is because the major contents such as the inputs, etc. are not changed. This results in a change in the hash value in some transactions, which is tracked

by the miners, who then proceed to reject the transaction due to the bad hash. That transaction thus never gets processed, and is "lost," thus simulating a denial of service attack (King, 2014).

Another threat that is beginning to worry Bitcoin proponents is the way in which Bitcoin is mined. The currency was developed in such a manner as to make mining a completely democratic process where anybody with a suitable computer and appropriate hardware could mine for Bitcoins. However, increasingly, large operators with enormous computing infrastructure at their disposal are beginning to capture the mining market. In such a scenario, it is possible the Bitcoin mining could become the hegemony of just a few operators, or worse, a single miner could control 51% of the Bitcoin mining activity. This is known as the "*51% Attack* (Cowrey, 2014)." If that happens, then that miner could use this majority power to validate or invalidate select transactions and control the availability of Bitcoins in the market.

BITCOIN OPPORTUNITIES

Bitcoin Acceptance

Despite the negative aspects discussed above, Bitcoin acceptance and usage continue to grow. The European Union recently recognized it as a currency. It's value has been stable, at around $250, for much of this year (The Economist, 2015). The market capitalization of Bitcoin at the time of this writing is USD 6.8 billion (coinmarketcap.com, nd). Many large companies now accept Bitcoins, albeit through a Bitcoin exchange, such as Coinbase and Bitpay and (Davidson, 2015). The customer's Bitcoin payment to a vendor is converted into dollars (or other appropriate currency) by the exchange, and transferred to the vendor's bank account. Over time, if the Bitcoin's value stops fluctuating wildly as it does at present, large companies may actually accept Bitcoin directly without a third party.

At the present time, Bitcoin seems to offer the most convenience to small businesses and stores, where Bitcoin could be conveniently used for micropayments. Kariappa notes that the block-chain protocol can be used to instantly transfer funds however small the size of the funds. One company, ChangeCoin, uses this protocol to create a micropayment infrastructure for the Web. Another innovation is "smart contracts," which also uses the block-chain protocol. According to Kariappa, smart contracts are programs that encode certain conditions in transactions. "When a transaction between 2 parties occurs, the program can verify if the product/service has been sent by the supplier. Only after verification is the sum transmitted to the supplier's account (Bheemaiah, 2015)."

In addition to its use as a micropayment mechanism, the concept of the block-chain and proof-of-work in the process of Bitcoin mining has given rise to many possible adaptations and uses. For instance, the proof-of-work idea (called *hashcash)* has been suggested as a means to prevent junk mail propagation and traffic (Bitcoin wiki, 2015). Simply stated, every email sent could be required to show a proof-of-work, using some of the same techniques used in Bitcoin mining. The particular work could be calibrated so that very little computing power is expended for simple person-to-person emails, whereas the 'work required' would increase as bulk mailings are generated. This would require bulk mailers to expend much more computing power, and thus act as a deterrent. This idea looks promising, and more empirical work has to be done to prove its usefulness in preventing email spam.

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

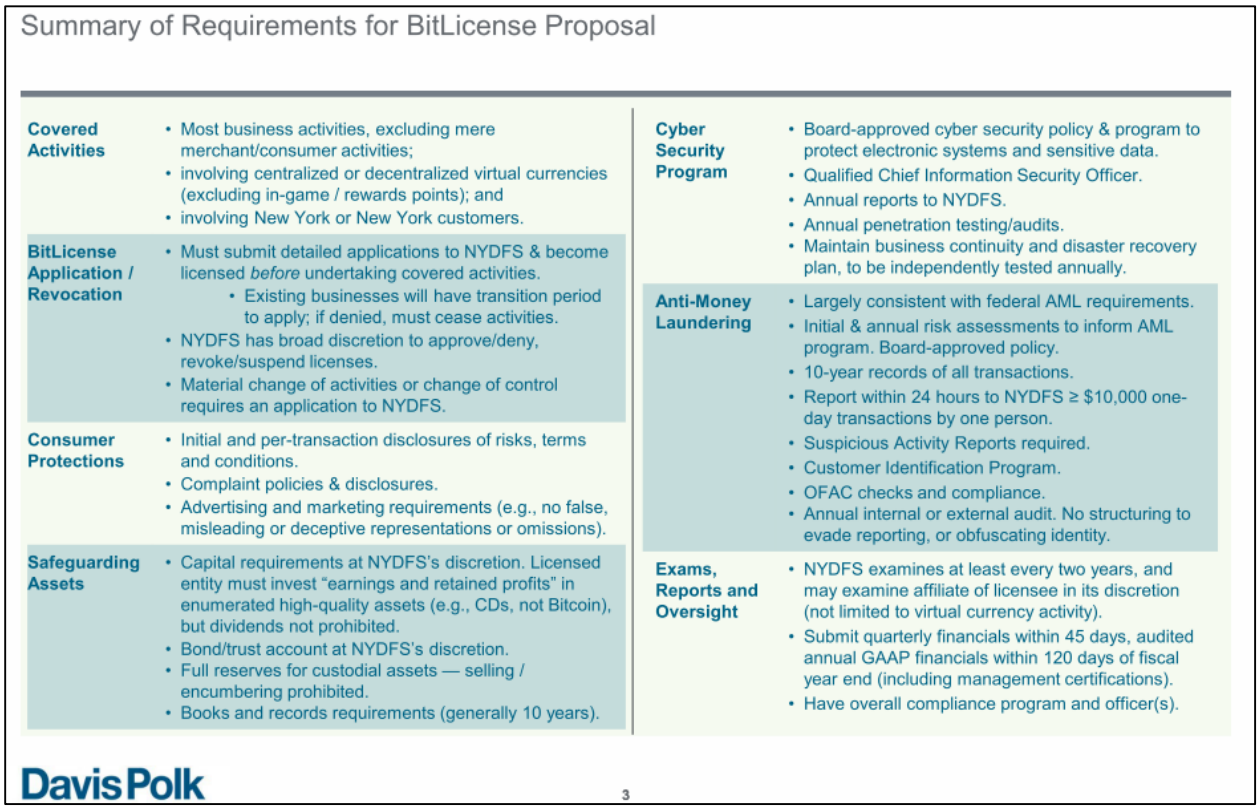
The block-chain concept could also be used for building fool-proof databases and trusted registries, such as land registries, art registries, etc. Thus, there would not be any need for notaries to vouch for their authenticity. As noted in a recent article in *The Economist*, twenty-five banks have recently join joined a block-chain startup, called R3 CEV, to develop common standards, and NASDAQ is on the verge of using block-chain technology to record trading in securities of private companies (The Economist, 2015).

Enter the Regulators

Over the last few years, numerous companies have sprung up that offer services as Bitcoin (or other cryptocurrency) exchanges. They also offer innovative new applications of the block-chain protocol for micro-payments as well as for transfer of value in a variety of applications. The rising popularity of cryptocurrencies has led to increased attention from lawmakers and regulators both at the national and state level in the US. The regulators are interested in protecting the interests of consumers who use cryptocurrencies, as well as preventing its use by criminals and terrorists.

On July, 2014, the New York Department of Financial Services released a draft of a proposed "BitLicense" that would regulate Bitcoin exchanges. A summary of the requirements published by Davis Polk is posted below in Figure 1.

Figure 1. Summary of Requirements for BitLicense Proposal.



(from (Polk, 2014a))

As can be seen, the NYDFS proposal covered several areas pertaining to the Bitcoin business. However, many Bitcoin businesses objected or complained about the proposal's over-reach. Davis Polk listed many of those complaints in (Polk, 2014b): The Electronic Frontier Foundation (EFF) predictably expressed concerns that the proposed rules would have a chilling effect on speech, and could "chill the associational and expressive activities of digital currency protocols, which can be considered speech." The Clearing House Association was worried that excessive regulation could add fresh burden to the already (in its opinion) over-regulated banking industry. The New York State Society of Certified Public Accounts (NYSSCPA) also raised concerns, particularly on the financial statement disclosure requirements of the BitLicense Proposal. It was felt that the main advantage of Bitcoin, i.e. anonymity, could be lost with over-regulation. Details of these complaints and concerns can be found in full in Polk, 2014b.

The complaints and feedback resulted in publication of revisions to the proposal in February 2015. In April, leaders from many Bitcoin firms, advocacy groups, representatives from academia and investment companies met in New York to discuss the proposal and express their concerns. Some of the reactions and comments during this meeting was reported in the Wall Street Journal by Michael Casey. Fred Ehrsam, a co-founder of the Bitcoin exchange Coinbase noted that Bitcoin companies were actually trying to fight for the rights of companies in the sector that didn't even exists, arguing that only if companies were allowed to innovate without any restriction, would the whole industry benefit. He indicated that the proposed licensing processes would cost the company $2 million to implement, and this could be a large barrier to entry for many small companies.

In a similar vein, the MIT Digital Currency Initiative Director Brian Forde noted in a blog posting that the NYDFS proposal had four critical flaws (from (Forde, 2015)):

1. ***Companies may** not **be allowed to ship new updates or security features to the residents of New York until NYDFS approves it.*** Forde argued that this would greatly slow down the process of rolling out innovations to the consumers, and make NY State "the Bitcoin backwater of the US."

2. ***Companies require NYDFS approval to raise a round of financing if any new investor provides an investment for more than 10 percent of the company.*** Forde argued that if this proposal was followed by other states, the companies would require approvals from 50 states in order to secure working capital.

3. ***The BitLicense proposal requires companies to get both a money transmitter license and a BitLicense—even though they have substantial overlapping requirements.*** Forde notes that this amounts to a regulatory double dip - if this is replicated in all 50 states, entrepreneurs would be required to get 100 licenses to start their company.

4. ***The proposal seeks to go after the developers of open*-source *Bitcoin wallets and regulate the wallet software in order to catch and punish money launderers.*** Forde argues that just as in the case of the Internet, the regulators should go after the ISPs rather than the developers.

  ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

On June 3, 2015, New York issued its final BitLicense framework. The reactions were immediate, and equally divided. Some earlier critics seemed satisfied with the changes added into the new framework, whereas many others saw no significant changes at all. At present, many Bitcoin community representatives are actively lobbying Congress to make further changes to the BitLicense framework – to relax the conditions further, so as to encourage more small operators to enter the Bitcoin arena.

CONCLUSION

In this paper we have attempted to discuss developments in the area of cryptocurrencies by focusing on Bitcoin. We have discussed various technical, financial and security considerations of cryptocurrencies in general and Bitcoin in particular. In the final section we have discussed policy considerations and regulations that are creeping into the hitherto fore unregulated cryptocurrency arena. Cryptocurrencies have been an interesting and profound development that has successfully tied concepts in cryptography to finance and banking. They hold tremendous prospects for peer-to-peer value transfer (and not necessarily just US dollars). The block-chain protocol can be adapted to include new and innovative applications aimed not just at big companies and big transactions, but also at very small businesses which typically deal with micropayments and small transactions. As in any new technical innovation, the regulators have woken up to the opportunities and threats associated with cryptocurrencies and New York State has become the first to propose and issue regulations to Bitcoin exchanges. While regulation is unavoidable, especially due to security considerations, the best innovations have always happened under lessor regulatory strictures. The regulatory bodies should use an enlightened approach in order to grow and nurture this new frontier in business and finance. Just as the Internet and the Web enjoyed a long period of almost no regulation, it would be beneficial if regulations were kept to a minimum, in order to allow innovations to flourish in this area. Future research could focus on innovative applications of the block-chain protocol, as well as newer approaches to cryptocurrencies that aims to eliminate some of the challenges presented by the Bitcoin protocol. Critical areas that should be addressed are: How to balance the need for innovation while safe-guarding the interest of the common citizen? (Should there be an independent insurance agency similar to the FDIC? How will this work?) How to reduce or eliminate criminal uses of the Bitcoin and block-chain protocol? This is just a short list of the directions that future research could take. It is clear that as Bitcoin grows, there is an increased need for more technologists, innovators as well as policy professionals to involve themselves more in crypto-currency and block-chain technology research and applications.

REFERENCES

Bamford, J. (1982). The Puzzle Palace: Inside the National Security Agency, America's Most Secret Intelligence Organization. Penguin.

Bheemaiah, K. (2015, January). Block-chain 2.0: The Renaissance of Money | WIRED. Retrieved July 1, 2015, from http://www.wired.com/2015/01/block-chain-2-0/

Bitcoin wiki. (2015, August 26). Proof of work - Bitcoin Wiki. Retrieved December 18, 2015, from https://en.bitcoin.it/wiki/Proof_of_work

Blight, P. (2013, September 6). The NSA's work to make crypto worse and better | Ars Technica. Retrieved June 20, 2015, from http://arstechnica.com/security/2013/09/the-nsas-work-to-make-crypto-worse-and-better/

blockchain.info. (2015, June 26). Bitcoin Statistics - Blockchain.info. Retrieved June 26, 2015, from https://blockchain.info/stats

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. Retrieved from http://www.ieee-security.org/TC/SP2015/papers-archived/6949a104.pdf

Burr, W. E. (2001). Data Encryption Standard. In A Century of Excellence in Measurements, Standards and Technology - A Chronicle of Selected NBS/NIST Publications 1901-2000 (pp. 250–253). NIST. Retrieved from https://books.google.com/books?id=5AdRAAAAMAAJ&pg=PA250&lpg=PA250&dq=%22In+1972,+the+NBS+Institute+for+Computer+Sciences+and+Technology+%28ICST%29+initiated+a+project+in+computer+security,+a+subject+then+in+its+infancy%22&source=bl&ots=HBIfC09CiG&sig=WwzkRkzOkW4HDn2EvmI2WLOFpVw&hl=en&sa=X&ved=0ahUKEwiUlfD6qbbJAhXC7CYKHTeFD8EQ6AEIIzAB#v=onepage&q=%22In%201972%2C%20the%20NBS%20Institute%20for%20Computer%20Sciences%20and%20Technology%20%28ICST%29%20initiated%20a%20project%20in%20computer%20security%2C%20a%20subject%20then%20in%20its%20infancy%22&f=false

Chaum, D. (1983). Blind Signatures for Untraceable Payments. In D. Chaum, R. L. Rivest, & A. T. Sherman (Eds.), Advances in Cryptology (pp. 199–203). Springer US. Retrieved from http://link.springer.com/chapter/10.1007/978-1-4757-0602-4_18

Chaum, D. (1985). Security without identification: Transaction systems to make big brother obsolete. Communications of the ACM, 28(10), 1030–1044.

Chaum, D. L. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 24(2), 84–90.

Chaum, D. L. (1982, April 4). Computer Systems Established, Maintained and Trusted by Mutually Suspicious Groups (Doctoral Dissertation). University of California Berkeley, Berkeley, CA.

coinmarketcap.com. (nd). Crypto-Currency Market Capitalizations. Retrieved December 18, 2015, from http://coinmarketcap.com/

Cowrey, D. (2014, June 20). Are 51% Attacks a Real Threat to Bitcoin? Retrieved July 1, 2015, from http://www.coindesk.com/51-attacks-real-threat-bitcoin/

Cox, B., Tygar, J. D., & Sirbu, M. (1995). NetBill security and transaction protocol. In Proceedings of the First USENIX Workshop on Electronic commerce (Vol. 13). Retrieved from http://static.usenix.org/publications/library/proceedings/ec95/full_papers/cox.ps

  ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

Davidson, J. (2015, January 9). No, Big Companies Aren't Really Accepting Bitcoin | Money.com. Retrieved July 1, 2015, from http://time.com/money/3658361/dell-microsoft-expedia-bitcoin/

Davis, J. (2011, October 10). The Crypto-Currency - The New Yorker. Retrieved June 25, 2015, from http://www.newyorker.com/magazine/2011/10/10/the-crypto-currency

Diffie, W., & Hellman, M. E. (1976). New Directions in Cryptography. IEEE Transactions on Information Theory, IT-22(6), 644–654.

Diffie, W., & Hellman, M. E. (1977). Special Feature Exhaustive Cryptanalysis of the NBS Data Encryption Standard. Computer, 10(6), 74–84. http://doi.org/10.1109/C-M.1977.217750

en.bitcoin.it. (2014, May 31). Protocol rules - Bitcoin Wiki. Retrieved June 30, 2015, from https://en.bitcoin.it/wiki/Protocol_rules#.22tx.22_messages

Feistel, H. (1974, March 19). Patent US3798359 - Block cipher cryptographic system - Google Patents. Retrieved June 19, 2015, from http://www.google.co.in/patents/US3798359

Felten, E. (2104, February 12). Understanding Bitcoin's transaction malleability problem. Retrieved July 1, 2015, from https://freedom-to-tinker.com/blog/felten/understanding-bitcoins-transaction-malleability-problem/

Forde, B. (2015, May 12). How to Prevent New York From Becoming The Bitcoin Backwater of the U.S. — MIT Media Lab Digital Currency Initiative — Medium. Retrieved July 2, 2015, from https://medium.com/mit-media-lab-digital-currency-initiative/how-to-prevent-new-york-from-becoming-the-bitcoin-backwater-of-the-u-s-931505a54560

Greenberg, A. (2013, October 25). FBI Says It's Seized $28.5 Million In Bitcoins From Ross Ulbricht, Alleged Owner Of Silk Road - Forbes. Retrieved June 30, 2015, from http://www.forbes.com/sites/andygreenberg/2013/10/25/fbi-says-its-seized-20-million-in-bitcoins-from-ross-ulbricht-alleged-owner-of-silk-road/

Higgins, S. (2014, July 7). ISIS-Linked Blog: Bitcoin Can Fund Terrorist Movements Worldwide. Retrieved July 1, 2015, from http://www.coindesk.com/isis-bitcoin-donations-fund-jihadist-movements/

King, R. (2014, February 10). Why nobody can withdraw bitcoins from one of the currency's largest exchanges - Quartz. Retrieved July 1, 2015, from http://qz.com/175565/why-nobody-can-withdraw-bitcoins-from-one-of-the-currencys-largest-exchanges/

Leech, D. P., & Chinworth, M. W. (2001). NIST Planning Report 01-2, The Economic Impacts of NIST's Data Encryption Standard (DES) Program - report01-2-DES.pdf. Arlington, VA. Retrieved from http://csrc.nist.gov/publications/secpubs/otherpubs/report01-2-DES.pdf

  ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

Liu, A. (2013a, March 19). When Governments Take Your Money, Bitcoin Looks Really Good. Retrieved June 30, 2015, from http://motherboard.vice.com/blog/cyprus-spain-when-governments-take-your-money-bitcoin-looks-really-good

Liu, A. (2013b, May 7). Who's Building Bitcoin? An Inside Look at Bitcoin's Open Source Development | Motherboard. Retrieved June 30, 2015, from http://motherboard.vice.com/blog/whos-building-bitcoin-an-inside-look-at-bitcoins-open-source-development

Merkle, R. C. (1978). Secure Communications over Insecure Channels. Commun. ACM, 21(4), 294–299. http://doi.org/10.1145/359460.359473

Micali, S., & Rivest, R. L. (2002). Micropayments Revisited. In B. Preneel (Ed.), Topics in Cryptology — CT-RSA 2002 (pp. 149–163). Springer Berlin Heidelberg. Retrieved from http://link.springer.com/chapter/10.1007/3-540-45760-7_11

Nakamoto, S. (2008a). Bitcoin: A peer-to-peer electronic cash system. Consulted, 1(2012), 28.

Nakamoto, S. (2008b, November 1). Bitcoin P2P e-cash paper. The Cryptography Mail Archive. Retrieved from http://www.mail-archive.com/cryptography%40metzdowd.com/msg09959.html

Narayanan, A. (2013a). What happened to the crypto dream?, part 1. IEEE Security & Privacy, (2), 75–76.

Narayanan, A. (2013b). What happened to the crypto dream?, part 2. IEEE Security & Privacy, (3), 68–71.

Polk, D. (2014a, July 31). New York July 2014 "BitLicense" Proposal: Visual Memorandum. 2014 Davis Polk & Wardwell LLP | 450 Lexington Avenue | New York, NY 10017. Retrieved from http://www.davispolk.com/download.php?file=sites/default/files/07.31.2014.New_.York_.July_.2014.BitLicense.Proposal.pdf

Polk, D. (2014b, November 7). 1.10.14.New_.Yorks_.Proposed.BitLicense.Regime.Summary.of_.Published.Comments.and_.Expected.Changes.pdf. bitcoin - reg.com Davis Polk & Wardwell LLP. Retrieved from http://bitcoin-reg.com/docs/11.10.14.New_.Yorks_.Proposed.BitLicense.Regime.Summary.of_.Published.Comments.and_.Expected.Changes.pdf

Szabo, N. (2008, December 27). Unenumerated: Bit gold. Retrieved from http://unenumerated.blogspot.in/2005/12/bit-gold.html

  ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

The Economist. (2015, October 31). The trust machine | The Economist. Retrieved December 18, 2015, from http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

Vigna, P., & Casey, M. J. (2015). The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order. St. Martin's Press.

Zetter, K. (2012, May 9). FBI Fears Bitcoin's Popularity with Criminals | WIRED. Retrieved July 1, 2015, from http://www.wired.com/2012/05/fbi-fears-bitcoin/

Zittrain, J. (2012). The End of Crypto. In R. Safavi-Naini & R. Canetti (Eds.), Advances in Cryptology – CRYPTO 2012 (pp. 86–86). Springer Berlin Heidelberg. Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-32009-5_6

APPENDIX A

Illustration of a block (from http://www.righto.com/2014/02/bitcoin-mining-hard-way-algorithms.html).