Bitcoin: Future transaction currency?

HOSAIN, MD SAJJAD

Sichuan University

25 June 2018

Bitcoin: Future transaction currency?

Md Sajjad Hosain
School of Business, Sichuan University

Abstract:
Bitcoin is a digital cryptocurrency that has attracted substantial interest in recent years from the general people, profit seekers, risk takers, academic practitioners and last but not the least, from economists. Most recently, particularly, after 2015, it has succeeded to gain even more attention for increase in value and volume of exchange. The Bitcoin system maintains a global, distributed cryptographic ledger of transactions, or blockchain, through a consensus algorithm running on hardware scattered across the world. This paper basically discusses on the nature of cryptocurrency & blockchain, how it works and present status of bitcoin blockchain in different countries around the world. The various aspects this technology in detail is yet to be revealed. The authors hope that this simple, basic and narrative paper will be helpful for those seeking the basic references regarding this newest issue.

Keywords: Bitcoin, Blockchain, Cryptocurrency, Internet, Trading, Mining, Block, Transaction.

1. Bitcoin: An introduction:
Bitcoin is a peer-to-peer cryptocurrency mainly used for monetary transactions on the internet (Nakamoto, 2014) and is intended to be similar to flat money and commodities. Bitcoins are inherently valueless, their worth is determined by those trading in them (O'Dwyer and Malone, 2014). It has generated a massive amount of interest in the media recently and has sparked a wave of copy-cat-currencies (Litecoin, Gaelcoin, etc.) and even a fully working parody currency (dogecoin). It has also generated interest in intellectual circles owing to issues it creates in user privacy (Androulaki et al., 2013), as well as attempts to gain insights into is behind transactions (Meiklejohn et al., 2013) and attempts to better understand its implications as a payment system Karame et al., 2012).

It is a kind of digital currency in which encryption techniques are used to control the generation of units of currency and verify the transfer of funds, operating independently of a central bank. Bitcoins are produced by users who 'mine' them by lending computing power to verify other users' transactions and are stored in a "digital wallet", which exists either in the cloud or on a user's computer. The wallet is a kind of virtual bank account that allows users to send or receive bitcoins, pay for goods or save their money (Anderson et al., 2017). The major difference between physical currency (e.g. GBP or US dollar) and bitcoin or between bank accounts and bitcoin wallets is that the former ones are insured by the Financial Services Compensation Scheme in the UK or The Federal Deposit Insurance Corporation in the US whereas the latter one are not.

Fundamental to bitcoin is a public ledger, acknowledged as the blockchain. At the beginning, a new "block" was added to this chain or ledger every 10 minutes (although it can take over an hour today). This ledger records all of the transactions that have occurred as well as the quantities of bitcoin are in possession at singular public addresses having each public one a

related classified key. The owner of the private key has the authority to transfer the digital coins that are held at that specific address only. Each key is 51 characters long in the same format as a public address. To spend an amount of bitcoin, one must use his/her private key to cryptographically sign the transaction, sending the bitcoin to another address. This message or transaction is then transmitted to the network, and the computers in the network begin working to record that the address no longer has the amount that was sent, but is now held at the receiving address. All of the computers that are working to write new blocks to the blockchain, are known as miners. These computers are all racing to solve a cryptographic puzzle, which is required to write the new block. The computer that solves the algorithm and writes the new block, receives an award of newly created bitcoin (now worth over $7,000 each) (Anderson et al., 2017).

2. The concept of blockchain:

Blockchain is the core technology behind bitcoin. It is a disseminated, decentralized database and is designed to accomplish consistent and reliable agreement over a record of events between independent participants. Participants in a blockchain network get to agreement about changes to the state of the shared database without needing to trust the integrity of any network participants or administrators. Anyone who participates in the blockchain network has their own data store that stores all of the transactions that ever happened on the network (also known as the distributed ledger) (Anderson et al., 2017).

Transaction entries are recorded within a cryptographic chain of blocks. At each stage, the networks of participants are required to agree about the most recent block of transactions. Agreement is reached through a process of mass consent, eliminating duplicate entries and dual spending. This process and the cryptographic layering of the blocks make the agreed blockchain irretrievable and unchallengeable. The ‘history’ of events within the blockchain cannot be tailored by any one of the participants without majority consensus from the group. This is vitally important to prevent the ‘double-spending’ difficulty (i.e. the same digital file being copied and transferred multiple times) without requiring a centralized ledger or third party that prevents users from duplicating/spending the same digital file twice. Blockchains can thus aid the transfer of assets and other data without needing a trusted central authority (like banks or other financial institutions).

The ability of blockchain system participants to autonomously authenticate the reliability of the shared database without having to rely on a trusted third party is one of the main value propositions of using the blockchain. Blockchains hold the promise of dropping the trust gap by making actions within the system autonomously verifiable by each participant, improving accountability, and dis-incentivizing misbehavior through public audit ability. In other words, the rules governing a blockchain can successfully eliminate the types of unauthorized transfers or deceptive activity that have become all too frequent in many areas of business and society(Anderson et al., 2017).

3. Bitcoin and blockchain: How the system works?

This segment provides a simple explanation of the blockchain protocol that is the basis of Bitcoin system and also, is the foundation of many other cryptocurrencies. Describing focuses on the economic elements and to explain what the Bitcoin system does, it would be helpful to explain initially what is required for a payment system such as PayPal, FedWire or the

continuance of electronic balances in a modern bank. An electronic payment system functions as a record (or a ledger) of accounts that is connected with a user and his balance. It allows users to check their balances and allows debiting his balance and crediting the debited amount to another account. Only an account owner can debit the account and the balances do not change without a legal transfer, e.g., a transfer that conforms to the system's stated rules.

One uncomplicated accomplishment is just a spread-sheet (or another bookkeeping device) that only a trusted authority can change. Allowing multiple computers to maintain and update the ledger requires a more complicated structure. This distributed ledger structure requires synchronization across the servers, which is, in principle, more robust than a single server system (Narayanan et al., 2016).

Maintaining harmony in a distributed computer system has been known to be straightforward, as long as the computers are trusted (Tanenbaum and Van Steen, 2007)). The Bitcoin system is intended for an environment which lacks a trusted authority. Therefore, its ledger must be maintained and updated by a collection of computer servers, called miners, none of which is trusted (Huberman et al., 2017). They are assumed to be profit oriented, e.g., to respond to incentives in a profit maximizing way. Moreover, they offer or withdraw their services according to profit seeking opportunities they perceive. Although, legal transactions are in procession of untrusted miners, the system as a whole is very secure, that is, it processes all legal transactions. The collection of miners jointly holds a single ledger, meaning that there must be consensus among miners about current balances. Moreover, consensus must be maintained as balances change. Bitcoin's ledger is a public database called blockchain, which can be verified by third parties through cryptography. The system arranges for the miners to be compensated for their services in such a way that when each of them maximizes his profit; and believes that other miners similarly maximize their profits too (Huberman et al., 2017).

Initially, all balances are at zero. Over time, the protocol mints new coins which it adds to the balances of winning miners holding the record of all balance changes. The demonstration of a transaction is a message which a sending account transmits to all the miners stating the sending account, receiving account, amount transferred, transaction fee, and a cryptographic signature by the sending account. A transaction is processed by adding the appropriate message to the end of the ledger. The cryptographic signature allows any third party to verify that the transaction was indeed authorized by the holder of the sending account. Since the ledger is public, any third party can verify that the sender indeed held a balance enough for the transfer. The public ledger is saved in the shared blockchain format where the transaction data is partitioned into a series of blocks. These blocks are periodic updates to the ledger. Notably, the ledger does not update instantly following the appearance of a new transaction. Rather, it updates on average every ten minutes with a block summarizing a subset of the recent pending transactions which hadn't been included in a previous block. Remaining unprocessed transactions wait to be processed in future blocks (Huberman et al., 2017). The maximum block size is 1MB. To ensure each block can be transmitted promptly throughout the network, the protocol limits each block to 1MB of data. As of July 2017, this limits each block to no more than approximately 2,000 transactions, as the average transaction uses 0.5KB of data (Zohar, 2015).

New transactions are processed when they are incorporated in a block that is added to the ledger, where, each miner holds a duplicate of the present ledger e.g., all preceding blocks. All transaction requests are transmitted to all miners. The set of awaiting transactions that get to each miner may differ a little across miners due to network imperfections, rendering non-trivial the choice of a unanimously agreed upon record of transactions. To ensure that bitcoin maintains an exclusive record of transactions, a solo miner is selected to add a block of transactions to the ledger. As there is no trusted authority to make the selection, a competition is used to randomly select a winning miner. To participate in the tournament miners exert effort (known as proof of work) that is practical merely for generating a verifiable random selection of a miner without the need of a trusted randomization device (Huberman et al., 2017).

Periodically (currently approximately every 10 minutes), the tournament aimlessly selects one miner as the winner, assigning his block as the next in the chain, thereby making that block a mined block. The mined block is transmitted to all the other miners, who verify the legality of that block and vet all transactions included in the block. Miners add a newly mined legal block to their copy of the ledger and proceed to add new blocks on top of it, ignoring mined blocks that are not legal (Huberman et al., 2017).

The tournament-winning miner is paid a reward when he mines a new block, but can withdraw his reward only after newer blocks augment the chain on top of his block. Other miners will build on top of his block only if they consider it legal incentivizing to assemble and create legal blocks. Consensus forms on a ledger that includes the new block. The process continues in the same manner for the following ten minutes (on average) and so on (Eyal and Sirer, 2014)

The miner that produced a block is paid from two sources: one consists of newly minted coins the exact number of which is protocol-determined and is decreasing with time (Crediting successful miners with newly minted coins moves the system early on from having zero balances to having positive ones) and the second consists of the fees offered by the transactions in the mined block (Huberman et al., 2017).

According to Huberman et al., (2017), this system will have the following desired properties:

1. All miners are synchronized to hold the same ledger of processed transactions.
2. No single miner controls the system, because every 10 minutes the ability to process transactions is given to a randomly chosen miner.
3. Balances change only with a legal transaction because any transaction that is added is vetted by other miners to be valid, and transactions cannot be deleted from the ledger.

4. Related Literature:

As a relatively new concept, there are few previous literatures regarding bitcoin and blockchain, although they are being attracted the by curiosity of the researchers very recently and it is continuing to do so. A relatively few number of authors investigated these issues. On the following sections such investigative experiments are highlighted:

4.1 Engineering of bitcoin:

Table-1: Literatures on bitcoin engineering

Author (s)	Year of investigation	Topic of investigation
Nakamoto	2008	First identified the name "Bitcoin" described the Bitcoin system.
Babaio et al.	2012	Explained the incentives to distribute information in the Bitcoin system
Kroll et al.	2013	Oered a description of the incentives faced by participants in the bitcoin system, especially the incentives faced by miners, thus, concluding a brief discussion of transaction fees.
Eyal & Sirer	2014	Analyzed the regularity between miners.
Sapirshtein et al.	2016	Established to proposition that appropriate design of the blockchain protocol produces a dependable system in equilibrium if all miners are significantly small.
Narayanan et al.	2016	Offered a sophisticated explanation and analysis of the bitcoin system
Croman et al.	2016	Provided cost estimates for the Bitcoin system and analyzed the potential for transaction throughout.
Eyal et al.	2016	Suggested another design aimed to develop a system with a higher transaction throughout.
Carlsten et al.	2016	Analyzed how incentives for miners change when they are rewarded with transaction fees instead of newly created coins.
Chiu & Koeppl	2017	Evaluated the welfare implications of printing new coins, adopting a mostly experimental orientation
Easley et al.	2017	Explained contemporary designing and performance of blockchain
Huberman et al.	2017	Explained the economics behind the bitcoin system: How does the system raise revenue to pay for its infrastructure? How are usage fees determined? How much infrastructure is deployed? What are the implications of changing parameters in the protocol?

4.2 Bitcoin usage as a currency and the cryptocurrency market:

Table-2: Literatures on Bitcoin usage as a currency and the cryptocurrency market

Author (s)	Year of investigation	Topic of investigation
Yermack	2013	Reviewed the history of Bitcoin and the statistical properties of its price history arguing that it does not behave much like a currency according to the criteria widely used by economists. Rather, bitcoin resembles a speculative investment similar to the Internet stocks of the late 1990s.
Ron & Shamir	2013	Provided analysis of the usage of Bitcoin and its value as a currency.
Gandal & Halaburda	2014	Analyzed competition between the various cryptocurrencies.
Gans & Halaburda	2015	Analyzed the economics of digital currencies, focusing on platform sponsored credits.
Athey et al.	2016	Explained the theory of bitcoin and using it as a currency.
Catalini & Gans	2016	Discussed possible opportunities that can arise from blockchain technology.

4.3 Related work in queuing theory:

Lui (1985), Glazer & Hassin (1986), and Hassin (1995) studied a queuing system in which users with various waiting costs volunteer to pay transaction fees (termed bribes in Lui 1985) in order to gain priority in a queue to solo service station which serves customers once at a time (Huberman et al., 2017). The main observation of Lui is that the server may amplify its revenues by raising the speed of service. Hassin (1995) showed that the service rate that maximizes the server's profit is always slower than the socially optimal service rate. Hassin & Haviv (2003) provide a summary of the results, and Hassin (2016) provided an updated review. The present

analysis considers a queuing system where transaction arrival and service arrival is stochastic, but the service is done is batch mode of fixed maximal size. The prior work corresponds to a batch size of one. The interaction among the arrival and service rates and the maximal batch size and their impact on the transaction fees and server's revenues are of major concern (Huberman et al., 2017). Independently, Kasahara & Kawahara (2017) analyzed delays in a priority queuing system with batch service inspired by bitcoin, but do not consider user incentives or equilibrium considerations.

4.4 Work on competition, monopoly and its regulation:

The social welfare implications of monopolistic vs. competitive provision of a good or service is of innermost concern to economic analysis, often leading to a debate regarding the extent to which regulation is desired and the best means through which to accomplish it (Huberman et al., 2017). According to Posner (1975), a model of the social cost of monopoly and monopoly-inducing regulation (Narayanan et al., 2016) assumes that competition to obtain a monopoly results in a conversion of monopoly profits into social costs. A major conclusion is that public regulation is perhaps a larger source of social cost than private monopoly. A Posner-inspired explanation of mining is that when a block is completed, e. g., the hard riddle has been solved by one of the miners, the solving miner is a monopolistic winner who takes all the revenues associated with the completion of that block. The social cost of one miner's winning is the amount spent by the community of miners to try to solve the hard puzzle. Noteworthy is that the monopolist is not a price-setter, contrasting with standard monopoly models, including Posner's (Huberman et al., 2017).

5. Present status of bitcoin around the world:

Different countries all over the world acted to bitcoin technology in a very different way. In the following table, the reactions of the countries to bitcoin have been depicted:

Table-3: Present status of bitcoin around the world

Name of the country/region	Action(s) taken
Australia, Canada, Estonia, France, Germany, Gibraltar, Isle of Man, Japan, Jersey, Luxembourg, The Netherlands, Singapore, Switzerland and USA	Acted or are acting to regulate bitcoin
Bangladesh, Bolivia, Iceland and Kyrgyzstan	Banned bitcoin
Brazil, Bulgaria, Denmark, Finland, Italy, Norway, Slovenia, Sweden and UK	Stopped sort of regulating bitcoin, but have imposed taxes
China, Colombia, Israel, Lithuania, Mexico, New Zealand, Philippines, Russia, South Africa, Spain, Taiwan, Ukraine and Vietnam	Undecided in respect of digital currencies

Albania, Argentina, Belgium, Croatia, Cyprus, United Arab Emirates, Ghana, Greece, Hong Kong, Hungary, India, Indonesia, Ireland, Malta, Malaysia, Nigeria, Poland, Portugal, Romania, South Korea, Thailand, Turkey and Venezuela	Do not regulate bitcoin

Source: Anderson et al., 2017

6. Future prospects:

The future of Bitcoin is very incomprehensible. This means the progression of Bitcoin can go in any direction which is presently and slowly recounting before our very eyes. There are too many speculations and opinions regarding what the future of bitcoin will look like. Until now, when cataloging out the wreckage, three dissimilar possible outcomes go up on top of the rest (Andersson and Wegdell, 2014):

1. It becomes a globally recognized currency, used all over the place, possibly, even eliminating cash and credit cards.

2. It remains active and fine, but performing in the background. Rather than being a major currency, it could function as an attribute and an accompaniment to the global financial sector. Exactly, like English has stretched across the world without taking out each existing language in its trail, bitcoin could spread across the world as a global payment system, co-existing with other world currencies.

3. Bitcoin prices collapse to their inherent value. It could be through a fizz or it fades away over time. In either way it ceases to survive in the public eye and ultimately gets forgotten as the years pass on.

No matter how possibly each option is can be extensively dubious and also, the probability in variations of the different outcomes should be taken into consideration. An attempt to describe the different scenarios has been made below:

6.1 A globally acknowledged currency:

Even though it seems almost impossible now, a few voices saying bitcoin could become a global currency. In order for this to take place, the whole world has to be “on the same wave length”. Such incident will not happen if all the requirements for a currency are satisfied, the three being: unit of account, medium of exchange and store of value (Andersson and Wegdell, 2014).

The first one, performing as a medium of exchange has been already somewhat achieved. There are ample ways of spending bitcoins and a lot of diverse services obtainable for the transactions to take place. Bitcoin’s technological drawing allows for swift transactions and as there is no third party that requires authenticating the legality of the transaction, fees are low. (The Economist, 2014). All merchandise are, however, not tradable on the bitcoin market, but is does not take away the precondition to function as a medium of exchange.

Bitcoin fulfills the obligation in the sense that it can be traded and stored for future use. The complicated element is achieving steadiness in the value of a bitcoin, as it lacks inherent value and is priced exclusively after demand (Yermack, 2013). One can guess with next to confidence how much 100 USD today will be worth one year from now, considering only current inflation. The price of a bitcoin, however, is very volatile; and there is no guarantee that one's bitcoins will be value as much, in even a few weeks' time. Such volatility makes the currency extremely vulnerable to speculative attacks, in another words, the consequences of group psychology and collective speculation for both bull and bear markets (Andersson and Wegdell, 2014).

Out of the three requirements, the one which is the furthest away from being fulfilled today is that it functions as a unit of account. In order to be truly accepted and adopted a currency like bitcoin, people must begin to "think in bitcoins", e. g. asking themselves how much things cost in bitcoin, rather than bitcoin converted into dollars (Andersson and Wegdell, 2014). If, for example, someone buys a coffee for $4 and the price is changed to $2 the next day, he/she can say with certainty that the coffee is now half the price from what it was earlier. This does not apply to bitcoin payments, as the value is too unstable. Although priced identically (in bitcoin) for two consecutive days, the price of the coffee during day two (in USD) could be half the price, twice the price, ten times the price or whatever the currency happens to be on that day. This means that sellers who accept bitcoin payments constantly must adjust the prices of their goods, in order for them to represent their current value in USD (Yermack, 2013).

A number of people around the globe, are using bitcoin as is anticipated, hoping one day it will be acknowledged as a globally accepted currency. For bitcoin to function as a currency, it is also essential that the velocity increases and more people start using it to purchase goods and services but at present, the typical users do not. The majority of users so far are speculative investors who have recently seen the possibilities of an investment profit, as the media coverage increased and the price skyrocketed (Andersson and Wegdell, 2014). According to Fred Ersham, co-founder of the digital wallet service "Coinbase", approximately 80 percent of the transaction activity is related to speculation. (Goldman Sachs, 2014).

6.2 Complementary and attributive currency:

If Bitcoin could by some means become a more controlled and stable currency, this way of transferring money globally has the prospective of entirely knocking out its present competition (e. g. cash offices). In 2013, remittances sent by immigrants to developing 33 countries amounted to $ 401 billion dollars and this is projected to increase to $ 515 billion by 2015. (The World Bank, 2013). This money usually flows through third parties such as MoneyGram or Western Union. In the 1st quarter of 2014, the global average total price of remittances was 8.36 percent, which was a lifetime low. (The World Bank, 2014) For this reason, bitcoin has a huge advantage to cash offices for using it as a medium of exchange. In this case, the volatility would not be a very big obstacle either. Money could be exchanged to bitcoins, cheaply sent across the world and exchanged back to a regular currency although for doing this, the recipient must have an account on an exchange platform in order to sell the bitcoin and receive the money. The exchange used must also be able to provide withdrawals in the currency wanted; and presently, many developing countries do not provide this service (Andersson and Wegdell, 2014).

In addition to having a wide range of applications, bitcoin can also give rise to new lines of products and services such as the possibility of micro-payments. Until now, micropayments of

less than $1 have seen little success due to the impracticalities that follow a transaction of this kind. Bitcoin enables extremely small payments at a reasonable cost; making the market for micro-payment services very much alive, in a way they have not been before. This would enable a more convenient “pay as you go” world where people could pay very small amounts for very small services or goods. Present transaction fees (using for example Visa, MasterCard or PayPal) make these types of purchases impractical as they easily could be equal to, or even more than, the actual purchase price itself (Andersson and Wegdell, 2014). One example of a micro-payment like this could be paying for WiFi access by the kilobyte, whenever passing a WiFi hotspot (Bitcoin.org.).

Some other positive characteristics of bitcoin, besides micro-payments and the cost efficiency are its global accessibility, the possibility of multi-signature accounts and simplifying donations/crowdfunding. The global accessibility makes everyone with an internet connection allowed to take part of the network, increasing global access to commerce and potentially helping international trade flourish. Multi-signature accounts allow accounts to be shared by 34 groups of people and do not allow any transactions to take place unless all the members are unanimous about it. This could be of great value to for example a board of directors, to make sure no company money is spent without the knowledge of the rest (Bitcoin.org.).

Crowdfunding is a type of fund raising, when members of a group each contribute with a small amount of money and collectively working towards a unanimous economic goal. This could be a project such as a non-profit, political or philanthropic campaign. (Canada Media Fund, 2012) With the help of technology of bitcoin, there is the possibility of even pledging money to a project, but not collecting it from anyone until the main economic target is reached (Andersson and Wegdell, 2014).

When the website WikiLeaks announced that they were in need of donations to be able to continue their work, both Visa and MasterCard denied donations from the general public (due to political pressure), making donations in bitcoin skyrocket instead (Matonis, 2012). The reson is that bitcoin transaction cannot be stopped by any authority. Also, in case of a catastrophe, such as a natural disaster or something similar, bitcoin donations could be very useful in quickly and cheaply organizing an international response and the money would arrive long before any normal currency could (Andersson and Wegdell, 2014).

The fact that money can be programmable opens up a world of possibilities. It could be regarded as an extrinsic value, e. g. the value assigned to an object via external factors. Things like “earmarking” money could become common in the future. This would make money impossible to spend, unless spent in the way it is intended. It might be programming economic support to third world countries so they can only be used for medical treatment/food and not for weapons or it might be parents programming their children’s allowances so that they cannot buy cigarettes or alcohol, but they can buy school lunches etc. (Andersson and Wegdell, 2014). This way it would have similarities with today’s system with food stamps for people on financial support in the US. Other applications for programmed money are cloud services. Money can be stored in clouds and programmed to be released, piece by piece or all at once, at a given point in time. This could be for example on a child’s 18th birthday or even after one’s death. (Wilhelm, 2013).

6.3 Fading away or crashing:

On the occasion of Bitcoin becoming extinct, it seems that there are two possible ways it might do so. It will either gradually die, as people lose hope and interest for it; or something extreme might happen that makes the public interest change overnight from great to non-existent. In either way, this would have to be something so major that Bitcoin cannot fight back against it (Andersson and Wegdell, 2014).

6.3.1 Ponzi scheme:

A Ponzi scheme (sometimes known as Ponzi game) is a fraudulent investment operation where the operator provides fabricated reports and generates returns for older investors through revenue paid by new investors, rather than from legitimate business activities or profit of financial trading. Operators of ponzi schemes can be either individuals or corporations, and grab the attention of new investors by offering short-term returns that are either abnormally high or unusually consistent (Frankel, 2012).

There are a number of theories in circulation regarding why bitcoin was formed. As mentioned earlier, one theory is that the idea was formed as a reaction to the global financial crisis in 2008, when there was great malcontent concerning the present financial system. The idea of a decentralized currency may have many positive sides but it has some flipsides too such instability and no safety net for users. The reality that it could be a trick in disguise is also a possibility that cannot be completely lined out. Some skeptics (for instance American economist Nouriel Roubini) have emphasized this approach and point at the fact that it could all be a huge ponzi scheme (Andersson and Wegdell, 2014).

A Ponzi scheme is an unsustainable business model that promises the investor great profit opportunities. It is made possible in the short run, due to the fact that these profit returns are in fact actually money collected from new investors and given to old investors. These new investors in turn get their returns paid by even newer investors and thus, the pyramid grows and creates instead an illusion that all Participants are profiting off a legitimate business (FBI, n.d.).

A ponzi scheme is unsustainable in the long run as it will only be able to operate as long as more people join and supply a steady new flow of money. In another words, dependent on an ever-growing supply of enthusiastic participants and in time it will always collapse. The collapse happens due to two reasons: when the original operator disappears with all the money or when no new participants can be found to supply previous investors with the money promised to them. (FBI, n.d.)

There is a risk that people like Satoshi Nakamoto (and the early adopters), who have accumulated millions of dollars, might one day start selling their bitcoins and pulling out. This scenario can happen without the rest of the world acknowledging it and realizing the “scammers” are deserting it. Soon after, the fairytale is likely to be over. The price could fall helplessly and there will be no regulations whatsoever to help innocent third party investors who have exposed themselves to the risks. The similarities with a classic “pump and dump” strategy will become obvious and hard to ignore. Attempts have been made to estimate how many bitcoins the founder Satoshi Nakamoto is sitting on and the number is expected to be around 1 million BTC, making him worth approximately $1 billion in December 2013 (Andersson and Wegdell, 2014).

7. Conclusion:

We have observed gold became cash and cash became credit cards. Is the next step cryptocurrencies? It would be interesting to see whether bitcoin finds a place in our financial world today. It is very unlikely to consider it becoming a real currency. Its properties are poorer on all aspects of being a performing currency besides acting as a medium of exchange. In theory, one solution to solve the store of value problem could be to nail it to, for example, the US dollar, making it more stable and predictable. Also, the unit of account difficulties would grasp to exist as people could more easily measure and compare prices and goods in bitcoin. But, in reality, this will never happen since the bitcoin network is programmed to be decentralized and unmanageable. The whole idea of bitcoin is that it is independent from a central entity and the price will go wherever the market drives it and legislation cannot solve this since it would entail a comprehensive conformity.

Bitcoin, without a doubt might be considered a radical innovation. Considering our focus on being a means of payment, it has the prospect to compel the existing system to adapt to it and thus, become more competent than it is today. As exactly in the similar way the possibility of illegal downloading has transformed the music and movie industry; the possibility of wiring money, virtually for free has the power to beat out its rivalry if no response to it is shown.

In conclusion it can be believed that bitcoin does have the prospective for a greater universal acceptance, depending upon the focus is on quick, cheap, convenient transactions. This would necessitate simple, more consumer friendly services, even for those who do not wish to understand the technicalities behind it. The path to such permanent establishment requires that the system remains fully transparent and secure, that a network effect takes place and that the bitcoin ecosystem is strengthened and made more dependable. Bitcoin might not by definition be a new currency, but it has placed a foundation for potentially improving money as we know it now.

References:

Anderson, T., Scanlon, L. and Smith, C. C. (2017). *Bitcoin, Blockchain & Initial Coin Offerings: A Global Review*. Pinsent Masons.

Andersson, G. and Wegdell, A. (2014). *Prospects of Bitcoin: An evaluation of its future.* Master Thesis presented on Spring of 2014 at the Department of Economics, School of Economics and Management, Lund University.

Androulaki, E., Karame, G. O., Roeschlin, M., Scherer, T. and Capkun, S. (2013). *Evaluating user privacy in bitcoin*. In: International Conference on Financial Cryptography and Data Security. Springer, Heidelberg, 34–51.

Athey, S., Parashkevov, I., Sarukkai, V. and Xia, J. (2016) *Bitcoin pricing, adoption, and usage: Theory and evidence*.

Babaio, M., Dobzinski, S., Oren, S. and Zohar, A. (2012). *On bitcoin and red balloons*. In: Proceedings of the 13th ACM conference on electronic commerce, ACM, 56–73.

Bitcoinfees (2014). Retrieved March 31, 2017. Available at: http://bitcoinfees.com/

Bitcoin.org, n.d. Retrieved April 5, 2017. Available at: http://bitcoin.org/

Canada Media Fund (2012). Crowdfunding in a Canadian Context (Retrieved April 16, 2017). Available at: http://www.cmf-fmc.ca/documents/files/about/publications/CMF-CrowdfundingStudy.pdf

Carlsten, M., Kalodner, H., Weinberg, S. M. and Narayanan, A. (2016). *On the instability of bitcoin without the block reward*. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ACM, 154–167.

Catalini, C. and Gans, J. S. (2016). Some simple economics of the blockchain. Technical report, *National Bureau of Economic Research*.

Chiu, J. and Koeppl, T. (2017). *The economics of cryptocurrencies–bitcoin and beyond*.

Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E. and Gu¨n, E. (2016). *On scaling decentralized blockchains*. In: Proceedings of 3rd Workshop on Bitcoin and Blockchain Research.

Easley, D., O'hara, M. and Basu, S. (2017). *From mining to markets: The evolution of bitcoin transaction fees*. Working paper series.

Eyal, I., Gencer, A. E., Sirer, E. G. and Van Renesse, R. (2016). *Bitcoin-ng: A scalable blockchain protocol*. In 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16), 45–59.

Eyal, I. and Sirer, E. G. (2014). *Majority is not enough: Bitcoin mining is vulnerable*. In: International Conference on Financial Cryptography and Data Security, Springer, 436–454.

Federal Bureau of Investigation (FBI). N.D. *Common Fraud Schemes*. (Retrieved April 28, 2017). Available at: http://www.fbi.gov/scams-safety/fraud/

Frankel, T. (2012). *The Ponzi Scheme Puzzle: A History and Analysis of Con Artists and Victims*. USA: Oxford University Press. ISBN 0199926611.

Gans, J. S. and Halaburda, H. (2015). Some economics of private digital currency. *Economic Analysis of the Digital Economy*, University of Chicago Press, 257–276.

Gandal, N. and Halaburda, H. (2014). *Competition in the cryptocurrency market*.

Glazer, A. and Hassin, R. (1986). Stable priority purchasing in queues. *Operations Research Letters*, 4(6), 285–288.

Goldman Sachs Global Investment Research. (2014). *All about bitcoin: Top of Mind*, 21, 8. March 11.

Hassin, R. (2016). *Rational queueing*. CRC press.

Hassin, R. and Haviv, M. (2003). To queue or not to queue: Equilibrium behavior in queueing systems. *Springer Science & Business Media*, 59.

Hassin, R. (1995). Decentralized regulation of a queue. *Management Science*, 41(1), 163– 173.

Huberman, G., Leshno, J. D. and Moallemi, C. C. (2017). *Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System*. Colombia Business School Press, 1-53.

Karame G. O., Androulaki, E. and Capkun, S. (2012) *Double-spending fast payments in bitcoin*. In: Proceedings of the 2012 ACM conference on computer and communications security, ACM, 906–917

Kroll, J. A., Davey, I. C. and Felten, E. W. (2013). *The economics of bitcoin mining, or bitcoin in the presence of adversaries*. In Proceedings of WEIS, 2013, Citeseer.

Kasahara, S. and Kawahara, J. (2017). *E□ect of Bitcoin fee on transaction-confirmation process*. Working paper series.

Lui, F. T. (1985). An equilibrium queuing model of bribery. *Journal of Political Economy*, 93(4), 760–781.

Matonis, J. (2012). WikiLeaks Bypasses Financial Blockade with Bitcoin. Forbes Magazine, Aug 20. (Retrieved March 20, 2017). Available at: http://www.forbes.com/sites/jonmatonis/2012/08/20/wikileaks-bypasses-financialblockade-with-bitcoin/

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M. and Savage, S. (2013). *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*. Paper presented in IMC, 2013, October 23–25, 2013, Barcelona, Spain.

Nakamoto, S. (2014). *Bitcoin: A Peer-to-Peer Electronic Cash System*. http://fastbull.dl.sourceforge.net/ project/bitcoin/Design\%20Paper/ bitcoin.pdf/bitcoin.pdf

Narayanan, A., Bonneau, J., Felten, E., Miller, A. and Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies*, Princeton University Press.

O'Dwyer, K. J. and Malone, D. (2014). *Bitcoin Mining and its Energy Footprint*. Hamilton Institute, National University of Ireland Maynooth Press, ISSC 2014 / CIICT 2014, Limerick, June 26–27.

Posner, R. A. (1975). The social costs of monopoly and regulation. *Journal of political Economy* 83(4), 807–827.

Ron, D. & Shamir, A. (2013). Quantitative analysis of the full bitcoin transaction graph. In: International Conference on Financial Cryptography and Data Security, Springer, 6–24.

Sapirshtein, A., Sompolinsky, Y. and Zohar, A. (2016). *Optimal selfish mining strategies in bitcoin*. In: International Conference on Financial Cryptography and Data Security, Springer, 515–532.

Tanenbaum, A. S. and Van Steen, M. (2007), *Distributed systems: principles and paradigms*, Prentice-Hall.

The Economist, (2014). *Money from nothing*. The Economist, March 15. (Retrieved May 3, 2017) Available at: http://www.economist.com/news/finance-and-economics/21599053-chronicdeflation-may-keep-bitcoin-displacing-its-fiat-rivals-money

The World Bank. (2013). *World Bank Launches Initiative on Migration, Releases New Projections on Remittance Flows*. The World Bank, April 19. (Retrieved April 16, 2017) Available at: http://www.worldbank.org/en/news/press-release/2013/04/19/world-bank-launchesinitiative-on-migration-releases-new-projections-on-remittance-flows

The World Bank. (2014). *An analysis of trends in the average total costs of migrant remittances services*. The World Bank, Issue no. 9. (Retrieved April 16, 2017) Available at: https://remittanceprices.worldbank.org/sites/default/files/RPW_Report_Mar2014.pdf

Wilhem, A. (2013). Inside Bitcoin, the programmable currency for our digital future. *Techcrunch*, Sep 10. (Retrieved April 4, 2017). Available at: http://techcrunch.com/2013/09/10/disrupt-sf-13-bitcoin-panel/>

Yermack, D. (2013). Is bitcoin a real currency? An economic appraisal, Technical report, *National Bureau of Economic Research*.

Zohar, A. (2015). Bitcoin: under the hood. *Communications of the ACM*, 58(9), 104–113.