Bitcoin, An SWOT Analysis

Sahar Mirzayi
Department of Electrical and Computer Engineering
University of Tehran
Tehran, Iran
s.mirzayi@ut.ac.ir

Mohammad Mehrzad
Department of Engineering
Tarbiat Modares University
Tehran, Iran
mehrzad.mohammad@gmail.com

***Abstract*— in the year 2009, a new virtual currency called Bitcoin was introduced to the world. Bitcoin generation and transactions are based on hashes and asymmetric encryption algorithms. Bitcoin is the first attempt at creating a decentralized virtual currency with no central bank or financial entity controlling it and is very attractive to different demographies of users. A lot of misunderstanding and doubt surrounds Bitcoin. Based on studying the few years of Bitcoin's circulation and usage, we presented the strengths and weaknesses of Bitcoin and analyzed what opportunities and threats it faces in the current financial environment. We summarized the strengths, weaknesses, opportunities and threats for Bitcoin in an SWOT analysis. We concluded that the most important factors to influence the future of Bitcoin circulation and price are technological advances and people's openness to Bitcoin, the intervention of governments and financial powers by creating laws around cryptocurrencies and external events that are closely tied to the Bitcoin community.**

Keywords*— *Bitcoin, Virtual currency, Blockchain Technology, SWOT analysis, cryptocurrency.

I. INTRODUCTION

Money is considered to be the most important part of world's financial systems. In the recent decades, a deep relationship has formed between computer science and banking systems. Some of the financial decisions taken by world powers has proven to be short sighted and has resulted in numerous recessions and financial meltdowns, the most recent one being the world financial crisis, which many researchers attribute to poor decisions by the Federal Reserve of the US. This might be the main reason why a group of cryptography experts and programmers designed a new financial architecture and system, which has been the beginning of digital cryptographic currency.

In the year 2009, a new financial instrument called "Bitcoin" was introduced. This instrument is based on algorithms first designed and introduced by Satoshi Nakamoto[1]. Nakamoto stipulates that he wanted to design a new type of currency that would not be affected by governments' unprecedented decisions, politics and fraud.

The main differentiation of this new currency is being virtual, which has empowered Bitcoin to the extent that it is being considered a serious contender for replacing strong currencies, by foregoing traditional financial systems' limitations.

Another interesting aspect of Bitcoin has been the extent of its effects in the world and the rise in its popularity. Bitcoin exchange rate has increased from a few cents in the year 2012 to 2500$ in the May 2017. Although many scholars consider Bitcoin to be a currency, some still consider it a commodity[2, 3]. In this article, Bitcoin will be considered a type of currency.

Bitcoin provides anonymous, fast and secure transactions. One can transfer any amount from one point in the world to another without involving a third party or being forced to pay fees. However, big seizures, robberies and heists exist in Bitcoin's history and using some techniques, the identities of owners and dealers are known to have been discovered. All these accidents create a looming doubt on Bitcoin's viability for the future.

In this paper, we are trying to analyze Bitcoin's intrinsic strengths and weaknesses and account for threats and opportunities in the current financial environment to build an SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis. A strength can be a resource, a unique approach, or capacity that would help the entity in reaching its goals. A weakness consists of an entity's intrinsic limitations or defects that work against it in reaching its goals. An opportunity consists of an entity's possible advantages in relation to its internal or external environment that help it provide its services more effectively and to a wider audience. Threats consist of a situation or barrier in the environment that limits an entity's success in providing its services or products.

An SWOT analysis is often used to build a concise outlook of a business or an entity, to provide a roadmap and strategy for its development. However, it can equally be effective in understanding new technologies, protecting assets and evaluating any other group effort. For example in [4] an SWOT analysis is provided for the field of virtual reality rehabilitation. The authors investigate the past of the field and guess what will happen in the future. Another good research analyzed the strengths, weaknesses, opportunities and treats of the object-based image analysis using SWOT method[5].

In the next section, a background on Bitcoin's creation and popularity is presented. In section 3, we will provide an SWOT analysis on Bitcoin and section 4 will provide a possible outlook on the future of Bitcoin. Finally, in the last section, we conclude.

978-1-5386-0804-3/17/$31.00 ©2017 IEEE

II. BACKGROUND

Bitcoin was first introduced in Feb. 2009 by Satoshi Nakamato's post on a website[1]. Nakamoto announced: "I've developed a new open source P2P e-cash system called Bitcoin. It's completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust" [1]. Let's look at the keywords used in this definition and their implication:

Open Source: the algorithm to create and transfer Bitcoin is accessible to everyone and it is not a secret.

P2P and decentralized: the Bitcoin network does not have a central control point or trusted entity and is not controlled by an organization. Bitcoin is in fact based on a peer to peer network, allowing it's users to transfer money without involving a third party and in a non-reversible fashion. This protects the anonymity of each party and also foregoes any tax obligations or transfer fees[2]. Bitcoin's peer to peer nature replaces a central control point that can go bankrupt or have its assets frozen. Almost all previous digital currencies like e-gold turned out to be unreliable and ultimately shut down because of relying on a single point of failure[6].

Cryptography: Bitcoin is based on cryptographic algorithms because Bitcoin transactions use cryptographic key pairs and hashing is used in processing transactions.

Nakamato's peculiar invention attracted widespread interest and many people started investing in Bitcoins and Bitcoin exchanges like Bitstamp.com and Coinbase.com were created so that people could exchange bitcoins for more general currencies like Dollars and Euros.

Virtual currencies were finally recognized by Europe's central bank as a digital unregulated currency that is usually used by its developers and is accepted in a particular virtual society [7]. Digital and virtual currencies should not be mistaken with each other. Virtual currencies like Bitcoin do not have a direct tangible equivalent.

Nakamoto's Identity has been kept a secret. Before the introduction of Bitcoin, no programmer was known by this name. Nakamoto used to use an anonymous email service. In 2009 and 2010, he/she/they published many posts in immaculate English asking other programmers to help with the development of Bitcoin and Nakamoto was in contact with many of them but he never revealed any details about his personal life [8]. In December 2010 he sent an email to one of the programmers stating that he was no longer involved with Bitcoin and disappeared and since then, the Bitcoin foundation has been managed by Gavin Anderson. Although many consider Nakamoto an internet fraud, others believe that he was politically motivated, Based on the fact that Nakamoto released his currency right after the world banks' crisis. The philosophy behind creating Bitcoin, might have been distrusting banks not to lower the value of a currency. Looking at the history of world's currencies, this trust has been repeatedly violated by the world's central banks [8].

It is imperative to know that Bitcoin was not the first effort to create a digital currency. Other efforts could be named such as the outdated currency e-Gold (1996-2014) and Liberty Reserve (2006-2013) both of which were shut down by the US government citing money laundering concerns. A successful example is Q-coin currency used in a Chinese messaging app, Tencent QQ, which was presented in 2005 and is used to buy items like avatars.

III. BITCOIN'S SWOT ANALYSIS

Based on what was represented here, Bitcoin's SWOT analysis can be summarized as follows:

A. Strengths

This section includes the first part of an SWOT analysis, strengths. A strength can be a resource, a unique approach, or capacity that would help the entity in reaching its goals.

1) Security

Secure transactions means that no one can alter Bitcoin transactions on the internet, because only the person that holds the private key to an account can sign transactions out of it. Also, changing the Bitcoin's transaction ledger (AKA the Blockchain) is almost impossible, because an entity must hold more than 50% of all of the network's processing power to change a transaction and continue to change transactions faster than the rest of the network.

2) Anonymity

In most countries, to open a bank account, one needs to present proper identification to the bank's authorities. To open a Bitcoin account, one only needs to generate a key pair and use the public key as the account number to receive funds and/or mine Bitcoins. Every account can be accessed using the private key of that account and no identification is required. Although all Bitcoin transactions are pubic knowledge, Anonymity can be achieved by spreading the flow of information, meaning that the user account number mapping, is only kept at the user's node and allows the user to create as many addresses as required [9]. The public can see which account number is transferring what amount to what account number but there is no public mapping between a user's identity and their account number. This is akin to stock exchange trading history, in which the amount bought or sold is public knowledge but the sellers and buyers are not readily identifiable. This can be summarized in fig. 1.

3) No single point of trust

Bitcoin algorithm stipulates that most of the trading nodes are reliable and uses a democratic mechanism to resolve any conflicts. In contrast, many electronic currencies require a central bank to 'print' money and stop double spending [10].

4) Fraud resistance

A bitcoin transaction is basically non-reversible. This is in contrast to traditional economic transactions [8]. Trades are mathematically irreversible to protect sellers from fraud and provide mechanisms to protect buyers. Also, by creating this

[1]A Mailing list on metzdowd.com

[2]The sending party can include a small transfer fee to encourage bitcoin miners and nodes to put the transaction in a higher priority, it is not a requirement though.

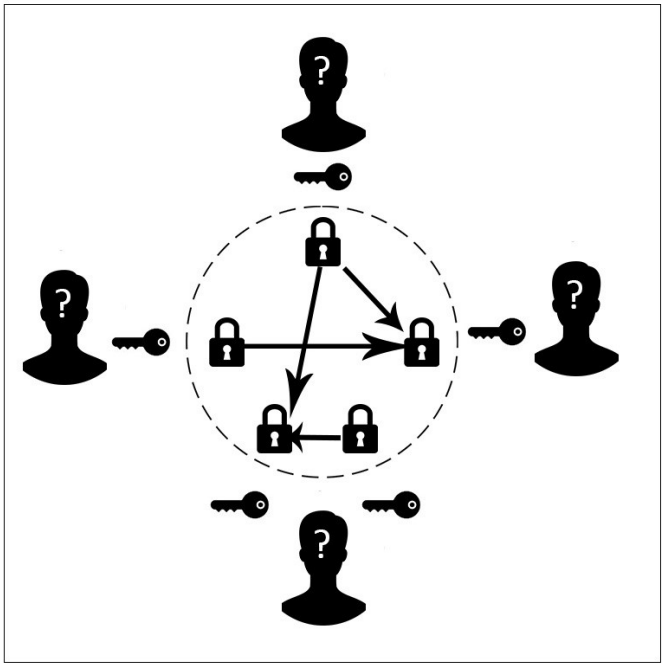

Fig. 1. Each Bitcoin user has a private and public key pair. The public key is available to all users and is used as an address for depositing and withdrawal of coins. Only the account owner has access to the private key which is used to sign transactions out of the account. The dotted circle represents all the information that is visible in to the Bitcoin peers. Everyone can see Bitcoin transactions and transfer histories, but there is no mapping of addresses to real entities. Each person can have an unlimited number of accounts (in the bottom of figure, we see a person with two account).

level of privacy of personal information, not only the public, but also no government can access personal details of trading parties [1].

5) Financial incentives

The Bitcoin ecosystem has been designed with financial incentives in mind. This system has been designed to financially reward users that take part in transaction processing by trying to mine Bitcoins and investing in mining hardware or spending their unused processing power to verify Bitcoin transactions [10].

6) Division and combination

Every Bitcoin can be divided up to 8 decimal points, bitcoins can also be readily combined into one account.

7) Predictable rate of coin generation

The Bitcoin algorithm guarantees Coins to be created at a semi constant rate, meaning that the more processing power is dedicated to mining Bitcoins, the harder it would become. This creates a strong incentive for technology pioneers [10].

8) Nonphysicality

The fact that Bitcoin transactions do not need any physical instrument such as bank bills, allows far simpler solutions than bank vaults to store wealth. Also the cost of printing and maintaining bills is pushed down to zero.

B. Weaknesses

This section includes the second part of an SWOT analysis, weaknesses. A weakness consists of an entity's intrinsic limitations or defects that work against an entity in reaching its goals.

1) Braking anonymity through transaction history

Based on Bitcoin algorithm and protocol design, all Bitcoin transactions for the whole history of Bitcoin can be traced back to the mining transaction that created them. This means that you might be identified if you have dealt with someone who knows you and they are identified. To fix that, many mixing services have been created, which essentially take many Bitcoins from different sources, mix them together and spit out newly minted coins into user provided addresses, effectively laundering dirty/traceable Bitcoins. In these services, you pay

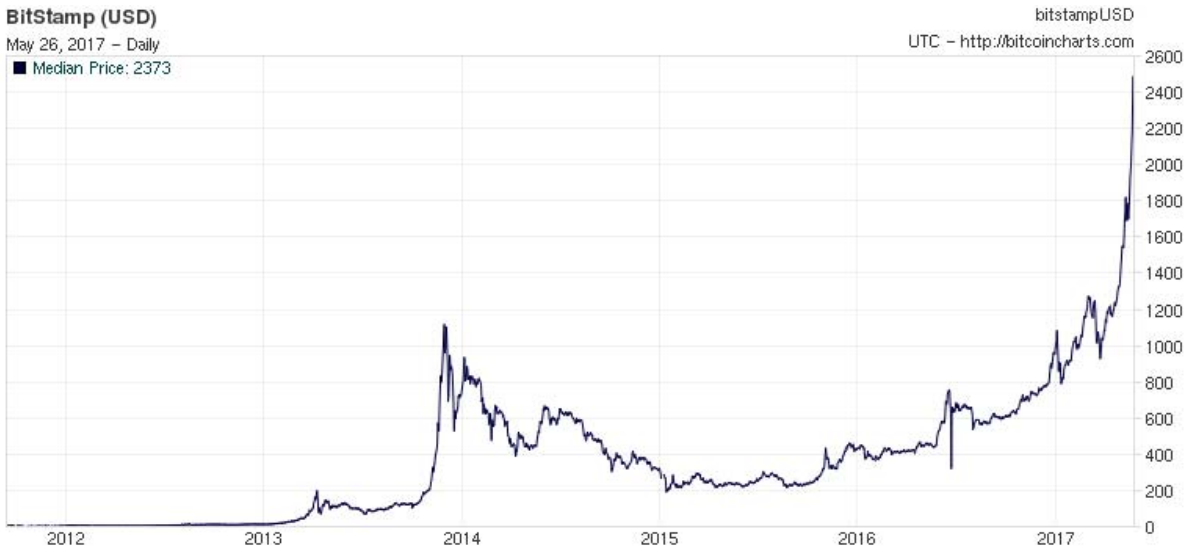

Fig. 2. Bitcoin Value in Bitstamp exchange from 2012 to 2017. Chart provided by bitcoincharts.com under Creative Commons, license.

an amount of Bitcoins to the service and receive the clean amount in the new address which makes tracking Bitcoins harder. In addition to that, the Bitcoin society suggests that you create a new address for receiving new funds which helps both you and the other trading party's anonymity.

2) The deflation and hording problem

One of the characteristics of traditional currencies is inflation. Authorities try to maintain a positive inflation ratio in the economy. This is an incentive for the financial entities to invest their money which creates cash flow and helps economies flourish. In the 1990s, Japan faced deflation and its central bank was forced to inject a huge amount of cash into the economy to counteract the negative effects of deflation [11].

Bitcoin was designed so that there would only be 21 million Bitcoins in existence and until May 2017, more than 16 million of those have been mined. Based on the algorithm, it can be calculated that around 12.5 bitcoins are mined every minute [12] though as time passes, the complexity to mine Bitcoins increases.

Fig. 2 shows the exchange rate of one Bitcoin sold on the Bitstamp exchange from the year 2012 to 2017. By analyzing the amount in this period, patterns of instability and value increase can be observed. The instability of Bitcoin's value and its increase over time creates a hording mentality among miners and owners [13], meaning that owners would rather use other currencies for transactions and save their Bitcoins which in turn decreases circulation of Bitcoins and its usage as a currency.

3) Lost Bitcoins

Looking around on the web, many stories could be found about the loss of digital wallets stored on failed hard disks or other media. Because private keys are needed to transfer money from an account, these Bitcoins can be considered lost, forever. This phenomena also intensifies the deflation of Bitcoins. Though, users have grown more aware of their Accounts' security and safety in recent years.

In contrast to traditional currencies, which are usually dividable up to two decimal point, Bitcoins can be divided to 8 decimal points, so the loss of some Bitcoins can be covered by the smaller units' gain in value. In essence the granularity of each Bitcoin allows it a very flexible nature against value increase.

C. Opportunities

This section includes the third part of an SWOT analysis, opportunities. An opportunity consists of an entity's possible advantages in relation to its internal or external environment that help it provide its services more effectively and to a wider audience.

1) Active software development community

The open source nature of Bitcoin allows new applications and businesses be developed around it. Due to its design flexibility and openness, the Bitcoin ecosystem is thriving. This ecosystem is not necessarily controlled by Bitcoin's main developers. For example, Nakamoto simply left Bitcoin's development in 2010 but others simply continued the development.

2) Dependable savings

Many banks and trusts have proven to be unreliable. Frauds and thefts are quit common in the banking industry. Even government backed banks might go bankrupt and the government might bail them out using tax payer dollars or non-backed printed money, which in turn decreases the value of savings. Because of the clarity in accounting, non-repudiation of signatures, unchangeable transactions and impossibility of double spending, the Bitcoin model presents a good solution to the problem of trusting banks. It also increases risk for shady bankers. No Bitcoins can printed to protect them from their mistakes.

3) Decrease in transfer fees

There are online financial institutions and services that help transfer money across borders and continents. These services usually have to abide by many tax laws and regulatory requests and also usually require a fee based on the amount of money transfer. Bitcoin allows you to simply include an optional reward with your transaction, based on the size of the transaction (in kilobytes, not the value of transaction!) and how fast you want it processed. This reward will automatically be sent to the account of the transaction processor, who spends their processing power to transfer funds between accounts. A bigger reward motivates to faster transfer.

D. Threats

This section includes the forth part of an SWOT analysis, threats. A threat consists of a situation or barrier in the environment that limits an entity's success in providing its services or products.

1) Identification through IP address

One of the items that threatens user's anonymity is the availability of the IP addresses used in transactions. The IP address of the sender and also the transaction processor are available and traceable. The IP address of a person could point to their location. To counteract that, users can use anonymizing software like the Tor network.

2) Identification through the point of sale/exchange.

Imagine that you buy a book online, and pay for it by Bitcoin. You will provide a physical address for the book to be delivered to, and by that, you will lose your anonymity and also endanger the anonymity of the chain of transactions leading to you. Also, most exchanges ask for personal identification[3] during registration. This is called Identification at the point of exchange.

3) Heists and robberies

Bitcoins are usually stored in a digital fashion. This method of storage could allow for access to digital wallets by hackers. Because of that, many different and usually complex solutions are devised to store and protect Bitcoins. A basic rule of thumb is never store your wallet unencrypted and chose a strong enough password for it. Another point is not to use online

[3]M. Bajalan, Interviewee, The interworkings of ice3x.com and btcmarketx.com. [Interview]. 17 05 2017.

wallet services that ask for your private key. It is also highly recommended that you store a cold copy of your wallet, not connected to internet or local networks.

4) Hacking Online exchanges

Another rewarding target for hackers can be online Bitcoin exchanges. These Exchanges need to receive Bitcoins from their users into the exchange's account to be able to sell them to other users. These systems also cannot cold store all their wallets because they need to immediately deliver the requested Bitcoins to buyers when a cash-in request is submitted by a customer. Online exchanges have faced many heists [14]. Some of the biggest in Bitcoin history are summarized in table 1.

TABLE I. SOME OF THE GREATEST FRAUDS AND HEISTS IN BITCOIN'S ONLINE EXCHANGES

Year	Exchange Name	Amount reported stolen or lost (Normalized based on the value at the time of the heist)
2014	MtGox	$400 Million
2013	Sheep Marketplace	$100 Million
2015	Evolution Marketplace	$12 Million
2014	Cryptsy	$6 Million
2015	Bitstamp	$5 Million

5) Possible usage in criminal scenarios

As stated, Bitcoin can deliver a high level of anonymity, especially if it is used in virtual and online services or anonymity is only important to the seller. That is how some illegal services and goods are sold on some websites. Narcotics, guns, illegal drugs and even hiring mercenaries are a few examples available on the web, especially on the Tor anonymity network, sometimes called the DarkNet. Another use of Bitcoin is money laundering and uninterrupted, simple, unregulated and illegal money transfers through financial borders. This has forced national financial institutions to respond. At the time of writing, laws are instated in China, Mexico and India to restrict access to Bitcoins and countries like Bolivia and Ecuador have completely banned the trading of Bitcoins. Bigger economies like the EU, the US and Russia have taken steps to legalize and regulate Bitcoins.

6) Volatility of Bitcoin Value

The exchange rate of a Bitcoin is highly dependent on the volume of transactions. As there is no central entity regulating Bitcoin, the only factor that affects the price is supply and demand. This means that hording or other environmental events can highly affect Bitcoin price. The bubble burst of 2014 Bitcoin price, following the MtGox exchange closing is one example. Another more tangible example is the price increase of May 2017 from 1300$ to 2300$. This was due to the widespread ransomware infection, WannaCry, which asked for Bitcoins to decrypt each victim computer, effectively multiplying Bitcoin demand.

IV. CONCLUSION AND THE FUTURE OF BITCOIN

In this paper, we presented an SWOT analysis on Bitcoin which is summarized in fig 3.

It appears that aside from its strengths and opportunities, Bitcoin has weaknesses which create doubt in its target users' minds. Bitcoin's openness has provided Bitcoin with great opportunities and anonymity is a double edged sword, both creating threats and opportunities.

Looking at the fluctuations in Bitcoin's price brings us to the conclusion that three main factors affect Bitcoin circulation and price. The first which is probably less effective, has been a matter of technological advances and understanding and people's openness to them. The second one is the intervention of governments and financial powers by creating laws which

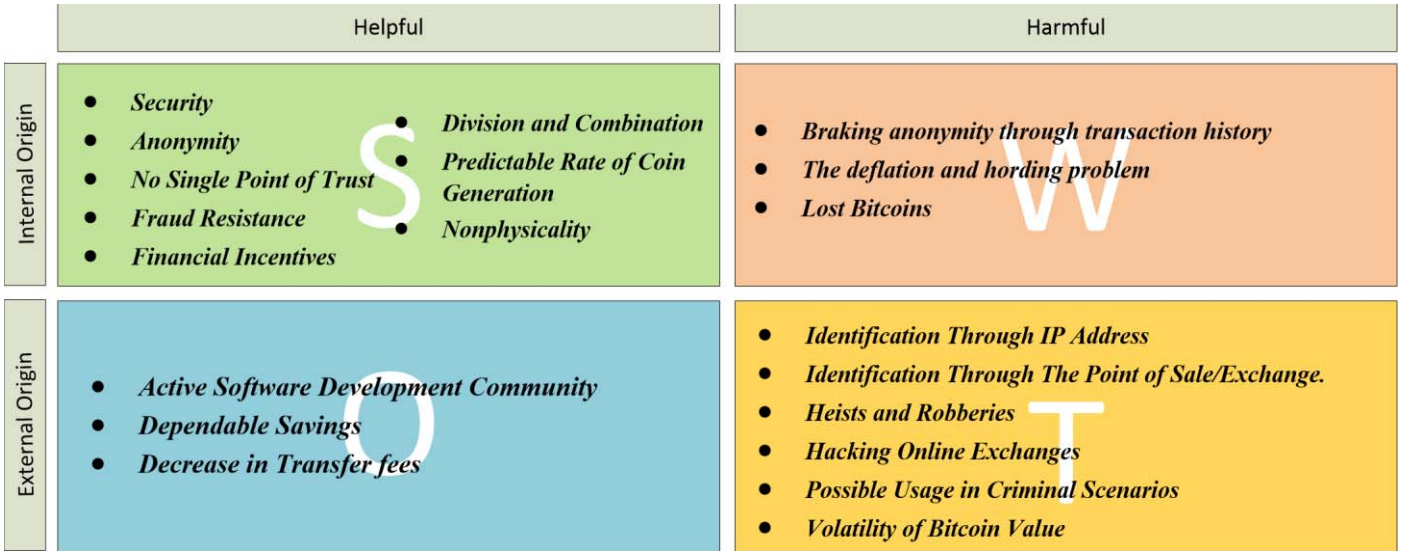

Fig. 3. Bitcoin an SWOT analysis

has had a bigger effect on Bitcoin's maturity and roadmap. This trend is set to continue as new governments study and create laws around crypto currencies. The third could be external events that are closely tied to the Bitcoin community, examples of which were given before.

The future of Bitcoin is bound by how the world reacts to it and how it affects the world. Whether or not, Bitcoin can fulfill its creators' dreams, the technological path and breakthrough seem important enough to be studied in detail and laws and regulation be devised as needed. There are numerous projects working on alternate virtual currencies that are collectively called altcoins[15]. For example, Zerocoin is an expansion on Bitcoin focusing on the anonymity and security of transactions[16].

In the current exchange and trading environment, Litecoin is the current runner up in terms of popularity. Mining lite coins is far easier than Bitcoins and each batch of transaction are processed in approximately 2.5 minutes compared to Bitcoin's 10 minutes. It is claimed that the main difference between Bitcoin and Litecoin is the amount of system memory involved which makes hacking Litecoin transaction history very hard and pricy[15].

Although methods to improve the scalability and creating inflation in Bitcoins have been researched but most current research has focused on users' anonymity in the system. This might be because anonymity is perceived to be most important competitive advantage of Bitcoin and advantages like the decrease in exchange rate are less interesting to scholars. This paper focused on the analysis of Bitcoin, without going into details of the technology behind it, the Blockchain. We believe that the Blockchain requires a separate analysis, because it can provide broader services other than Bitcoin, like smart contracts, licensing and copyright registration[17].

REFERENCES

[1] S. Nakamoto. (2008, 02.02). Bitcoin: A peer-to-peer electronic cash system.

[2] B. Maurer, T. C. Nelms, and L. Swartz, "When perhaps the real problem is money itself!": the practical materiality of Bitcoin, Social Semiotics, vol. 23, pp. 261-277, 2013

[3] D. Bryans, "Bitcoin and money laundering: mining for an effective solution" Indiana Law Journal, vol. 89, p. 441, 2014.

[4] G. J. Kim, "A SWOT analysis of the field of virtual reality rehabilitation and therapy" Presence: Tele operators and Virtual Environments, vol. 14, pp. 119-146, 2005.

[5] G. Hay and G. Castilla, "Object-based image analysis: strengths, weaknesses, opportunities and threats (SWOT) " in Proceedings of the 1st International Conference on Object-based Image Analysis (OBIA), Salzburg University, Austria, 2006, pp. 4-5.

[6] R. Grinberg, "Bitcoin: An innovative alternative digital currency," Hastings Science & Technology Law Journal, Vol. 4, p.160, 2011.

[7] European Central Bank, "Virtual Currency Schemes", 2012.

[8] J. Fletcher, "Currency in Transition: An Ethnographic Inquiry of Bitcoin Adherents" Master Thesis, University of Central Florida, College of Sciences, 2013.

[9] F. Reid and M. Harrigan, "An analysis of anonymity in the bitcoin system," book section in Security and privacy in social networks, ed: Springer, pp. 197-223, 2013.

[10] S. Barber, X. Boyen, E. Shi, and E. Uzun, "Bitter to better—how to make bitcoin a better currency," in proceedings of International Conference on Financial Cryptography and Data Security, 2012, pp. 399-414.

[11] G. Ahearne, J. Gagnon, J. Haltmaier, S. B. Kamin, C. J. Erceg, J. Faust, et al., "Preventing deflation: lessons from Japan's experience in the 1990s" (June 2002). FRB International Finance Discussion Paper No. 729.

[12] D. Ron and A. Shamir, "Quantitative analysis of the full bitcoin transaction graph" in proceedings of International Conference on Financial Cryptography and Data Security, 2013, pp. 6-24.

[13] S. Vassiliadis, P. Papadopoulos, M. Rangoussi, T. Konieczny, and J. Gralewski, "bitcoin value analysis based on cross-correlations," Journal of Internet Banking and Commerce, vol. 22, p. 1, 2017.

[14] List of Bitcoin Heists, Online source (access date 26 May 2017).Available: https://bitcointalk.org/index.php?topic=83794.0

[15] S. Ahamad, M. Nair, and B. Varghese, "A survey on crypto currencies," in proceedings of 4th International Conference on Advances in Computer Science, AETACS, 2013, pp. 42-48.

[16] Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed e-cash from bitcoin," in 2013 IEEE Symposium on Security and Privacy (SP), 2013, pp. 397-411.

[17] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where Is Current Research on Blockchain Technology?—A Systematic Review," PloS one, vol. 11, p. e0163477, 2016.