2015

# The Bitcoin Phenomenon Analysis

Boris Tomaš
*Faculty of Organization and Informatics, Croatia*, Boris.Tomas@foi.hr

Ivan Švogor
*Faculty of Organization and Informatics, Croatia*, ivan.svogor@foi.hr

**28th Bled eConference**

**#eWellBeing**

June 7 - 105, 2015; Bled, Slovenia

# The Bitcoin Phenomenon Analysis

**Boris Tomaš**

Faculty of Organization and Informatics, Croatia

boris.tomas©foi.hr

**Ivan Švogor**

Faculty of Organization and Informatics, Croatia

ivan.svogor@foi.hr

**Abstract**

*Bitcoin, the latest Internet phenomenon branded as a game-changer. It is a revolution in financial system and money creation mechanics which currently holds the market of almost 13 billion USD. At the same time, its inner working is presented as hard to understand but perfectly trustworthy and safe. This trust is what gives Bitcoin value, however due to its mystical creator and recent headlines with negative connotation, what to really make of it? - In this paper we try to explain the Bitcoin and present the latest related research to provide a discussion ab out its potential impact on economy, financial world and society.*

**Keywords:** Bitcoin, economy, cryptocurrency, digital money, society

## 1 Introduction

Very recently a new online phenomenon came to a focus in the form of digital currency. Among others, the best known one is Bitcoin. Since its appearance in 2009 it has been a source of controversy and myths, but recently, there has been a campaign to popularize it and brand it as a state of the art, mathematics-security game changer in a world of finance. In this paper we will explain the mysterious Bitcoin phenomenon circumventing oversimplified explanations of it, address the state of the art and infer some social implications of its applications.

## 2 Bitcoin - a crash course

Although one can find a lot of papers about Bitcoin, in this section we will briefly present the most important facts about how its inner workings.

## 2.1 What is really a Bitcoin?

Bitcoin refers to two things. First, Bitcoin is a currency like a *dollar*, *euro*, *yen*, etc. with a smaller called *satoshi* which represents 1 billionth of a single bitcoin value ($10^{-9}$). The second meaning, more accurate one, referees to Bitcoin as a name for the pseudo-anonymous, peer-to-peer currency protocol (Hobson, 2013).

In reality, Bitcoin is a number created out of nothing, and its value is given by the Bitcoin protocol, or even more so by the trust of its users. It has been designed by unknown individual who calls himself Satoshi Nakamoto. In his paper (Nakamoto, 2008) Nakamoto described Bitcoin as a peer-to-peer electronic cash system.

## 2.2 Typical transaction and Bitcoin creation

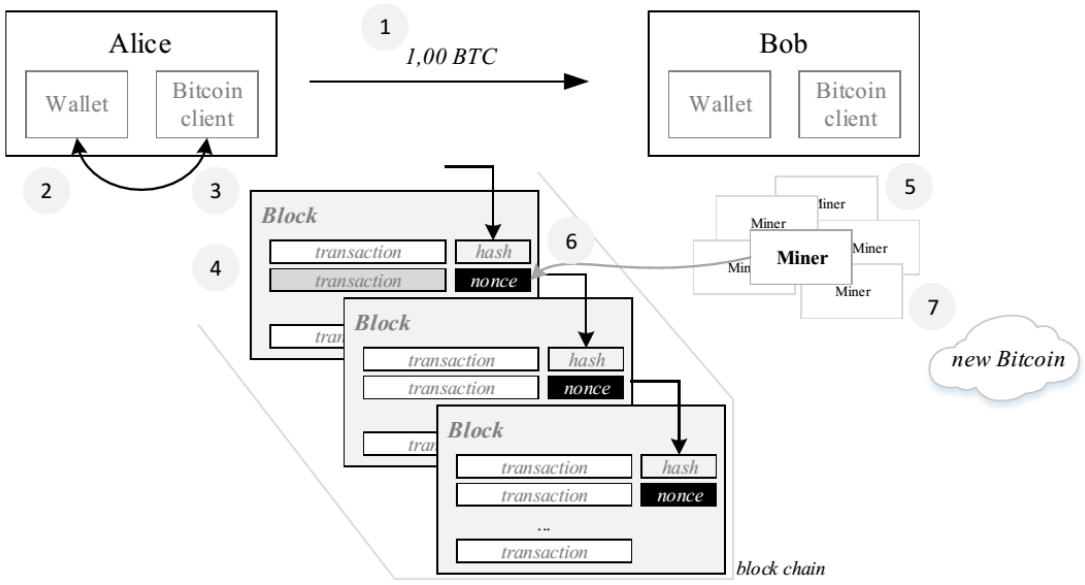


**Figure 1:** Typical Bitcoin transaction

A typical Bitcoin transaction involves 3 parties: a) sender (in Figure 1 Alice), b) receiver (in Figure 1 Bob) and c) Bitcoin miners. Additionally there are two more; *Bitcoin exchange* and *Bitcoin developers*, however for this example they are irrelevant. In the Bitcoin network, both Alice and Bob have their addresses which represent their account numbers. Each address, as a bank account does, has a balance (in Bitcoins). Alice and Bob can have multiple addresses and instead of remembering them, they use a software called a *Bitcoin wallet*. It uses a public key cryptography, and for every address it generates an appropriate private key pair (Nechvatal, 1991). Let us consider a transaction depicted in Figure 1, where Alice sends 1 Bitcoin to Bob (1). To do so, Alice uses a Bitcoin client software to create a transaction. Using the private key from Alice's Bitcoin wallet (2), Bitcoin client signs the transaction request (3). Using Alice's public key, anyone on the Bitcoin network can verify its authenticity. Alice's transaction, along with other transactions on the Bitcoin network are bundled together in something known as Bitcoin block (4). The transaction is now verified by Bitcoin miners (5). In order for a block to be recorded in the Bitcoin network, miners need to provide the *proof of work* (6). Once proof of work is confirmed, block is added to a

*block chain* which is a list of all confirmed blocks in a Bitcoin network. Each block contains the address of a previous block, thus forming single chain. A process of adding a block (also known as: completing a block) to a block chain is called *Bitcoin mining*. In Bitcoin protocol proof of work is called *nonce*, i.e. a 32-bit number. When the block is hashed a nonce with a specific lead of zeros must be found and be confirmed by more than 50% of the network. Miner, who has found the nonce is rewarded with newly minted Bitcoins (currently 25BTC) (7). Finding such nonce is tremendously difficult for individual find so Bitcoin users join to mining groups called a *mining pools*.

# 3 Related work – state of the art

In this section we present related work in the academic community regarding the Bitcoin. For this purpose we browsed the following bibliographic databases: *Springer, Web of Science, Scopus, Science direct, IEEE Xplore* and *ACM Digital Library*. The best papers we found for this overview were categorized in seven topics:

- *Introductory papers* - reporting general remarks about Bitcoin
- *Analytical papers* - investigating some aspect of Bitcoin in detail and presenting results
- *Anonymity papers* - reporting on the issues, benefits and improvements of anonymity
- *Economic papers* - investigating and reporting economic implications of Bitcoin and its market influence
- *Improvement suggestion papers* - suggesting an improvement of some aspect of Bitcoin
- *Mining papers* - reporting on technical challenges of mining
- *Bitcoin issues papers* - presenting weaknesses and drawbacks of BitcoinAuthors' Information

## 3.1 Introductory papers

Most of the introductory papers about Bitcoins are popular articles in magazines or featured articles in scholarly journals. However, most of these papers present only a partial and simplified image of a Bitcoin. Also, depending the background of the author, focus is on different aspects of Bitcoin.

In his paper (Hobson, 2013), Hobson explains the nature and proof of concept of Bitcoin virtual currency. While author pinpoints several weaknesses of Bitcoin, he presents the 51% problem as the most significant one. 51% problem refers to hash power owned by single entity. This amount of power cannot be matched with any today's supercomputer, however it can be matched by mining pools. Actually, there are some pools like *ghash.io* which are very close in reaching that number (CEX.IO Ltd., 2014). Peck presented a Bitcoin as a "Crypto-anarchist's answer to hash" (M. E. Peck, 2012). In non-bias way he presented Bitcoin as a flow of balances between peer-to-peer entities without a bank, credit card company and any other central authority. Peck also says that this is by no means a novel idea, and arguments that Timothy May and

Cyberpunks had a similar idea in 1992. Author points out that restoring of online payment privacy is a good thing but wans that it can introduce new problems such as collecting donations for political decedents or money laundering. In order to get more insight to Bitcoin we suggest some credible sources such as: (Grinberg, Primer, Ecosystem, Sustainable, & Issues, 2012; Hobson, 2013; Nakamoto, 2008; Ron & Shamir, 2013).

## 3.2 Analytical papers

In Nature Scientific Reports, Kristoufek published a great analysis of Bitcoin (Kristoufek, 2013). He presented absurd profits of people who invested in Bitcoin in beginning of 2013 when its value was 13 USD. By the end of 2013, price of a single Bitcoin went to 395 USD bringing the owners 2900% increase of investment. At the time of writing of this paper, the value is 450 USD, however, the largest was recorded in end of November of 2013 when it was 1126 USD (Coinbase, 2014). Author analyzed the phenomenon of Bitcoin and argues that such behavior cannot be explained by standard economic and financial theories, e.g. future cash-flows model, purchasing power parity, and uncovered interest rate party. Furthermore, he analyzed market entities and reports that the market is dominated by short-term investors, trend chasers, noise traders and speculators. Fundamentalist segment of the market is missing due to the fact that there is no basis for setting a fair price. It is solely driven by investors' faith in the growth. Kristoufek used user search queries on Wikipedia and Google Trends to analyze the dynamic relationship between Bitcoin price and interest in currency measured by search queries. There is a causal bidirectional relationship between prices and search terms. If prices are high, the increase of interest pushes them further to top when they are low, growth of interest pushes them deeper. This follows the pattern of bubble behavior which has been observed with Bitcoin (Kristoufek, 2013).
Kondor et. al. analyzed the Bitcoin by measuring network characteristics in function of time (Kondor, Pósfai, Csabai, & Vattay, 2014). They identified two distinct phases in the lifetime of the system: 1) when it was new and 2) when it received public attention.
In first phase this was characterized by large fluctuations in its network characteristics, heterogeneous in-degree and homogeneous out-degree distribution, and in the second phase one can see stable network measures. Ron and Shamir published a paper with quantitative analysis of Bitcoin transactions (Ron & Shamir, 2013). They used transactions carried out since the beginning of Bitcoin, up to May 2012. In the Bitcoin transaction flow graph authors discovered that most Bitcoins remain dormant, this means that they are not used, but simply stored on a wallet for safe keeping. Most Bitcoins (55% of total volume) are not circulating in the system.

## 3.3 Anonymity papers

Due to its anonymity properties Reid and Harrigan see a Bitcoin as an alternative to cash (Reid & Harrigan, 2011). According to them cash still has competitive advantage in anonymity of payment, however, Bitcoin seems like an alternative. Authors actually found that using the appropriate network representation, it is possible to associate public-keys with identifying information. Also, large centralized services such as exchange markets and online wallets are capable of identifying and tracking user activity. Bitcoin community says that anonymity is not a prominent design goal, however users should be aware when sending Bitcoins to organizations they would

prefer not to be publicly associated with. Peck has been able to identify several key entities in the Bitcoin economy: markets, mining pools, stores, gaming sites, and many more (M. Peck, 2013). Some papers in this group are not directly related to Bitcoin, however they present an anonymity aspect. One of them analyses drug dealing site called Silk Road inside Deep Web and paying options with anonymous currency – Bitcoin (Van Hout & Bingham, 2014). Authors have shown that cash replacement for Bitcoin is actually being valid, valuable and reliable digital currency in the case of Silk Road. Since Bitcoin is actually pseudo-anonymous, Miers et.al. proposed a solution to this issue, with the Zerocoin, i.e. a Bitcoin extension (Miers, Garman, Green, & Rubin, 2013). However, accepting changes in existing environment could cause some issues, but since it has been done before without larger consequences, it is up to the community to decide.

## 3.4 Economic papers

Due to its anonymity features Bitcoin is prone for money laundering. Bryans analyzed the Bitcoin network form an economic viewpoint focusing on legal issues (Bryans, 2014). He identified that a typical transaction involves 5 parties. 1) sender (e.g. dirty money), 2) receiver (launderer which obfuscates the source), 3) Bitcoin miners which act as transaction verifiers by completing a block, 4) development team which updates codebase, 5) currency exchange. Bryans asked the question, which party should carry the legal responsibility when a breakdown occurs (money laundering, theft, fraud, etc.), and therefore whom to regulate? It is hard to regulate a sender due to pseudo-anonymity and dispersed nature of identities on the Bitcoin network. The same applies to the receiver and miners. Perusing them would be inefficient and detrimental. Miners act as payment processors with no real interest other than small (and non-obligatory) fee, and in the most cases they are unaware of the nature of transaction. Also, mining is done by a software without any intervention of people. Bitcoin developer team has hardly any actual input on the individual transactions and they act more like a standards agency rather than central authority. Finally, we reach currency exchanges. Bryans concludes that because exchanges deal with fiat currency, they will more likely fall under money exchange laws which define money as currency backed by government. Regulation of such currencies should occur at point where law enforcement can most effectively punish civil and criminal violators with the least overhead. Since Bitcoin is decentralized it makes little sense to regulate others than Bitcoin currency exchanges. In fact, some exchanges showed interest by registering as MSBs under AML schemes. Author suggests that instead of predicting regulations for next generation of disruptive technology like Bitcoin, we need to understand current ones better, and police the points of public contact with existing legal schemes.

Although the idea of digital currency exists for a while, they never cough on. Barber et.al. analyses the success of Bitcoin and reported that despite no fancy cryptography features, it is “ingenious and sophisticated” but not perfect (Barber, Boyen, Shi, & Uzun, 2012). There are several advantages of Bitcoin over its predecessors: a) Bitcoin ecosystem ensures that users have economic incentive to participate by mining the coins, b) coin generation has an exponential rate which enables predictable money supply, c) it is distributed which is appealing due to is ease of dividing, d) although it is a e-cash system, denominations are possible, e) it is open and flexible, f) transactions are irreversible, g) fees are low and h) implementations exist. But there are also

imperfections such as: a) Zombie coins[1], b) deflationary spiral, c) history-revision attack[2], d) countering revisionism by checking the past. They conclude the following: ”While instantiation is impaired by its poor parameters, the core design could support a robust decentralized currency if done right” (Barber et al., 2012).
Yermack reports that proper currency functions as medium of exchange, unit of account and sore of value. Bitcoin has first two functions but lack function to store value. This is mainly because Bitcoin volatile nature. Traditional currencies have institutional stability and security, deposit insurance and international treaties. Bitcoin lacks such instruments. If Bitcoins are widely used then controlled inflation will not be sufficient and effects of deflation may arise. This could lead to political protests like one happened in U.S during Populist movement at the end of 19th century. (Yermack, 2013)

## 3.5 Improvement suggestion papers

Decker and Wattenhofer analyzed how information in the Bitcoin network is disseminated in order to synchronize the ledger replicates (Decker & Wattenhofer, 2013). They report that reliance on blocks delays clearing of transactions and poses a threat. An example of this are larger blocks which are propagated slower. This causes a Blockchain fork[3]. Authors implemented changes in Bitcoin protocol which reduces a risk of Blockchain fork by 50%. Babaioff et. al. studied a scenario in which all the nodes that become aware of the information compete for the same prize, have incentive not to propagate the information (Babaioff, Dobzinski, Oren, & Zohar, 2011). This is related to false identities where one would keep the information about any transaction that offers a fee for itself as other nodes compete to authorize it and claim the associated fee. This would be the problem when payment to the nodes is slowly phased out and Bitcoin owners who want their transactions approved would pay a fee to authorizing nodes. Authors propose a novel rewarding scheme in Bitcoin mining and propose a novel low cost reward scheme that incentivizes information propagation and is Sybil proof.
Clark and Essex presented the problem with proof of work which Bitcoin network uses to generate a block. Since it is costly and time consuming it limits the rate at which new blocks can be generated. Authors argue that employing a proof of work protocol as commitment time will later allow anyone to ”carbon date” when the commitment was made, approximately without trusting any external party. Authors present *commitcoin*, an instantiation of this approach which harnesses the existing computing power of Bitcoin network to mint and trade digital cash. With their approach users do not need to trust the timestamps or any node in the network, and proof of work would itself be used to carbon date the transaction. (J Clark & Essex, 2012)

## 3.6 Mining papers

Bitcoin mining is not the focus of many scientific publications. We suspect that this is because all the algorithms are well known, and from the computational viewpoint it is just the matter of making mining faster, i.e. engineering better chips (ASIC, FPGA,

1 Bitcoins which are lost cause reduction of available supply
2 When incentive to mine will diminish, then, the computers will become stronger and revision attack will be easier
3 A time when nodes in the network don’t agree on which block, in current Blockchain, is the head

CPU, GPU, etc.). In his publication Taylor presented a review of advantages and disadvantages of Bitcoin mining hardware (Taylor, 2013). It is proven that Bitcoin, using existing hardware, on a small scale is inefficient. This is the basis of the protocol of value creation mechanism. Over time mining will become completely inefficient and will reside on transaction fee which is going to grow as Bitcoin transaction volume grows. Next big thing in mining technology would the application of quantum computers, which will do computing several orders of magnitude faster and efficient. Unfortunately, use of quantum computer will probably endanger core of Bitcoin currency, so its appearance should result in changes of Bitcoin protocols.

## 3.7 Bitcoin issues papers

Bitcoin supporters often use mathematics to argument the validity of Bitcoin idea. It is said that mathematics has trust embedded into it and since the mathematical proofs which back up Bitcoin is irrefutable. It presents trust unlike one tied to present day banking system. In his report, Bradbury presents this idea of a solid currency however issues are also mentioned; stealing identities, double spending, dust transactions etc. (Bradbury, 2013). Here are several large incidents related to Bitcoins.

Sheep Marketplace has been closed following the theft of millions of dollars' worth of Bitcoins. Article reports it as one of biggest cybercrime heists in history. Also, there was another heist in Denmark BIPS using DDoS and a similar one in Australia (1m BTC - 1295), Inputs.io (1.2m BTC - 4100). In Germany, hackers used Botnets to mine 700.000 BTC, while in US E-Sports Entertainments reported that their anti-cheating software for online gaming has been used to mine. A hacker made added some mining code which was distributed among gamers, making him 4.000,00 USD (Computer Fraud & Security, December, 2013).

Analyzing Bitcoin exchange markets volume and characteristics has proven that high volume markets are more often hacked and targeted for fraud (Moore & Christin, 2013). Moore and Christin investigated this issue and found that low level markets are irrelevant for malicious actions, however, it is proven that trading on high volume markets is safer because foul action will be easier to detect. Authors claim that high volume markets have lower probability of crashing. However, crash of MtGox in 2014 obviously proves them wrong (Moore & Christin, 2013). Finally, one issue with Bitcoin is the botnet exploit, which first occurred in 2010. Bitcoin mining feature was used using multiple Bitcoins addresses and mining pools, but due to Bitcoin pseudo-anonymous nature it is hard to reveal identity of botnet creators. It is notable that existence of botnet Bitcoin miners is not the issue of Bitcoin system rather the standard issue of computer security. More on this topic can be found in a paper by Plohmann and Gerhards-Padilla (Plohmann & Gerhards-Padilla, 2012).

# 4 Discussion

Bitcoin is a product of computer science, i.e. cryptography, and as such represents the latest achievement. However, it is expected that some changes to the Bitcoin will occur in future as they occurred several times in history (bitcoin, n.d.). Bitcoin is by no means perfect and like any trail entity it needs to go through some changes in order to evolve. Changing the Bitcoin is not easy because it is decentralized and open source. This means that everyone can contribute to the Bitcoin, but changes will not come to place until the community (users) accepts them. This is the problem, since the user chooses

weather to update or not it is likely that one point there will be two Bitcoin networks. Process of updating peer-to-peer network is security critical and has to be carried out carefully.

**Bitcoin and inflation**

Bitcoin has implemented inflation and it is called Controlled supply[4]. It states that by the end of 2140 there will be not more than 21 million of Bitcoins. Current Bitcoin value is around 450 USD which means that all 21 million of Bitcoins would be worth 9 $.45 * 10^9$ USD. Current USA money supply in circulation is around $1.05 * 10^{13}$ USD, i.e 10.5 trillion USD (Josh and Clark & Whitbourne, 2013). Imagining that USA swap USD for BTC it would mean that Bitcoin should be worth 1100 times more nearing 500.000,00 USD for 1 BTC, assuming that current demand comes only from USA. So, 1 USD beverage would cost 0,000.002 BTC. This is only for USA, considering rest of the world in this thought experiment would make this fraction several magnitudes smaller which is quite impractical for everyday use. Although, Bitcoin network can handle such small quantities, impression can be made that the creator of Bitcoin did not had global coverage in mind, i.e. to have one global currency which will replace all national currencies. Moreover, the implemented inflation is not ”true inflation”. It is simply controlled money supply with finite number of units. Bitcoins will get lost or forgotten, and no new Bitcoins can be produced. So, the value of Bitcoin will rise even more, over time. Many of those issues simply prove that Bitcoin is just the first attempt for ubiquitous and global currency. It would be wise to wait see other, alternative cryptocurrencies (Luther, 2013) that have different characteristics. There are several interesting alternative cryptocurrencies such as the one with only 42 coins minted[5], or Doge coin which is available in unlimited volume. Bitcoin can be observed as unifying currency like Euro. Introducing Euro to the euro-zone took several years of preparation and lots of political good will. Although practical, some countries like UK still won’t join euro-zone due to political and economic interests (Mulhearn & Vane, 2005). Current state of politics is such that it will try to prevent any loss of power over money (currency) because implicitly money is power. This is also why some countries oppose Euro. Bitcoin is decentralized and under no authority in the world.

4 en.bitcoin.it/wiki/Controlled supply

5 www.42coin.org

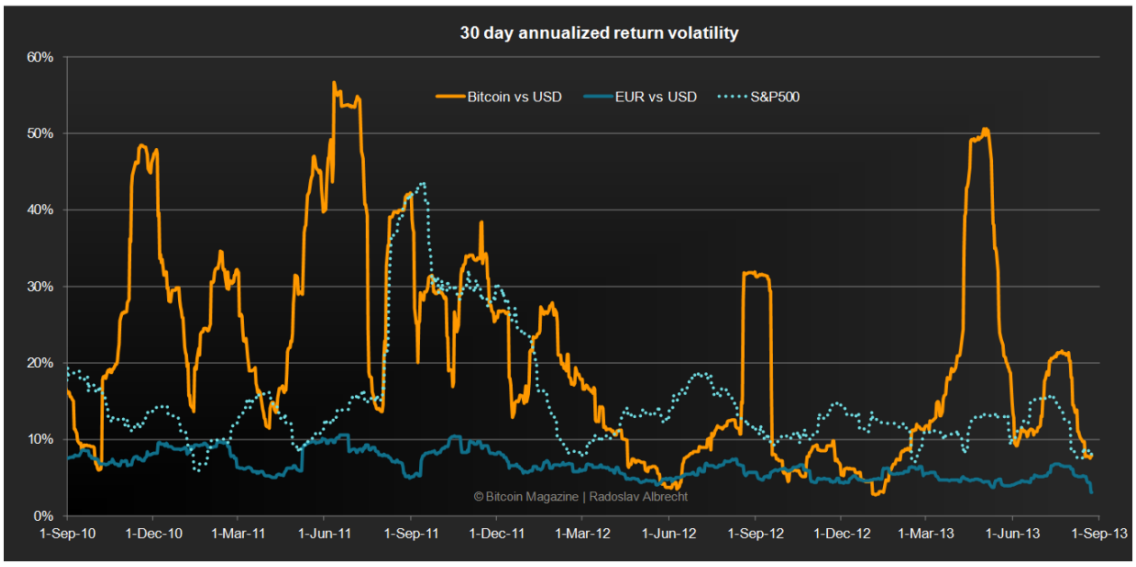


**Figure 2** Bitcoin volatility (Albrecht, n.d.)

**Bitcoin in the world**

Due to limited inflation Bitcoin price depends only on supply and demand. If more people need Bitcon value of it will rise. Consider a scenario in which there are enough Bitcoins and is used worldwide. It would be expected that Bitcoin in one country has greater value than Bitcoin in other country. Earning wages would produce Bitcoins for individual, and he/she would possess a value which is greater in developed country due to greater labor value. In undeveloped countries prices would be lower because of low labor value. Although Bitcoin is decentralized the market which defines Bitcoin value, is not. This means that Bitcoin has different values in different countries, which might lead to social, economic and political instability. If we assume that market is decentralized and everyone has the same opportunities to earn and spend money, then all people would be equal, which often defined as a desirable society by Utopian socialists (Mises, 1994).

Value of Bitcon can be controlled by country using taxes and social policy. In a country with higher taxes one Bitcoin would be worth less because value added tax (VAT) would consume large part of Bitcoin value. So, there is mechanism to change or control the value of Bitcoin; this means that powerful countries will be able to influence the value of Bitcoin. There is a danger that first large country that accepts Bitcoin will tie Bitcoin to its economy.

**Bitcoin volatility**

Being a newborn currency, Bitcoin on Figure 2 one can notice it is very volatile. According to Albrecht (Albrecht, n.d.), Bitcoin volatility is declining, slowly but steadily. Albrecht also concludes that Bitcoin behaves more like an asset rather than currency. Over time, volatility will settle with more acceptance of Bitcoin as valid currency. Unfortunately this behavior is circular, meaning that volatility will decline if more people accept it, and people will accept it more if it is less volatile.

**Bitcoin vs. other currencies**

Bitcoin is not the first digital currency; currently, digital currency is a currency stored on our bank accounts and it can be used digitally using Internet banking systems. This process is safe, centralized, non-anonymous and fast. Table I shows the comparison

between different types of currencies: Digital currency, Bitcoin and paper money. Currency characteristic used to compare are:

- *Volatile*: states the currency volatility.
- *Anonymous*: defines anonymity of the currency. Currency is anonymous if *transaction* source and destination cannot be linked to physical person or any other entity.
- *Centralized*: currency is centralized if it is monitored and governed by central institution like Central Bank or government.
- *Secure*: is currency theft and fraud secure?
- *Offline*: can currency be used without Internet connection?

Selection of characteristics used is based on a previous research papers, identified in this work, that pinpoint key features and weaknesses of cryptocurrency comparing to real currency.

| Characteristic | Digital currency | Bitcoin | Paper money |
|---|---|---|---|
| Volatile | No | Yes | No |
| Anonymous | No | Yes (Maybe)6 | Yes |
| Centralized | Yes | No | Yes |
| Secure | Yes | Yes (Maybe)7 | Maybe8 |
| Offline | No | No (Maybe)9 | Yes |

**Table 1: Summary** comparison of different currency types

## 4.1 Conclusion

This paper presented facts about Bitcoin and current research about its influence in order to clarify some of the reasons for its popularity. It is pinpointed that Bitcoin is noteworthy idea which has great economic and social potential, however there are some issues that may delay adoption of this digital currency and postpone the revolution it promised. By design, Bitcoin is decentralized and cannot be controlled - due to this feature it is not politically friendly, hence there is huge effort among large economies (China, USA, Russia, etc.) to slow down Bitcoin. Even though, every day more and more merchants accept Bitcoin as legal payment option. The future is still to show what it holds for Bitcoin.

6 In this paper it has been noted that Bitcoin is not completely anonymous.
7 There has been several security incidents.
8 Paper money has been tried to be copied constantly.
9 There are attempts to make offline version of Bitcoin: www.casascius.com

**References**

Albrecht, R. (n.d.). Bitcoin Volatility – The 4 perspectives. Retrieved from http://bitcoinmagazine.com/6543/bitcoin-volatility-analysis/

Babaioff, M., Dobzinski, S., Oren, S., & Zohar, A. (2011). On Bitcoin and red balloons. *ACM SIGecom Exchanges*, *10*(3), 5–9. doi:10.1145/2325702.2325704

Barber, S., Boyen, X., Shi, E., & Uzun, E. (2012). Bitter to better—how to make bitcoin a better currency. *Financial Cryptography and Data …*, 399–414. Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-32946-3_29

bitcoin. (n.d.). Bitcoin version history. Retrieved from https://bitcoin.org/en/version-history

Bradbury, D. (2013). The problem with Bitcoin. *Computer Fraud & Security*, *2013*(11), 5–8. doi:10.1016/S1361-3723(13)70101-5

Bryans, D. (2014). Bitcoin and Money Laundering: Mining for an Effective Solution. *Indiana Law Journal*. Retrieved from http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=11100&context=ilj

CEX.IO Ltd. (2014). Crypto and Bitcoin Mining Pool. Retrieved from https://ghash.io/

Clark, J. and, & Whitbourne, K. (2013). How much actual money is there in the world? Retrieved from http://money.howstuffworks.com/how-much-money-is-in-the-world.htm

Clark, J., & Essex, A. (2012). CommitCoin: carbon dating commitments with Bitcoin. *Financial Cryptography and Data Security*, 390–398. Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-32946-3_28

Coinbase. (2014). Bitcoin Wallet - Coinbase. Retrieved from https://coinbase.com/charts

December, I. (2013). Massive Bitcoin thefts and seizures leave many users nervous and poorer. *Computer Fraud & Security*, *2013*(12), 1–3. doi:10.1016/S1361-3723(13)70106-4

Decker, C., & Wattenhofer, R. (2013). Information propagation in the bitcoin network. *Peer-to-Peer Computing (P2P), …*. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6688704

Grinberg, R., Primer, B., Ecosystem, B., Sustainable, I. B., & Issues, L. (2012). Bitcoin: an innovative alternative digital currency. *Hastings Sci. & Tech. LJ*, 50. Retrieved from http://heinonlinebackup.com/hol-cgi-

bin/get_pdf.cgi?handle=hein.journals/hascietlj4&section=6\nhttp://papers.ssrn.com/sol3/papers.cfm?abstract_id=1817857

Hobson, D. (2013). What is Bitcoin? *XRDS: Crossroads, The ACM Magazine for Students*, *20*(1), 40. doi:10.1145/2510124

Kim, G. (2014). New Virtual Currency Bitcoin Its Past, Present, and Future.

Kondor, D., Pósfai, M., Csabai, I., & Vattay, G. (2014). Do the rich get richer? An empirical analysis of the Bitcoin transaction network. *PloS One*, *9*(2), e86197. doi:10.1371/journal.pone.0086197

Kristoufek, L. (2013). BitCoin meets Google Trends and Wikipedia: quantifying the relationship between phenomena of the Internet era. *Scientific Reports*, *3*, 3415. doi:10.1038/srep03415

Luther, W. (2013). Cryptocurrencies, Network Effects, and Switching Costs. *Mercatus Center*, 37. doi:10.2139/ssrn.2295134

Martins, C. S., & Yang, Y. (n.d.). Introduction to Bitcoins : A pseudo-anonymous electronic currency system Theme : Abstract : Integrated Solution : Smarter Commerce, 349–350.

Miers, I., Garman, C., Green, M., & Rubin, A. D. (2013). Zerocoin: Anonymous Distributed E-Cash from Bitcoin. *2013 IEEE Symposium on Security and Privacy*, 397–411. doi:10.1109/SP.2013.34

Mises, L. von. (1994). Economic Calculation in the Socialist Commonwealth. In *Classics in Austrian economics: A Sampling in the History of a Tradition* (Vol. 3, pp. pp. 2–30). Retrieved from http://www.mises.org/

Moore, T., & Christin, N. (2013). Beware the middleman: Empirical analysis of Bitcoin-exchange risk. *Financial Cryptography and Data Security*, (June 2011), 25–33. Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-39884-1_3

Mulhearn, C., & Vane, H. R. (2005). The UK and the Euro: Debating the British Decision. *The World Economy*, *28*, 243–258. doi:10.1111/j.1467-9701.2005.00648.x

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *Consulted*, 1–9. doi:10.1007/s10838-008-9062-0

Nechvatal, J. (1991). *Public-key cryptography*.

Peck, M. (2013). The Bitcoin Arms Race is on! *IEEE Spectrum*, *50*(6), 11–13. doi:10.1109/MSPEC.2013.6521016

Peck, M. E. (2012). The cryptoanarchists' answer to cash. *Spectrum, IEEE*, *49*(6), 50–56.

Plohmann, D., & Gerhards-Padilla, E. (2012). Case study of the Miner Botnet. *Cyber Conflict (CYCON), …*. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6243985

Reid, F., & Harrigan, M. (2011). An Analysis of Anonymity in the Bitcoin System. *2011 IEEE Third Int'l Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third Int'l Conference on Social Computing*, 1318–1326. doi:10.1109/PASSAT/SocialCom.2011.79

Ron, D., & Shamir, A. (2013). Quantitative analysis of the full bitcoin transaction graph. *Financial Cryptography and Data Security*, 6–24. Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-39884-1_2

Taylor, M. B. (2013). Bitcoin and The Age of Bespoke Silicon How Bitcoin Works : User Perspective Bitcoin Mining : Miner ' s Perspective.

Van Hout, M. C., & Bingham, T. (2014). Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading. *The International Journal on Drug Policy*, *25*(2), 183–9. doi:10.1016/j.drugpo.2013.10.009

Yermack, D. (2013). Is Bitcoin a Real Currency?, 1–14. Retrieved from http://www.nber.org/papers/w19747