Zoran Cekerevac - Zdenek Dvorak - Ludmila Prigoda - Petar Cekerevac *

RISKS OF BITCOIN VIRTUAL CURRENCY

Bitcoin, digital money got into focus after the Mt Gox crash. It uses P2P interaction where an owner transfers the electronic coin to the next owner signing and adding a hash of the previous transaction and the public key of the next owner. Payment verification is accomplished by notifying the entire network about the transaction. This prevents double-spending and generation of non-existent money. Among the users, there is uncertainty about the safety on the theft and fraud. Among the authorities, there are dilemmas about present and future risks related to the Bitcoin implementation. The article deals with the benefits and risks of Bitcoin use.

Keywords: *Bitcoin, e-business, eWallet, fiat money, hash, P2P.*

1. Introduction

In history there were different means of payment. The U.S. dollar was the most frequently used means of paying almost fifty years after the World War II, but thanks to many problematic moves of the Federal Reserve reputation of dollar declined significantly and many began to seek alternatives [1]. To be a suitable means of payment, an asset must have some important features, such as: to remain valuable for a long time, to be in limited supply, to be easily divisible into parts, to be portable ... If these characteristics are compared to the dollar, gold (silver) and bitcoin, one can get the results shown in Table 1.

Payments through financial institutions are associated with numerous limitations and include relatively high costs whose amount is measured in percentage. Thus, for example, when money changes hands, significant amount remains in the banks. Because of that, and many other reasons, bitcoin[1], digital money, was created and launched in the year 2009. For Bitcoin creation Satoshi Nakamoto[2] is credited. He published the principles of its creation in the article Bitcoin: A Peer-to-Peer Electronic Cash System [2]. Bitcoin concept implies P2P interaction, and electronic coin is defined as a chain of digital signatures. Each owner transfers the coin to the next owner by signing a hash[3] of the previous transaction and the public key of the next owner, and adding it all to the end of the coin. The recipient can verify the signatures to verify the chain of ownership. Payment verification is accomplished by notifying the entire network about the transaction. This prevents double payment and avoids the generation of non-existent money. Checking may take a few minutes. Average time of transaction

Comparison of characteristics of dollars, gold (silver) and BitcoinTable 1

Characteristic			
Stays Valuable	×	✓	✓
Limited Supply	×	✓	✓
Divisible	✓	✓	✓
Portable	✓	✓	✓✓

Source: Authors modelled on FEE [1]

[1]bitcoin – written in small letter b is considered as a currency; Bitcoin – with upper case letter B capital implies Bitcoin as a concept [29].

[2]It is not yet known whether „Satoshi Nakamoto" is real name or a pseudonym [31].

[3]More information about hash can be found in [28 and 30].

* **[1]Zoran Cekerevac, [2]Zdenek Dvorak, [3]Ludmila Prigoda, [4]Petar Cekerevac**
[1]Faculty of Business & Industrial Management UNION" University in Belgrade, Serbia
[2]Research Department of Crisis Management, Faculty of Security Engineering, University of Zilina, Slovakia
[3]Maykop State Technological University, Maykop, Russia
[4]Faculty of Political Science, University of Belgrade, Serbia
E-mail: zoran@cekerevac.eu

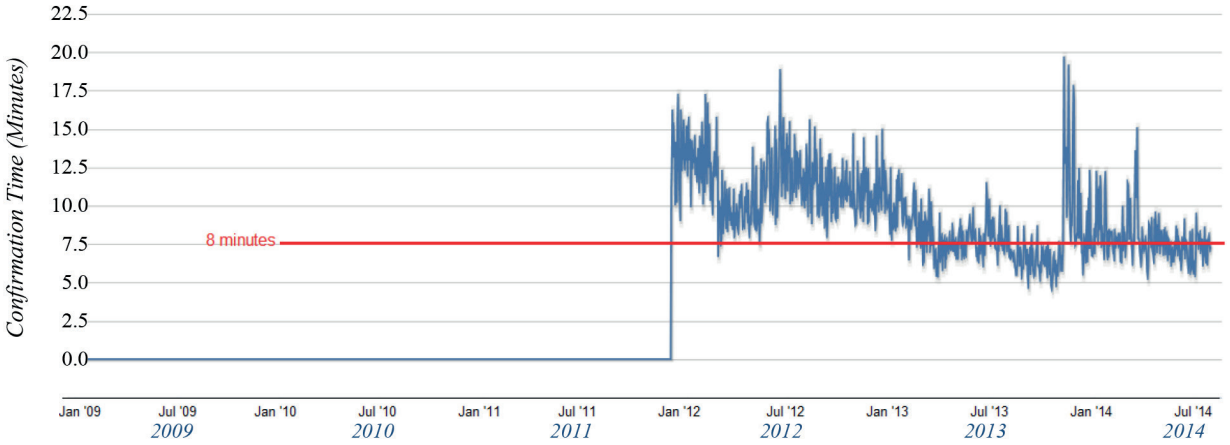

Fig. 1 Average transaction confirmation time in minutes. (Source: blockchain.info [3])

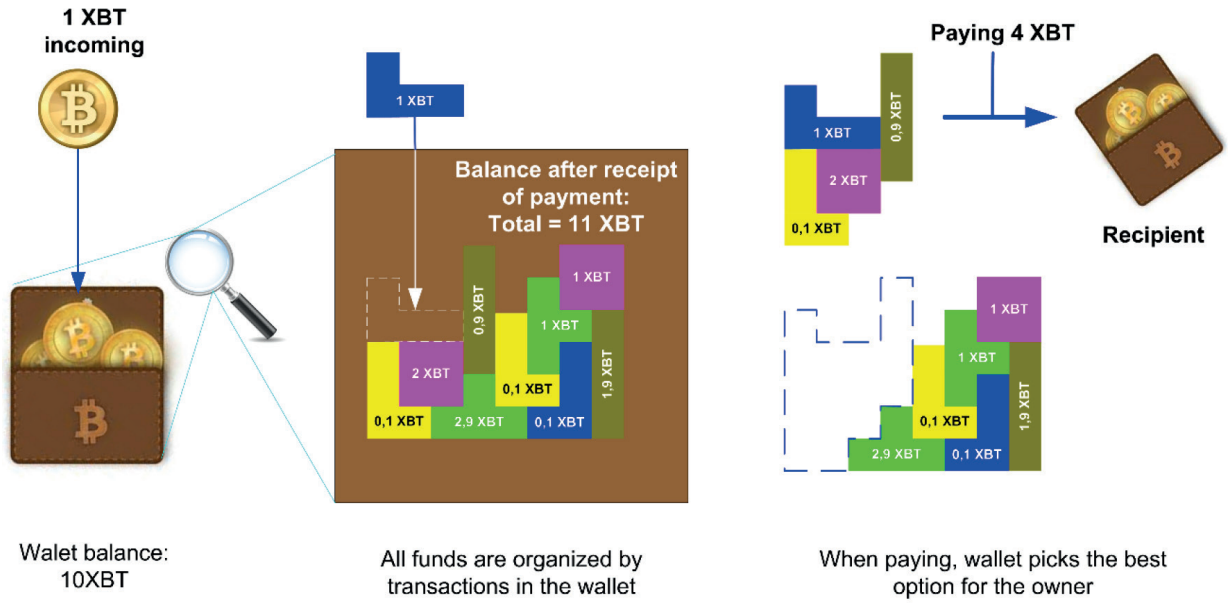

Fig. 2 Bitcoin payment technology (Source: Authors modelled on [4])

checking in 2014 was around 8 minutes. The transaction confirmation time in previous years is shown in Fig. 1.

These transactions do not transfer personal information between parties in the transaction. Unlike completely anonymous transactions, Bitcoin payment record of the transaction remains recorded and available to public. The participants in the transaction do not have to operate under their own names, but they can log in through aliases.

Bitcoin mining and payment details are discussed in [5, 6, and 7]. Figure 2 shows an example of Bitcoin payment. Some other examples of payments and the fees determining are presented in the Bitcoin Transaction Fees Explained [4]. Details on the application of Bitcoin technology are explained in R. Skudnov´s thesis: Bitcoin Clients [8].

2. Benefits and risks of using Bitcoin

2.1 Economic aspects of Bitcoin

Bitcoin offers lower transaction costs to users, increased privacy and protection of the purchasing power from inflation in the long run. However, Bitcoin still doesn't have enough participants and a financial base to ensure stability and bitcoin value considerably oscillates, as it is shown in Fig. 3 [9].

Still among the users there is uncertainty about the safety on the theft and fraud. Among the relevant state authorities, there are also numerous dilemmas and analyses of existing and future risks related to the implementation of Bitcoin. Despite all the dilemmas, many see the Bitcoin as an excellent means of payment that allows [10]:

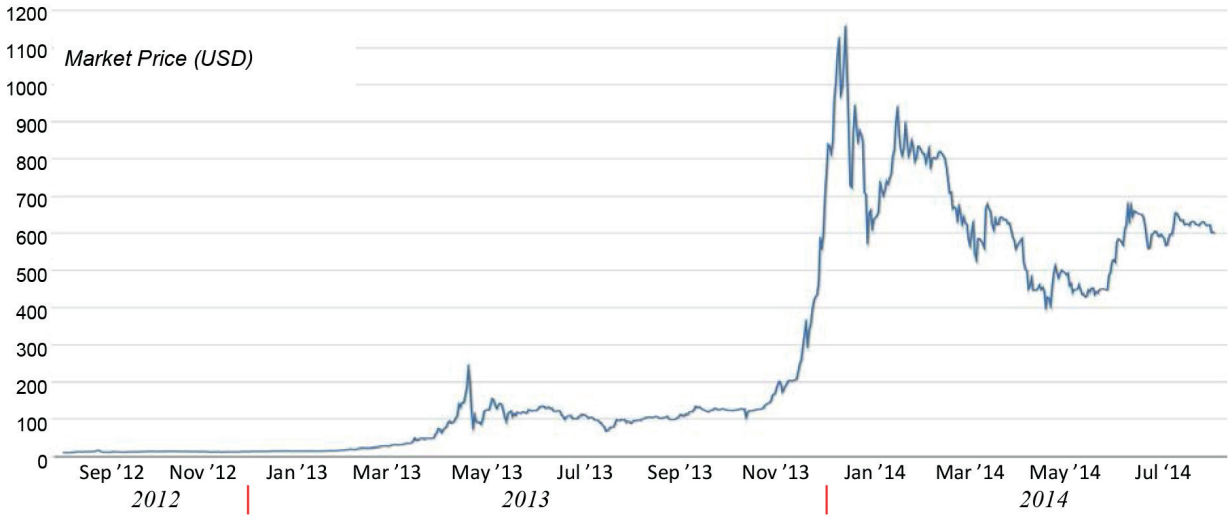

Fig. 3 XBT market price in USD Source: blockchain.info [9]

- buying anything in secret,
- absence of banks in the chain of payments,
- paying without commission,
- no worries that inflation will devalue the money in the future.

For the latter, as an example can serve the analysis of changes in the value of USD during the time. For example, if someone had 100 USD in his wallet in 1953, due to inflation, using the Consumer Price Index, today he could count with $11.48. The situation is even worse if calculation is made according to other criteria. Table 2 shows the equivalents of 100USD in comparison with 1913 and 1963.

Equivalent value of 100 USD from 1913 and 1963 in 2013 Table 2

	$100 from the year:	1913	1963
Equivalent in 2013	Using Consumer Price Index	$2,430	$761
	Using GDP deflator	$1,750	$588
	Using unskilled wage	$9,960	$817
	Using Production Worker Compensation	$14,200	$987
	Using nominal GDP per capita	$13,100	$1,570
	Using relative share of GDP	$42,500	$2,630

Source: Authors' compilation of data from MeasuringWorth.com [11]

How did it come to such a decline in the USD value? Simply! By printing money without backing. Bitcoin lets users know exactly how many bitcoins and when will be on market. Due to the applied algorithm it is known that the number of Bitcoin will asymptotically approach the figure of 21 million. From the first bitcoin launched in 2009, their number grew to 13 million in mid-July 2014 [12], and there will be 18 million (in 2024), and 21 million in 2140. After that, the number of issued bitcoin practically will not change. In this manner the second essential criterion from Table 1 is provided.

USD, silver, and gold are difficult to forge. Since the Bitcoin is based on the open source software it may seem that it is easier to falsify. However, Bitcoin is based on cryptography and it is practically impossible (or rather, unprofitable) to forge bitcoin. In addition, each transaction requires confirmation of other participants in the system, which prevents any wrongdoing of double payment.

In addition to the aforementioned benefits, there are also other benefits Bitcoin offers:

- Bitcoin can be very easily transferred from and to any point on Earth regardless of the quantity and geographic location if there is an Internet connection;
- accepting of Bitcoins is free;
- no chargeback;
- Bitcoin can be exchanged for any currency.

As a result of these advantages a favourable gradient increase in the daily number of transactions is recorded. From about 550 in January 2012, it rose to about 80,000 in January of 2014. After Mt Gox bankruptcy and disorder that was created, the number of transactions fell to about 55,000 in January 2014, but then suddenly increased to 70,000 in April, and then with oscillations fell to 60,000 in July of 2014 [13]. It can be said that it is very likely that Bitcoin will overcome the crisis caused by Mt Gox bankruptcy.

It's hard to declare some of the payment methods as the best, especially because the conditions are constantly changing, but it is likely that the Bitcoin, thanks to all its advantages will be able to take a very high position. Also, it is likely that the current dollar payment method can (will) be pushed toward the (much) lower positions [1].

2.2 Legal aspects of the risk of the use of Bitcoin

Bitcoin, due to the relative anonymity of its users, allows individuals to generate, transmit, launder and/or steal funds. Its application brings to investigators similar challenges as other virtual money, for example WebMoney, but also additional difficulties because of its decentralized nature. According to FBI estimates, with medium confidence, in the near future "cyber criminals will treat Bitcoin as another payment option alongside more traditional and established virtual currencies such as WebMoney, which they have little reason to abandon" [14]. This conclusion is based on the large bitcoin fluctuations in 2011. With the same confidence FBI believes that the Bitcoin will be used for money laundering. These assumptions are difficult to prove because there are too few reports on Bitcoin. Due to its decentralization, attacks to Bitcoin system will likely prove to have little success. Criminals will focus their attacks on private Bitcoin wallets and the third-party services.

Bitcoin transactions are public, but the only information that identifies Bitcoin user is pseudo random generated Bitcoin address that makes the transaction fairly anonymous. The transaction is not completely anonymous. Although the Bitcoin is highly decentralized, there is a place that can provide information about the participant in the payment. This is where the bitcoin is converted to fiat currency[4]. To increase the anonymity of transaction, users can [15, 16, 17, and 18]:

- create and use a new Bitcoin address for each incoming payment;
- route the entire traffic across the Bitcoin anonymisers;
- combine old Bitcoin addresses into a new address to deliver a new payment;
- use specialized services for money laundering;
- use eWallet services of third parties to consolidate their addresses. Today, there are third-party services that offer the option of creating eWallet which allows users to consolidate many Bitcoin addresses and to access simply to their bitcoins from any device;
- create Bitcoin clients and to increase anonymity easily, and to have a choice of Bitcoin addresses from which they wish to make the payment. In doing so users do not have to be particularly technically educated to make anonymous transactions.

Specifics of Bitcoin today represent a special challenge to detection and stopping of illegal activities. As a decentralized system, Bitcoin does not have a central institution and is not able to control and to report suspicious activities in accordance with the program of prevention of money laundering or to accept and enforce legal requirements, e.g. subpoenas. According to the FBI [14] the main vulnerabilities of decentralized payment systems are:

- lack of software or the ability to monitor and identify suspicious monetary pattern occurring in money laundering;
- lack of identification of the actual account holders as well as their physical location;
- absence of the history of transactions associated with the actual participants in the transaction;
- much more difficult identification of sources of funds compared to other types of online money;
- law enforcement cannot target one central location or company in investigations, or turn the system off.

As mentioned above, Bitcoin, like most virtual money, requires the user to use the services of a third party when converting Bitcoin in fiat money. Buying, selling, or bitcoin conversion to other types of money are done outside of P2P system. Due to the number and diversity of third-parties there is a real possibility of money laundering [19, 20, and 21]. Users who do not wish to use the services of third parties are given the opportunity to put their "buy" or "sell" the request on the freenode IRC (Internet relay chat) [5].

In July 2011, FinCEN[6] revised the definition of "money transmission services" which now means "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means." It is likely that the business model of many third-party Bitcoin services qualifies third party as money transmitter, and therefore, the money transfer services subsumes under 31 CFR Part 1010.100(ff) [22]. Third parties, Bitcoin service providers qualified as transmitters of money when want to work legitimately are required to register with FinCEN, and to implement programs to combat money laundering, to keep certain records, and to report suspicious activity and Foreign currency transactions. In some states Bitcoin third party service providers are required to obtain an official state license [23]. Therefore, under the pressure of legal norms, some of the service providers of Bitcoin set as a condition to the members to agree to provide provider "with current, accurate, and complete information about yourself as prompted by the registration process, and to keep such information updated" [25].

2.3 Aspect of system users

The risk of using Bitcoin exists and can also be analysed from system users' aspect. As mentioned, criminals cannot attack a central server, but can attack individual wallets and a third party - Bitcoin service providers. The first malware designed to

[5]fiat money: money (as paper currency) not convertible into coin or specie of equivalent value [24]
[6]http://webchat.freenode.net/
[7]Financial Crimes Enforcement Network – US Department of the Treasury

steal bitcoins from compromised Bitcoin wallet, "Infostealer. Coinbit" was discovered in mid-June 2011. The program was able to infect user's computer and to transfer digital Bitcoin wallet to the server in Poland [26]. Particularly at risk are users who do not use encryption in their Bitcoin wallets. About 25,000 Bitcoin theft cases, an attempt of fraudulent sale of Bitcoin worth 7 million USD, and stealing Bitcoin with online gaming sites in 2011, as well as theft of computer resources for bitcoin mining are discussed in the FBI report [14].

It is easy to conclude that banks will not look with favour to the development of competition and it wouldn't be odd if they tried to disrupt Bitcoin business.

A particular problem for many Bitcoin system users appeared when Mt Gox went down. It occurred from December 2013 until the final downfall of February 2014 when a message appeared on the website: "In light of recent news reports and the potential repercussions on Mt Gox's operations and the market, a decision was taken to close all transactions for the time being in order to protect the site and our users. We will be closely monitoring the situation and will react accordingly" [24]. Details about the Mt Gox fall were published in [27, 28, 29 and 30], and other sources. The other major providers of Bitcoin to fiat money exchange services distanced themselves from the Mt Gox act, and announced that they continue to operate normally.

Mark Karpeles, a former director of the service Mt Gox, spoke on the uncertainty of investing in Bitcoin. In his presentation, he explained that investing in Bitcoin is risky and that the high value of the Bitcoin is based on high demand, but there is no guarantee that tomorrow it will not be reduced to a value of 0. In the statement he said that it is not expected, but that it is possible [31]. Users have to decide whether they will continue to do business with bitcoins.

3. Conclusions

Number of users of Bitcoin system is growing, but it is still small compared to the number of credit card or fiat money users. Bitcoin system is great conceptual and technical achievement that can be used by existing financial institutions, and even governments.

Application of the Bitcoin system brings a number of benefits to users. It enables them to transact in a reasonably short time, for free or a minimal fee. In addition, this system allows them freedom and independence of financial institutions. With the growing number of participants the Bitcoin system should become more stable, and the value of bitcoin should less oscillate allowing to owners security in terms of the value of their money, bitcoin.

On the other hand, when the bitcoin stabilizes itself, and when the number of users becomes big enough, according to the FBI, and many others, Bitcoin will become a very useful tool for a variety of fraud and criminal activity. However, it is the same with any other money, including gold. Neither gold, nor paper money keep any record of previous money owners.

A slowdown in growth of number of Bitcoin system customers can be caused by unpleasant events, such as it was the case of the Mt Gox, as such as some reported cases of Bitcoin theft, or the legal prohibition on Bitcoin trade (China and India), but when the situation stabilizes and a legal framework is established, climate can change in a positive direction for Bitcoin.

Based on the above it can be trusted that Bitcoin will not be only a temporary phenomenon and that it will take its place on the Internet as a regular means of payment.

References

[1] FEE:. *The Truth about Bitcoin and Alternative Currencies*. YouTube. [Online] 12 11, 2013. [Cited: 07 26, 2014.] www.youtube.com/watch?v=AVdKgQ0jmH8.

[2] NAKAMOTO, S.: Bitcoin: *A Peer-to-Peer Electronic Cash System. bitcoin*. [Online] 2008. https://bitcoin.org/bitcoin.pdf.

[3] BLOCKCHAIM.INFO: *Average Transaction Confirmation Time*. BlockChain. [Online] 02 19, 2014. https://blockchain.info/charts/avg-confirmation-time?timespan= all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=.

[4] ANON: *Bitcoin Transaction Fees Explained. Bitcoin Fees*. [Online] 02 05, 2014. http://bitcoinfees.com/.

[5] VELDE, F. R: Bitcoin: *A Primer*. Chicago Fed Letter. [Online] 12 2013. http://www.chicagofed.org/digital_assets/publications/chicago_fed_letter/2013/cfldecember2013_317.pdf.

[6] CEKEREVAC, Z., CEKEREVAC, P.: *Bitcoin - Benefits and Risks*. Belgrade : Faculty of Business and industrial Management, 2014. Intern. scientific conference Management 2014, 978-86-6375-012-8.

[7] CEKEREVAC, P., CEKEREVAC, Z.: *Bitcoin - Benefits and Risks*. FBIM Transaction. [Online] 03 11, 2014. [Cited: 07 25, 2014.] http://www.meste.org/fbim/fbim_srpski/ FBIM_najava/V_Cekerevac.pdf. 2334-704X.

[8] SKUDNOV, R.: *Bitcoin Clients*. Turku : University of Applied Sciences, 2012.

[9] BLOCKCHAIN: *Market Price (USD).* Blockchain. [Online] Blockchain, 07 26, 2014. [Cited: 07 26, 2014.] https://blockchain.info/charts/market-price?timespan=2year&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=.

[10] LUKIC, M.: *Electronic Currency Bitcoin Could Destroy the Dollar (in Serbian)*. Biznis & Finansije. [Online] 12 07, 2013. http://bif.rs/2013/12/elektronska-valuta-bitkoin-bi-mogla-unistiti-dolar/.
[11] WILLIAMSON, SAMUEL H: *Seven Ways to Compute the Relative Value of a U.S. Dollar Amount - 1774 to Present.* MeasuringWorth.com. [Online] 2014, http://www. measuringworth.com/uscompare/result.php?year_source=1913&amount=100&year_result=2013.
[12] BLOCKCHAIN.INFO. *Total Bitcoins in Circulation*. BlockChain. [Online] 02 19, 2014. https://blockchain.info/charts/total-bitcoins.
[13] BLOCKCHAIN. *Number of Transactions Per Day*. Blockchain. [Online] 07 26, 2014. [Cited: 07 26, 2014.] https://blockchain.info/charts/n-transactions?timespan=all&show DataPoints=false&daysAverageString=1&show_header=true&scale=0&address=.
[14] FBI: *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity*. Directorate of Intelligence, Washington : Federal Bureau of Investigation, 2012.
[15] WIKI: Anonymity. *Bitcoin wiki*. [Online] 05 30, 2013, https://en.bitcoin.it/wiki/ Anonymity.
[16] CODERRR. *Patching the Bitcoin Client to Make it More Anonymous*. Bitcointalk Forum. [Online] 06 30, 2011, https://bitcointalk.org/index.php?topic=24784.msg 307661#msg307661.
[17] LEE, T. B: *How Private Are Bitcoin Transactions*? Forbes. [Online] 07 14, 2011. http://www.forbes.com/sites/timothylee/2011/07/14/how-private-are-bitcoin-transactions/.
[18] LOWENTHAL, T.: *Bitcoin: More Covert than it Looks*. *Active Rhetoric.* [Online] 07 14, 2011. http://activerhetoric.wordpress.com/2011/07/14/bitcoin-more-covert-than-it-looks/.
[19] BITCOIN.IT. *Selling Bitcoins. Bitcoin wiki*. [Online] 01 20, 2014. https://en.bitcoin.it/wiki/Selling_bitcoins.
[20] *Buying Bitcoins.* Bitcoin wiki. [Online] 02 19, 2014. https://en.bitcoin.it/wiki/Buying_bitcoins.
[21] *Secure Trading.* Bitcoin wiki. [Online] 10 24, 2012. https://en.bitcoin.it/wiki/Secure_Trading.
[22] FDIC: *FDIC* Law, *Regulations,* Related Acts. FDIC Federal Deposit Insurance Corporation. [Online] 09 16, 2013. [Cited: 07 28, 2014.], http://www.fdic.gov/ regulations/laws/rules/8000-1400.html#fdic8000fra1010.100.
[23] FEDERAL REGISTER: *Bank Secrecy Act Regulations: Definitions and Other Regulations Relating to Money Services. Rules and regulations.* [Online] 07 21, 2011. http://www.gpo.gov/fdsys/pkg/FR-2011-07-21/pdf/2011-18309.pdf.
[24] MT.GOX TEAM: *Mt.Gox.* [Online] 02 25, 2014. https://www.mtgox.com/.
[25] MT.GOX: *Acceptance of Terms of Use.* BITSTAMP. [Online] BitStamp. [Cited: 07 28, 2014.] https://fi.bitstamp.net/terms-of-use/.
[26] POULSEN, K.: *New Malware Steals Your Bitcoin*. Wired. [Online] 06 16, 2011. http://www.wired.com/threatlevel/2011/06/bitcoin-malware/.
[27] A.N.R: *Platform for Bitcoin Trade Mt.Gox Stopped Working (in Serbian).* Pobjeda. [Online] 02 25, 2014. http://www.pobjeda.me/2014/02/25/platforma-za-trgovinu-bitcoin-valutom-mt-gox-prestala-sa-radom/#.Uw0nS_ldWYw.
[28] TAKEMOTO, Y., KNIGHT, S.: *Mt. Gox Files for Bankruptcy, hit with Lawsuit.* Reuters. [Online] Reuters, 02 28, 2014. [Cited: 07 26, 2014.], http://www.reuters.com/ article/2014/02/28/us-bitcoin-mtgox-bankruptcy-idUSBREA1R0FX20140228.
[29] MTGOX: *Announcement of Commencement of Bankruptcy Proceedings. MtGox.* [Online] MtGox, 04 24, 2014. [Cited: 07 26, 2014.], https://www.mtgox.com/img/ pdf/20140424_announce_qa_en.pdf.
[30] PICK, L.: *U.S. MtGox Bankruptcy Filing Approved to Clear Way for Japan Proceedings.* Digital Currency Magnates. [Online] Digital Currency Magnates, 06 18, 2014. [Cited: 07 26, 2014.] http://dcmagnates.com/u-s-mtgox-bankruptcy-filing-approved-to-clear-way-for-japan-proceedings/.
[31] KARPELES, M.: *The Greatest Service to Exchange Bitcoin Shuts Down (in Serbian).* [interv.] Lejla Madlic : Aljazeera. 02 25, 2014.