ЕКОНОМИКА
ISSN 0350-137X, EISSN 2334-9190, UDK 338 (497,1)
Vol. 64, october-december 2018, № 4
P. 109-120

Jasmina Smigic Miladinovic[1]
High Economic School of Professional Studies Pec in Leposavic

SCIENTIFIC REVIEW ARTICLE
doi:10.5937/ekonomika1804107S
Received: October, 09, 2018
Accepted: November, 27, 2018

BITCOIN - ITS CONDITION AND TENDENCIES

Abstrakt

The appearance of cryptocurrency marks the arrival of a new unlimited global system with no intermediaries and costly intercontinental transactions. Digital money would make it possible for us to have significantly quicker and cheaper transactions, which, along with present technology, is considered inevitable in the future. This paper includes three topics and deals with the bitcoin phenomenon and its influence on economic growth. The paper presents the bitcoin technology, its advantages and some risks to which the system's users are exposed. Bitcoin represents an exceptional technical achievement, and specific features of bitcoin present a particular challenge for its users.

***Keywords**: cryptocurrency, bitcoin, blockchain, cryptography, digital money*

JEL classification**: **E 40, F 30, G 10

БИТКОИН - СТАЊЕ И ТРЕНДОВИ

Апстракт

Настанак криптовалута може се означити као долазак новог глобалног, безграничног система без посредника и скупих интерконтиненталних трансакција. Дигитални новац би нам омогућио значајно брзе и јефтиније трансакције, што се уз постојеће технологије сматра неминовношћу у будућности. Рад обухвата три тематске целине и бави се феноменом биткоина и каква је његова улога на привредни раст. У раду је приказана технологија Биткоина, предности и неки ризици којима су изложени корисници овог система. Биткоин представља једно изузетно техничко достигнуће и саме специфичности Биткоина представљају посебан изазов његовим корисницима.

***Кључне речи:** криптовалута, биткоин, block chain, криптографија, дигитални новац*

Introductory discussion

Bitcoin is a phenomenon known worldwide, but not many people are able to explain its essence and finer details. Everyone knows that it is an ever more popular digital money, but few are familiar with how to earn, who pays and how to spend that money.

[1] jasnacs0411@yahoo.com

Nowadays, bitcoin is in the spotlight. This cryptocurrency has not gold backing, has not a country of origin, and is not backed by any particular country or banking organisation. Bitcoin is completely digital and is created in a process called "mining", which can be performed on standard computers or by using a specialised hardware, by respecting strict rules provided by automatic cryptographic systems and the bitcoin community. The cryptocurrency as a digital form of money is based on the digitized so called , the main book of all crypto watch transactions called blockchain. Blockchain records individual transactions and ownership of all cryptocurrencies that are in circulation, and this system is managed by the so-called blockchain miners who have to update all transactions that have occured and ensure the accuracy of the informations (Milutinović, 2018, p.105) . Those computers and specialised hardware solve a complex series of mathematical algorithms, with the speed and efficiency of their mining depending on the speed of their solving. In addition, mining is an automatic process carried out continually by a computer, preferably 24 hours a day and seven days a week. Bitcoin can be mined by anybody, regardless of their country or nationality. A question presents itself: How can money be created from calculations that serve nothing? Paper currency is neither worth by itself until its value appears on the market. Amount of bitcoins is limited, and their appearance "out of nothing" occurs to the predictable rhythm, which prevents inflation and becomes the basic prerequisite for the confidence of brokers and merchants who accept bitcoin. It includes a P2P interaction, in which each owner transfers electronic money to the next owner, by signing and adding to the end of the coin a hash of the previous transaction and a public key of the next owner. Payment verification is done by informing the whole Bitcoin network about the carried out transaction. By doing so, double payment is prevented and generating of nonexistent money is avoided. These transactions are carried out without transferring personal information between participants in a transaction. In contrast to totally anonymous transactions, payment in bitcoins leaves a trace that is recorded and accessible to the public. Participants in a transaction, however, do not have to do business under their own names, for they may apply by using pseudonyms. Bitcoin offers to its users lower transaction costs, an increased privacy, as well as a long-term protection of purchasing power from inflation. Nevertheless, bitcoin still has not enough participants and a financial basis to secure stability, so the price of bitcoin oscillates significantly. Its users still feel uncertain about being safe from thefts and frauds. Even authorised state agencies have numerous dilemmas and analyses of the existing and future risks related to the application of bitcoin. As there is no controlling agency (bank), there is neither a transaction log, and money refund, in the case of a non-delivery of paid goods and services, cannot be legally regulated. Even though the number of bitcoin users is growing, it is still insignificant compared to credit cards and the use of USD, EUR and other currencies (Dinić, 2014). Nevertheless, bitcoin system represents a remarkable conceptual and technical achievement. It can also be used by the existing financial institutions (which can issue their own bitcoins). There are also no obstacles for state governments to use the technology.

The birth of the idea of crypto currencies can be characterized as a kind of globalization of the international payment system, where perhaps it is more accurately to use the term individualization and privatization instead of globalization. Does , however, this phenomenon of crypto currency carry a new latent form of dominination of world powers with the aim of achieving virtual colonization? Are crypto currencies only semingly exempt from national characteristics ? (Djordjevic, 2018, p.95).

1. Basic characteristics of digital payments

The history of the human kind has known various means of payment. The american dollar has been the most used means of payment for nearly fifty years since World War II, but its reputation has decreased considerably thanks to many acts of the USA Central bank (Federal Reserve), and many have begun looking for an alternative (FEE, 2013). If a closer look is taken at the past, we see that people have used different means of payment, such as silver, gold, wheat, shells, tobacco, salt, paper, etc. Almost none of these means is used today, except for gold, silver, and paper currency. For a means to become suitable for payment, it has to have some important characteristics; for instance, it would have to remain valuable for a long time period, its quantity should be limited, it should be easy to divide it into parts, and it should be portable

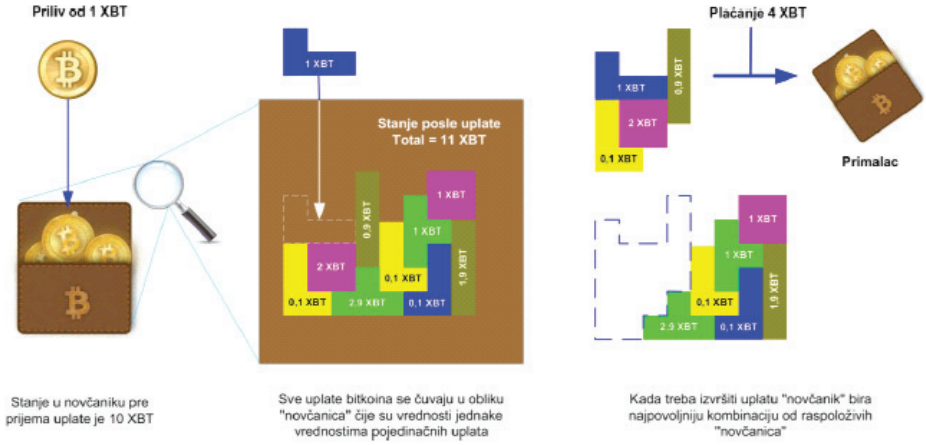
Modern-day payments that include financial institutions are exposed to a number of limitations and entail relatively high costs, the amounts of which are measured by percentage. That way, when money changes several owners, a significant amount remains in the banks. This reason, along with others, brought to creation and launching of bitcoin, digital currency, in 2009. The credit for creation of bitcoin is given to a creator who used a pseudonym Satoshi Nakamoto, and who published his creation principles in the article "*Bitcoin: A Peer-to-Peer Electronic Cash System*" (Nakamoto, 2008). Bitcoin includes a P2P interaction, and electronic currency is defined as a chain of digital signatures. Each owner transfers a coin to the next owner by signing a hash of the previous transaction and public key of the next owner, and by adding all of that to the end of the coin. The receiver may check the signatures in order to check the property chain. The payment verification is done by informing the whole network of the executed transaction. In that fashion, double payment is prevented and generating of nonexistent money is avoided. The verification may last a few minutes.

These transactions do not involve transferring of personal information between transaction participants. In contrast to completely anonymous transactions, bitcoin payments leave a transaction record, noted and accessible to the public. Transaction parties do not have to do business under their own names, for they may apply through pseudonyms. An important question presenting itself is: How are bitcoins created? For something to have value, it is necessary for its creation to be expensive, that is to say more expensive than the market value of that something being created. For instance, there is gold in the ground and it is accessible to everybody, but its extraction from the ground is expensive and unprofitable for the vast majority. That is why the majority of gold users are not able and neither is it in their interest to mine for gold, and each new kilogram of produced gold brings significant worth to the producer. Bitcoins are created in a similar manner. Quite a few arithmetical operations for a complex alorithm need to be carried out for one bitcoin to be mined. It is quite probable that an individual bitcoin miner would try very hard before they manage to mine some. It is, therefore, recommended to have several miners joined together, who should try mining bitcoins by using their joint forces and a number of computers. Roughly put, the problem being solved by miners is reduced to the following: If $\boldsymbol{x}$ represents a series of blocks (so-called *blockchain*), if $\boldsymbol{y}$ stands for an additional block and $\boldsymbol{n}$ for an additional number, the aim is to find the $\boldsymbol{n}$, so that the resulting hash function $\boldsymbol{f(x,y,n)}$ has a value lower than the set value of $\boldsymbol{\alpha}$. (Velde, 2013)

Hash function maps a text or numbers of an arbitrary length into a number of a fixed length. For instance, taking the first letter of a word or addition of all the digits of a number, until one obtains as a result a number that can be expressed through one digit, maps any word or number by hash of length one. The bitcoin hash function is deterministic, but so much complex that the result looks like accidental numbers. That is why it is very difficult for miners to reach an appropriate solution to the problem. They need to test a lot of different combinations for various values of n, which demands high computer capacities and a considerable consumption of time and energy, until the required condition is met. The lower the value of α, the harder it is to meet the condition. By contrast, a suggested solution (x,y,n) can easily be verified. A part of the number n includes verifying that the bitcoin added to the block y has not already been spent in the block x.

The code makes it possible for any miner to take into the block y a certain kind of transaction, which creates N of new bitcoins and attributes them to the miner. The first miner to reach a solution sends the information to all other miners who verify it. After the verification (performed by the majority of miners), a new block is added to the chain and the lucky miner becomes an owner of N of new bitcoins. A part of the bitcoin protocol regulates the temporal values of N and α. The difficulty of α is adjusted every two weeks so as to provide the dynamics of bitcoin creation of six times an hour. The more miners who work on creating new bitcoins, the stricter are conditions. The initial value of 50 of the number N is halved every 210.000 blocks. It leads to a definition that the number of available bitcoins asymptotically approximates the number of 21.000.000 (Velde, 2013). Therefore, just as the mines' deposits become ever poorer after a long production and gold production becomes ever less profitable, so does bitcoin mining become unprofitable. In order for mining not to die out, a reward for the work of miners is anticipated from other funds. During bitcoin transactions, a participant is enabled to "pay for" the transaction, so that it could be carried out in a quicker procedure. The transaction rates are defined according to a special algorithm, in which the size of the transaction, the age of the record, or the length of the record in kB, are all taken into consideration. If any of the "banknotes" from the wallet in the transaction is less than 0,01 XBT, or if the money change is less than 0,01 XBT, then it is required to pay a compensation for the transaction to the amount of 0,0001 XBT per such a banknote (Matonis, 2013). By doing so, the intention is to discourage sending of too little values. The task of the wallet is to choose the most favourable combination of banknotes for a payment. An example of the means of payment in bitcoins is shown in Figure 1.

Figure 1: *Technology of payment in bitcoins*



Payment per kB means that the compensation for a transaction is determined according to the length of the record in bytes. The length of the record depends on the number of inputs and outputs for a transaction. The length of the record *L* is roughly determined according to this formula:

$$L = 148 \cdot input\_number\ of\_banknotes + 34 \cdot output\_number\ of\_banknotes + 10$$

The input number of banknotes includes the number of banknotes and records excluded from the wallet, and the output number of banknotes includes the amount being sent, as well as a refund for the difference between the paid amount and the necessary one - the change. If L is <10000 bytes, and the transaction's value is high enough, with the records old enough, then the transaction is free of charge. Otherwise, it is charged for. In the case of a compensation payment per kB, other compensations are not charged for.

In transactions, the priority is given to older bitcoin records, and to records with a greater value. Every transaction shows a priority defined by the age, size and the number of inputs. For each input, the wallet calculates the product of values of inputs with the age of input within a block, and then the products are summed up and the obtained amount is divided by the size of transaction given in bytes. If the obtained quotient is smaller than 0,576, then such a transaction requires paying for compensation. That means that a transaction may involve a lot of small or new banknotes, and that the compensation need not be paid if a big old banknote is included, because the transaction estimate takes a mean value as an authoritative one. It happens sometimes that a compensation should be paid for, and that the compensation is not required if the transaction is carried out at a later stage because the banknotes have aged enough

2. Advantages of bitcoin use

Bitcoin offers to its users lower costs of transactions, an increased privacy and a long-term protection of purchasing power from inflation. However, bitcoin still has

not enough participants and a financial base to secure stability, so its price oscillates significantly. Its users still feel uncertain about being safe from thefts and frauds. Even authorised state agencies have numerous dilemmas and analyses of the existing and future risks related to the application of bitcoin. Regardless of those dilemmas, many people, including Ron Paul, see the bitcoin as an excellent means of payment, which makes the following possible (Lukić, 2016):

- Purchase of anything in secrecy;
- Absence of banks in the chain of payment;
- Payment with no commission charged;
- No concern that inflation will devalue currency in the future.

That can be exemplified by a temporal change of value of the USD. For instance, by using Consumer Price Index, if somebody had had 100 USD in their wallet in 1952, he would have to expect to have 11,56 USD today due to inflation. The situation becomes even worse, if some other criteria are considered. Table 1 shows values of today's amount of the USD, as an equivalent of a 100 USD value from 1912 and 1962.

Table 1: *2012 values, equivalent of 100 USD value from 1912 and 1962*

$100 from		1912.	1962.
Ekvivalent u 2012	by using Consumer Price lndex (lndex of consumer prices)	$2400	$751
	by using GDP deflator (BDP deflator)	$1730	$579
	by using unskilled wages	$9900	$794
	by using Production Worker Compensation	$14000	$966
	by using a nominal GDP per capita	$14300	$1490
	by using a relative share of GDP	$45600	$2450

How did such a drop in the USD value occur? The explanation is simple - by printing money without backup. Until the 70s of the twentieth century, printing of the dollar had been carried out with numerous restrictions, but for a few decades now the USA Central bank has been printing billions of dollars, and thus devaluing the worth of the USD.

Basel Committee on Banking Super Vision, since 1988, has brought a series of instructions and amendments, knows as Basel Standards, with the aim of developing a system of rules and standards thet will be a mechanism for improving the stability of the financial system, establishing equitable market conditions for the operation of international banks by defining uniform solvency coefficients anddefining the role of regulators in situations with unclear jurisdictions, as no bank with subsidiaries in different jurisdictions could escape contro and audit. By these standards, banks are allowed to determine capital adequacy to cover market risk by applying VaR and Expected Shortfall (ES) Model (Radivojevic, Curcic, Marcetic, 2018, p.100).

As for the bitcoin currency, it is known precisely when and how much of it is going to be on the market. Thanks to the applied algorithm, one knows that the number of bitcoins is going to approximate asymptotically the figure of 21.000.000. Since the first

bitcoin, launched in 2009, their number had grown to about 12 million on 12 December 2013, and it is estimated that their number will reach 18 million in 2024, and that there will have been about 21 million bitcoins by 2140. After that, the number of issued bitcoins should not change at all. The second important values criterium from Table 1 is thus fullfilled.

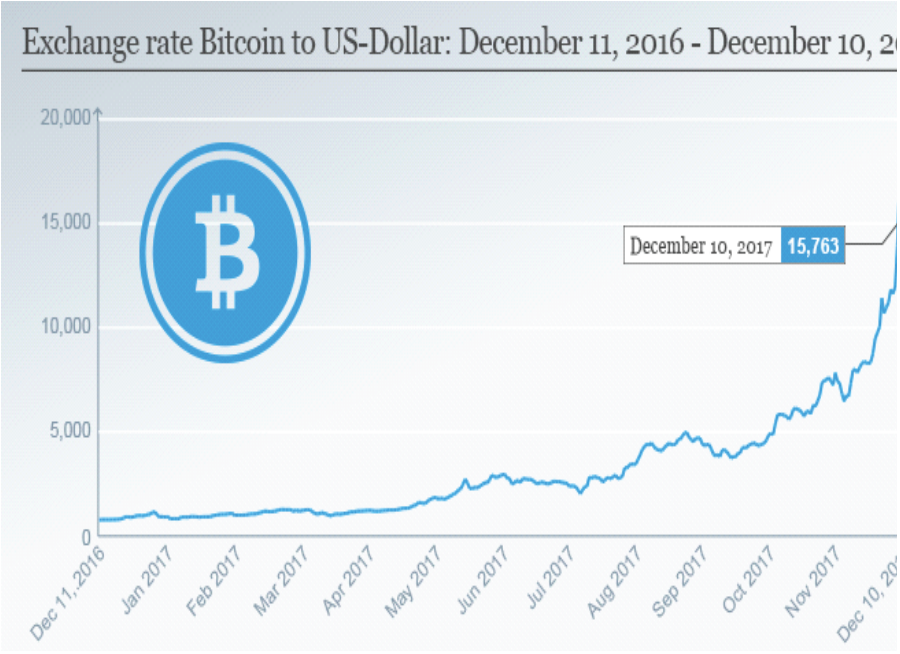
It is hard to counterfeit the USD, as well as silver and gold. Given that bitcoin is based on an open-code software, one might think that it is easier to counterfeit. However, bitcoin is based on cryptography, and it is practically impossible (or, apparently, unprofitable) to counterfeit it. In addition, each transaction requires a confirmation by other system participants, which prevents possible manipulations through double payments. Bitcoin includes some more advantages, as well (Lukić, 2016):

- It can be very easily transferred from one spot to another on Earth, regardless of quantity and geographical position if there is an Internet connexion;
- Acceptance of bitcoins is free of charge;
- There is no money refund (chargeback);
- Bitcoin can be exchanged for any other currency.

Based on the advantages cited above, one can note a favourable gradient of increase in the total number of transactions, as shown in Figure 2.

It is not easy to say which means of payment is the best, especially if the conditions change all the time, but it is probable that bitcoin will likely manage to reach the top of the list, primarily thanks to its advantages. It is also most probable that the today's dollar-led means of payment will be pushed to a considerably lower position.

Figure 2: *Total number of transactions for the period of 2016 – 2017*



3. Risks related to bitcoin use

Bitcoin makes it possible for a user to create an unlimited number of wallets. That is why one can say with certainty how many miners there are on the network, and what the real number of bitcoin users is, but it is noticeable that the number of wallets increased rapidly for the period of January 2013 and January 2014. Since its creation, and until January 2013, some 50 thousand wallets have been created. The total number of bitcoin wallets is presented in Figure 3.

Due to a relative anonymity of its users, bitcoin makes it possible for individuals to generate, transfer, launder or steal financial resources. With its application, it presents for investigators challenges similar to those of other virtual money, such as WebMoney, and there are also additional difficulties due to its decentralized nature. The FBI estimates, which are considered reliable, state that criminals will treat bitcoin as an alternative payment option in the near future, although they would not give up on the existing traditional means of payment.

Less reliable are considered the FBI estimates that mention a use of bitcoin for money laundering (FBI, 2012). This hypothesis is difficult to prove, because there are not enough reports on bitcoin. Thanks to its decentralized status, the system will most probably resist possible attacks, but criminals will focus on attacking private bitcoin wallets and they will try it by using third-party services.

Bitcoin transactions are accessible to the public, although the only information identifying a bitcoin user is a randomly pseudo-generated bitcoin address, which makes the transaction pretty anonymous. However, transactions are not completely anonymous, even though bitcoin is clearly decentralised, for there is a place that can provide data on participants in a payment. That place is where bitcoins turn into a *fiat currency*, i.e. decree money. In order to increase the anonimity of a transaction, users can do the following (Dhaliwal, 2017):

- Create and use a new bitcoin address for each incoming payment;
- Route the whole bitcoin traffic through an anonymiser;
- Combine the old bitcoin addresses into a new address, in order to make new payments;
- Use specialised services for money laundering;
- Use third-party eWallet services to consolidate addresses. Today there are third-party services that offer an option to create an eWallet that would enable

users to consolidate many bitcoin addresses and that provides a simple access to its bitcoins from any device;
- Individuals may create bitcoin clients to increase anonimity easily (as well as being able to choose a bitcoin address from which to make payments), and for all that users do not have to have a particularly technical education in order to make transactions anonymous.

There are patterns of behaviour of taxpayers, facing a possibility to evade taxes, which appear in the financial literature. Of importance here is the relation between the expected benefit from tax saving and the expenses they would have to bear if uncovered and punished (Marcetic, Curcic, Lazovic, 2016, p.239).

Nowadays, the specific features of bitcoin represent a special challenge to uncovering and preventing of illegal activities. Being a decentralised system, bitcoin does not have a central institution and it cannot control or notify of suspicious activities in accordance with the money laundering prevention programme, and it does not accept or carry out legal requests, such as court orders. According to the FBI, the main vulnerability of the decentralised systems of payment include (Dhaliwal, 2017):

- Absence of software or ability to track and identify suspicious monetary patterns appearing in money laundering;
- Absence of identification of real owners of accounts, as well as their real location;
- Absence of records about transaction history, related to the real participants in transactions;
- A considerably harder identification of sources for means of payment, compared to some other types of online currency;
- Law enforcement agencies cannot target a particular central location or a company, and they cannot switch the system off while conducting their investigation.

As stated above, bitcoin requires that its users use third-party services during conversion of their bitcoins into fiat money. Buying, selling, bitcoin trade or their conversion to some other currency, all of that is performed outside of the P2P system. Due to the number and variety of the third parties, there is a real possibility for a transfer or a conceivable money laundering. The users who do not want to use those third-party services might post their own "buy" or "sell" requests on *freenode IRC* (Internet relay chat).

In July 2011, FinCEN revised the definition of "money transfer service" and now it means "accepting of money, means or other values, exchanged for money from one person, and transfer of money, means or other values to another place or person in any of the ways". It is most likely that the business model of most third-party bitcoin services qualifies those third parties as money carriers, and assigns the money transfer services to 31 CR Part 1010.100 (ff) (FDIC, 2015). The third parties, bitcoin service providers, which are qualified as money carriers and want to work legitimately, have to register with FinCEN, and they have to implement money laundering prevention programmes; they would also have to keep certain records and submit reports on suspicious activities and currency transactions, as required. Some countries demand that those third parties secure a state licence (Federal Register, 2011). That is why some bitcoin service providers,

under the pressure of legal norms, lay down a condition stating that "members agree to provide precise, up-to-date and complete data on themselves, as required in the registration procedure, and that they should keep them updated" (MT.GOX, 2012).

The risks of using bitcoin should also concern the system's users. Criminals cannot attack a central station, but they can attack individual wallets and third-party bitcoin service providers. The first malware programme "Infostealer Coinbit", designed to steal bitcoins from compromised bitcoin wallets, was discovered in June 2011. The programme could infect a user's computer, and transfer a digital bitcoin wallet to a server in Poland (Poulsen, 2011). Especially exposed to risks are the users who do not use an encryption with their bitcoin wallets. An FBI report (2012) mentions cases of theft of 25.000 bitcoins, an attempted counterfeit selling of bitcoins worth 7 million USD, as well as a theft of bitcoins from online gaming sites in 2011, and a case of theft of computer resources for the purpose of bitcoin mining.

The fact of the matter is that banks will not either act friendly towards the development of a competition, and it would not be strange if they tried to disrupt the business with bitcoins. On the other hand, at the end of February 2014, some rumours appeared about the bitcoin code not being totally reliable, with possible errors in the code, but the biggest attack on bitcoin so far came from one of the largest exchange service (bitcoin to other currency) providers, Mt. Gox. A message, appeared on their site on 07/02/2014: "In light of recent news reports and potential repercussions on MtGox'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" (Mt.Gox Team, 2014).

As a reason for the interruption in their work they cited technical causes, as well as a drop in prices on the bitcoin stock exchange by 20% - almost 180 USD - due to an overwithdrawal of bitcoins. Unofficially, some 750.000 bitcoins were taken away, which means, in the case of a hacking or a forcible blockade of the web site, that Mt Gox's losses amounted to about 350 million dollars (A.N.R., 2014). It was not the first time that Mt Gox's clients had problems with accessing their accounts. The other six bitcoin exchange service providers dissociated from Mt Gox's actions, and they said that they would continue to do business as usual. In regard to this event, there is an interesting statement of a German student of science, Max Hampel, who posted it on his blog, saying that once and for all the bitcoin community should be ready to renounce exchange of bitcoins for money through Mt.Gox. More details on this point of view can be found in an article by Rob Wile, published in the *Business Insider* (Wile, 2014).

Mark Karpeles, Mt Gox's former service manager, also spoke about the insecurity of investment in bitcoins. He explained in his presentation that bitcoin investments were risky, and that the high value of bitcoins was based on high demand, but that there were no guarantees that even the next day the value would not be reduced to 0. In the statement, he does not expect that to happen, but it is probable (Karpeles, 2014).

Conclusion

Although the number of bitcoin system users is growing, it is still small in comparison with the number of credit card users, and compared to the use of the

USD, EUR and other currencies. Nevertheless, bitcoin system represents a remarkable conceptual and technical achievement. It can also be used by existing financial institutions (which may issue their own bitcoins). There are also no obstacles for governments to use this technology. The application of the bitcoin system offers quite a few advantages to its users, by making it possible for them to realise transactions free of charge or with a minimum compensation, within a reasonably short time period, and by providing them with freedom and independence from financial institutions. The bitcoin system will be getting more stable with the number of its participants growing, and its value will be ever less oscillating, thus providing its users with security in terms of the worth of their money, that is to say bitcoins.

On the other hand, with the stabilisation and growth in number of users, the bitcoin will, according to the FBI and others, become a very useful means for various manipulations and criminal activities. The situation, however, is the same with any other currency, be it electronic or fiat money. Moreover, neither gold nor paper currency bear any record on their previous owners. Indeed, there are banknotes' numbers that are filed during bank transfers, but that is applicable mostly for the big-denomination USD banknotes. The slowing down of growth in the number of bitcoin system users may be affected by unpleasant events, such as it was in the case of the business cessation of Mt Gox, one of the biggest bitcoin exchange service providers, then some reported cases of theft of bitcoins, as well as legal bans on bitcoin trade in China and India. It is hoped that, with time and stabilisation of circumstances (in terms of legal regulations), the climate will become positive for bitcoin. According to the above, it is believed that bitcoin is not a temporary phenomenon, and that it will get to feel at home on the Internet as a regular means of payment.

References

A.N.R. (2014). *Platforma za trgovinu bitcoin valutom Mt.Gox prestala sa radom.*

Bohme, R., Christin N., Edelman, B., Moore, T.(2015),"*Bitcoin: Economics, Technology and Governance", Journal of Economic Perspectives, Vol.29.*

Coderrr. (2011). *Patching the Bitcoin Client to Make it More Anonymous*.

Čičin-Šain D. (2007). *Novac i poslovno bankarstvo.* From Sveučilište u Zadru,

Dinić V. (2014). *Bitkoin kao decentralizovana valuta*. Bankarstvo Journal issue 2/ 2014.

Dhaliwal S. (2017). *Poland Officially Recognizes Trading in Bitcoin and Other Cryptocurrencies*.

Djordjevic A.,(2018). *The application of advanced technologies in the field of international finances: bitcoin pfenomenon, Ekonomika 1/2018 , p.95, Drustvo ekonomista "Ekonomika" , Nis*

FDIC (2013). *FDIC Law, Regulations, Related Acts.* From FDIC Federal Deposit Insurance Corporation

FEE (2013). *The truth about Bitcoin and alternative Currencies.*

Federal Register. (2011). *Bank Secrecy Act Regulations; Definitions and Other Regulations Relating to Money Services.*

FBI (2012). *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity.* Directorate of Intelligence. Washington.

Kaye B. (2016). *Australian says he created bitcoin, but some skeptical.*

Karpeles M. (2014). Ugasio se najveći servis za razmjenu bitcoina.

Lee T. B. (2011). *How Private Are Bitcoin Transactions?*

Lowenthal, T. (2011). *Bitcoin: More Covert than it Looks.*

Lukic, V. (2016). *Potentials and limits of private digital currencies, Ekonomski fakultet , Beograd, ekof.bg.uploads2016/03*

Marcetic M, Curcic N., Lazovic K., (2016*) . Modalities of Value Added Tax Evasion in the Republic of Serbia, ANALI Ekonomskog fakulteta u Subotici , Vol 52, broj 35/2016, p.239,Univerzitet u Novom Sadu*

*Matonis, J., (2013**).**The appeal of a nonpoliticalcurrency. Paymentsource.com.*

Milutinovic, M.,(2018). Crypocurrency, Ekonomika 1/2018, p.105, Drustvo ekonomista "Ekonomika", Nis

MT.GOX. (2012). *Terms of use*. From MT.GOX:

https://mtgox.com/terms_of_service

Mt.Gox Team. (2014). *Mt.Gox*. From Mt.Gox: https://www.mtgox.com/

Nakamoto, S.(2008).*Bitcoin : Apeer/to/peer Electronic Cash System. http/bitcoin.org/bitcoin.pdf*

Radojevic N., Curcic N., Marcetic M., (2018)., *Quantifying Extreme Market Risk in the selected Western Balkan Coutries, Industry JSE, Current Issue Vol.46, No.2/2018, p.100.*

Poulsen K. (2011). *New Malware Steals Your Bitcoin*.

Velde F. R., (2013). *Bitcoin: A primer*. From Chicago Fed Letter.

Wiki (2013). *Anonimity*. From Bitcoin.

Wile R. (2014, 02 07). *The Fall Of Mt. Gox.* From Business Insider.