

FUNCTIONING MECHANISM OF BITCOIN

UDC 336.744

004.738.5:339

Aleksandar Đorđević*, Miloš Todorović

University of Niš, Faculty of Economics, Niš, Serbia

Abstract. *The connection between financial innovation and information technology industry has provided and kept the crypto currencies for some ten years on the market, a kind of offset of monetary evolution after the introduction of virtual, electronic and digital money. Although their essence is still wrapped up under the veil of secrets, the facts show that the value of Bitcoin as the first crypto currency has a rising trend, and that an increasing number of firms and individuals are deciding to use it. This will result in the emergence of over 1000 new crypto currencies. This paper explains the emergence and functioning of the Bitcoin, its characteristics and functions, the benefits and risks that it carries, as well as possible scenarios of further development of the international monetary system with crypto currencies.*

Key words: *virtual currencies, crypto currencies, Bitcoin, money functions, international payments*

JEL Classification: E40, F30, O30

INTRODUCTION

The end of the 20th and the beginning of the 21st century in economic history will be recognizable by the final victory of liberal capitalism and the superiority of individualism over the collectivist structure of society. If we can summarize these processes in two words, they could be reduced to privatization and globalization. An indispensable requirement for these processes was an Information Technology revolution that compressed time and space. But it has also created a parallel, virtual world that is increasingly present

Received November 14, 2017 / Revised December 10 / Accepted January 24, 2018

Corresponding author: Aleksandar Đorđević

* PhD student at University of Niš, Faculty of Economics

University of Niš, Faculty of Economics, Trg kralja Aleksandra 11, 18000 Niš, Serbia

E-mail: djaleksandar91@gmail.com

in both real and financial flows. The combination of privatization and informatics has also created electronic money, crypto currencies and perhaps even the privatization of monetary flows. This is exactly how the idea of a currency that is totally independent of central and commercial banks, monetary authorities, different rules and regulations of the state arose.

The economic motive for the emergence of the crypto currencies is very strong given that the most profitable export product of all time is the US dollar and that it has brought huge profits to the United States. If the private sector took on many jobs and profits that traditionally belonged to the state, why would not this happen with the profit brought by the issuance of the currency? Who is the creator of the crypto currency, the state or individuals? The question is even more intriguing if it is known that the creator of the crypto currency is unknown, and that a lot of capital, time and computer work should have been invested in the project. Finally, will the world accept the new international monetary system built on a completely virtual basis?

1. FUNDAMENTALS, TYPES AND SPECIFICS OF THE CRYPTO CURRENCIES

The analysis of the etymology of the word "crypto" leads us to the Greek language in which the adjective "kryptos" means hidden, secretive. In most Indo-European languages, even in Serbian, this prefix is used to construct a compound word with the meaning of hidden or secret. According to this logic, crypto currencies would be hidden or secret currencies. And indeed, these currencies exist only in the hidden, virtual world of information technology and computers. That is why the biggest mystery will remain how this unreal money came in touch with real goods. The legend says that the first transaction with crypto currencies – Bitcoin was done in Jacksonville, Florida on May 22nd, 2010, when 10.000 Bitcoins were offered for two family pizzas (Zohar, 2015). The amount of 10.000 Bitcoins today is worth over \$60 million, and then it was assumed that their value was only \$100 with a suspicion that they could be exchanged for a real currency at all. So, with crypto currencies it is not known either who issued them or whether there is any real value behind them. By making a parallel with real assets, we could say that the crypto currencies are genetically modified currencies because they are present in international payments, but it is unknown what effects can they cause over long-term use.

The intention of the creators of new virtual currencies (crypto currencies) is to be used within a specific virtual community, within a specific web site or a network of users who have special software for managing this currency and making payments. Each new virtual currency has a certain type of rules for its creators about where and how it can be used as well as the specific technical infrastructure in which payment is made. The virtual currency itself, a special set of rules and technical infrastructure together form a small payment system, also called a virtual currency scheme. In closed schemes, virtual currency can neither be bought nor sold (digital currency) but only in some way earned and utilized within that system (for example, the computer game World of Warcraft and gold coins in that game). If a virtual currency can be bought with a national currency, but cannot be subsequently replaced for the national currency, it is a one-way flow scheme (a coin example on Amazon.com). Such crypto currencies are considered non-convertible. In case when a virtual currency can be bought and sold outside a particular website, it is a two-way flow scheme (convertible crypto currency). As an example of such a double-flow scheme, bitcoin appears. However, these categories can overlap (Segendorf, 2014). Therefore, virtual currencies are those that do not exist in the form of cash,

but they perform some functions of money, most often the unit of account and function of medium of exchange. As virtual currency forms, digital currencies operate in closed systems and cannot be included in real financial flows. Electronic money is the one that is kept on accounts in the form of files (electronic, not on paper). Finally, the crypto currency will also be a form of virtual currency, not being emitted by the central bank, and it will be in a specific way (by encrypting) the transmitted payment messages. It is interesting that the International Monetary Fund considers virtual currencies as a form of digital currency (Dong et al., 2016), which is in some ways illogical because virtual currencies existed even before the informational revolution. Even the IMF itself used such unit of account - special drawing rights (SDR).

Further differentiation is done depending on whether the crypto currency is centralized or decentralized. As with banknotes and metal money, the payment with crypto currencies is done by changing the ownership of the means of payment. Therefore, the ownership structure must be registered somewhere, otherwise the one who has the crypto currency would try to use it more than once. The centralized crypto currency scheme has a centralized system for verifying and executing transactions mainly by the issuer. In practice, the issuer manages all payment orders. In a decentralized virtual scheme, such as Bitcoin, transactions are verified and executed through a network of users who actively participate in it. The right to register an event is delegated to participants in the network. Decentralized virtual currencies are often based on the exchange of encrypted (coded) messages and are therefore called the crypto currency. This provides anonymity and security, and these are the key principles under which the Bitcoin, the first and the most famous crypto currency, functions.

Bitcoin is a decentralized virtual currency scheme with two-way flow and a crypto currency (Peng, 2013). It is designed to be independent of governments, banks and other institutions. It can essentially be purchased on special websites where it is exchanged for national currencies. The exchange rate of Bitcoin is determined as a function of supply and demand on the market. Bitcoin payments can be made between any entities that possess the appropriate software on a computer, smartphone or tablet. This software is called a wallet. However, Bitcoin is not digital cash, since these are not digital value units which are stored on a computer, but it is considered as a certain asset in the account. When a payment is made, the payer does not send digital notes and coins to the payee, but the account of the payer is debited, and it is claimed by the receiver's account. Payment is done by exchanging encrypted messages and it is verified within the user's network.

Bitcoin payment is not executed in real time. It takes up to 10 minutes for the payment to be verified and the general rule is that it usually takes up to six verification circles to ensure that the payment is added to the list. Sometimes obtaining verification for payment can take up to one hour. Depending on the situation, this can be understood as a short but also as a long period of time. It should also be noted that due to the sharing of technology and the verification process, there is no central data warehouse, but each network user has the information on all parts of the data.

The concept of "electronic money" should not be confused with the crypto currency. Electronic money is an electronically stored monetary value representing an issuer's claim, it has a value equal to the amount for which it was purchased, and it is accepted by others, not only by the issuer. Crypto currency must be accepted by a sufficiently wide circle of companies. Precisely because of this, the Bitcoin is not electronic money, since it does not represent the claim of the issuer. Crypto currency can fulfill some of the aforementioned criteria, but not each one of them. This refers to the fact that most of the

crypto currencies are not accepted by a sufficiently wide circle of recipients. It is also not possible to always exchange the crypto currency for the national currency and they are expressed in different units as well. Currency is usually controlled by its issuer, however, here there is no supervision and the issuer is a non-financial company, so it is not possible to gain control over crypto currencies.

The oldest crypto currency is Bitcoin. The etymological analysis of the word Bitcoin indicates that it represents a compound composed of the word bit - which denotes the smallest unit of information in the computing (usually required to distinguish two mutually exclusive states, often represented as one (1) and zero (0), yes/no, true/false, has/no voltage, etc.), and the word coin - which is usually used to denote a metal coin of mostly smaller denominations.

Bitcoin is created with the appearance of the original article on October 30th in 2008, issued by the author under the pseudonym Satoshi Nakamoto. It has never been discovered who was the person or the team of people who actually created Bitcoin. Here exists a doubt about the connection with the World Financial Crisis that took place in 2007, and in 2008 spilled over into the real sector and turned into the World Economic Crisis. However, it is unlikely that such a complex code system could be created in such a short time. It is more likely that this system was created and that it waited for a convenient moment to enter the world stage and the crisis just created the ambiance. Due to uncertainty in the banking and financial system, the electronic crypto currency appears, which according to the original published article is not controlled by any institution but by the users themselves. This seems attractive for the placement of capital, circumvention of tax obligations and banking fees, as well as for secret transfers.

What is Bitcoin exactly? Opinions here are widely divided. One group of authors considers Bitcoin as a brand new, virtual currency. The second group says that in fact it is a kind of digital good, while some place it a means of international liquidity, whose popularity in recent years has been steadily rising primarily thanks to the ever more massive use of this crypto currency. It is interesting that there is no answer to several key questions about the Bitcoin, that the whole story is covered by a veil of secrets, despite the fact that its share in transactions has grown for years.

Bitcoin allows payments via the Internet directly with a peer-to-peer payment without the involvement of financial institutions and without their fees. What makes this currency more intriguing is the increasing number of clients operating in the real world and accepting payments in Bitcoin in return for products or services. There are thousands of websites that accept Bitcoin: in December of 2015, there were approximately 200,000 daily Bitcoin transactions (Carrick, 2016), but this volume is tiny compared to other currencies. Probably the greatest popularity of the Bitcoin is given by numerous celebrities from the world of business who optimistically look at its future. Richard Branson, a billionaire and founder of Virgin Airlines even announced the acceptance of payments in this currency for his new travel project into space. Then there is Bill Gates, who still does not accept this currency in exchange for his products, but he predicts that it will have bright future. It is possible that all this is part of a wider marketing campaign, so this inevitably poses some questions: Who benefits from Bitcoin? Are certain brokers who sell this currency, the users themselves, or maybe IT companies that sell equipment to use and create Bitcoin, earning the most? Is there latent support by some countries towards this currency and what is their ultimate motive? Naturally, there are Bitcoin skeptics who believe that it is a pyramidal structure, a monetary fraud on the global level, and that the question is when the organizers of the game will

withdraw from the story, and this virtual monetary structure will collapse in one day. The most reputable banks in the world kept their deposits anonymous, while the crypto currencies hide the transactions even from the banks that showed their unreliability in the mortgage crisis. High volatility and the possibility of speculative deals on stock exchanges, the possibility of avoiding taxes, money laundering and financing of secret actions (even terrorism) will result in an increase in the use of these currencies.

After the Bitcoin, other crypto currencies have been created, but Bitcoin remained dominant, measured by the scope of the transactions and market capitalization. More than 1000 currencies seek their place in international monetary flows. All of them are called with one name – altcoin (alternative coin) and they are trying to compensate the observed defects of Bitcoin. Long-lasting market share of Bitcoin that was over 90% fell in 2017 to below 50%. The highlight will be the creation of crypto currency derivatives that will allow additional speculation considering the high volatility of crypto currency value (Brito, 2014).

2. BITCOIN PERFORMANCE

Bitcoin is conceived as an electronic crypto currency with a final offer of 21 million units. There is a complex system for creating these currencies, the literal translation would be mining the currency. A block of 25 Bitcoins can be formed over a period of 10 minutes (Nakamoto, 2008). A block arises when a series of data is found, to which a special algorithm is applied, and it creates a precisely determined specific pattern. The size of the block decreases with the amount of already "mined" Bitcoins, and finding new Bitcoins is getting harder.

The emission of the Bitcoin is fully planned, i.e. programmed, and its management is assigned to the network itself, that is, to those computers that perform the verification of transactions. Such an algorithm is chosen because it approximates to a large extent the growth rate of extraction of certain ores such as gold, since the amount of Bitcoin that can exist at one point in the system and the maximum amount that can be "excavated" are limited. It is supposed that the Bitcoin should evolve like gold. When its excavation becomes very difficult, its value will be determined by the amount of transactions being executed and by the demand for this currency.

Some believe that this is a significant financial innovation in the last few years, and what certainly attracts attention is the sudden rise in the price of Bitcoin. The final goal of Bitcoin is to become an alternative to existing payment systems. It provides cross-border transactions without interference by states or central banks, as well as without commercial banks.

In order to use Bitcoin users must have an ID number i.e. a public key and a "private key" for verification on the public ledger, also called a blockchain. Individual users – "miners" use the power of their computers to verify the credibility of the transaction by solving technically complex problems. In return, the first user who finds the solution to the problem is rewarded with a certain number of Bitcoins, being added to the total number of Bitcoins, thereby encouraging the creation of this currency. The pre-programmed algorithm adjusts the complexity of transaction verification with the computer to ensure that each transaction takes an average of 10 minutes to verify. This same algorithm also sets the total supply of Bitcoin which is limited to 21 million and programmed not be

"excavated" by the year 2140, although it does not show the exact path of growth of this crypto currency. Certain randomness when verifying each transaction is inevitable so verification time will vary.

There are two ways to become the owner of Bitcoin, one is the aforementioned – mining, while the other is purchasing the already created Bitcoins with real currencies, on many stock exchanges that operate around the world and trade with Bitcoin. In Serbia, there are three ATMs where you can buy Bitcoin.

3. BENEFITS AND RISKS FOR BITCOIN USERS

Bitcoin and other crypto currencies record large oscillations in value on both daily and annual levels. The fact that, globally speaking, the trend of demand for Bitcoin is growing indicates the benefits that the transactions with this crypto currency are bringing. But the veil of secrets, as well as the lack of any guarantee, also carries the risk of converting real into the crypto currency. Benefits are mostly related to anonymity or integrity, convenience and speed of transaction execution, and a maximum reduction in the cost of payment. As a noted shortcoming, mostly mentioned is the lack of any kind of user protection. The most important characteristics of the Bitcoin could be indicated as (Segendorf, 2014):

- Payment by Bitcoin covers the identity of the participants in the transaction. Hence, only the person who pays and the person to whom the payment is done know the transaction. In this way, banks that guaranteed the secrecy of data and transactions were bypassed. Even the users who confirm the transaction receive only the codes, but not the names of the participants in the payment.

- Bitcoin is not regulated by any national legislation, and no appeal can be made to these business transactions. The whole system rests on the users' confidence. There is no central emitter of Bitcoin because the value units are created automatically in the network itself. Bitcoin does not represent a claim from a party, but its value is entirely based on the expectation that it can be used in further transactions. Therefore, the value is very sensitive to changes in these expectations.

- The user also has a risk of losing value either by deceit or accidentally by destroying hardware. The Bitcoin wallet and encryption keys are stored on the media (hard disk). Its damage inevitably leads to the destruction of the wallet. Also, by hacking a computer, access to the wallet and the Bitcoins in it can be gained. That is how Mt Gox was hacked, the world's largest virtual currency exchange company, located in Japan, that has been offering services around the world. It is suspected that the hackers manipulated a list of payments, so it seemed like the payment did not reach the beneficiary, and Mt Gox then made a repayment which ultimately led to the fact that it was left without Bitcoins in the long run. The company had difficulty with paying off at the end of 2013 and it completely discontinued payment at the beginning of February 2014. It is suspected that nearly 850,000 Bitcoins were missing. According to the current value, this would amount to over \$2.5 billion. In Canada, there was also a \$600,000 theft from a company Flexcoin that worked with Bitcoin.

There are three main types of benefits that virtual currencies like Bitcoin bring to society. Primarily, the payment is accompanied by lower transaction costs compared to the traditional payment method. This can bring significant savings to the users of Bitcoin because payments will be exempt from banking and other fees. Another significant advantage of the crypto currency is the introduction of an alternative method of payment in relation to, for

the time being, the only one officially possible through the banking system. This competition will also affect the reduction of the prices of banking services. Existence of the alternative is always beneficial to market flows. Third, as the IT revolution has eased and lowered the cost of transferring money and capital, so it might happen that the crypto currency is an innovation that will technically and economically improve international business. Permanently improving the programs on which the crypto currencies are based makes it truly possible.

Crypto currencies carry a certain risk for the economy and society. First, there is a risk that potential distrust in Bitcoin can be expanded and lead to distrust in other retailers. This can further lead to a massive rejection of this type of payment by users and companies and the return to more expensive and slower payment methods. Second, if key market participants such as banks and financial companies hold a large amount of Bitcoin, it can expose them to significant financial risk. If a fall in value occurs, there may be a halt in the functioning of the entire system. Certainly, one of the negative sides is that these virtual currency schemes, like Bitcoin, since they allow anonymous payments, can be used for money laundering and for criminal activities. An example of this is the Silk Road web site offering drug and criminal services in exchange for Bitcoins. It was closed in 2013 by the FBI.

Currently, Bitcoin is mainly used for relatively low value payments and for speculative deals on the stock market. A drastic rise in stock prices certainly contributed to the increase in its market share, but there are also factors that act in the opposite direction. Those are:

- Lack of user protection or control; legal regulation of this area would, on the one hand, reduce the risk and favorably affect the trust of clients, but would also bring a loss because it practically contradicts the essence of the Bitcoin i.e. independent functioning in relation to monetary and executive authorities.
- Bitcoin is not suitable for all types of payments; to verify the transaction, it usually takes around ten minutes, but sometimes even more than an hour which makes it unsuitable for some common payments (for example, paying cash at the supermarket).
- Variation of interest in the extraction of Bitcoins; if there is no more motive for mining Bitcoin, the whole system can easily collapse. Every day, there is an ever-decreasing amount of Bitcoin at the disposal of miners, which deteriorates the ratio of investment in hardware, electricity, and other costs relative to the value of mined Bitcoins;
- Permanently increasing the list of executed transactions; the public ledger currently has over 140 gigabytes. This makes the network bulky. The incentive to manage such an extensive list has declined, and the number of those who own it on their machines has been reduced. If this trend continues, Bitcoin can become more centralized. If the miners' incentives disappear, there is a risk of halting the decentralized transaction verification and thus making it impossible to use Bitcoins.
- The emergence of other crypto currencies; It should be kept in mind that Bitcoin is the first, but not the only crypto currency in the market. Currently, there are over 1000 crypto currencies and the number is constantly increasing. Some of them took Bitcoin's structure as the basis and then modified or improved it. Others simply wanted to exploit and profit from the attention caused by the Bitcoin by introducing better solutions for its perceived defects. But, no doubt, they all compete with one another, seeking greater market share.

4. FUNCTIONS OF BITCOIN

If the use of Bitcoin as an international liquidity asset is being talked about and it is conditionally referred to as a currency, it is necessary to see if it could perform the function of money. The three basic functions of money are: medium of exchange, unit of account and store of value. These three functions distinguish money from other types of property in the economy, such as shares, bonds, real estate and art works. The exchange of goods and services is maximally facilitated by the discovery of money, i.e. its universality. This explains the function of money as a means of exchange (payment means). But the money itself will become the object of the exchange and will also perform the function of the trading asset. The function of the accounting unit is exhausted through the unit of measurement. Calculating and presenting values and debts is practically impossible without the accounting function of money. Finally, money with its universality allows to store value and to preserve wealth that can be replaced at any moment for any good or service.

To serve as a medium of exchange, Bitcoin must be accepted as a means of payment for a sufficiently large number of goods, services, by individuals and legal entities that will accept it as a symbol of value. Namely, fiduciary money is accepted as a medium of exchange for products and services if the market participant is certain that other participants will also accept and use this asset. However, unlike national currencies behind Bitcoin there is not one sovereign institution that guarantees its value. So, if it wants to function as a means of exchange, it has to rely on the individual expectations and confidence of the market participants who decide whether to accept it or not. From the very beginning, its use was limited to e-commerce sites, primarily on the purchase of products and services of lower values. However, with the rise in the value of Bitcoin the circle of participants in the market that accept this crypto currency is expanding. In order to protect themselves from the high volatility of Bitcoin, sellers are expressing all the prices in dollars, while prices in Bitcoins are calculated every 10 to 15 minutes, since that time is necessary to create a new block of Bitcoin and potentially influence on the change of exchange rate. Some sellers point out how much is saved by buying with Bitcoins, and what sellers are doing is reducing taxes and expenditures that are usually paid to banks and financial institutions. It can be said with certainty that Bitcoin fully functions as a means of exchange in the circle of partners who have accepted this crypto currency. But, for the time being, it does not possess the universality as the real top currencies do.

The accounting and the function of keeping value for Bitcoin and other crypto currencies are under the big question mark. The reason for such a claim lies in the high volatility of the crypto currency exchange rate. That is why sellers who accepted Bitcoin as a means of payment immediately convert it into a real currency just after the transaction is completed. Even the prices are generally expressed in real currencies, and only the payments can be realized by Bitcoins. Rogojanu and Badea (2014) noted that one of the challenges with Bitcoin is that the number of Bitcoins is limited to 21 million, but Van Alstyne (2014) pointed out that fractional ownership of a Bitcoin is possible; therefore, the 21 million is not a limiting number. Compared to national currencies whose basis is the real value of monetary gold or the guarantee of a central bank that covers trust in fiduciary money, trust in the crypto currency should be built by the market participants themselves by massively accepting the crypto currency. Because of this, Bitcoin is also subject to speculation and prone to price "bubbles". High volatility, numerous headlines about large speculative investment in Bitcoin, as well as possible hacker attacks make it not so desirable for the store

of value function and the accounting unit. However, many currencies incur extreme volatility and are still considered currencies (Dornbusch et al., 1995). Beyond the crypto currency, there is not one institution whose priority task is to fight for the stability of their value as the central bank does for the value of national currencies. Speaking of crypto currencies, all participants are motivated exclusively by profit, which in case of a major change in exchange rate can result only in inflating the bubble.

Large oscillations of Bitcoin value can be characterized as ideal for speculative stock trading. Given that the supply is relatively constant, planning the future business activities of speculators is facilitated to only following the demand. Only in May 2017, Bitcoin increased its value from about \$1200 to \$2400 in just ten days. This will be a sufficient motive for the emergence of other crypto currencies and their listing on the stock exchanges. Therefore, as the dominant function of crypto currencies and Bitcoin is the exchange in which they represent goods in the hands of speculators on the stock exchanges. The reason for such a conclusion is clear – such use of the crypto currency can make the greatest profit by taking the appropriate risk. The number of profit-oriented individuals is likely to be the reason for expanding its usage in practice, as well as the unexpected rise in the value of Bitcoin and other crypto currencies.

There is also a question whether Bitcoin is a medium of an international liquidity used for international payments. Since it is necessary to have partner's consent for paying with Bitcoins, this crypto currency could be declared as a medium of international liquidity. But it does not meet all the necessary conditions for performing international payments, since these transactions are not yet recorded in the balance of payments. Of course, it is a matter of time when this area will be regulated by both national legislations and the International Monetary Fund.

5. MOVEMENT OF BITCOIN VALUE

The value of Bitcoin depends exclusively on the market, i.e. on offer and demand. The maximum supply on the market is 21 million Bitcoins, but is currently it is lower (around 16 million), since the number of Bitcoins in circulation can be increased exclusively by "mining". Additionally, it is possible to control the number of mined units through software, but that would, on the other hand, abolish the decentralization of the system.

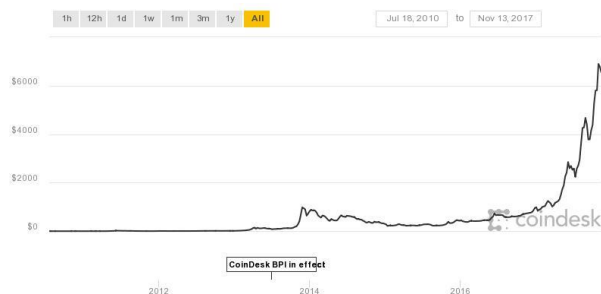


Fig. 1. Bitcoin value in US dollars over time

Source: Coin desk

From its very appearance, almost until 2013, the value of Bitcoin was negligible and was used by technologically enthusiastic people as well as those interested in cryptography. However, after that, there is an immense jump in value, especially at the end of 2013, when the price on some stock exchanges reached the maximum at that time of 1,000\$. Then, after reaching the peak, numerous fluctuations occurred, but the value did not fall below 250\$. Up until 2014 the trend of rapid growth in the value of Bitcoin was recorded. Steepest drop in value was recorded in 2014 (about 50%) due to a hacker attack, which led to a loss of confidence in the entire system. Since 2015 there has been a steady increase in the value of Bitcoin. As early as March 3rd, 2017, the price of Bitcoin exceeded the price of gold. On that day, the ounce of Gold reached 1233\$, while Bitcoin was worth 1290\$. Bitcoin was split into two derivative crypto currencies, classic bitcoin (BTC) and Bitcoin Cash (BCH) on August 1st, 2017. As a result, price climbed to 3.000\$, then 4.000\$, and it peaked on September 1st, 2017, when a Bitcoin was worth 5.000\$. But on September 12th, 2017, the price of Bitcoin sharply declined because of a slump in the Chinese market as it represents almost one quarter of the world's global Bitcoin market, and the price dropped to \$2,900 reaching its recent bottom. After recovering from this, price reached an all-time high of 7.850\$. Currently the value is fluctuating between 6.000\$ and 7.000\$.

As demand almost exclusively affects the value of Bitcoin, it is possible to assume that the intention of the creators of this currency was to offer a very small quantity to the market and to make the market projected shallow. This means that a relatively small number of new clients could significantly increase the percentage of demand and with a presumption of stable supply would lead to a drastic increase in the price of Bitcoin. It would have a double effect. On the one hand, this would diminish the suspicions of Bitcoin that followed it from its creation, while on the other hand it would be a magnet for speculators on stock exchanges, which would further increase the demand. Thus, these two processes would feed each other, which would result in a constant increase in the value of Bitcoin. In any case, whether this strategy was planned or not, it has borne fruit and the value of Bitcoin has a growing trend with occasional falls that are necessary for popularity with speculators.

CONCLUSION

Based on the most important features of the crypto currencies (user anonymity, elimination of tax and payment fees, the risk of converting real currencies into virtual ones for which no one offers any guarantees, high volatility of value), the future of Bitcoin and other crypto currencies can take several directions:

- An optimistic scenario assumes an increase in the popularity of Bitcoin that would lead to further growth in value, provided that the maximum amount of Bitcoin that can be found on the market remains limited to 21 million units. But that would also mean the pressure to increase the supply that is probably not a problem to do from the software point, but would open doubts about the manipulation of the creators with the entire system. Also, the risks from losing state control over the monetary and fiscal policy measures are automatically opened up.

- Another possibility is the strengthening of other crypto currencies to meet the growing demand. There is already a serious competition between the crypto currencies for acquiring clients who are willing to take the risk and do business with virtual money without the guarantee of any institution;
- The third scenario is advocated by supporters of the conventional monetary system concept. According to them, it is a matter of time when the creators of crypto currencies would make a fatal error that would eliminate them from the market, or when the organizers of the game from the top of this pyramidal structure would withdraw and the whole building would collapse in one day. This could happen even if serious frauds were detected in payments with these currencies. The blast that would occur around the Bitcoin would resemble a real estate bubble in America that burst in 2007. Many also compare Bitcoin with the "Tulip Mania" that was actual in the Netherlands during the 17th century. Pessimists assume that one steep decline in the price of this virtual currency would lead to its general abandonment, huge sums of money would be lost, and Bitcoin would become just another interesting story;
- The most optimistic view is that these currencies will take a firm position in monetary relations. This does not mean that they will completely suppress the national currencies, and especially the real value of gold, as the emergence of electronic money did not completely expel the cash from circulation. It could be said that, according to this scenario, the crypto currencies would acquire their stable share in the portfolio of assets of an individual, firm, and perhaps a state. The longer the crypto currencies remain on the market, the states would be under greater pressure to legally regulate this area.

It is hard to believe that through crypto currencies private interests could be embedded into monetary policy, which should protect the interests of the state. But hasn't the Federal Reserve System, which has been functioning as a central bank of the United States, since its creation, been functioning as a private institution? Perhaps the monetary system should be put into the function of generating profit and private interests so that liberal capitalism can reach its maximum amplitude. Perhaps this is the only way to prove that economy and society, as well as nature, do not rest on extremes, but that they are only passing points, and that the essence of survival and development lies only in movement.

REFERENCES

- Brito J., Houman B. Shadab & Castillo A. (2014). Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling. *Columbia Science and Technology Law Review*.
- Carrick J. (2016). Bitcoin as a Complement to Emerging Market Currencies. *Emerging Markets Finance and Trade*. Volume 52, 2016 - Issue 10., 2321-2334.
- Charlie S. (2013). *Why I want Bitcoin to die in a fire*. *Charlie's Diary, December 18*. Retrieved from: <<http://www.antipope.org/charlie/blog-static/2013/12/why-i-want-bitcoin-to-die-ina.html>>. Accessed on 20.10.2017.
- Chu J., Nadarajah S. & Chan S. (2015). Statistical Analysis of the Exchange Rate of Bitcoin. *PLoS ONE* 10(7): e0133678. doi:10.1371/journal.pone.0133678.
- Coin desk, Retrieved from: <https://www.coindesk.com/price/>, Accessed on: 13.11.2017.
- Dong H., Habermeyer K., Leckow R., Haksar V., Almeida Y., Kashima M., Kyriakos-Saad N., Oura H., Saadi Sedik T., Stetsenko N. & Verdugo-Yepes C. (2016). IMF STAFF DISCUSSION NOTE: Virtual Currencies and Beyond: Initial Considerations. *INTERNATIONAL MONETARY FUND Monetary and Capital Markets, Legal, Strategy and Policy Review Departments*.

- Dornbusch R., Goldfajn G., Valdés R., Edwards S. & Bruno M. (1995). Currency Crises and Collapses, *Brookings Papers on Economic Activity* Vol. 1995, No. 2, 219-293.
- European Central Bank Retrieved from: <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> Accessed on: 12.05.2017.
- Joshua R. Hendrickson, Thomas L. Hogan & William J. Luther. (2015). “*The Political Economy of Bitcoin*. (working Paper, p. 5.) Retrieved from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2531518. Accessed on: 21.10.2017.
- Kubát M. (2015). Virtual currency bitcoin in the scope of money definition and store of value, *Procedia Economics and Finance* vol. 30, 409 – 416.
- Lo S. & Wang C. (2014). Bitcoin as money?. *Current policy perspectives*, Federal Reserve Bank of Boston. 2014 Series, No. 2014–4.
- Mankiw G. & Taylor M. (2008). *Ekonomija* [Economics]. Beograd: Data status.
- Marković I. & Todorović M., (2017). *Spoljnotrgovinsko i carinsko poslovanje* [Foreign trade and customs operations]. Niš: Ekonomski fakultet Niš.
- Nakamoto S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from: <https://bitcoin.org/bitcoin.pdf>. Accessed on: 15.10.2017.
- NBS Retrieved from: <http://www.nbs.rs/internet/latinica/scripts/showContent.html?id=7605> Accessed on: 20.05.2017.
- Peng S. (2013). BITCOIN: Cryptography, Economics, and the Future. *Senior Capstone Thesis School of Engineering and Applied Science*, University of Pennsylvania.
- Segendorf B. (2014). What is Bitcoin?. In: Berg C., Edlund T., Jönsson K. & Roos-Isaksson C. (Eds.) *Sveriges riksbank economic review* 2014:2. Sweden: Claes Berg.
- Todorović M. & Marković I., (2013). *Međunarodna ekonomija* [International economics]. Niš: Ekonomski fakultet Niš.
- Van Alstyne M., (2014). Why Bitcoin has value, economic and business dimensions. *Communications of the ACM*, Vol. 57 No. 5, 30-32. doi: 10.1145/2594288.
- VRBÍKOVÁ L. & VYSKOČIL J. (2014). Právní a daňové aspekty Bitcoinu. In: Zkušenosti s virtuálními měnami - Bitcoin měna budoucnosti?. [Legal and Tax Aspects of Bitcoin. In: Experience with Virtual Currencies - Bitcoin Future Currency?]. Praha: Vysoká škola manažerské informatiky, ekonomiky a práva, 136-139.
- Zohar A. (2015). Bitcoin: under the hood. *Communications of the ACM*, 58(9), September 2015, 104-113. ACM New York, NY, USA.

MECHANIZAM FUNKCIONISANJA BITKOINA

Spoj finansijskih inovacija i informatičke tehnologije je iznedrio i već desetak godina na tržištu održava kripto valute, svojevrstan izdanak monetarne evolucije nakon uvođenja virtuelnog, elektronskog i digitalnog novca. Iako je njihova suština još uvek obavijena velom tajne, činjenice pokazuju da vrednost bitkoina kao prve kripto valute ima rastući trend, te da se sve veći broj firmi i pojedinaca opredeljuje za njegovo korišćenje. To će rezultirati pojavom preko 1000 novih kripto valuta. Ovaj rad objašnjava nastanak i funkcionisanje bitkoina, njegove karakteristike i funkcije, koristi i rizike koje sa sobom nosi, kao i moguće scenarije daljeg razvoja međunarodnog monetarnog sistema sa kripto valutama.

Ključne reči: virtuelne valute, kriptovalute, bitkoin, funkcije novca, međunarodna plaćanja