THE RISKS OF BITCOIN USE

Mircea PLOTEANU[1], licentiate in economic sciences,
Academy of Economic Studies of Moldova
Oleg STRATULAT[2], PhD, Professor,
Academy of Economic Studies of Moldova

Actuality and purpose of work. Bitcoin is a currency that exists only virtually and has appeared due to the global financial crisis and development of technologiesof technologies. Cashless payments become more popular and in this context e-commerce has improved. There were Aanalized the ysis of bitcoin perspectives in the banking system, by emphasizing analyzing the strengths and weaknesses of this currency and the point of view of investors, central banks and commercial banks. The methods used. The methodological approaches used bymentioned in special literature were used. The results of the work. Analysis can be used to improve electronic commerce and cashless payments in Moldova, where cash is still very widely used.

Key words*. Bitcoin, cryptocurrency, blockchain, transactions, bank, investor.*

Actualitatea și scopul lucrării. Bitcoinul este o monedă care există doar în mediul electronic și a apărut în urma crizei financiare globale și datorită dezvoltării tehnologiilor informaționale. Plățile fără numerar devin tot mai populare, în acest context, evoluează comerțul electronic. Este studiată analiza perspectivelor utilizării bitcoinului în sistemul bancar, cercetate punctele forte și punctele slabe ale acestei monede, precum și opinia investitorilor, băncilor centrale și băncilor comerciale. Metode. Suportul metodologic este consituit din abordările folosite în literatura de specialitate. Rezultatele lucrării. Analiza poate fi aplicată în dezvoltarea comerțului electronic și a plăților fără numerar în Republica Moldova, unde numerarul este folosit pe larg.

Cuvinte-cheie. *Bitcoin, criptovalută, lanț în bloc, tranzacție, bancă, investitor.*

Актуальность и цель работы. Биткойн является валютой, которая существует только в электронном виде, которая появилась из-за мирового финансового кризиса и развития информационных технологий. Безналичные платежи становятся все более популярными и развивалась в этом контексте и электронная торговля. Анализ использования биткойн в банковской системе, анализируя сильные и слабые стороны этой валюты, а также точки зрения инвесторов, центральных банков и коммерческих банков. Используемые методы. Методологические подходы, которые используются в специализированной литературе. Результаты работы. Анализ может быть использован в целях развитии электронной торговли и безналичных платежей в Молдове, где наличные средства по-прежнему очень широко используются.

Ключевые слова. *Биткойн, криптовалюта, цепочка блоков, транзакция, банк, инвестор.*

JEL Classification: G24; E5; L81; O30.

Introduction. The modern technologies have changed the world of money and the essence of currency. Moreover, it has generated a new form of currency – cryptocurrency. Among these, the most highlitedhighlighted is the bitcoin.

The bitcoin phenomenon. Bitcoin is a virtual currency – cryptocurrency, invented by Satoshi Nakamoto in 2008. It seems that the disappointments regarding flat currencies – dollar, euro and others have reached a critical point. The evolution of this currency is amazing. At the beginning of 2015 there were over 14 million Bitcoin in circulation (Figure 1).

[1] © ***Mircea PLOTEANU, ploteanumircea@yahoo.com***
[2] © ***Oleg STRATULAT, ostratulat@yahoo.com***

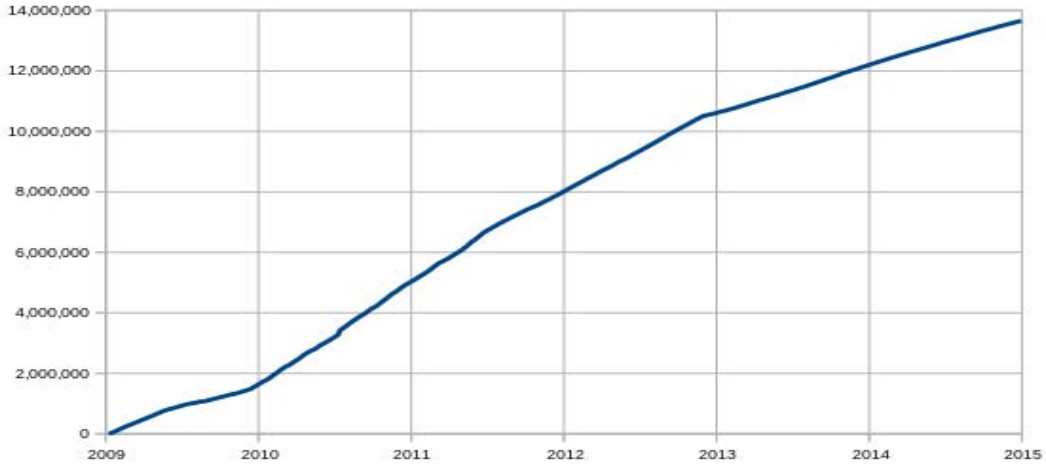

Fig. 1. Amount of bitcoins in circulation

Source: https://en.wikipedia.org/wiki/Bitcoin#/media/File:Total-bitcoins.svg [1].

From 2009, Bitcoin had a stable evolution until 2011, but from 2011 the exchange rate against the US dollar increased from $ 0.30 for a bitcoin (BTC), to about $ 17. In early 2011, a number of issues of entities that conduct transactions in dollars led to rapidly falling prices at $ 5 / BTC. 2011 and 2012 were periods of consolidation, and the exchange rate increased to 14 $/BTC.

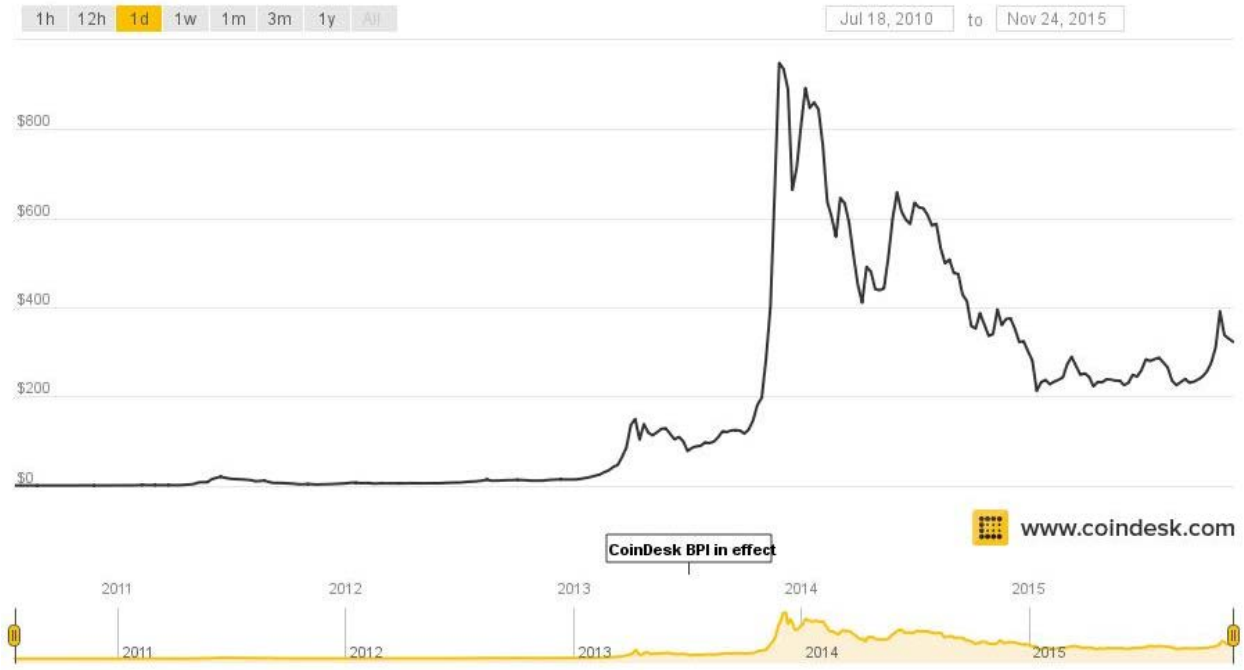

Fig. 2. The evolution of exchange rate, BTC/$ [2]

Source: http://www.coindesk.com/price/.

In 2013, the price of Bitcoin has exploded from 14 $/BTC in January to over $ 1000 in November - December 2013. An important role in this growing had the crisis in Cyprus (after blocking of the accounts in several banks). If 2013 was dominated by small bitcoin network "players", after involving of companies and investors the use of bitcoin has raised. The exploding rise of the exchange rate against the dollar has attracted the attention of authorities in many countries and bitcoin is not recognized as legal payment instrument. The exchange rate has declined steadily and was ranging several months between 550 to 650 $/BTC.

The whole structure is based on the ideas of bitcoin that Nakamoto defined as a chain of digital signatures, it is possible to consider the coin as a token digitally signed by the owner that desires to

transfer the currency. So each user transfer the coin to other subject in the network digitally signing a hash of the previous transaction and the public key of the next owner, the signature is then added to the end of the token.

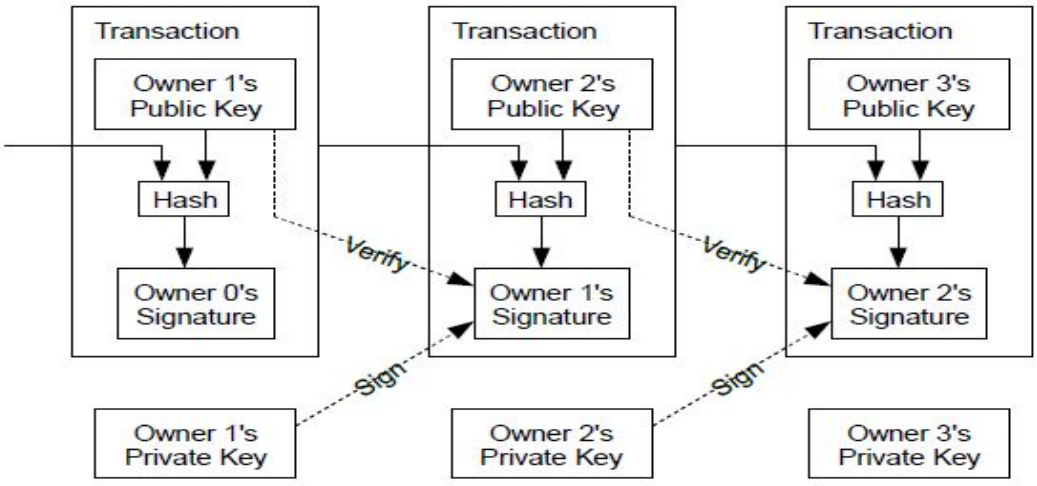

Fig. 3. The scheme of a bitcoin transaction

Source: http://www.4flush.com/bitcoin [3].

Only beneficiary could verify the previous transaction using its private key because the coin has been signed using its public key and this permit it to verify the chain of ownership. The described process has solved the problem of authentication of the payment, but we are not able to avoid the duplication of the transaction, in practice the circuit must avoid that the same coin could be used in multiple transactions.

The model is assured with the task of verifying that each coin is spent only once, this central authority is named "mint". After each transaction the mint acquires the coin used to issue a new coin, in this way only the coins distributed directly from the mint are valid and only for them there is the assurance that have not already been spent.

Each new transaction is spread to all nodes of the network that collect the information related to the operation into a block. After verifying the time validity of the data the node spreads the block to other elements in the network.

The bitcoin software links to the network and generates the private and public keys necessary to take part to the process. The security of the model consists in the impossibility to exploit user's private key from its public key, making impossible to impersonate the user. The keys could be moved from a PC to another because are stored in a file resident on the user's PC.

Each transaction is characterized by beneficiary's public key, owner private key and of course the amount of bitcoins that have to be transferred.

When a user A transfers the money to another user B prepares an information block which has the public key of B (the address) and the amount of coins to be transferred, by signing with the A private key. The information is then spread in the network and the nodes validate the signatures and the amount of numbers implicated before accepting it. When a node verifies the correctness of the transaction, it sends the details to the network to permit to other entities to verify them to permit to specific machines to add the transaction to a public record of transactions, and these machines are known as "*miners*". The security level of the model is high, and makes impossible the creation of false transactions, each user can use only the bitcoins he has.

A transaction declares to the network that the holder of a number of bitcoins has accepted the transfer of some of bitcoins to another holder. The new owner can now spend these bitcoins by making another transaction that authorizes transfer to another owner, and so on, in a chain of ownership. Each transaction contains one or more "inputs", which are debits against a bitcoin account. On the other side of the transaction, there are one or more "outputs", which are credits added to a bitcoin account. The debits and credits do not necessarily add up to the same quantity.

The inflation program is initially planned for bitcoin and is known to all holders of bitcoin. Thus, inflation cannot be manipulated in order to affect the central spreading of value from ordinary users.

Bitcoin customer nodes transmit transaction, and the system is sending it in the network. Doubtful transactions are rejected by honest nodes. Transactions are free, but a fee could be paid to other nodes to facilitate transaction processing.

The risks of bitcoin use. Use of the bitcoin by banks is also questionable at the moment. But along the way, banks could use this money, such as Goldman Sachs and Standard Chartered, who published their recent reports that could use this money in the future. J. Panachyata, employee of BNP Paribas, says that use of Bitcoin will contribute to the development of global trade, in an article posted on his blog. Also Societe Generale is showing interest in bitcoin – the bank seeks an IT cryptocurrency specialist. Meanwhile, Swiss bank UBS has announced it will open a laboratory that will handle blockchain technology. US bank Goldman Sachs published a report in 2014 on virtual currencies, where is underlined the importance of cryptocurrencies. Spanish bank Santander says that thanks to blockchain technology, the costs could be reduced by 15-20 billion euro annually by 2022. A. Patwardhan from the bank Standard Chartered said that bitcoin will never become an alternative to fiat currencies [4]. Thus, we see that most commercial banks have an optimistic attitude towards this currency, while other analyzes market trends. But the central banks have taken a much tougher position against bitcoin, arguing that the use of cryptocurrencies implies shocking risks. With all its phenomenology, the use of bitcoin implies shocking risks. "Virtual currencies such as bitcoin, include potential risks to the financial system. Virtual currency is not a national currency and any currency and a payment acceptance is not binding legally. However, the virtual currency is not a form of electronic money within the meaning of Law no. 127/2011 regarding the activity of issuing electronic money", citing a National Bank of Romania release [5].

"The central bank shows that using virtual currency schemes as an alternative payment is potentially risky to the financial system because of lack regulation and supervision, money laundering, terrorism financing, price volatility and lack of adequate security", citing data from a report recently issued by the European Central Bank [6]. Unlike national currencies issued by central banks, bitcoin is generated by a complex chain of interactions between huge networks of computers worldwide. The coin has been criticized for its anonymous character and absence of regulation, there is concern about the possible use of it for financing terrorist activities or organized crime. Chair of FED, Janet Yellen, said the institution she leads cannot control a virtual currency [7], while countries like Russia and China have strongly restricted the use of bitcoin [8]. And some skeptical investors such as Warren Buffett, who said that in next 50 years the assets will have a higher value than paper money or bitcoin [9]. Famous economist Nouriel Roubini said that "Bitcoin is not a currency. It is a Ponzi scheme and a good conductor for criminal or illegal activities" [10]. Other investors such as Richard Brenson supports the idea of cryptocurrencies, believes in their future and in their potential [11]. If we are analyzing the topic from the security point of view, the issue is very huge. According to a study by Kapersky Lab [12], bitcoins can be stolen by wallet scammers and bitcoin softwares are attacked by malicious viruses.

Conclusions. Virtual currency schemes, such as bitcoin, are not full forms of money as usually defined in literature. Anyway, these schemes may replace banknotes, scriptural money and e-money in some situations. For the tasks of central banks, the materialization of these risks depends on the amount issued for the respective schemes, their bond to the real economy, including through regulated institutions implied with cryptocurrencies schemes, their traded volume and on user acceptance. Participation in such schemes exposes users not only to key payment system-like risks but also to other risks coming from the characteristics of cryptocurrencies. In particular, users are exposed to exchange rate risk related to high volatility, to counterparty risk related to the anonymity of the beneficiary and to investment fraud risk related to the absence of transparency. So there are both general and specific ways in which users could lose their whole virtual money. Some aspects of these risks are peculiar to the cryptocurrency concept and the risks mostly remain unmitigated by legislation, regulation or supervision.

The reactions from governments to the phenomenon are different, partly depending on the part of the world these originate from and on the type of authority. Responses differ from warnings about risks, statements and clarifications on the legal status, licensing and supervision of cryptocurrency-related activities, or the interdiction of those.

To conclude, we can say that the future of bitcoin is uncertain because it exists only in virtual environment and has a decentralized character. Commercial banks see a perspective in bitcoin, but do not rush to accept the payment instrument and analyze trends. But central banks have taken a tough stance against bitcoin, because the currency has a decentralized character and risks, such as money laundering, terrorist financing and anonymity.

REFERENCES

1. Bitcoin [accesat 02 septembrie 2015]. Disponibil: https://en.wikipedia.org/wiki/Bitcoin#/media/File:Total-bitcoins.svg
2. Bitcoin Price Index Chart [accesat 02 septembrie 2015]. Disponibil: http://www.coindesk.com/price/
3. GILL, T.J. Bitcoins. The Future of Currency*?* [accesat 02 septembrie 2015]. Disponibil: http://www.4flush.com/bitcoin
4. PEREZ, Yessi Bello. 8 Banking Giants Embracing Bitcoin and Blockchain Tech, 27 july 2015. [accesat 02 septembrie 2015]. Disponibil: http://www.coindesk.com/8-banking-giants-bitcoin-blockchain/
5. BANCA NAŢIONALĂ A ROMÂNIEI. Comunicat referitor la schemele de monedă virtuală, 11 martie 2015 [accesat 02 septembrie 2015]. Disponibil: http://www.bnr.ro/page.aspx?prid=10016
6. EUROPEAN CENTRAL BANK. Virtual currency schemes – a further analysis. Frankfurt am Main, Germany, 2015. 37 p. ISBN 978-92-899-1560-1 [accesat 02 septembrie 2015]. Disponibil: http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf
7. YELLEN, Janet. Federal Reserve has no authority to regulate Bitcoin, 27 february 2014 [accesat 8 septembrie 2015]. Disponibil: http://www.theguardian.com/business/2014/feb/27/janet-yellen-federal-reserve-no-authority-regulate-bitcoin
8. SMART, Evander. Top 10 Countries in Which Bitcoin is banned, 27 may 2015 [accesat 02 septembrie 2015]. Disponibil: https://www.cryptocoinsnews.com/top-10-countries-bitcoin-banned/
9. БАФФЕТТ, Уоррен. Активы лучше денег в следующие 50 лет. 2014, 3 martie 2014 [accesat 02 septembrie 2015]. Disponibil: http://www.vestifinance.ru/articles/40146
10. ROUBINI, Nouriel. Bitcoin Is a 'Ponzi Game', 10 mars 2014 [accesat 02 septembrie 2015]. Disponibil: http://blogs.wsj.com/moneybeat/2014/03/10/nouriel-roubini-bitcoin-is-a-ponzi-game/
11. BRANSON, Richard. How digital currency could transform the world, 13 november 2014 [accesat 03 septembrie 2015]. Disponibil: http://www.virgin.com/richard-branson/how-digital-currency-could-transform-the-world
12. BĂDĂRĂU, Elena. Securitatea naţională şi diminuarea riscurilor ciberameninţărilor = National security and reducing of cyber-attack risks. In: Economie şi Sociologie = Economy and Sociology. 2014, no. 4, pp. 85-103. [accesat 03 septembrie 2015]. Disponibil: http://ince.md/ro/complexul-editorial/publicacii-periodice/reviste-tiinifice/economie-si-sociologie/

Recommended for publication: 14.09.2015