finiz
Singidunum University International Scientific Conference
Međunarodna naučna konferencija Univerziteta Singidunum

FINANCE, BANKING AND INSURANCE
Professional paper

MONETARY AND TECHNOLOGICAL ASPECTS OF THE EMERGENCE AND THE DEVELOPMENT OF CRYPTOCURRENCIES

Zoran Jović*,
Goran Kunjadić

Singidunum University,
Belgrade, Serbia

Abstract:

An emergence and a rapid development of cryptocurrencies have its monetary and technological background. From the monetary aspect, cryptocurrencies emerged as one of the solutions to the consequences of the last major World financial and economic crisis. To address the consequences of this crisis, the solution was the expansive monetary policy on the global level. Increasing the quantity of money in circulation leads to the fall of its value, and makes depositors search for the solutions for preserving the value of savings, apart from gold and other precious metals, outside the existing monetary system. In addition to this investment opportunity, the nature of cryptocurrencies as an easily transferable payment method, without an intermediary, further increased their attractiveness. From a technological point of view, the emergence of cryptocurrencies was enabled and supported by the emergence of a blockchain technology as a distributed database. This technology represents a decentralized, publicly available database containing registers of asset and transactions in the so-called peer to peer network run by globally connected computers without the impact of any state institutions or powerful individuals and corporations. Therefore, there is a common belief that transactions with cryptocurrencies are anonymous and, thus, often used on the black market. However, these transactions are only partially anonymous. Governments, as well as other users, may check each and every bitcoin address, the amount of money on these addresses, and the flows of money between those addresses through the Internet. There are also browsers called "blockchainexplorers", on the Internet, where after entering the address, it is possible to obtain information about the cash balance and all incoming and outgoing transactions.

Keywords:
cryptocurrency, blockchain, banking, security, bitcoin

INTRODUCTION

The emergence of cryptocurrencies went relatively unnoticed and in the beginning it was not given special attention. They were considered more as the method of payment in trading illicit goods and services as well as subject of speculative financial activities. There was hardly any comment on this phenomenon in the academic circles. Over time, certain academic works that deal with different aspects of cryptocurrencies have appeared, but their number is still relatively small compared to other academic topics (Jovic, Kunjadic, 2017). The first cryptocurrency, bitcoin, was launched in 2009. Bitcoin is a digital, decentralized cryptocurrency. It is digital because it exists only in a digital form and does not exist as a banknote or in the form of coins. It is not governed by any central bank or any other institution. It is exclusively managed by its users. Therefore, it is characterized as a decentralized cryptocurrency (Jovic, Kunjadic, 2016). The term "crypto" was established because cryptography was used in verifying transactions and creating new currency units. This cryptocurrency is not based on the golden foundation, it has no country of origin and there is not any state or bank organization behind it. Today, the legitimate paper and electronic money does not represent a real value, but a symbol of

Correspondence:
Zoran Jović

e-mail:
zjovic@singidunum.ac.rs

DOI: 10.15308/finiz-2018-63-67

exchange supported by central banks with their authority. Therefore, virtuality does not represent the main difference between conventional and crypto currencies, but the decentralization of cryptocurrencies does. The basic partition of all cryptocurrencies relates to the fact whether they belong to a decentralized or centralized blockchain system. A decentralized system or a peer to peer system functions in such a way that each individual computer is an integral work unit without the authorization by any central point. There is not any individual, bank or government of any country behind these systems. An important feature of these systems is the anonymity of transactions, whereas each transaction is broadcast online and all users have an insight into the validity and execution of the transaction itself, but no one has a personal insight into who sent it to whom and where a certain number of coins is. Counterfeiting is made difficult by the user's digital signature, a private and a public key, and a combination of the transaction message itself. In this way it is achieved that everyone has control, and no one has the power (Jovic, 2014b). Centralized systems function in such a way that behind them there is a group of people who, by their credibility and seriousness, guarantees for the success of the cryptocurrency. In these systems, the identity of the person who holds the currency is known through the KYC procedure - know your customer. In this way, by checking, cryptocurrencies can be introduced into the legal business flows and taxation and avoid the possibility of misuse and concealing the origin of money.

MONETARY ASPECTS OF EMERGENCE AND DEVEOPMENT OF CRYPTOCURRENCIES

From the monetary aspect, cryptocurrencies represent one of the answers to the repercussions of the major world financial and economic crisis. As a resolution of the crisis repercussions, central banks of the developed countries are implementing an expansive monetary policy. This policy aims at increasing the amount of money in circulation which leads to its devaluation. Deposits in the banks are being devaluated and the savings lose their attractiveness. When there is only one country whose currency is being devaluated by its expansive monetary policy, the depositors may find a solution in exchange for savings in another stable currency. However, when such a monetary policy is applied on the global level for a longer time period then, there is no such a solution and the exit must be searched outside the existing monetary system. As always, the solutions to these problems lie in the gold and silver with the aim of preserving value, but, on the other hand, precious metals are complicated for transfers and payment. Moreover, the phenomena of savings confiscations are not unusual in the history, whether in gold or in the national currency. Therefore, there is a real need for easily transferable means of payment which may be used anywhere in the world. Cryptocurrency, by its decentralized nature represents a possible solution to a problem. The state has no monopoly over its supply nor it can use coercion of any kind. Even on the presumption that a state confiscates a cryptocurrency, it can not use it if it does not hold a code which protects an electronic wallet. In a conventional monetary system the government has a monopoly over emission of money which it can use to finance its expenditures through inflation taxation, whereas, the expenses are eventually taken by citizens, primarily by depositors.

On the contrary, all cryptocurrencies have preprogrammed tempo of their construction, so that their amount in circulation is always a known fact, providing greater transparency and predictability comparing to the conventional currencies. Cryptocurrencies simplify transfer of money. The conventional money transfer system involves an intermediary that charges a commission for money transfer, and the amount of the commission increases the risk of a country where the money is sent. By using cryptocurrencies, intermediaries are completely excluded considering the transfer of money. The expenses of sending cryptocurrencies are equal as the expenses of sending any information, actually, the transfer of money becomes accessible as sending an e-mail. The presence of any bank or transfer agent is needless. Internet access from a cell phone or another device is sufficient. Many websites dealing with exchange of cryptocurrencies can be provided with the currency risk protection by exchanging cryptocurrency for the desired conventional currency. As a method of payment, cryptocurrencies are in its initial stage as there are still rare places that accept cryptocurrencies as a regular means of payment, but the tendency of expanding network does exist. Besides, cryptocurrencies are used, today, for long term investments due to their tendency of increasing value, as well as for speculating activities because of expressive volatility of their prices on cryptocurrencies stock exchange (Jovic, 2014). It is assumed that, on a national level, cryptocurrencies will not be able to take primacy over conventional currencies, in the first place, due to a high resistance of central banks. Yet, the faster growth is possible on the global level. Globally, cryptocurrencies could run towards an alternative global currency, but also a better means for calculation and payment than Special pulling rights among countries which would greatly contribute to the future of cryptocurrencies.

Supporters of cryptocurrencies believe that governments might take part in issuing their cryptocurrencies while streaming the monetary policy towards satisfying needs of market participants and not the government. Some countries, like Canada, have already started emission of their version of cryptocurrencies, while certain

banks have associated in creating common cryptocurrencies intended for public. However, there will be significant differences in features of suggested currencies. Bitcoin and other cryptocurrencies are featured by anonymity, whereas in the bankers cryptocurrency, anonymity will disappear as by the bank rules, everything will be under control, such as who the currency belongs to, where it comes from, who has bought or sold what, where and for how much.

Designing a banking digital currency should enable the banking system to become more efficient and cheaper. This leads to the conclusion that it is the question of the day when multinational companies and banks themselves will begin to insist on using cryptocurrencies themselves in order to save large amounts of money on the costs of transfer. Real expansion of cryptocurrencies use may occur when they are created by individual states, their central banks or a group of significant commercial banks. Then, the focus of using cryptocurrencies can be shifted from the population sector to the economic and banking sector, which can mark the beginning of a completely new monetary era.

Since cryptocurrencies are based on the blockchain infrastructure with the basic characteristic that once entered, data cannot be deleted, thus, in addition to monetary transactions, a revolutionary application may occur in other spheres of society such as records in the catastre, records in a medical card, exercising copyrights in the music and video industry etc.When considering the future of cryptocurrencies, we should look into their advantages and disadvantages. There are several great advantages compared to conventional currencies. Cryptocurrencies do not require an intermediary, so there are no commission fees, and at the same time transactions are anonymous. On the other hand, the benefits also result in disadvantages because, by the nonexistence of a controlling authority, the return of money in case that the seller does not deliver the goods or services paid cannot be regulated by law. Some statistics say that in the last few years about 45% of the bitcoin transactions ended with such a fraud. Such problems indicated the development of online exchange offices and the first ATMs where a bitcoin can be exchanged for the standard currency. Wallstreet does not doubt the future of cryptocurrencies as they claim that digital money largely replaces gold, already, especially with younger investors. In these circles, there are opinions that it is only a matter of time when and which crypocurrency will appear officially on the world stock exchanges. Despite the optimistic thinking that at some point bitcoin or some other cryptocurrency might replace the dollar in international transactions, many economists warn that cryptocutrencies can represent a new tulip bubble.

TECHNOLOGICAL ASPECTS OF EMERGENCE AND THE DEVELOPMENT OF CRYPTOCURRENCIES

There is a common belief within public that transactions with cryptocurrencies are anonymous and are therefore often used on the black market. However, these transactions are partially anonymous. Through the Internet, governments, as the other users, can check each bitcoin address, the amount of money on these addresses, and the flows of money between these addresses. There are also "blockchainexplorers" browsers on the Internet, where, after entering the address, one can obtain information about the cash balance and all incoming and outgoing transactions.

It is not possible to make any data changes on the transactions, nor their deletion, addition or any other type of forgery. In this way, fraud is prevented. Secret state information, bank accounts and other centralized data may be hacked. However, Blockchain hacking implies hacking the whole chain of blocks, which is, in fact, impossible. Therefore, this way of storing data in the future can be widely used which goes beyond the era of the cryptocurrencies. In addition to its application as means of payment, Blockchain technology can be used in many areas, for example, for the determination of ownership of shares, fair voting in elections, games of chance, registration of property, copyright, health, etc.

In addition to Blockchain technology, there is also a new concept based on the mathematical mod called Directed Acyclic Graph (DAG). The model is derived from graph theory that uses mathematical structures for modeling relationships between objects. In this model there are no blocks, but transactions are linked by a strictly defined scheme. The concept is called Tangle and its operation is based on a network of controllers of devices connected to the Internet or the Internet of Things (IoT).

Nodes in the process are the devices themselves while the transactions are done by exchanging signals between the devices. One of the fundamental differences is that with using the DAG model processes can be branched in all directions as well as towards existing entities, while in Blockchain, this process is one-way and the process cannot be returned to the existing block. The rule of this system is that every new transaction that has been created - A, confirms two old - B and C.

Verification can also be done indirectly. In the above example, if there is a transaction D, which confirmed A, then it simultaneously confirms the conditional transaction E which has been confirmed by B. The number IoT devices has increased from about 6 billion in 2016 to over 10 billion this year, 2018, which illustrates the degree of network expansion. Although the devices themselves have modest processor capabilities, their number allows the execution of a large number of simultaneous transactions.

In the blockchain system as a support to the Bitcoin cryptocurrency, an asymmetric cryptographic system supported by PKI (Public Key Infrastructure) was adopted as the cryptographic solution. The PKI system implies that CA (Certification Authority), as a third party of trust, generates a pair of keys, public and secret. The secret key is delivered to the owner over the secure channels and never leaves the token or other device on which the owner of the private key keeps his private key. At the same time, CA publicly publishes a public key of the user that is available to all other participants in the transaction.

It is very important to note that a couple of keys must be generated in one place due to a certain mathematical interdependence of the public and the secret key. At the point of generating a pair of keys at the time of creation, the entity that generates the keys is familiar with both keys. In this way, CA, as a trusted entity, actually has all the information about the participants in the transactions and it is possible to absolutely authentically create the identity of any participant. Activities of CA are regulated by strict regulations. The basic question that arises in the virtual world is: Who is, actually, CA? Which regulation regulates his work? And in the end: Who is responsible for controlling the work of CA?

CONSEQUENCES OF CURRENCY DIGITALIZATION

Cryptocurrencies provide free transactions through the blockchain technology, which represents a great saving in money transfer costs. Avoiding high fees for money transfers is a tangible material reason for the increasing use of cryptocurrencies. In addition to being a technological innovation, cryptocurrencies become another method in a series of sources of financing that becomes interesting to large investors. Initial Coin Offerings - ICO becomes an alternative but still unregulated method that enables investing in blockchain technology. The number of ICOs is growing steadily, and their revenues have already exceeded hundreds of millions of dollars.

Bitcoin, as the first cryptocurrency, has already become an instrument of hedging for periods of instability and has grown into a legitimate alternative to gold. The main obstacle to the adoption of bitcoin as a significant alternative to gold is the high volatility of its value. The current situation in the global financial markets is characterized by low, even negative interest rates, so there is not much choice for capital investors. This is a situation that is favorable for investments in cryptocurrencies, besides already mentioned ease of trading at the global level, it still misses the tools for investing and keeping cryptocurrencies, all contributing to the fact that investing and trading in cryptocurrencies is still on the margins of the global financial market. Further behavior of institutional investors and hedge funds will determine the direction of the development of cryptocurrencies. The development of new protocols and blockchains and the ease of financing through the ICO give cryptocurrencies the nature and attractiveness of entrepreneurial ventures and the current global lack of innovative entrepreneurial ideas also contribute to this.

The significance of the blockchain technology that lies at the core of the cryptocurrencies significantly exceeds the monetary and financial sphere. It is a kind of revolutionary technology that allows the credibility of a database whose historical data cannot be changed either from inside or from outside. It is a system in which it is known who exactly and when they signed a certain entry into the database, where every entry into the database is verified by all the other participants in the system before the entry permanently becomes part of the database. Because of these facts, this technology can completely reform the financial sector. Depending on the amount sent to various transaction systems, the commissions range from 3 to 12% with the mandatory waiting for the money to appear in the account, and waiting varies depending on where the money is sent from. Economic logic predicts that cheaper and faster transactions via digital money will be inevitable in the future.

This technology could greatly contribute to the improvement of state governance model, as it is based on the immutability of information or the non-bribery of the system. What is applicable are digital contracts, digital signatures, reduction of paperwork, land ownership registers, people identification, driving automation and insurance field, abolition of seals, queuing, unnecessary procedures, etc. These are all the areas in which the application of blockchain technology could make a major contribution to reducing costs in the financial sector, increasing efficiency of government's administration at all levels and in different areas, and contributing to the development of the economy as a whole.

Moreover, we could be aware of the fact that, as technological developments have recently led workers in factories to unemployment, replacing them with machines that could perform different operations better and more efficiently than humans, likewise, the blockchain technology can leave many officers and administrative workers out of work. Finding balance between efficiency and savings of this technology on the one hand and social costs on the other will certainly have to take place, therefore, opening a series of sensitive issues for all countries of the world (Jovic, Kunjadic, 2017).

A legal position of the cryptocurrencies differs considerably from country to country and varies in its field of use from indirect treatment as a currency to the treatment as taxable property. The lack of uniform regulations and

rules which regulate transactions in cryptocurrencies has its consequences. On the one hand, their disadvantage, to a certain extent, represents a benefit by providing independence from political and economic centers of power, but on the other hand it opens up a polygon for speculation and illegal criminal activity. Since the transactions in cryptocurrencies are independent of formal banking systems, the realization of profit and taxation system is virtually impossible to track, and anonymity itself makes it a convenient money laundering tool.

CONCLUSION

The analysis of the mathematical apparatus that supports the cryptography of crypocurrencies revealed undisputedly that the generation of cryptographic keys must be done in one place that is CA. From the above, it can be concluded that there is an entity that controls the generation of cryptographic keys, and, therefore, controls the entire cryptographic system.

Starting with such assumptions, two possible theories about the purpose of the cryptocurrencies can be made. On the one hand, it can be assumed that, behind the development of cryptocurrencies, there are powerful countries in the world that enormously increased their state debts and money supply during pre-crisis and crisis times. The emergence and purchase of cryptocurrencies leads to the sterilization of surplus of conventional money, and in time, the debts in conventional currencies can be converted into debts in cryptocurrencies. Since the cryptocurrencies are not regulated in the same way as the conventional currencies are, the various nation states are not in any way prevented, when there is a significant portion of their debt in cryptocurrencies, to proclaim cryptocurrencies an illegal payment method intended for money laundering and criminal activities. In this way, they would solve part of the state debts overnight.

On the other hand, it might be that this is a great monetary war for defense or forming the new standards in international payments. It is known that the BRICS countries are trying to establish their system of mutual payments beyond the world's leading currency and that it is those countries who are taking the lead in the development and use of cryptocurrencies. It is possible that they intend to break the primacy of the world's leading currencies through the cryptocurrencies. However, it is possible that the relevant factors behind the world's leading currency today are also creating a leading global cryptocurrency that could become an accepted standard of payment in the future and therefore retain the primacy in the world monetary market in the new conditions.

The behavior of the Central Banks in the world is important for the future of cryptocurrencies. From their point of view, it is desirable to have only one means of payment in a certain territory, as this gives a stronger effect for the monetary policy. Some of the central banks are considering introducing their own cryptocurrencies, because, essentially, the digital currency of the Central Bank would be like a banknote, only in digital form. For the population and the economy, this can bring significant benefits, as the digital currency does not charge transaction fees and interest rates such as, for example, credit cards, nor there is any greater processing costs as in the case of banknotes. What the Central Banks can offer as an advantage over decentralized cryptocurrencies is the fixed nominal value of the digital currency. Potentially strict regulations of Central Banks would provide additional stability to new cryptocurrencies and reduce the level of sensitivity to market trends, but, on the other hand, they would influence the basic postulates of existing cryptocurrencies, taking away one of their essential characteristics which is the purpose why they were created in the first place.

LITERATURE

Jovic Z., (2014), Application of information technology in the financial performance of non-cash transactions, Zbornik radova, VI naučni skup sa međunarodnim učešćem Mreža 2014, Valjevo, pp.14-19.

Jović Z., (2014b), The use of the Internet in modern banking and stock exchange activities, Zbornik radova, Međunarodna naučna konferencija Sinteza 2014, Beograd 25.-26.04.2014., pp.180-185.

Kunjadić G., Jović Z., (2016), Bitcoin – banking and technological challenges, FINIZ, Singidunum University International Scientific Conference – Risks in contemporary business, Collection of works, Beograd, pp.185-189.

Jovic Z., Kunjadić G., (2017), Economic, Security and Information Aspects of the Use of Cryptocurrencies and their Impact on the Black Sea Region Countries, Second International Scientific Conference "Cross-Border Cooperation, Security and Development Perspectives of the Wider Black Sea Region, Collection of works, Veliko Trnovo.

Marcelo Fiore, Marco Devesas Campos (2013), The Algebra of Directed Acyclic Graphs, Computer Laboratory University of Cambridge, UK.