CRYPTOCURRENCIES – ADVANTAGES AND DISADVANTAGES

ISSN 1857-9973 336.743:004.031.4

Flamur Bunjaku[1], Olivera Gjorgieva-Trajkovska[2], Emilija Miteva-Kacarski[3]

[1]Doctoral student, University Goce Delcev Stip, Faculty of Economics, flbunjaku@gmail.com

[2]University Goce Delcev Stip, Faculty of Economics, olivera.trajkovska@ugd.edu.mk

[3]University Goce Delcev Stip, Faculty of Economics, emilija.miteva@ugd.edu.mk

Abstract

Recently, cryptocurrencies and bitcoin have become the main topics in the financial industry. A cryptocurrency is a digital or virtual currency that uses cryptography for security. A cryptocurrency is difficult to counterfeit because of this security feature. A defining feature of a cryptocurrency, and arguably its most endearing allure, is its organic nature; it is not issued by any central authority, rendering it theoretically immune to government interference or manipulation. Cryptocurrencies have their benefits and drawbacks. The paper elaborates different aspects of cryptocurrencies, starting with their early development, challenges and risks, opportunities, advantages and disadvantages, and their future. In addition, the paper covered issues related to the practical and technical function of cryptocurrencies. It was concluded that is not easy to predict the future of cryptocurrencies, since there is a lot to be done especially in the field of formal regulations. However, the banks and other financial institutions should see and consider cryptocurrencies as an alternative for the financial transactions in the future.

Key words: cryptocurrencies, development, advantages disadvantages, financial transactions

1. Introduction

In a historical retrospective, markets in general and financial markets in particular, have experienced a huge development. In this regard the instruments used as exchange instruments have also experienced change and have evolved in accordance to the markets needs aiming to make trade transactions as easy as possible. Those instruments used to intermediate the exchange of goods are known as money. Most of the economists define money as something that serves as a medium of exchange, a unit of accounting, and a store of value. Money is a medium of exchange in the sense that we all agree to accept it in making transactions. Merchants agree to accept money in exchange for their goods; employees agree to accept money in exchange for their labor. As a unit of accounting, money provides a simple device for identifying and communicating value. Money serves as a store of value in that it allows us to store the rewards of our labor or business in a convenient tool. In other words, money lets us store the value of a long, hard week of work in a tidy little stack of cash. Without money, how would we set aside the compensation we receive for later use? From the era of barter to commodity money, metal and coins, to gold and silver, continuing by modern monetary systems and checks and ending with the latest global currency developments, such as introduction of cryptocurrencies known as bitcoin and ethereum and alike, have passed centuries. Each type of the money has played it indispensable role in transaction activities for the respective time period. However, as the human society in general and markets in particular evolved, there was a need for more sophisticated goods exchange instruments. In this regard the introduction of cryptocurrencies has revolutionized the international payment system in a scale that just few years ago were unimaginable. A cryptocurrency is a digital or virtual currency that uses cryptography for security. A cryptocurrency is difficult to counterfeit because of this security feature. A defining feature of a cryptocurrency, and arguably its most endearing allure, is its organic nature; it is not issued by any central authority, rendering it theoretically immune to government interference or manipulation. Cryptocurrencies have their benefits and drawbacks. The main benefits of cryptocurrencies use are that they make it easier to transfer funds between two parties in a transaction; these transactions are facilitated through the use of public and private keys for security purposes. These fund transfers are done with minimal processing fees, allowing users to avoid the steep fees charged by most banks for internet online based transactions. The threat of hacking is the biggest threat of cryptocurrency system of payments. For example, In Bitcoin's short history, the company has been subject to over 40 thefts, including a few that exceeded 1 million USD in value. However, despite the potential risks, still, many observers look at cryptocurrencies as hope that a currency can exist that preserves value, facilitates exchange, is more transportable than hard metals, and is outside the influence of central banks and governments. There are approximately 856 cryptocurrencies (see the following link https://coinmarketcap.com/all/views/all/. According to Gandal and Halaburda [3] the market of competing cryptocurrencies is an interesting market to analyze for several reasons. First, it was a brand new market, with many players entering and competing. It is also an excellent laboratory with well defined and high quality data on prices and volumes over time.

In regard of market capitalization Bitcoin is the lider in the long list of crypto currencies, followed by Ethereum and Ripple, which have double million digits. The other crypto currencies have less value, with an increasing trend (see the above link).

2. Literature review

Cryptocurrencies in general and bitcoin in particular came outside of the academia. However, since their introduction contribution of academia in this financial monetary field has been very significant. However, since the cryptocurrency market is evolving with an enormous speed and there is a significant dose of confusion of what is going on, it is in our opinion that academic research in this field should be taken with reserves and caution. Despite these facts, academic research on cryptocurrencies has contributed by exposing limitations and pitfalls of cryptocurrency system of payments, but also by proposing ways to overcome those. [1] The above mentioned authors claim that the main three advantages of cryptocurrencies are anonymity, privacy and confidentiality. However, it is our opinion that the most important feature of cryptocurrency system of payments is transparency.

One may ask why! The reason we believe that transparency is the key to success of cryptocurrency system of payments is the fact that in this system unlike the conventional bank system of payments where the client has information only about its own account. Whereas, in crypto-currency system of payments, everybody within the system can see the financial transactions of all other participants, thus, making the system extremely transparent. Hence, although not backed by a sovereign authority, it is the high level of transparency that makes cryptocurrencies acceptable for its users. However, some authors, such as Camoron (2016) claims that it is very unlikely that governments will allow the use of cryptocurrencies in the way that are currently operating. On the contrary claims the author, most of the governments are well positioned to prevent integration of cryptocurrencies within current formal financial institutions. Without these institutions, claims the author, the hurdles cryptocurrencies face to supplanting more legally privileged and centrally issued currencies appear to be insurmountable. In regard of exchange rate issues of cryptocurrencies against traditional currencies such as US Dollar, despite receiving extensive public attention, theoretical understanding is limited regarding the value of blockchain-based cryptocurrencies. In this regard Li & Wang [5] have conducted a theory-driven empirical study of the Bitcoin exchange rate (against USD) determination, taking into consideration both technology and economic factors. According to above mentioned authors, in the short term, the Bitcoin exchange rate adjusts to changes in economic fundamentals and market conditions. The long-term Bitcoin exchange rate is more sensitive to economic fundamentals and less sensitive to technological factors. The latter authors furthermore claim that they have identified a significant impact of mining technology and a decreasing significance of mining difficulty in the Bitcoin exchange price determination.

Some authors, such as Smalley [8] have raised the issue of cryptocurrencies and tax, claiming that there is more to be done in this aspect since the taxability of cryptocurrency transactions

are not yet regulated formally. Finally, Vora (2015) claims that cryptocurrencies and variants of virtual currencies are a welcome development, they will offer competition to the existing modalities of money and governmental regulation, they will provide alternative means to economic agents for their transactions, and their innovative existence should be encouraged so that their beneficial features outperform any deleterious ones. Bitcoins are here to stay suggest the above mentioned author, unless considered illegitimate by governments or banned by regulatory actions.

3. What is Bitcoin and how does cryptocurrencies (bitcoin) work

According to Sarah Meiklejon et al (2016) Bitcoin is a purely online virtual currency, unbacked by either physical commodities or sovereign obligation; instead, it relies on a combination of cryptographic protection and a peer-to peer protocol for witnessing settlements. Consequently, Bitcoin has the unintuitive property that while the ownership of money is implicitly anonymous, its flow is globally visible. Bitcoin initially was introduced by the (pseudonymous) Satoshi Nakamoto in 2008. From that time it has experienced a huge boom and generated millions of profit to those engaged in this business. But how the bitcoin works? The above mentioned authors, Sarah Meiklejon et al (2016, p. 87) explain that as follows: “Briefly, a bitcoin can be thought of as a chain of transactions from one owner to the next, where owners are identified by a public key from here on out, an address that serves as a pseudonym; that is, users can use any number of addresses and their activity using one set of addresses is not inherently tied to their activity using another set, or to their real-world identity.

In each transaction, the previous owner signs using the secret signing key corresponding to his address a hash of the transaction in which he received the bitcoins and the address of the next owner. (In fact, transactions can have many input and output addresses, a fact that we exploit in our clustering heuristics in Section 4, but for simplicity we restrict ourselves here to the case of a single input and output.) This signature (i.e., transaction) can then be added to the set of transactions that constitutes the bitcoin; because each of these transactions references the previous transaction (i.e., in sending bitcoins, the current owner must specify where they came from), the transactions form a chain. To verify the validity of a bitcoin, a user can check the validity of each of the signatures in this chain. To prevent double spending, it is necessary for each user in the system to be aware of all such transactions. Double spending can then be identified when a user attempts to transfer a bitcoin after he has already done so. To determine which transaction came first, transactions are grouped into blocks, which serve to timestamp the transactions they contain and vouch for their validity. Blocks are themselves formed into a chain, with each block referencing the previous one (and thus further reinforcing the validity of all previous transactions). This process yields a block chain, which is then publicly available to every user within the system. This process describes how to transfer bitcoins and broadcast transactions to all users of the system. Because Bitcoin is decentralized and there is thus no central authority minting bitcoins, we must also consider how bitcoins are generated in the first place. In fact, this happens in the process of forming a block: each accepted block (i.e., each block incorporated into the block chain) is required to be such that, when all the data inside the block is hashed, the hash begins with a certain number of zeroes. To allow users to find this

particular collection of data, blocks contain, in addition to a list of transactions, a nonce. (We simplify the description slightly to ease presentation.) Once someone finds a nonce that allows the block to have the correctly formatted hash, the block is then broadcast in the same peer-to-peer manner as transactions. The system is designed to generate only 21 million bitcoins in total. Finding a block currently comes with an attached reward of 25 BTC; this rate was 50 BTC until November 28, 2012 (block height 210,000), and it was expected to halve again in 2016, and eventually drop to 0 in 2140".

4. Evolution of cryptocurrencies

Historically, cryptography was mainly used by military, secret services and intelligence agencies as a protection from the leak of classified information. Most of the academics of this field believe that an autonomous digital currency that is not connected to any government or other intermediary such as a bank is appealing because of the anonymity and liberty that it affords. Transfer of money across geographic regions both domestic and international can be easily and quickly accomplished without worrying about governmental regulations. A pioneer of cryptography in USA is considered Horst Fietsel with its publication of the Digital Encryption Standard (DES) on March 17, 1975 in the Federal Register. Fitsel, in that time IBM researcher, working on a project codenamed Project Lucifer, filed a patent application for a 48-bit block cipher cryptographic system (also known as the Lucifer cipher). The project was commissioned by Lloyds Bank for encrypting ATM transactions. In 1972, the National Bureau of Standards (NBS) identified the need for an encryption standard for encrypting unclassified but sensitive government documents, and in May 1973, solicited proposal for such a system. The NBS then chose, with the approval of the National Security Agency (NSA), a modified version of IBM's algorithm. The project was commissioned by Lloyds Bank for encrypting ATM transactions. The original algorithm was strengthened to a 56-bit block cipher by a team led by Walter Tuchman and aided by Carl Meyer [2]. The publication of DES did lead to many discussions and debates in the academic community and civil society. Some academics such as Martin Hellman and Whitfield Diffie at Stanford University felt that the original 56-bit block cipher was altered by IBM at NSA's behest to provide that NSA a backdoor into the cryptographic system (Subramanian and Chino) [7].

There were also questions raised that time regarding the security of 56 bit cipher. However, DES became very popular and was soon adopted internationally as the encryption standard. Another development that contributed in cryptocurrency creation is the so called Cypherpunk movement that "formally" emerged in the early 1990s. The cypherpunk movement is an activist movement whose participants seek to engineer social and political change and subvert the status-quo by enhancing security and privacy through cryptographic techniques. The founders of the cypherpunk group were Eric Hughes, a UC Berkeley mathematician, Timothy C. May, a former chief scientist at Intel, and John Gilmore, one of the early employees (the fifth employee) at SunMicrosystems and founder of Cygnus Support as well as the Electronic Frontier Foundation. All three were wealthy, and shared a strong libertarian streak. The group started with a meeting in 1992 in the Bay area of San Francisco. They started the cypherpunk mailing

list in 1992 and within two years, the mailing list garnered over 600 subscribers. Another major contributor to creation of cryptocurrency is David Chaum, a cryptologist who got his doctoral degree from the University of California Berkeley. As a doctoral student in the 1980s, Chaum explored several concepts and developed several methods focusing on anonymous communication and anonymous financial transactions. In 1981 Chaum published the article "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms" which described a method, using public key cryptography, to hide the identity of a participant in an email communication, as well as the contents themselves. He explained one of its uses in elections where an examiner could verify that all the votes have been correctly counted without revealing the identity of the voters. A huge contribution of Chaum in this field is creation of a digital currency based on cryptography that he called E-Cash, and in 1990 founded a company called DigiCash, an electronic money corporation. The world's first electronic cash payment took place in May 1, 1994. However, most attempts at creating a workable cryptocurrency have failed to gain consumer acceptance, until bitcoin was introduced in January 2009 when Satoshi Nakamoto who is believed to use this name as a pseudonym mined the first block of bitcoins, known as the genesis block, gaining a reward of 50 bitcoins.

5. The future of cryptocurrencies – advantages and disadvantages

There are different and confronting opinions regarding the future of cryptocurrencies in general and bitcoins in particular. Whils, those with libertarian views of life are optimistic and embrace the cryptocurrency system, other authors, economists, and scholars from this field are not enthusiastic about the use of cryptocurency in the system of payments and financial transactions. The optimistic view of cryptocurrencies use is backed by the fact that they make it easier to transfer funds between two parties in a transaction; these transactions are facilitated through the use of public and private keys for security purposes. These fund transfers are done with minimal processing fees, allowing users to avoid the steep fees charged by most banks. In addition, many countries have started to accept bitcoin as a valid currency. Especially, countries that aim to get rid of cash have a very friendly approach to cryptocurrencies. An argument that promoters of bitcoin use is Market Capitalization of bitcoin, ethereum and other cryptocurrencies, claiming that cryptocurrency market has become very large and powerfull, so banning it would be to costly for any country.

On the other side the opponents of cryptocurrencies claim that cryptocurrencies are very volatile, can be used for money laundry or financing illegal activities. In this regard, Tymoigne (2015) for example, is not enthusiastic over cryptocurrency use, providing reasons why he believes bitcoins are not a viable electronic currency. He notes that bitcoins are illiquid and have shown high price volatility, and that the discounted cash value of a bitcoin is zero. He further observes the currency lacks a central issuer, and that there is no financial or economic basis for its creation. Ivaschenko [4] provides the advantages and disadvantages of bitcoin as stated below.

5.1. Advantages

1. Open code for mining crypto currency – BTC applies the same algorithms that are used in online banking. The only difference of Internet banking is the disclosure of information about the users. All information about the transaction in the BTC network is shared (how, when), but there is no data about the recipient or the sender of the coins (there is no access to the personal information of the owner`s wallet).
2. No inflation – the maximum number of coins is strictly limited by 21 million Bitcoins. As there are neither political forces nor corporations able to change this order, there is no possibility for development of inflation in the system.
3. Peer-to-peer cryptocurrency network – in such networks there is no master server, which is responsible for all operations. Exchange of information (in this case — money) is between 2-3 or more software clients. All installed by users program-wallets are part of a bitcoin network. Each client stores a record of all committed transactions and the number of bitcoins in each wallet. Transactions are made by hundreds of distributed servers. Neither banks or taxes, nor governments can control the exchange of money between.
4. 4. Unlimited possibilities of transaction – each of the wallet holders can pay to anyone, anywhere and any amount. The transaction can not be controlled or prevented, so you can make transfers anywhere in the world wherever another user with a Bitcoin wallet is located.
5. No boundaries. Payments made in this system are impossible to cancel. The coins cannot be faked, copied or spent twice. These capabilities guarantee the integrity of the entire system. Every month the number of online shops, resources, and companies to accept BTC is expanding.
6. Low BTC operation cost. The BTC cryptocurrency works as physical cash, combining the functions of e-commerce. No need to pay commission and fees to banks and other organizations. The main part of such process is mathematics, which does not need money. The commission fee in this system is lower than in any other. It amounts to 0.1% of the transaction amount. The operation interest charges go to BTC miner’s wallets.
7. Decentralization. There is no central control authority in the network, the network is distributed to all participants, each computer mining bitcoins is a member of this system. This means that the central authority has no power to dictate rules for owners of bitcoins. And even if some part of the network goes offline, the payment system will continue to operate stable.
8. Easy to use. Taken into account that the procedure of opening an account for the company in Ukrainian banks is overcomplicated and can be refused without explanation, using BTC is convenient for companies. The company needs approximately 5 minutes to create a BTC wallet and immediately starts to use it without any questions and commissions.
9. Anonymity. It is completely anonymous and at the same time fully transparent. Any company can create an infinite number of bitcoin addresses without reference to name, address or any other information.

10. Transparency. The BTC stores the history of transactions that have ever taken place. It is called a sequential chain of blocks or blockchain. The block chain keeps information about everything. So if the company has publicly used the BTC address, then anyone can see how much BTC is owned. If the company address is not publicly confirmed, then no one will ever know that it belongs to this company. For complete anonymity companies usually use the unique BTC address for every single transaction.
11. Speed of transaction. The ability to send money anywhere and to anyone in a matter of minutes after the BTC network will process the payment.
12. It belongs only to the wallet owner. There is a unique electronic payment system where the account belongs to the owner only. For example, on PayPal if for any reason the company decides that the owner somehow uses the account in a wrong way, the system has the right to freeze all funds on the account without even warning the owner about it. Verification of the proper usage of account is the total responsibility of the owner. With BTC, the owner has a private key and a corresponding public key, which is the address to the BTC wallet. No one but the owner can withdraw bitcoins [6].
13. . No chances to use some personal data for fraud. This is an important point. Today the majority of purchases are made with credit cards. They are unreliable. Filling forms on websites, customers are required to enter the following data: card number, expiration date and code. It's hard to come up with a less secure way to make payment. Therefore, credit cards are very often stolen. BTC transactions do not require disclosure of any personal data. Instead, it uses two keys: public and private. The public one is available to all (i.e. the address of BTC wallet), but the private key is known only to the owner. The transaction needs to be signed by interacting private keys and applying a mathematical function. This creates evidence that the transaction is performed by the owner.
14. The possibility of investing funds in the transparent and profitable resource

5.2. Disadvantages

According to above mentioned author, Ivaschenko (2016) the disadvantages are as follows [9]:

1. Strong volatility – almost all of the ups and downs of the BTC value depend directly on the declared statements of the governments of different countries. This volatility creates the problem in the short term.

2. Large risks of investing in cryptocurrency that should be considered in the medium and long term.

It is our opinion that the list of cryptocurrency (bitcoin) disadvantages are much longer, and are related to risk of money laundry, terrorist and other illegal activity financing, lack of a central issuer, which means that there is no legal formal entity to guaranty in case of any bankruptcy, and alike. However, although it is very difficult to predict, many academics and professionals of this topic claim that the future of cryptocurrencies is bright since it will remove trade barriers and intermediaries, it would decrease the cost of transactions, and therefore boost the trade and the economy. Nevertheless, we should consider and pessimistic voices in the academic world as

well, suggesting that the high risk of volatility, hacking risks, and lack of institutional backup makes the future of cryptocurencies not very optimistic [10].

6. Conclusions

The paper aimed to provide analysis of cryptocurrency use in general and of the bitcoin in particular. Our empirical research found that the future of cryptocurrencies could be bright if some institutional – formal conditions are fulfilled. The advantages of cryptocurrency use in facilitating trade, cost reduction, and alike, are recognized by majority of academics. Bitcoin and other cryptocurrencies have the potential to replace traditional and new payment methods. But to achieve that and become a dominant power in global system of payments, they must provide distinctive incremental value, to address and overcome a number of critical challenges, such as formal regulatory issues. That is unlikely to happen in the short time period. But banks should look closely at the technology underlying these cryptocurrencies as a potential generic new way to transfer ownership of value in the longer term.

References:

1. Bailis, P. & Song, H. (2017). Research for Practice: Cryptocurrencies, Blockchains, and Smart Contracts; Hardware for Deep Learning. *Communications of the ACM,* 60(5), p. 48-51.
2. Bamford, J. (1982). The Puzzle Palace: Inside the National Security Agency, America's Most Secret Intelligence Organization. Penguin.
3. Gandal, N. & Halaburda, H. (2016). Can we predict the winner in a market with network effects? Competition in cryptocurrency market. *Games*, 7(3), p. 1-21.
4. Ivaschenko, A.I. (2016). Using Cryptocurrency in the Activities of Ukrainian Small and Medium Enterprises in order to Improve their Investment Attractiveness. *Problems of economy*, (3), p. 267-273.
5. Li, X. & Wang, C.A (2017). The technology and economic determinant of cryptocurrency exchange rates: The case of Bitcoin. *Decision support system*, 95, p. 49-60.
6. Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, Geoffrey, M. & Savage, S. (2016). A fistful of bitcoins: Characterizing payments among men with no names. *Communications of the ACM*, 59(4), p. 86-93.
7. Subramanian, R. and Chino, T. (2016). The state of cryptocurrencies: Their issues and policy interactions. *Journal of International Technology & Information Management*, 24(3), p. 25-40.
8. Smalley, C. V. (2017). Cryptocurrency and taxes. *Tax adviser*, p. 1-3.
9. Tymoigne (2015). Do Cryptocurrencies Such as Bitcoin Have a Future? No: As a Currency, Bitcoin Violates All The Rules of Finance. *Wall street journal – Eastern edition*, 265(49), p. 1-2.
10. Vora, G. (2015). Cryptocurrencies: Are Disruptive Financial Innovations Here? *Modern Economy*, 6(7), p. 816-832.