ISSN 2449-7479
eISSN 2543-8840
amme.wne.sggw.pl

Annals of Marketing Management & Economics
Vol. 4, No 2, 2018, 47–56
DOI 10.22630/AMME.2018.4.2.16

BITCOIN AS AN EXAMPLE OF CRYPTOCURRENCY – CURRENT STATE AND PERSPECTIVES

Seweryn Gajdek
Warsaw University of Life Sciences – SGGW, Poland

INTRODUCTION

With the development of informatization, more and more aspects of social and economic life are moving to the web. One of the effects of this process is the popularization of the idea of electronic money. The dynamically developing Internet and computerization has created suitable conditions for the creation and operation of cryptocurrencies. The first one, Bitcoin was launched on 3 January 2009. After more than nine years of dissemination of block chain technology, based on which Bitcoin operates, there are over 2,000 cryptocurrencies in the world. This means that there are several times more than traditional currencies.

Bitcoin for about two years from its inception was treated rather as a curiosity and did not have a significant monetary value. It functioned mainly in the environment of Cypherpunks and in a small group of people associated with them. The sudden increase in demand for this currency recorded in the second quarter of 2017 caused that at the end of December that year, the total value of the Bitcoin market exceeded USD 220 billion. The dynamic growth of Bitcoin's importance in the financial system means that the emerging subsequent cryptocurrencies require in-depth attention of financial institutions and supervisory authorities. In the long term, cryptocurrencies might have an impact on the structure of the financial system, as well as on the shape of monetary policy of central banks.

For this reason, the purpose of the article is to present the genesis and motivation for creation, as well as the principles of Bitcoin and other cryptocurrencies. According to the author's knowledge, the literature on the topic of cryptocurrencies is limited and this article fills in the informational gap in this area. The principles of operation of cryptocur-

rencies have been described on the example of Bitcoin, whose basic technological solutions are similar to most of other cryptocurrencies.

The remaining part of the article has the following structure. The next section presents the principles of functioning of Bitcoin and other cryptocurrencies, and further the analysis of the current situation of the Bitcoin market and the perspective of its development. The entire analysis is summarized in conclusions.

BITCOIN – PRECURSORS AND CREATION

The idea of cryptocurrencies emerged at the turn of the 1970s and 1980s. Bitcoin has become the result of a combination of many ideas and solutions proposed by theorists or creators of other forms of electronic money over the last 40 years. Its essential feature was the ability to function independently. The creation of secure electronic money that can be used in trade and operation, regardless of traditional currencies, became the goal of financial and IT programmers' efforts already at an era when the Internet was not so widely use [DeMartino 2016].

Dawid Chaum, who made a major contribution to the field of cryptography and laid the foundations for the emergence of cryptocurrencies, was the promoter of anonymous electronic payments. In 1982, he proposed a cryptographic solution that would make it possible to hide the identity of a person making a digital money payment [Chaum 1982]. His application of the protocol known as "blind signature" allowed for asymmetrical anonymity. As part of the transaction, the payer was unrecognizable, while the person accepting the payment could be identified. However, he believed that the progressive automation of payment systems could have a significant impact on the personal privacy of transaction participants, and could also contribute to the criminal use of such payment channels. He believed that information about the time, value and subject of the transaction reveal unnecessarily many personal information about consumers, for example about their locations, lifestyle and connections. In addition, the collection of such data by financial intermediaries is not necessary to complete the payment. On the other hand, the anonymity of the payment system would limit security by giving the possibility of its criminal usage.

To eliminate both of these important problems, Chaum proposed to implement such a solution that would prevent the financial intermediary from identifying the payer and the time of execution and the amount of the transaction. At the same time, the new system would provide the payer with proof of payment and would enable the recipient of the payment to be disclosed if there are appropriate premises. In addition, transactions with funds reported as stolen could be withheld [Chaum 1982].

To address these postulates and solutions Chaum created, in the turn of the 1980s and 1990s, the software company DigiCash. The purpose of its operation was to conduct a centralized electronic payment system ecash. DigiCash together with the electronic currency became a base for creation of the electronic payment system [DeMartino 2016]. Cryptographic solutions that were applied in the currency developed by DigiCash had a fundamental impact on the creation of Bitcoin. In the system used, the identity of users

was protected, payments took place without financial intermediaries and the costs associated with their operation were excluded [Vigna and Casey 2016]. These cryptocurrency functions have been implemented in Bitcoin. Without existence of blind signatures Bitcoin would probably not be invented [Wiśniewska 2015].

Another important technological solution that found application in the operation of cryptocurrencies was Hashcash – presented in 1997 by Adam Back. Hashcash is not a payment system or a currency, but a proof-of-work algorithm that was originally used as a tool to limit the reception of undesired mass mailings. It was a mechanism for denying access from all types of Internet services. The hash stamp of the system was an evidence of the execution of a certain amount of computational work by the sender's device [Back 2002]. This algorithm identifies the cost that the sender is burdened with when wants to send information or make the service available to a given recipient. It is the most frequently used algorithm in the process of extracting new bitcoins or other cryptocurrencies.

In the creation of Bitcoin, the environment of Cypherpunks played an important role. The group began operations in the early 1990s and made up of cryptologists expressing their concern about the progressive limitation of privacy and personal rights and freedoms in modern society [Vigna and Casey 2016]. The activities of the group helped to improve the level of the privacy and security using cryptography. Communication between group members was conducted by mailing-list, to which belong also Satoshi Nakamoto – an anonymous person or a group of people that created Bitcoin. One of the first ideas of this activity was to create anonymous digital money. In the mechanism of its functioning, it was assumed that revealing the identity of the payer is unnecessary and ensuring anonymity would provide cryptographic solutions [Hughes 1993]. This concept was developed by Wei Dai and led to the creation in 1998 of a virtual anonymous currency called b-money [Dai 1998]. This system functioned without the need for a central settlement unit. The transactions were carried out anonymously on a peer to peer (P2P) basis. The main technological solution, implemented latter in Bitcoin system, was that every user had a full copy of transaction ledger. B-money, however, had drawbacks, the most important of which related to the method of verifying and rejecting transactions that did not take place [Piotrowska 2018]. The security solution for this currency used a penalty system. Its users had to deposit a certain amount of cash at a special account which could be used to collect fees for improper use of the system. Such a model was inefficient because it approved unethical cooperation between users.

Bitcoin, developed by Satoshi Nakamoto, unlike the system of penalties implemented in b-money, proposed a remuneration system that motivates fair use of the network [Vigna and Casey 2016]. It also implemented two economic principles: decentralization and resilience to inflation, which were two main propositions made by Nick Szabo in creation of bit gold [Szabo 2005], that is considered as direct precursor of bitcoin, even that it was only theoretical creation. Hal Finney was another contributor to Bitcoin development. He invented reusable proof-of-work, which was Adam Back's modified algorithm, adapted to be used in cryptocurrency system. He was known, not only as the second, after Nakamoto, user of bitcoin, but also as a person who helped to develop bitcoin code [Grzybkowski and Bentyn 2018].

PRINCIPLES OF OPERATION

Inventing the Bitcoin system, Nakamoto stated that currently online trading requires the use of a financial system in which the third parties guaranteeing the security of transactions are financial institutions. Although, the system works to a large extent correctly, its weakness is based on the need for a transaction model based on trust to a third party. Irreversible transactions are virtually impossible to implement, because financial institutions, being involved in intermediation between the parties, are not able to avoid mediation disputes. The cost of mediation therefore has an impact on the increase of transaction costs. These costs reduce the cost-effectiveness of low-value daily payments and limit the scale of their implementation. There is also an additional cost resulting from the inability to make irreversible transactions when paying for irreversible services. The possibility of withdrawal of the transaction creates the need for building trust in the system. There is therefore a need to seek information on the identity of participants in market transactions that would otherwise not be needed [Nakamoto 2018].

It must be assumed that a certain amount of fraudulent behavior in any system is inevitable. Additional costs and uncertainties that accompany online transactions could only be avoided by making payments in person. There is no mechanism that would enable payment via communication channels without the intermediation of a trusted institution. An electronic payment system is therefore needed in which trust would be based on a cryptographic proof. This will allow two participants to negotiate a direct transfer of funds without using financial intermediation. These transactions are impossible to withdraw, which protects the sellers, and the routine deposit mechanism is simple to implement and protects buyers. To avoid the problem of double spending, the Bitcoin system applies a timestamp that gives proof of the chronological order of transactions [Nakamoto 2018].

Such a settlement system functions outside the structure of traditional banking and would enable individuals to send digital money directly. Regardless of which entity would act as an intermediary, it is unnecessary from the point of view of the correctness of settlements [Piotrowska 2018].

Bitcoin is a type of P2P money. Each participant of the Bitcoin system uses the protocol at the same level. There are no privileged entities. Such system makes Bitcoin the first financial network, like the Internet, which identifies the principle of neutrality. It is neutral for each participant sending and receiving funds as well as for the amount of the transaction. Neutrality makes every user of this currency able to create innovations in this system in categories such as financial instruments, payment systems and banking, regardless of whether he is a private person, an organization, a bank or a government institution [Antonopoulos 2016].

CREATING NEW BITCOINS AND SECURITY SYSTEM

The Bitcoin supply is increased due to operation of the so-called miners. Their computers are equipped with software that searches for mathematical functions that the Bitcoin protocol algorithm is based on. After finding the solution, a block is generated that contains the transaction record [Franków and Kopyściański 2016]. One new block is

added to the chronological block sequence every 10 minutes. Adding it to the register allows Bitcoins to be available to the new owner. Miners receive payment in the form of newly generated Bitcoins for confirming the transaction. So digging is a process that allows confirming transactions by means of a consensus achieved in the network between its participants, without the need for a central settlement unit. In addition, digging allows getting new coins, from a total finite pool of 21 million, which are rewarded for sharing Bitcoin network computing power. However, this is not an objective in itself, but the effect of the mechanism by which the security of the Bitcoin system can be decentralized [Antonopoulos 2018]. The more devices participate in process of digging the currency, the more secure the network is. Such protection of the chronology of cash flows ensures the stability and security of the system.

In case of an attempt of a dishonest entity to change the record in the transaction history, it would have to go back to the block in which the record would like to interfere. After making the change, the entity would have to complete the entire calculation process from the moment of digging up the given block to the present moment faster than the group of devices working on the correct block sequence [Homa 2015].

THE CURRENT STATE OF THE BITCOIN GLOBAL MARKET

The Bitcoin supply depends on the digging process. According to the algorithm encoded in this currency, the maximum number of units is 21 million. Active participants of this market, so-called miners, can add a smaller and smaller number of new currency units over time. Initially, i.e. since the Bitcoin system was launched in January 2009, 50 Bitcoins were disposed to miners every 10 minutes. In 2012, this number decreased to 25 Bitcoins, and in July 2016 to 12.5 Bitcoins. This process will proceed exponentially as part of the 32 operations to reduce the miners' salary by half (so-called halfings), until the prize of digging new units will be 1 satoshi, i.e. 0.00000001 Bitcoin. According to this rule, it will happen around 2140, after which the issue of the new Bitcoins will end completely [Antonopoulos 2018].

Currently, Bitcoin is the only cryptocurrency that counts in the global financial system (see Table 1). Since 2017, the market capitalization of this currency significantly exceeds USD 100 billion and is more than five times higher than the capitalization of the next two cryptocurrencies, i.e. Etherum and Ripple. The value of daily turnover is close to USD 5 billion. Due to the limited ability to extract new coins, in the years 2016–2018 the number of Bitcoins remaining in circulation stabilized at around 17 million coins.

Since its inception, the capitalization of the Bitcoin market has been growing (see Figure). However, it is characterized by considerable variability. With a relatively constant Bitcoin number in circulation, its value depends mainly on the price of the Bitcoin unit. The sudden increase in demand for Bitcoin recorded in 2017 pushed the price of the currency to around USD 19,000 at the end of the year. Consequently the market capitalization rose to USD 314 billion.

The growing interest in Bitcoin caused that the number of market participants, or more precisely addresses, holding this cryptocurrency exceeds 20 million. The majority, around 11 million persons, possess less than one thousandth of Bitcoin. The total value

TABLE 1. Market capitalization and daily turnover in the cryptocurrency market, as of 28 October 2018

Crypto-currency	Market capitalization (USD mn)	Unit price (USD)	Daily turnover (USD mn)	Unit numer in circulation (mn)
Bitcoin	110 264.61	6 352.58	3 915.24	17.36
Ethereum	20 578.68	199.85	1 398.70	102.97
Ripple	18 334.08	0.46	297.04	40 205.51
Bitcoin Cash	8 290.05	475.41	592.99	17.44
EOS	4 851.08	5.35	651.24	906.25
Stellar	4 461.01	0.24	57.52	18 913.56
Litecoin	3 016.52	51.13	370.34	59.00
Cardano	1 857.55	0.07	19.56	25 927.07
Tether	1 778.21	1.00	2 313.70	1 776.42
Monero	1 740.11	105.20	8.38	16.54

Source: [WWW 2].

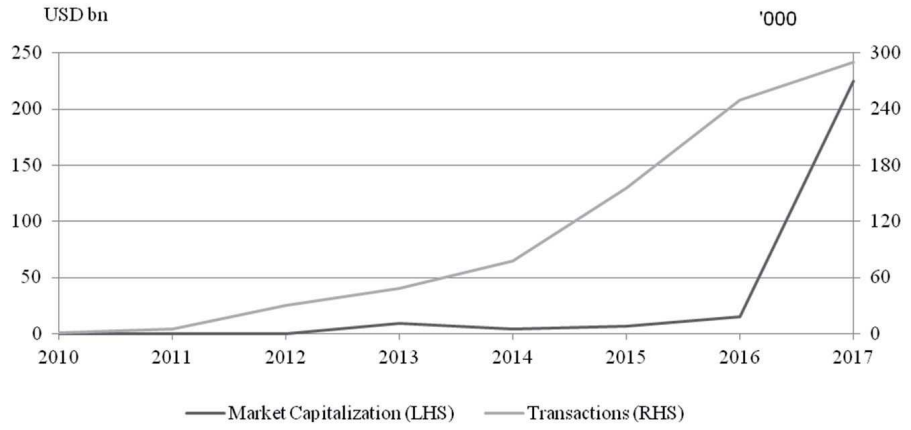

FIG. Capitalization and number of daily transaction in the Bitcoin market as of 28 October 2018

Source: CoinMarketCap.com

of currency collected by these addresses equals to approximately USD 14.6 billion, i.e. around 0.01% of the total market capitalization (see Table 2).

The highest value is accumulated by addresses with between 10 and 100 Bitcoins per address. The total capitalization of addresses with such and higher Bitcoin balance represents 87% of the total market capitalization.

Market capitalization of bitcoin is still several times smaller than for instance capitalization of the gold market or capitalization of any global corporations like Microsoft, Apple or Facebook. Market capitalization of this currency is therefore relatively small,

TABLE 2. Distribution of the Bitcoin capitalization according to the value of individual account

Balance of individual address (BTC)	Number of addresses	Total value (USD mn)
0–0.001	11 329 894	14.6
0.001–0.01	5 134 631	134.3
0.01–0.1	3 851 709	790.2
0.1–1	1 776 717	3 656.3
1–10	564 632	9 465.3
10–100	132 774	27 845.7
100–1 000	14 844	23 664.3
1 000–10 000	1 638	22 581.8
10 000–100 000	120	19 856.9
100 000–1 000 000	3	2 386.1

Source: [WWW 1].

but it is characterized by high volatility of quotations. An interesting issue from the point of view of price stability of this currency is the structure of the value of user portfolios, which is characterized by a large disparity. Over 87% of all circulating Bitcoins are assigned to only 0.66% of private addresses, while 49.6% of addresses are in possession of only 0.01% of the whole unit of this currency (see Table 2). In the history of Bitcoin quotations, it happened that the order to sell Bitcoins constituting hundredths of all units in circulation was able to lower the Bitcoin rate by several dozen percent [WWW 3]. The instability of the currency's price may deter investors with a weak speculative attitude. From this point of view, Bitcoin may appear as a risky investment and at the same time arouse aversion in a large part of society, companies and organizations. The high volatility of the exchange rate against traditional currencies makes it difficult at this stage to perform the function of expressing the price in Bitcoin and making daily transactions in it. However, this does not change the fact that the number of institutions from different countries accepting the settlement of payments in Bitcoin is systematically growing, including such large international companies as: Microsoft, Paypal, Ebay or NewEgg [Bala et al. 2016]. The continuous operation of the Bitcoin system, as well as the ever growing market capitalization and Bitcoin price seem to deny all fears and inconveniences. The average daily number of transactions made in the Bitcoin network also shows a strong upward trend – from an average of several hundred transactions in December 2010, by around 50,000 at the end of 2015 to over 290,000 in 2018. These facts make possible that this currency might become an alternative global currency. Currently, there are no new cryptocurrency projects, that could fulfil this role. Among ten cryptocurrencies of the highest market capitalization (Table 1) there are both relatively old currencies, like Litecoin or Monero, with rather stable positions in the market and fairly new projects, like EOS, Stellar or Cardano. The newer ones like Cardano or EOS are still in the development phase and do not offer all of the planned features yet. High popularity and significant market capitalization of those new currencies show speculative, but also rapidly evolving character of the cryptocurrency market.

CONCLUSIONS

Currently, cryptocurrencies seem to be an inseparable part of economic reality. History shows that the need to create securely functioning digital money dates back to at least the beginning of the 1980s, it means times when the Internet operated in the early stages. Cryptocurrencies are the next stage in the development of this idea.

The need to conduct transactions independently from the financial intermediary was one of the main motives for creation of cryptocurrencies. Cryptocurrencies were designed to be able to transfer funds directly between two persons. The payment system they create can exist outside of the current traditional banking system. Low transaction costs are important effects of such payment system. The creators were also guided by the issue of anonymity and respect for personal privacy. The disclosure of personal information was not necessary to effectively make payments in the case of cryptocurrencies. Although, many of them, including Bitcoins, are only pseudo-anonymous, which means that on the basis of a publicly available register of transactions and turnovers with the involvement of traditional currencies, it possible to identity of the owner of a given public address of a given currency. However, there are alternative currencies in the market that better protect information about the identity of the parties to the transaction and its details.

On the one hand, huge disproportion in distribution of the Bitcoin capitalization, according to the value of individual account and rise of numerous Bitcoin alternatives, makes investing in Bitcoin risky. On the other hand, growing average of a daily number of transactions made in BTC and growing market capitalization show rather large interest in Bitcoin and in cryptocurrencies in general. There are more reasons for that. The cryptocurrency market responds to many needs related to e-commerce. Thanks to smart contracts, it is possible to omit a notary in effective contract enforcement. Regardless of the path that the future development of cryptocurrencies will take, according to the author's knowledge, cryptocurrencies already at the current stage make possible to make payments better than the current banking system could offer. From the perspective of the implementation of daily payments, funds transfers using cryptocurrencies are much faster, cheaper and more anonymous than those that support the traditional banking system. Further dissemination of cryptocurrencies seems unavoidable.

REFERENCES

ANTONOPOULOS A.M., 2016. The Internet of Money, Merkle Bloom LLC.

ANTONOPOULOS A.M., 2018. Bitcoin dla zaawansowanych (Mastering Bitcoin) [in Polish], Helion, Gliwice.

BACK A., 2002. Hashcash – A Deniall of Service Counter-Measure, retrieved from: http://www.hashcash.org/papers/hashcash.pdf [accessed: 04.11.2018].

BALA S, KOPYŚCIAŃSKI T., SROKOSZ W., 2016. Kryptowaluty jako elektroniczne instrumenty płatnicze bez emitenta – Aspekty informatyczne, ekonomiczne i prawne (Cryptocurrencies as electronic payment instruments without issuer – computer, economic and legal aspects) [in Polish], Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław.

CHAUM D., 1982. Blind Signatures for Untraceable Payments, (in:) D. Chaum , R.L. Rivest, A.T. Sherman (eds) Advances in Cryptology: Proceedings of Crypto '82.

DAI W., 1998. B-money, retrieved from: http://www.weidai.com/bmoney.txt [accessed: 27.10.2018].

DeMARTINO I., 2016. The Bitcoin guidebook – How to obtain, invest, and spend the world's first decentralized cryptocurrency", Skyhorse Publishing, New York.

FRANKOW M., KOPYŚCIAŃSKI T., 2016. Analiza perspektyw rozwoju Bitcoina w kontekście możliwości pełnienia funkcji pieniądza (Bitcoin-analysis in terms of its ability to perform functions of money) [in Polish], Zeszyty Naukowe Wyższej Szkoły Bankowej we Wrocławiu 16, 2.

GRZYBKOWSKI M., BENTYN Sz., 2018. Kryptowaluty (Cryptocurrencies), [in Polish] Cryptologic Sp. z o.o., Poznań.

HOMA D., 2015. Sekrety Bitcoina i innych kryptowalut (Secrets of Bitcoin and other cryptocurrencies) [in Polish], Helion, Gliwice.

HUGHES E., 1993. A Cypherpunk's Manifesto, retrieved from: https://www.activism.net/cypherpunk/manifesto.html [accessed: 29.10.2018].

NAKAMOTO S, 2008. Bitcoin: A Peer-to-Peer Electronic Cash System, retrieved from: https://bitcoin.org/bitcoin.pdf [accessed: 18.09.2018].

PIOTROWSKA A.I., 2018. Bitcoin – Płatnicze i inwestycyjne zastosowania kryptowaluty (Bitcoin – Payment and investment applications of cryptocurrencies) [in Polish], CeDeWu, Warsaw.

SZABO N., 2005. Bit Gold, Satoshi Nakamoto Institute, retrieved from: https://nakamotoinstitute.org/bit-gold/ [accessed: 29.10.2018].

VIGNA P., CASEY M. J., 2016. The age of cryptocurrency – How Bitcoin and the blockchain are challenging the global economic order, Picador, New York.

WIŚNIEWSKA A., 2015. Bitcoin jako waluta wirtualna (Bitcoin as a virtual currency), Institute of Economic Research Working Papers 155.

WWW 1. Cryptocurrency statistics, retrieved from: https://bitinfocharts.com/ [accessed: 31.10.2018].

WWW 2. Top 100 Cryptocurrencies by Market Capitalization, retrieved from: https://coinmarketcap.com/ [accessed: 31.10.2018].

WWW 3. Bitcoin Historical Price & Events, retrieved from: https://99bitcoins.com/price-chart-history/https://99bitcoins.com/price-chart-history/ [accessed: 07.11.2018]

Summary. The idea of anonymous digital money existing outside of traditional banking system lasts at least 40 years. It appeared as soon as technological solutions, which such a system requires, became available. The article analyses the genesis of the crypto-currencies and technological solutions implemented into the Bitcoin digital currency. The article shows current state of the Bitcoin market and changes in its price, market capitalisation and number of transactions during last decade of operations of the crypto-currency market. Although there are difficulties in using Bitcoins, which include technical background and resulting from the high volatility of prices of this currency, the continuing upward trend of the Bitcoin price and the average daily number of transactions shows that interest in this currency is growing. Bitcoin features that attract new users are a large dose of anonymity, security of funds guaranteed by the extremely high computing power of the Bitcoin network, the speed of transactions and their low cost associated with the exclusion of a financial intermediary. The features of this money and data from the market allow to expect that Bitcoin will gain more individual and institutional users.

Key words: cryptocurrency, bitcoin, cryptography, digital currency

JEL: G10, G19

Corresponding author: Seweryn Gajdek, Warsaw University of Life Sciences – SGGW, Faculty of Economic Sciences, Nowoursynowska 166, 02-787 Warsaw, Poland, e-mail: seweryn.gajdek@gmail.com, htpps://orcid.org/0000-0001-5199-6758