

UDC 336.74

JEL Classification Code E42

J. Kuck

The State Higher School of Technology and Economics in Jarosław, Poland, Doctor

e-mail: Jerzy_ku@yahoo.com

INNOVATIVE TRANSACTIONS OF THE FUTURE WITH CRYPTOCURRENCY

Abstract. Nowadays, cryptocurrency is gaining popularity. Used for a few years, it has been independent, anonymous, resistant to influence of banks or governments. The paper presents digital value carriers that have only a form of computer readable information and do not have a material equivalent (e.g. banknotes, coins or tokens). The paper discusses the history and characteristics of Bitcoin, analyzes what influence cryptocurrency has on traditional cashless payments, the methods and the most popular excavators to dig cryptocurrency, and how and where to buy and sell cryptocurrency at the exchange. In the conclusion it is indicated that the comprehensive legal regulations are necessary for proper cryptocurrency operations. The paper also includes instructions how to register at the CoinCasso exchange and how to use a “recommendation” link to do transactions at the exchange.

Key words: cryptocurrency, Bitcoins, cryptocurrency exchange, Coincasso, cryptocurrency excavators

Cryptocurrency is getting more and more popular in the world, it has been used only for a few years, is independent, anonymous, resilient to any influence of banks or state governments. It is defined in various ways, generally as a computer-based medium of exchange and it does not have any material representation (e.g.: banknotes, coins or counters).

Cryptocurrency can serve as a medium of exchange for business transactions. The market of cryptocurrency is expanding, attracts a huge number of investors who have not had any experience in trading before and what is more it is a real revolution in a present payment system. The

advantages are: high anonymity, low costs and fast transactions, independence from a banking system.

To secure transaction and anonymity, the authors of the cryptocurrency protect the information exchange system (value) with the advanced cryptographic (coding) techniques. The cryptography gave the name to “Cryptocurrency”. The implemented solutions enable to exchange the local currency in particular countries in the world round o’clock, 7 days in a week, 365 days in a year.

The first most known cryptocurrency is bitcoin. There are over 1000 various cryptocurrencies in the world, which are alternatives for bitcoin. Experts estimate that cryptocurrency is an innovative solution in finance and IT in the last decade.

The number of bitcoins is never to exceed 21 mln. It is projected that practically the emission of bitcoins will cease completely in 2140, however 99 % of bitcoins will be mined around 2030 and 99.8 % in 2040.

Bitcoin uses peer-to-peer software programs (a computer network communication model to connect computers/peers all over the world and assigns them the same status) therefore the virtual currency can be transferred to any place on the globe within a few seconds. The virtual currency does not have its physical counterpart, is not tangible – it can be called a set of code lines. Every single **Bitcoin** has its own, unique code. This feature is the most difficult to understand – how can bitcoins have value if they are not physical legal tender but “virtual” money? The answer is

quite simple – it is people who decide about the value of a bitcoin. It is a kind of unwritten agreement in which we presume that Bitcoin has the value equal the value of traditional money – as long as virtual currency is popular its American one-dollar banknote has value of \$1 because we accepted so. The whole present world uses virtual money – bank transfers, credit card payments, online shopping, etc.

Bitcoins are mined while the transaction is verified – this requires better and bigger computer power [1]. This is a reason why the bitcoin has become a speculative currency with which a lot can be earned in a very short time. This currency is not under control of any central bank and transactions are anonymous so it attracts more and more users. The question arises: can completely decentralized “currency”, independent from any regulatory institutions be recognized as a legal money? This question is asked by economists, politicians and experts all over the world. Classification of Bitcoin - a product is controversial, as it brings profits but also threats to its users. Therefore, virtual coins have as many followers as opponents. There is not one clear definition of Bitcoin. It can be defined as a contemporary innovative, decentralized digital currency and its units are created on Internet. Bitcoin has a very particular feature – it does not have a physical form.

From the historical perspective, Bitcoin is a third-generation payment system in the world after the era of money and banknotes and era of electronic banking.

From the IT perspective Bitcoin is an implementation of the cryptocurrency concept, which was described for the first time by a programmer Wei Dai in 1998. Thus, Bitcoin is a decentralized information base with defined digital value flow between users’ accounts of the system.

From the financial perspective, Bitcoin can be identified as a currency similar to Euro or US Dollar with an exception that they are controlled by governments, central banks and financial institutions. Bitcoin is not controlled by any central issuing institution. It is a virtual coin that can be gained by mining or bought from users at the market with other currency.

To simplify the issue Bitcoin can be defined as the electronic data ledger in a form of a file

“bitcoin wallet” or stored by the third parties on the external server (a computer hard disk).

The amount of coins that can be produced (mined) is limited and closed, so the time to mine next virtual coin is longer and level of difficulty higher every time. Therefore, the huge Bitcoin “mines” composed by hundreds of cooperating processes, graphic charts and other subsystems are created all over the world. **Practically, it means that average user is not able to mine virtual coin on their own.**

Every mined Bitcoin reaches *blockchain* – the information archive where the lines of code for every Bitcoin and transaction are stored. These transactions are coded with complex and comprehensive mathematical formulas. Thus, we can be sure that particular Bitcoin is assigned exclusively to one person at the same time. This guarantees that if we possess that coin nobody else in the world cannot have it in their wallet – unless we send it ourselves or are the victim of hackers’ attack.

The certain user who published in November 2008 the idea for creating virtual currency which he called Bitcoin is recognized as a pioneer of Bitcoin. He used the Japanese name Satoshi Nakamoto [2].

This innovative Internet currency bears the following features:

- Anonymity of transactions (Bitcoin address is completely anonymous and can be changed. So, it is not known who completed an operation and who owns this money,
- Lack of intermediary during transactions (transferred money reaches the addressee directly, omitting banks and financial institutions,
- Opposition to currency of particular countries (based on trust of governments and banks and social agreement, unexchangeable in gold) its value is established at the free market,
 - Based exclusively on its users’ trust,
 - No physical form – its system is based on transaction ledger between various addresses,
 - The right of possession does not depend on banks and governments (the right to possess Bitcoins is granted with private key – stored in a file wallet.dat, familiar only to the

owner, so the state security services cannot freeze/block the account,

- The whole system is based on the computer performance, mathematics, cryptography and distributed network,

- Resistance to inflation (no possibility to print/produce additional coins over its maxima; number of 21 mln Bitcoins),

- No owner or manager of the system – Bitcoin functions in a Peer-to-Peer (P2P) network which is not controlled or governed,

- Immediate transactions to any place in the world – only Internet are needed,

- Convenient, simple and fast transfers.

Bitcoin has become global only within 9 years. Its beginning is dated on 2009 when the “Bitcoin algorithm” was created and introduced to the public. Creating virtual currency is of technical nature as it is about solving algorithms (using comping knowledge). The effect of this kind of operation i.e. “mined Bitcoin” is automatically introduced to the public sphere with automatically assigned functionality. It can be traded directly or on virtual platforms (a kind of exchange points) There have already been automatic teller machines (ATM) for transactions with bitcoins.

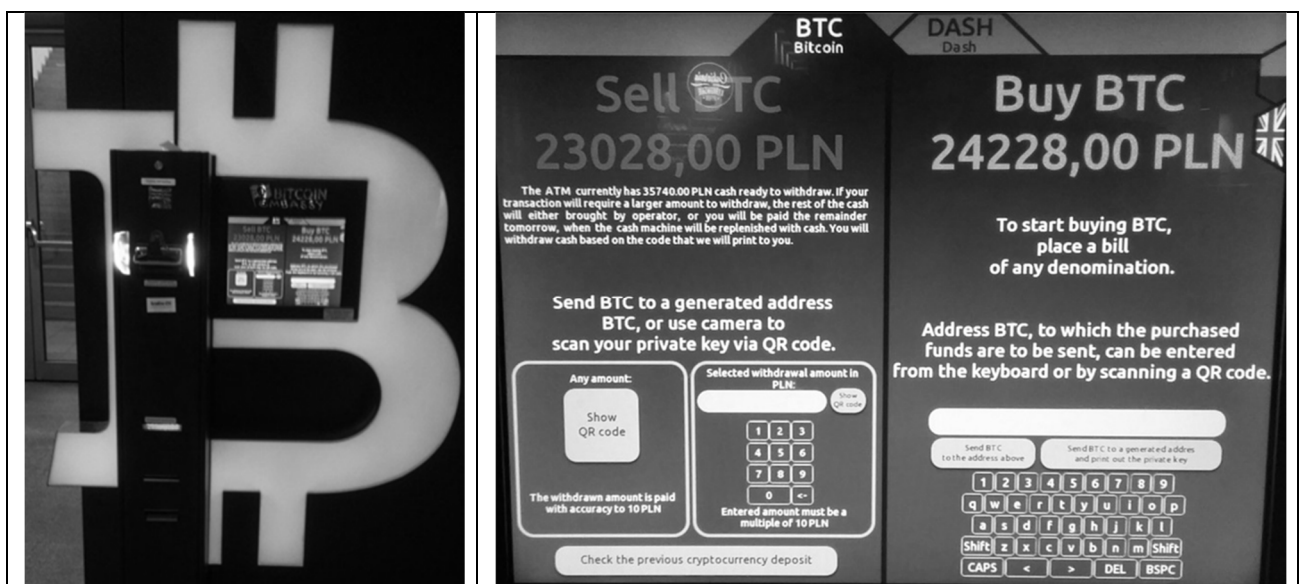


Fig. 1. Automatic teller machine (ATM) in Krakow for transactions with cryptocurrency

Bitcoin is a system based on mathematics and cryptography which makes it one of the safest currencies in the world impossible to print, block or forge.

To trade Bitcoin a new user should **install a Bitcoin wallet** on Internet first. There are various kinds of wallets with their strong and weak points. The most popular wallet for transactions is a **desktop wallet** installed on a computer/mobile phone which enables to manage Bitcoins.

Bitcoin is completely free from regulations and decentralized and can be traded all over the world. There are hundreds of bigger and smaller exchanges where bitcoin can be bought for traditional money. We can pay for services, buy products or invest with Bitcoin.

Cryptocurrency – virtual coins are treated in the same way as traditional money. The wallet and deposit in a wallet are secured. Transactions with suspected entities or unverified exchanges are not possible. Once completed transaction of a coin sent with its code cannot be reversed.

Mining is a process of creating block chains included in a shared public ledger. The mining terminology is adapted mainly because the process is similar to gold mining (**Bitcoin is often called a digital gold**), so the people or companies involved in a process of bitcoin mining (and other cryptocurrency) are called miners or diggers. Similar to miners in a carbon mines – “diggers” receive payment for completed work in coins which can be entered into circulation. This

mechanism is called *Proof of Work (PoW)*. The additional motivator for a digger is commission for accepted transactions. So, they can receive a double payment – an award for mining and validation of transactions. To simplify Bitcoin mining resembles gold mining or a bit money printing by governments. Mining is based on prior programmed algorithms without any central institution which owns the whole pot and distributes money according to some criteria – which is typical to most state issuing institution of the physical money.

Comparing mining to lottery is also quite adequate – bitcoin mining is about guessing or more precisely, solving very complicated mathematical riddles, yet it is not ad hoc guessing but complex and intensive process.

ASIC – presently the main mining system

Application Specific Integrator Circuit Chips (ASIC) is a system adapted to Bitcoin mining, commonly known as an excavator an actually it is a name for an electronic system, dedicated to perform specialized mathematical calculations.

Bitcoin ASIC takes transactions through hash SHA-256 algorithm. This hardware is an independent unit which operates after plugging in and connecting to a mining pool. The excavators make mining faster and energy efficient. The more popular Bitcoin gest the more miners join.

The weak points of excavators are that they can perform only one specific task and cannot be used for other functions. So far Bitcoin mining was very tiresome and unbearable at home as the hardware fans, a part of the cooling system, produced big noise. The latest versions of excavators have the cooling system much quieter. ASIC can calculate hashes hundreds time faster than the best processor (CPU).

Mining process and its difficulty level

BTC network automatically changes the level of difficulty depending on the speed of solving tasks. The rule is that sometimes the amount of an award gets smaller. Presently it is 2.5 bitcoins for one block – then the value decreases (every four years at average, exactly every 21 0000 blocks) to 6 BTC, consequently decreasing till the last coins mined.

These top-down rules were formulated by Bitcoin designers before the first block was mined

to regulate the number of issued coins. Thus, the more people participate in transaction confirmation the more difficult the “mathematical riddle” gets, which for Bitcoin is the hash with particular parameters. Introduction of this solution allows to adjust the level of difficulty and so stabilize the issuing speed on a desired level.

Solving the riddle is not a matter of logic but guessing on a big scale. It is as if every miner got a locker with a code to decipher. Only after decoding he succeeds as his block joins the system and he is paid. The most important is computer power of a particular miner of a group (hash rate) – the higher the hash rate the faster the combination is solved. The algorithms are designed in such a way that the mining a coin should take about 10 minutes. The bigger group of miners the higher level of difficulty. It is worth mentioning that the process of “guessing” itself is energy consuming and most trials finish unsuccessfully.

Mining pool is a place where the computing power (miners’ power) is shared to mine block together and share an award in proportion to the individual input. Presently, lonely searching for blocks can take even hundreds of years so the best way of mining is joining groups cooperating to mine a block. Building “a mine” was the answer to difficulties in receiving payment by individual miners. There are also the specialized farms concentrating huge computing power of connected ASIC units or GPU. A typical Bitcoin farm operates on the assumption – the more computing power is generated the more bitcoins are mined. Therefore, the huge rooms (at first sight similar to server rooms) only for mining are built all over the world. The biggest cluster is located in China, Russia, the USA, Scandinavian countries and Island.

Only in 2013 the financial security agencies and central banks in some countries started to announce publicly their position to virtual currency. Bitcoin is not banned in most countries and its validation is not regulated. It proves that in these countries the law is not adapted not only to bitcoin market but even to already very popular “traditional” cashless settlements.

The price of Bitcoin similar to other cryptocurrencies went through many upward and

downward trends. In 2011 its value dynamically increased from 30 cents to \$32 to come back to the level of \$2. The relevant example is the end of 2013 when the record price reached \$1135 (higher than the gold price) and almost 50 % decrease to \$693 three days later.

Alternative for national currency

Bitcoins are more and more often playing an important role for the national currencies in small and big communities – taking a form of a kind of a local currency. In a few American towns local politicians decided to enter Bitcoin into circulation to improve budgetary position and motivate people to do businesses.

An increase in Bitcoin supply is predefined by the system protocol. Presently, 12 million coins are in circulation – 25 new coins enter every ten minutes. Generally, the supply is blocked and cannot outreach 21 million (Bitcoin is a closed system) and every four years the number of coins mined every ten minutes decreases. Although some experts believe that the pot of 21 million will be closed in 2033 of the others experts' analysis show that the mining will continue for the next one hundred years.

In the face of such changeable Bitcoin rate any long-term projections seems to be pointless. The world-famous economists gave their opinion on Bitcoin – some of them claimed that \$ 40 000 for one coin would not surprise anyone, the others predicted the total failure of the system just a dozen or so month ago. So far none of these projections have not worked. One thing can be certain – as long as people are interested in cryptocurrency trading and exchange the value of cryptocurrency including Bitcoin would not reach critically low levels. The price is supported by growing popularity of Bitcoin as a means of payment for everyday services and products.

What is the Cryptocurrency Exchange?

Most trade in cryptocurrency, similar to stocks and goods, is carried out at the Exchanges. They are not a physical place for currency exchange but virtual and completely decentralized (similar to Forex market). They provide an access to most important information about the market –

value of the particular virtual coins, assessments, trends, volumes, etc.

The Exchange is crucial for every virtual currency investor irrespectively to their skills. It is are created in a way to meet the needs of this market which is unique and double in its nature. The Exchange mechanism is adjusted to the traders' expectations who are familiar with the traditional exchanges and the beginners who have never invested at the exchange before.

Buying and selling at the Cryptocurrency Exchange

There are two ways of buying and selling at the cryptocurrency exchanges. The first method is direct buying from the exchange – no other investor is involved in this transaction. It is very simple- from your bank account the physical currency is transferred and exchange into virtual currency at the current rate. It is important to remember, however that buying virtual coins directly from the exchange owners the transaction is subject to additional handling charges. For the second method the exchange serves only as a broker, is a platform where buyers and sellers meet to complete transactions. The offers are presented in a form of a tender or a direct commission – we inform how many coins we want to buy and at what price. This solution is popular with investors as the role of the exchange is limited and no or very little additional charges are imposed.

Wallet – a place for your BTC

The user can store their virtual money like traditional money in a *wallet*. Wallet is a place on the computer disk surface or a cloud where the bitcoins are stored. It is a conventional term as every Bitcoin is an integral part of a blockchain. Bitcoin uses coding with a key (every time two keys are created) One key is public and another private one. Wallet is a set of these keys.

Where can I pay with Bitcoin?

Bitcoin thanks to its popularity although is a completely virtual concept is gradually entering to the reality. The internet payment systems a; over the world start to accept Bitcoin and, in a media, we can hear about schools/hospitals and other

institutions which accept virtual currency as a form of payment. In the shops, clubs and hypermarkets the special readers are placed to pay with Bitcoin for shopping – it is possible with a wallet saved on

a mobile phone. The list of the most popular payments with Bitcoin includes payments for food, accommodation, Internet services, education and online shopping [3].













Przykłady wybranych kryptowalut				
 MONERO.PL	 CASH		 peercoin	
Monero	Zcash – ZEC	Dogecoin	Peercoin	Tether (USDT)
	 LISK	 IOTA	 E O S	 ethereum
Decred	Lisk	IOTA	EOS	Ethereum (ETH)
				
NEO	Qtum	Ripple (XRP)	Dash	Litecoin
 namecoin				
Namecoin	Hshare (HSR)	Siacoin	TRON (TRX)	Stellar (XLM)

Fig. 2. Examples of selected cryptocurrencies

One of the solutions for building cryptocurrency exchange is CoinCasso project. CoinCasso Exchange is a licensed cryptocurrency exchange with the office in Estonia (PRO(AU)- Token Issuer, CoinCasso OU (EST) – Cryptocurrency exchange platform. As the first in the world this platform adopted a unique system of withdrawing to 80 % of profit from the whole CoinCasso infrastructure for every user in proportion to the number of CCX tokens they possess – CoinCasso Exchange Token. The whole infrastructure earns profit from the commissions for the intermediations in transactions. This is the only system in the world which share its 80 % profit with CCX token owners – CoinCasso Exchange Token [4].

CCX Token is based on a popular and tested blockchain technology. It is ERC-20 token based

on Ethereum. It is a popular and universal solution with good transparency and variety of token protection and storage methods [4].

CCX tokens are available immediately after buying and can be withdrawn to the dedicated address with META MASK or ImToken application. The guaranteed trade with CCX tokens is provided at the cryptocurrency exchange – CoinCasso Exchange just after the end of selling tokens (after 30 December 2019). You can buy services or membership for any period of time with CCX tokens, which gives profits from the whole infrastructure [4].

CoinCasso Exchange tokens (CCX) can be bought at the official Internet site **coincasso.io**. We can pay for them by CoinPayments with a dozen

various cryptocurrencies: [BTC], [LTC], [BCH], [ETH], [ETC], [DASH], [DGB], [LSK], [WAVES], [ZEC], [ZEN], and other. PerfectMoney in USD are also accepted [4].

To become a member of CoinCasso project you should register by filling the form with: login, email address, password, confirm the password, PIN, year of birth, name and a surname, address, location, zip code, sex, number of the person who recommends us, e.g.: <https://coincasso.io/register.aspx?u=2084>.

Cryptocurrency are not stable and their value changes at present, which leads to many speculations and lack of its rate predictability. Consequently, at that stage these tendencies do not influence positively development and use of cryptocurrency.

The first comprehensive regulation in cryptocurrency business was introduced on the 1st January 2020 in Lichtenstein. The Token and Trustworthy Technology Service Providers Act (TVTG) called Liechtenstein Blockchain Act is to increase protection of investors, prevent money laundering and end legal dispute on that issue [5]. In Principality of Lichtenstein Frick Bank as the first bank in that country extended the range of its services by trade with cryptocurrency. This service is addressed to the “professional market users and financial intermediaries”. Trade is possible with five cryptocurrencies: Bitcoin (BTC), Bitcoin Cash (BCH), Litecoin (LTC), Ripple (XRP) and Ether

(ETH), exchangeable into Euro, USD and Swiss franc [5].

The above examples and experts’ opinions indicate that in the near future cryptocurrency market will be regulated and international and national legal regulations will foster its further development and proper trading.

The introduced regulations should protect cryptocurrency owners from any kind of threats and dishonest actions. The faster they are enforced the faster, in the author’s opinion cryptocurrency will become a global common means of payment.

References

1. *Siemionczyk. (2015). Bitcoin w głównym nurcie. Tradycyjne instytucje zaczynają wspierać rozwój rynku wirtualnych walut, „Rzeczpospolita” z 26 marca 2015 r., s. B6.*
2. *Tomański R. Co powinniśmy wiedzieć o bitcoin? Retrieved from: <http://technowinki.onet.pl/artykuly/co-powinnismy-wiedziec-o-bitcoin/b30nk>.*
3. *Wojdyło K. Bitcoin a polskie prawo Retrieved from: <http://www.codozasady.pl/bitcoin-a-prawo-polskie/>*
4. *Cryptocurrency exchange platform. Retrieved from: <https://coincasso.io/pl> Pierwszy kraj uregulował w całości kryptowaluty. Tokeneo News. Retrieved from: <https://tokeneo.com/news/pl/pierwszy-kraj-uregulowal-kryptowaluty/>*