ASEJ
Scientific Journal
Bielsko-Biala School of Finance and Law

Volume 26 | Number 2 | July 2022

ISSN2543-9103
eISSN2543-411X
www.asej.eu

Bielsko-Biała

ISSN: 2543-9103 ISSN: 2543-411X (online)

Cryptocurrency Exchange. Bitcoin – Risks And Opportunities

Bronisław Młodziejowski[1], Kamil Martyniak[2], Dariusz Szydłowski[1]

[1] Department of Law and Social Science, Bielsko-Biala School of Finance and Law
Cz. Tańskiego 5, 43-382 Bielsko-Biała - Poland

[2] Municipal Police Station in Bielsko-Biała
Wapienna 45, 43-300 Bielsko-Biała – Poland

***Abstract*— the article presents an outline of a virtual currency-cryptocurrency exchange and the possible risks and opportunities associated with it. The genesis of cryptocurrency was discussed on the example of bitcoin. The aim of the article is to present various aspects of functioning of bitcoin in association with the events influencing the growth of interest in it. The article presents the creation of bitcoin and the concept behind its creation. An analysis of the advantages and disadvantages of this cryptocurrency was carried out. Bitcoin as an entirely virtual currency, which is not sub-ject to any state institution or central bank, requires much more trust from its users than traditional states' currencies. Also, the method of storing bitcoins is far from traditional. The article also describes the technical steps for using said cryptocurrency.**

Keywords— cryptocurrency, bitcoin, Internet, virtual currency, monetary system.

I. INTRODUCTION

The development of technology, and especially the Internet, in the last two decades has contributed to changes in many areas of life. One of the areas in which technological progress is most apparent is banking and finance sector. The emergence of online banking has changed the perception of the role of banks as institutions. Payment and credit cards have revolutionized the way payments are made. The computerization of financial markets caused the emergence of previously unknown phenomena. High-frequency trading can be pointed out as an example of such phenomenon. This applies to transactions during which the asset is purchased and then immediately sold (often within less than 1 second). All these changes undoubtedly have a huge impact on the shape of the contemporary economic reality. In such a dynamically changing reality and in times of enormous technological progress, it seems that it would be difficult to find an event that could be called a revolution. However, the emergence of a new phenomenon: bitcoin- a virtual currency based on cryptography, which is not subject to any state or international institution, can be considered as such. Of course, this is not a revolution in the literal sense of the word. Interest in the new cryptocurrency did not translate into the weaking of the role of traditional currency. It also did not lead to significant changes in the financial markets. This "revolution" took place in the way of thinking about what money is and what can fulfill its function. From the Middle Ages, the concept of money was closely related to the ruler, i.e. to the state represented by the King, and to the law of which he was the source. The connection between money and the state weak-ened slightly in the late Middle Ages when banks and the scriptural they created emerged. How-ever, from the 17th century onwards, countries began to take an interest in monetary policy anew. In subsequent countries, central banks were established, whose role was to control the money creation process conducted by the commercial banks. In this way, a deeply rooted belief in the inextricable relationship between money and the state was present until the beginning of the 21st century. Therefore, the emergence of bitcoin-a cryptocurrency that is not subject to or controlled by any state, constitutes a kind of "revolution".

The aim of the article is to present the current state of the bitcoin cryptocurrency, broken down into risks and opportunities as simply and reliably as possible. There is a noticeable social need to develop such material. Often, various doubts and fears concerning virtual currencies and cryptocurrencies in particular, result from ignorance or media feeding on sensational reports. However, they should be looked at in a broader context: not only in the context of fears, tech-nical or legal difficulties related to a new phenomenon, but also in the context of innovative technology and the emergence of the new sector of the economy.

ASEJ - Scientific Journal of Bielsko-Biala School of Finance and Law
Volume 26, No 2 (2022), pages 4
https://doi.org/10.19192/wsfip.sj2.2022.2
Received: May 2022 Accepted: June 2022
Published: July 2022

II. BITCOIN – AN OUTLINE OF THE CONCEPT

The most well-known cryptocurrency is bitcoin (BTC) created in 2009 by a Japanese under the pseudonym Satoshi Nakamoto. The motivation for his invention was a limited trust towards the state authorities. The cryptocurrency is based on advanced cryptography and a P2P exchange network, i.e. computer-to-computer, without intermediaries. The source code of the currency is open and accessible to everyone. The algorithm that generates bitcoins has been developed in such a way that their number will never exceed 21 million. At first glance, this might not seem like a sufficient number when taking into the account current market demand for currencies. However, every bitcoin is divisible to eight decimal places, so scarcity shouldn't be an issue (Palczewski, 2021).

Bitcoin is a type of a cryptocurrency or virtual currency (VC). Cryptocurrencies are de-fined as "monetary units of participation in a distributed accounting system based on cryptography" (Tax Chamber, 2015), which "while having no centralized issuer or institution controlling their exchange and autonomous consumption value, constitute a measure of debt redemption which is contractually agreed between the parties of a given legal relationship of the value agreed to by the parties which accept the option of debt redemption by the means of Cryptocurrencies. Thus, cryptocurrencies solely function as a monetary value exchange medium." (Tax Chamber, 2015). Main distinction between bitcoin and the traditional currency is the lack of a central issuer and an institution which supervises the exchange rate of this currency. In the community of Internet users, virtual currencies are concidered as money, as they basically fulfill all its characteristics. First of all - with some reservations, described below - cryptocurrencies perform a monetary function. In addition, they are the means of exchange and a measure of value. In addition, cryptocurrencies perform the function of storing value and transferring risk much more effectively than money (which has become the main reason for their popularization). (Gruszecki, 2004, p.70). Virtual currency systems are diverse. Bitcoin belongs to a system with two-way flow that works like any convertible currency, with two exchange rates (buy and sell) (Srokosz, 2014, p.846). It is decentralized, which means that there is no central issuer, and it is the users who 'mine' individual entities of the currency. Virtual currencies are based on a complex system of cryptographic protocols. The creation of bitcoin consists of generating a code (cipher) by using a so-called excavator, i.e. specific software and hardware with high computing power, in a peer-to-peer network (Tax Chamber, 2015). Network users, known as miners, acting on their own, in a group or with the participation of special companies, the so-called server farms, provide computing power and special computer software, allowing at the same time to check a set of transactions and add them to the chain, i.e. the blockchain (Piotrowska, 2013, p.277). Mining is a competitive activity in which the miner has no control over what gets attached to the blockchain and consequently who will get the bitcoin, hence mining is considered to be "the counterpart of lottery base on competition" (Bitcoin.org, 2014). The acquisition of the right to bitcoin is primary, which means that the right to bitcoin is not dependent on the existence of a right on the part of another entity, it arises regardless of the rights of the possible previous owner. K. Zacharzewski accurately compares the above-described situation to the acquisition of ownership of no one's movable property pursuant to article 181 of the Act of 23 April 1964 Civil Code (Journal of Laws 2017, item 459) (Zacharzewski, 2014, p.1134). Mining (acquiring) bitcoin is a legal event, but it does not constitute a declaration of will, which resembles the creation of a legal substantive relationship as a result of finding no one's property or creating a new property from one's own materials (Zacharzewski, 2014, p.1134).

Although, because of the technical reasons and assumptions of the bitcoin algorithm, it is not possible to mine it physically, the property right arises in favor of one of the parties participating in the operation. Therefore, bitcoin creation should be qualified as a right-shaping event, i.e. the right to unilaterally lead, by means of declaration of will, to the creation, change or termination of a legal relationship (Radwański, 2008, p.177).

III. BITCOIN AS AN INNOVATIVE DIGITAL CURRENCY EXCHANGE SYSTEM – OPPORTUNITIES

Bitcoin, like other virtual currencies, is only created and stored electronically (Nian, Chuen, 2015, p.15). However, the solution developed by Satoshi Nakamoto differs from centralized virtual currencies by using cryptography in all aspects of bitcoin's functioning, i.e. in terms of controlling the supply of bitcoin units, as well as for comprehensive control of the transaction execution process (including the verification of its correctness) (Badev, Chen, 2014, p.7). The essential novelty, even described as "revolutionary" (Nian, Chuen, 2015, p.15) in relation to the previous concepts of cryptocurrencies, is the elimination of the well-known problem of cryptographers namely multiple spending of funds.

The bitcoin system made it possible to eliminate both the need for a third party securing the transaction and the central unit responsible for issuing the cryptocurrency. This was achieved by basing the operation of the system on a distributed communication model, and more specifically on a network of equal entities (P2P). As M. Szymankiewicz points out, in the P2P model, "each user is equal and connects to other computers in the network. There is no clear hierarchy or designated roles such as a machine requesting resources and a machine providing resources, which is the case in the client-server architecture" (Szymankiewicz, 2014, p.38). The bitcoin system is created by a network of involved users, and its operation does not depend on any central unit, as such does not exist in bitcoin's case (Szymankiewicz, 2014, p.38).

The issuance of bitcoin consists of usage of the computing power of Internet users' devices. This means that each Internet user, after installing special software on his computer, can become not only a participant in the bitcoin system, but also an issuer of this cryptocurrency. The issuance of bitcoin has been programmed and occurs automatically as a consequence of certain mathematical events. Creating the system in this way limited the possibility of its termination by the creators or any other entity and made it impossible to withdraw the transaction

- which is positive for the Merchant, but hazardous for the payer (Polasik et al., 2015, p.14).

The primary tool that allows using the bitcoin system is the bitcoin wallet (Bamert et al., 2014, p.65). Installing its software does not require providing personal data. The functionality of the wallet, the security of storing bitcoin and the virtual currency exchange depends on the choice of the provider of software that interacts with the bitcoin network and the place of its installation. The bitcoin wallet software generates bitcoin addresses. Each user can have an unlimited number of bitcoin addresses. A specific BTC balance is assigned to each bitcoin address. The value as-signed the bitcoin address refers to the blockchain maintained by the bitcoin network. Funds stored on addresses are aggregated within the wallet so that the user can see their total value. The bitcoin address is in the form of a string of 34 characters (randomly selected numbers and letters) (Franco, 2015, p.17), for example: *17A9ZyscFDsosYiQ3KAmiRaVmQgMLX4in3*. The fact that it can be displayed in the form of a QR code should be emphasized. This address can be compared to a bank account number (Carignan, p.66). Except that in the case of bitcoin, the address and its balance are publicly available, while the owner of the address is anonymous (un-less he decides to disclose himself). In the case of a bank account, however, knowing the number may allow you to determine its owner, but there is no publicly available data on the amount of funds accumulated on it. This structure of the system ensures that the identity of the holders of funds expressed in the bitcoin cryptocurrency is hidden.

In the light of the presented features and functions of the system and the bitcoin crypto-currency functioning within it, this solution can certainly be considered an innovation. Bitcoin is an invention of a global scale which revolutionizes the existing concepts and technological solutions in the field of e-commerce payments.

IV. BITCOIN – RISKS AND THREATS

One of the most important threats associated with bitcoin exchange is the phenomenon of money laundering. In light of the broadly defined subject side of the money laundering offense (article 299 § 1 of Act of 6 June 1997 The Penal Code (Journal of Laws 2016, item 1137)) there is no doubt that the cryptocurrencies, including bitcoin are subject to the property law provisions (Zacharzewski, 2014, p.197). However, the analysis of the provisions of the Act of November 16, 2000 on Counteracting Money Laundering and Terrorism Financing (Journal of Laws 2018, item 723) indicates that its application to transactions involving bitcoin is problematic (Directive (EU) 2015/849 of the European Parliament and of the Council, article 2). Although this regulation applies not only to money, but also property rights, there is no entity obliged to inform about a 'suspicious' transaction. It is not possible to consider entities operating as the transaction platforms as the so-called obligated institutions which, when carrying out the transaction, are required to register the transaction (cf. Art. 2 point 1). In addition, cryptocurrency exchange platforms operate on the basis of allowing the exchange of cryptocurrencies for traditional currencies by the portal users themselves. Also for this reason, the activity of this entity is not subject to the definition of an "entity providing currency exchange operations" contained in the Act (Article 2 point 1p). Moreover, the Act, as a rule, covers transactions whose equivalent exceeds EUR 15,000 (Article 8 Paragraph 1), and when determining the equivalent in EUR, the average National Bank of Po-land's exchange rate for a given currency is used, applicable on the day of the transaction or on or the day the transaction is ordered (Art. 2a). Bitcoin doesn't have an average rate against any currency. Moreover, the obligation to register transactions does not apply to transactions concluded on the interbank market, which include cryptocurrency transactions (Article 8, Paragraph 1e, point 5).

Bitcoin cannot be the subject of theft, which relates to the seizure for the purpose of appropriation of someone else's movable property, computer program, energy or a card entitling to withdraw money from an ATM (Article 278 § 1-5 of the Penal Code). As bitcoin is not money, it cannot be the subject of the offense of money counterfeiting, as the provision concerns the concept of "other means of payment" referred to in Art. 310 of the Penal Code (Zacharzewski, 2014, p.197). In this case, the criteria of the following prohibited acts can be meet: extortion (Article 282 § 1 of the Penal Code), misappropriation (Article 284 § 1 of the Penal Code) and fraud (Article 286 § 1 of the Penal Code), which also apply to property rights. It is also obvious that interference in the bitcoin holder's wallet may fulfill the disposition of Article 287 § 1 of the Penal Code: the so-called computer fraud (Zacharzewski, 2014, p.197).

Virtual currencies have no foundation in conventional economy, which means that they are susceptible to risks related to manipulating its value and exchange rate risks - they can be used as a pyramid scheme (Musiał, 2013, p.17). The threat is the lack of supervision by the Polish Financial Supervision Authority and the National Bank of Poland, which causes doubts as to the safety of the virtual currency exchange and guarantees of the transferred assets, and the lack of guarantees from the Bank Guarantee Fund for transactions and exchanges does not ensure their safety and the safety of accumulated assets. The value of a virtual currency depends on supply and demand and in no way reflects the value of the economy and the financial viability of the issuer. There are no stabilizing tools on the market, therefore the variability one way or the other is practically unlimited. The financial aspect in cyberspace is carried out in the form of banking and financial transactions with the use of authorized entities such as PayPal, Western Union and virtual currencies. Entities carrying out virtual currencies transactions are exposed to the risk of money laundering, concealing assets, tax avoidance or financing terrorism. The aforementioned conditions lead to the conclusion that the most serious threat is the lack of supervision of the anti-money laundering or anti-terrorist financing institutions whose task is to register transactions and conduct analyzes in terms of threats. For individual investors, in addition to the loss of value of the accumulated

cryptocurrencies, during the transaction, there is a risk of "poisoning" it i.e., placing additional illegal information (files, images, text data). A transfer of funds may contain files, e.g. with pornography, for which the contractor may be prosecuted. The instability of cryptocurrencies may be affected by political and legal decisions of other countries in the world. For example, when the Chinese government decided to close the three largest bitcoin exchanges (September 2017), the price of this currency fell by several dozen (Charatynowicz, 2016), and JP Morgan stated that "bitcoin is a scam" (Żuławiński, 2017). The threat to the Internet users is using their computers to "mine" cryptocurrency. The information provided by Kasperski Lab shows that there is software distributed via torrents on the Internet, which allows bootnets to be included in the network and, without the owner's consent, to use the computer's power consumption and computing power, which of course exposes the owner of the infected computer to losses. (Żuławiński, 2017).

V. Conclusions

The lack of precise and consistent regulations regarding cryptocurrency market participants means that institutions that are not subject to control by supervisory authorities take part in it. At the same time, the increasing volume of cryptocurrency exchange and the increasingly widespread acceptance of this method of payment by business entities operating in the traditional economy means that one should expect the introduction of legal regulations regarding cryptocurrencies and participants of cryptocurrencies' market, including the introduction of licenses for exchange market organizers. The increasing interest of Internet users in cryptocurrencies and the increasing liquidity of this market mean that it may be attractive in the future for institutions operating on the Polish financial market. Currently, it is difficult to imagine that bitcoin, whose volume of ex-change is still marginal, would become a currency such as the US Dollar or the Euro. However, it is to be expected that it may become widespread over time. Since people have become accustomed to non-cash payments with the use of payment and credit cards, over time, under favorable conditions, they may also accept this new form of money due to its simplicity, convenience and security. Whether bitcoin will remain only as speculative good or does it have a chance to become the currency of the future and whether there will be more opportunities than threats in its ex-change- time will tell.

VI. References

Badev A., Chen M.,2014. Bitcoin: Technical Background and Data Analysis, in: Finance and Economics Discussion Series, Federal Reserve Board.

Bamert T., Decker C.,2014. Wattenhofer R., Welten S., Blue Wallet: The Secure Bitcoin Wal-let, in: Lecture Notes in Computer Science.

Carignan M. A., The Bitcoin Tutor. Unlocking the Secrets of Bitcoin, The Bitcoin Tutor.

Charatynowicz J., 2016. Ekonomiczne aspekty cyberprzestępczości. Zagrożenia związane z konwersją i transferem wirtualnych walut, in: Editor: J. Kosiński. Przestępczość teleinformatyczna, Szczytno: Police Academy in Szczytno.

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Coun-cil, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (the Anti-Money Laundering Directive, AMLD 4).

Franco P.,2015. Understanding Bitcoin: Cryptography, Engineering and Economics, Wiley.

Gruszecki T., 2004. Teoria pieniądza i polityka pieniężna. Rys historyczny i praktyka gospodar-cza, Cracow.

Ignatowicz J., Stefaniuk K., Radwański Z., 2009. Prawo rzeczowe, in: Editors: Drozd E., Kor-dasiewicz B., Pazdan M., Radwański Z., Zieliński A., System prawa prywatnego, Warsaw

Musiał M., 2013. Technologiczne uwarunkowania korzystania z pieniądza wirtualnego, in: Editor: E. Bogacka-Kisiel, Pieniądz wirtualny i determinanty jego rozwoju w sferze ekonomii i finansów i prawa, Opole

Nian L. P., Chuen D. L. K., 2015. Introduction to Bitcoin, w: Handbook of Digital Currency. Bitcoin, Innovation, Financial Instruments, and Big Data, Editor: D.L. K. Chuen, Elsevier.

Piotrowska A.,2014 Bitcoin a definicja i funkcje pieniądza, Annales UMCS .

Polasik M., Piotrowska A. I., Wiśniewski T. P., Kotkowski R., Lightfoot G., 2015. Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry, "International Journal of Electronic Commerce" .

Srokosz W.,2014. Prawo a rozwój elektronicznych środków płatniczych w XXI wieku in: Edi-tor: Ofiarski Z. XXV lat przeobrażeń w prawie finansowym i prawie podatkowym. Ocena dokonań i wnioski na przyszłość, Szczecin .

Szymankiewicz M., 2014. Bitcoin. Wirtualna waluta Internetu, Helion, Gliwice .

Act of 23 April 1964 Civil Code (Journal of Laws 2021, item 1509).

Act of 6 June 1997 Penal Code (Journal of Laws 2021, item 2345).

Zacharzewski K.,2014. Bitcoin jako przedmiot stosunków prawa prywatnego, in: Monitor Prawniczy 2014.

Żuławiński M., 2017. Prezes największego banku w USA: Bitcoin to oszustwo, in: Bankier.pl

WSFiP conducts research and educates students in the following fields:

Finance and Accounting
- Treasure Administration
- Banking
- Corporate Finance
- Accountancy
- Accounting and Finance in Public Sector Institutions
- Corporate Accounting and Controlling
- Audit
- Management and Finance in Real Estate

Law
- this program gives strong legal foundations to undertake further professional training for judges, prosecutors, atorneys, notaries, bailiffs.

Administration
- Fiscal Administration
- Local Government Administration

Logistics
- this program gives good preparation for work in logistics companies as well as in other economic and administrative units.

Cyberspace and Social Communication
- Communication and Image Creations
- Safety in the Cyberspace

Internal Security
- Administration and Management in Security
- Security and Public Order
- Security and Development in Euro-region
- Security of Information and Information Systems
- Security in Business
- Criminology and Investigative Studies
- Criminology and Forensics
- Protection of People and Property
- Public Order Agencies

Information Technology
- Databases and Net Systems
- Computer Graphics and Multimedia Techniques
- Design of Applications for Mobile Devices
- IT Services in Public Administration Units

Postgraduate courses
- Administrative studies
- Fiscal Administration
- Law and management in health service