Cryptocurrencies and Blockchain – Challenges and Threats

By Kamil Jurczyk

ABSTRACT

In recent years, one of the most frequently discussed aspects in the world of economics has been the use of blockchain technology in economic life and the growing popularity of cryptocurrencies. Both blockchain and cryptocurrencies have incredible potential, and it is only a matter of time before they become part of daily life. The world’s largest companies regularly invest in projects related to cryptocurrencies and blockchain. On the other hand, some countries have decided to ban all private cryptocurrencies and instead develop their own concepts of a digital currency issued by a central bank. This paper aims to discuss the issues related to the potential and threats posed by the development of cryptocurrencies and blockchain technology. The analysis involves technical, social and legal aspects linked to the development of virtual money. All the considerations in the paper are based on a critical analysis of the literature on the subject and the descriptive method.

JEL Classification: E40, E42, E51.

I. INTRODUCTION

Recently, virtual money has become one of the most frequently discussed topics within economic circles. Technological advances in the last 20 years have led to a change in the perception of many areas of life, even those that seemed to be unchangeable. The creation of networks based on Blockchain technology has opened up brand new possibilities. Blockchain was originally created for the world’s first virtual currency. In 2009, Satoshi Nakamoto created the bitcoin cryptocurrency, the popularity of which started a discussion about a new direction in money development. Today, even those who are not involved in the economy show a keen interest in cryptocurrencies. At some point, the world was engulfed in a "cryptocurrency rush" of sorts, and the best proof of this was the price that Bitcoin reached on the global market. The popularity that cryptocurrencies have achieved may indicate a certain crisis of confidence in money in its current form. This phenomenon provokes reflection on whether there is an evolution, or maybe even a revolution, in the world of economics. Currently, there are around 6,5 thousand cryptocurrencies traded on the market. New projects, that sometimes differ radically from the currently available coins, continue to be set up. In the initial stage, cryptocurrencies were created with the intention of separating the means of payment from the supervision of the central authorities. Their greatest advantages were anonymity and independence, but over time also state governments decided to launch their own virtual money projects. The People’s Republic of China can currently be regarded as the major player in this area. Taking into account the global tendency to transition to a cashless economy, it should be emphasized that the future of money bears the mark of cryptocurrencies. The pandemic that has been prevalent since early 2020 has further accelerated the process of digitising many aspects of our life.

The purpose of this paper is to analyse the opportunities and threats resulting from the dynamic global development of cryptocurrencies.
II. LITERATURE REVIEW

At the beginning, it is worth mentioning a few definitions related to cryptocurrencies. Agreeing on the very definition of a cryptocurrency is not easy. The European Central Bank classified it as virtual money, which it defines as "unregulated digital money that is issued and usually controlled by creators and used and accepted by members of a specific virtual community" (ECB, 2012). The World Bank also adopted a similar definition, defining cryptocurrencies as a type of digital money based on cryptographic techniques (World Bank, 2017). Sieroń defines bitcoin as "a decentralised, market-selected internet currency, designed by a person (or group of people) nicknamed Satoshi Nakamoto based on the principles of cryptography that uses P2P networks and whose application code is open source" (Sieroń, 2014). On the other hand, Robert Stokes describes it as "an experimental virtual currency created, managed and transferred via the Internet within a peer-to-peer network, using special software used by its users" (Stokes, 2012). Nikolei M. Kaplanow defines bitcoin as "the first digital, private cryptocurrency exchanged over the Internet through the use of peer-to-peer networks", also stating that no institution, whether state or privately owned, upholds its value and notes bitcoin's similarity to fiat money currently in use (Kaplanov, 2012). Piotrowska defines the bitcoin cryptocurrency as "the first practically verified cryptocurrency, based on publicly available source code, operating within a system characterised by dispersion of emissions, verification of correctness and registration of transactions, which is used for payment and investment purposes" (Piotrowska, 2018). Finally, it is also worth quoting the definition of Richard Caetano, who considers bitcoin to be "a truly new kind of money" (Caetano, 2015).

Most cryptocurrencies are based on blockchain technology. Cryptocurrencies and blockchain have become closely related concepts. Experts define blockchain as distributed database technology operating in a peer-to-peer network that allows posting transactions, payments and accounting entries without the need for a central unit recording the information flow (https://fintek.pl/co-to-jest-blockchain/). It is a specific type of distributed ledger technology (DLT), i.e. technology for recording and sharing data in a distributed network (World Bank, 2017). The very name "blockchain" says a lot about the way it works. All transactions within the network are stored in blocks that are grouped together in a chain. A block is an aggregate of all transactions made on the network. Depending on the type of blockchain used, acquiring new coins can vary significantly. In the case of bitcoins, subsequent coins are obtained in the process of so-called mining. Due to the fact that bitcoin is based on the Proof of Work algorithm, miners are responsible for acquiring new coins. In this case, a miner is a network user who supports the maintenance of the network by making available the computing power of their hardware in order to solve a mathematical problem and thus discover a new block to which new transactions will be assigned. In return for their work, each miner who acquires a new block receives a reward in the form of a certain number of bitcoins. The difficulty of the algorithms increases systematically. In the early days of the Bitcoin system, the hardware requirements for coin mining were not onerous. Anyone with a laptop could successfully "mine" bitcoins. However, with the increasing difficulty of the algorithm solutions, the situation slowly changed. The so-called mining pools or "mines" were created. These are places that combine the computing resources of many miners to increase the probability and frequency of finding a new block (Gileman, Rauchs, 2017). Mining rewards are distributed among participating miners based on the proportion of contributed computing resources. The emergence of mines resulted from an increase in the level of difficulty, since currently mining a new block could take a single miner as many as several hundred years. The increasing level of difficulty and the emergence of increasingly larger mines boosted the concentration of bitcoin mining. According to experts from the University of Cambridge, currently about 65% of bitcoin mining takes place in China, where the technology is relatively cheap. The United States is ranked second, with a score of 7.24% (https://cbeci.org/mining_map). Besides the most popular bitcoin, there are many other cryptocurrency projects out there. The second most famous cryptocurrency is Ether, i.e. the coins used in the Ethereum network. This project, launched in 2014, was created by Vitalik Buterin, a Russian immigrant living in Canada. In 2014, Buterin began work on new blockchain network software. The developer wanted to give users features not available in the Bitcoin system. What distinguished Ethereum was its ability to create and use applications in the blockchain that can perform basically any calculations or store information. These applications have been dubbed "smart contracts". The idea of a smart contract can be defined as a legal bond that functions independently in virtual space. As a result, it is possible to conclude contracts in digital form.
without the need for paper documents. The contract is automatically performed after the conditions set out in that contract are met. The advantage of smart contracts is that their conclusion, modification or performance is independent of any third party (https://www.wardynski.com.pl/w_publication/blockchain-inteligentne-kontrakty-i-dao/). Each contract is attached to a blockchain, so it is impossible to interfere with its content, which means that they keep operating as programmed. The creator of Ethereum wanted their network to become a register that records cryptocurrency transactions and a "world computer" – a platform that allows the creation of distributed applications using the benefits of blockchain technology, which they would be embedded in (Klinger, Szczepański, 2017). The Ethereum network was launched on 30 July 2015. Currently, it is the second-largest open blockchain, and its functionality extends far beyond the transfer of cryptocurrencies. Much like bitcoin, Ethereum uses the Proof of Work consensus algorithm. It is planned to switch to a hybrid algorithm combining the current one with the Proof of Stake algorithm in order to ultimately switch to PoS only (https://www.fxmag.pl/edukacja/kryptowaluty/ethereum-eth-opis-kryptowaluty-kurs-notowania).

The Ether cryptocurrency has no upfront limited supply and therefore is inflationary in nature. When it comes to the process of acquiring the cryptocurrency, the mining process takes place here, just like in the case of bitcoin.

The third most popular cryptocurrency is XRP, i.e. coins used in the Ripple network. This platform is older than bitcoin itself since it was created in 2004 under the name RipplePay. The creator of the system is the Canadian developer Rayan Fugger. The idea behind Ripple is the immediate posting of transactions that were implemented through the use of the IOU model (short for I owe you). IOU is about creating a network of obligations between trusted parties (https://www.fxmag.pl/edukacja/kryptowaluty/ripple-xrp-opis-kryptowaluty-historia-notowania-opinie/). The cryptocurrency itself was established in 2012. As in the case of bitcoin, it is a decentralised network; however, both cryptocurrencies are radically different in terms of their operation. Ripple has very high scalability, which has been achieved thanks to greater centralisation and the introduction of a "middleman" in the form of network gateways. There is also no typical consensus algorithm here, since the agreement in relation to transactions is obtained through communication between network gateways. There is also no mining process in the Ripple network, and all units were created in one instance. The supply of XRP is set at 100 billion units of currency, but not all of them are in circulation. Initially, the creators decided that 45% of all coins will go into circulation. In May 2017, decisions were made to increase the supply systematically. 55 billion units of XRP have been placed in a special account which performs the contract every month, resulting in the introduction of another one billion coins into circulation. If the market is out of balance due to the number of XRPs released (the demand is too low), they will be carried over to the next contract. A vital feature of the Ripple network is that it can function without XRP, as it can use various fiat currencies such as the dollar or the euro. Ripple is, therefore, not a classic cryptocurrency like bitcoin. It uses blockchain technology for a completely different purpose than other virtual currencies. XRP is also known as the "cryptocurrency of banks". It has a good chance of revolutionising traditional banking and can be a real competitor to the SWIFT banking system or services such as Western Union rather than to other cryptocurrencies. Litecoin can also be considered a very popular cryptocurrency. It is one of the first cryptocurrencies strongly inspired by bitcoin. It is also referred to as digital silver. The creator and leading developer of Litecoin is Charlie Lee, an American computer scientist. Litecoin was supposed to be faster and cheaper to use than bitcoin. The first block was mined in 2011. Technically, Litecoin is very similar to Bitcoin as it is based on its source code. The block time is four times shorter than that of bitcoin; it is 2.5 minutes (https://www.fxmag.pl/edukacja/kryptowaluty/litecoin-ltc-opis-kryptowaluty-historia-notowania-opinie). The block capacity is 1 MB, as in the case of the original. The transaction fees are much lower and do not exceed 5 cents (USD). The supply of litecoin has been set at 84 million units. A common feature of both cryptocurrencies is mining because litecoin also features a mining process. The reward for acquiring a block was originally 50 cryptocurrency units; however, in 2019 the reward was reduced to 12.5. The main difference between litecoin and bitcoin is the hash function, which is the cryptographic part of the technology. The Bitcoin system uses the SHA256 feature, while the Litecoin system uses the Scrypt algorithm. The use of this algorithm results in high costs of creating ASIC miners, which in turn translates into a lower probability of the professionalisation of mining, as was the situation in the case of bitcoin.
There are hundreds of other cryptocurrencies, and new projects are emerging, differing in terms of use. Undoubtedly, the cryptocurrency industry is one of the fastest-growing branches of the global economy. Some countries, such as Venezuela, create their own tokens. Leading banks and companies, including Goldman Sachs and Microsoft, are investing in the development of cryptocurrencies because they see the future in this technology.

III. DATA AND RESEARCH METHODOLOGY

All new technologies can have a positive and negative impact on the current state of reality; therefore, this paper analyses the challenges and threats facing the development of cryptocurrencies and blockchain technology. The section dedicated to challenges discussed issues related to inflation, the lack of intermediaries and other advantages of cryptocurrencies. Then, the threats linked to virtual money were analysed. Issues connected with, among others, legal conditions for the development of cryptocurrencies or the security of this technology were also discussed. The entire analysis was based on the descriptive method and a critical analysis of the literature on the subject. The data consists of numerous literature studies, including a report from 2021 prepared by the Bank of America on cryptocurrencies or a study by the World Bank. Moreover, this article is based on several Polish and foreign publications on cryptocurrencies and blockchain technology.

IV. EMPIRICAL ANALYSIS – RESULTS AND DISCUSSION

1. Challenges

Low account maintenance costs are an advantage, especially when making global transactions. The lack of intermediaries and the lack of a currency spread result in cost reductions. This can positively affect the efficiency of international trade. Resistance to inflation does not eliminate it completely. Undoubtedly, cryptocurrency is not very susceptible to inflation. With this, it is impossible to spoil this money. This is a very desirable feature in the case of developing countries (Perez, Urbaniak, 2013). These countries often struggle with the problem of high inflation. In Argentina, where price increases have reached double-digit values, bitcoin is seen as a real alternative to the native currency (https://www.washingtonpost.com/news/the-switch/wp/2013/08/21/five-surprising-facts-about-bitcoin-2/?noredirect=on). A unit’s high divisibility is a guarantee of cryptocurrency flexibility. If there was a sharp rise in the value of bitcoin and 1 satoshi had the same value as $ 1, the supply of bitcoin would be 2.1 trillion dollars, which is much more than the supply of all the money in the world. One of the most important advantages is the anonymity of parties to the transaction. The transaction ledger is available to everyone; however, details of the entities participating in the operation are not available. The mechanism can be compared to the stock exchange, where the time and volume of the transaction are published, but there is no information about its participants (Perez, Urbaniak, 2013). The inability to interfere with blockchain also ensures a very high level of security in relation to the security measures used in commercial banks.

Both fiat money and cryptocurrencies are based on social trust, which gives them actual value. If the public loses trust in the issuer, the money becomes completely worthless. Many Bitcoin users mistakenly claim that it was created as a response to the pathologies of the financial system that surfaced during the Great Economic Crisis in 2008. It should be noted, however, that the convergence of these two events is coincidental, as work on the Bitcoin system must have started much earlier, when there were no indications of an impending collapse of the global economy. In his manifesto, Nakamoto only addressed the issue of building a financial system, and more specifically, the presence of an intermediary institution in every transaction. The key aspects in creating bitcoin were: the anonymity of the transaction and the creation of a transaction mechanism with no need for a third party. As for the anonymity of transactions, it should be said that there is pseudonymity in the case of bitcoin. “Pseudonymity in this case means that if you put an enormous amount of energy into operational safety and do it thoroughly and very carefully, then you may remain anonymous. However, only for a limited time.” (https://bitcoin.pl/bitcoin-nie-jest-nie-do-konca-anonimowy-mowi-andreas-antonopoulos/) – these
are the words of Andreas Antonopoulos, blockchain expert and author of some of the most popular books on bitcoin. Meanwhile, it is necessary to answer the question of whether complete anonymity is the most beneficial for society. Opponents of cryptocurrencies pay attention to the role of virtual coins in the criminal world. Many portals on the dark web selling drugs or weapons use cryptocurrencies to settle their transactions. The most popular cryptocurrency in this practice is Monero, as it ensures complete anonymity. In this case, anonymity may be unfavourable from the point of view of the broadly understood public interest. The lack of an intermediary in transactions also has its drawbacks. Bitcoin has no customer service department or a hotline. In the event of an erroneous operation, the coins will not be returned, as is the case with payment cards using the "chargeback" service (Piotrowska, 2018). The use of cryptocurrencies also requires users to comply with the basic rules of safe network use, that is: having up-to-date antivirus software, using different passwords for various services related to cryptocurrencies, and using secure wi-fi networks. Thus, the spread of bitcoin also depends on the degree of public education in cybersecurity. There are also many possibilities of using blockchain technology itself. Żuława points to the ease of implementing blockchain-based solutions, e.g. in the real estate market, where land and mortgage registers would appear in a blockchain, and transactions would be made in the form of smart contracts (Żuława, 2018).

2. Hazards

In times of rapid development of new technologies, legislators are often unable to keep up with the adaptation of legal regulations to modern realities. This has its positives, as the lack of detailed regulations allows for an unlimited development of innovations appearing on the market. However, at some point, it becomes an obstacle in the process of popularising new solutions. Legal regulations introduce certain standards applicable in a given field and increase trust in innovation by a wider group of recipients (Piotrowska, 2018). Considering that bitcoin has been around for 11 years, legal regulations, in this case, have become necessary for the continued development of the cryptocurrency. Depending on the type of regulations adopted, they may have different effects: they may support the development of cryptocurrencies, limit their role to a specific market niche or make their trading completely illegal (Piotrowska, 2018). Currently, legislative bodies in various countries have a different approach to the subject of cryptocurrencies. The People’s Republic of China introduces restrictions on bitcoin transactions (https://www.bloomberg.com/news/articles/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions), while the Ecuadorian government prohibits its use altogether (https://www.coindesk.com/ecuador-bans-bitcoin-legislative-vote). Most countries, however, see the potential in cryptocurrencies and are trying to introduce sensible regulations in this area. The European Parliament has issued a resolution on virtual currencies in which it clearly states that cryptocurrencies have potential but also associate them with their popularisation (https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52016IP0228&from=SL).

The very classification of bitcoin is a moot point. Some definitions define it as the equivalent of a foreign currency (https://www.theguardian.com/business/2013/dec/21/bitcoin-legal-status-uk), others as private money (Kurek, 2017), while yet another definition considers it an asset or property (https://www.irs.gov/newsroom/irs-virtual-currency-guidance). The legal definition of cryptocurrencies is fundamental from the standpoint of tax law. In Poland, the General Inspector of Financial Information has prepared a study relating to cryptocurrencies. An attempt was made to qualify and define virtual currencies. It also indicates the benefits of the development of cryptocurrencies and the risks associated with their functioning. Particular attention was paid to consumer protection and the possibility of using virtual currencies by organised crime groups or terrorist organisations.

In the UK, an official position has been adopted regarding taxation when carrying out business related to cryptocurrencies or making payments with their use. UK authorities have classified virtual currencies as a "negotiable financial instrument".
The Polish legislation was very slow to deal with legal issues related to Bitcoin. In the initial stage, only individual tax interpretations were issued. For some time, the Ministry of Finance considered classifying bitcoin under property law. However, due to the inconsistency of this action with the principle of rational economic trading, this idea was abandoned.

In 2015, the European Court of Justice issued a judgment in which it was indicated that the purpose of virtual currencies is the role of a tender. It was assumed that bitcoin should be treated as a means of payment for tax purposes and thus should be exempt from VAT (Piotrowska, 2018). In July 2016, a special expert group was set up at the Ministry of Digital Affairs, called Blockchain and Cryptocurrency Stream. Its goals include enabling favourable conditions for development and creating standards for companies in this sector. It also became focused on educating administrative institutions, security authorities and businesses in the use of this technology. The Stream also analysed Polish law in the context of blockchain and virtual currency applications (https://www.gov.pl/documents/31305/52168/przegląd_polskiego_prawa_w_kontekscie_zastosowan_technologii_rozproszonych_rejestrow_oraz_walut_cyfrowych.pdf/f6e74ec0-09e5-776d-bd3b-c21fa96cece2). The analysis covers civil, commercial, criminal, administrative and tax law. It was found that there is no need to create separate legal acts relating to these issues in Polish law. According to experts, bitcoin can be treated by law as a measure of value other than money. The group indicated that administrative and tax law had to be adjusted in the context of cryptocurrencies. At the same time, the need to systematise the concepts and definitions in this area was emphasised.

A big dilemma in the case of cryptocurrencies remains the balance between individual freedom and the security of the general public. From the EU directive relating to virtual currencies it can be concluded that, according to EU officials, criminals and terrorists are the ones most active in securing online anonymity, while honest people have little need for it (http://www.witoldskroksz.pl/pl/blog/anonimowosc-kryptowaluta-legalna-definicja-wirtualnych-walut-projekt-dyrektywy-zmieniajace). This position can significantly hinder the development of the cryptocurrency sector. Current world trends, particularly evident in the European Union, aim to increase the authorities’ control over an individual.

There is no doubt that cryptocurrency law needs to be improved. Sensible legislation may contribute to a faster spread of virtual currencies in society. However, the authorities must remember the ideas that guided the creation of cryptocurrencies. Individual freedom expressed in this case by the ability to make anonymous transactions is one of the main advantages of virtual currencies, which should not be limited. Citing the disadvantages of cryptocurrencies, one can mention the lack of a guarantee of value. In the case of traditional currencies, the guarantor is the state that cares for a high level of public confidence in money. In the case of cryptocurrencies, there is no guarantor, which may cause instability in the currency’s reliability. Certain cryptocurrencies can also be vulnerable to speculative attacks. Market capitalisation allows for an effective attack, which is impossible with traditional currencies backed by stock and bond markets. Also, the legal environment of cryptocurrencies can be classified as a disadvantage. The current state does not allow the full use of cryptocurrencies, if only due to the lack of an unambiguous classification of cryptocurrencies. A person who steals an improperly secured private key can also be challenging to identify. The problem may also be the inability to recover a private key, which causes the irreversible loss of coins. The disadvantage of cryptocurrencies is also the possibility of using them for criminal purposes. Anonymity creates a friendly environment for terrorist organisations, drug cartels and other illegal organisations such as WikiLeaks. Virtual currency can also be used as a means of money laundering. Recently, much controversy has been caused by the ecological aspect of cryptocurrencies. The bitcoin mining process at the current stage of development generates a very high demand for electricity. The mining process of this cryptocurrency generates carbon dioxide emissions comparable to those of Greece (Bank of America, 2021). Also in Iran, the authorities banned cryptocurrency mines from operating because the energy consumption was too high, which resulted in network overload in some cities.
V. CONCLUDING REMARKS

In conclusion, both cryptocurrencies and blockchains are undoubtedly technologies of the future. Interest in blockchain technology, which offers complete anonymity and transparency, allows us to believe that its use on a large scale is only a matter of time. In practice, the use of blockchain can positively affect the effectiveness of enterprises and improve the quality of life of ordinary people. However, for the sake of the development of this technology, it is necessary to stop perceiving it only through the prism of cryptocurrencies. The potential of bitcoin has prompted states and private institutions to take steps to develop their own cryptocurrencies. All the cryptocurrencies offered on the market today are no longer seen as a money substitute but as the funding of innovation resulting from a given project’s functionality. However, this does not mean that you cannot use cryptocurrencies as a means of payment. However, there are a number of risks that can hinder development. First of all, the complex legal situation of cryptocurrencies requires that legislators take immediate action. The issue of ecology can also be a significant barrier to the development of this sector.

REFERENCES

World Bank Group, (2017). Distributed Ledger Technology (DLT) and Blockchain.
CONFLICT OF INTEREST:
The authors declare that they have no material or financial interests associated with the research presented in this article. The authors declare that the study was conducted in the absence of any commercial or financial relationship giving rise to a conflict of interest.

COPYRIGHT AND LICENSE:

This article is published under the terms of the Creative Commons Attribution – NoDerivs (CC BY-ND 4.0) License
http://creativecommons.org/licenses/by-nd/4.0/

Published by Podhale State College of Applied Sciences – Nowy Targ, Poland