DOI : 10.14746/pp.2021.26.3.7

Wojciech MINCEWICZ
Uniwersytet Warszawski
ORCID ID: 0000-0003-0460-9158

Social sciences to the rise and development of cryptocurrencies: an analysis of the notion[1]

Abstract: The aim of the article is to conceptualize, that is, to explain, analyze the meaning and indicate the framework for the interpretation of the concept of "cryptocurrency" in social sciences, including political science. As issue an interdisciplinary, polysemic and at the same time novum technological novelty, cryptocurrencies are a challenge for representatives of the world of science. The proposed heuristic model of concept analysis based on the technological, legal and economic aspect indicates that in the broad sense of cryptocurrencies it should be understood as: decentralized, functioning in a network with a peer-to-peer architecture, cryptographically secured, based on trust and consensus, type of virtual currency, that meets some of the functions of money. Explaining the content by one aspect of the functioning of cryptocurrencies is its narrowing down.

Key words: cryptocurrencies, Satoshi Nakamoto, blockchain, technological revolution, financial instruments

Introduction

The technological revolution taking place in the realities of the 21st century changes the functioning of modern man. One of the manifestations of the development of new technologies is the creation of a segment of alternative financial instruments, completely decentralized, independent of state institutions, with a dispersed infrastructure. Work to create an internet currency that could would make it possible exchange without the need for a trusted third party began in the 20th century (Chaun, 1983, 1985; Szabo, 1997; Dai, 1998). However, it was only in 2008 that a person or people with the pseudonym Satoshi Nakamoto presented a reliable project, free of errors and problems that his predecessors did not overcome. At the time of the publication of *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008), knew about the new payment system a small, exclusive group of people, focused around the metzdowd community and enthusiasts of cryptography and online anonymity. Until 2011, the price of one bitcoin did not exceed one dollar and the number of network users grew slowly. At the beginning of 2021, the stock exchange rate price of bitcoin, the first cryptocurrency, exceeded $40,000, establishing the new All Time High (ATH), and the market capitalization of the entire market was over $1 trillion. The number of digital asset holders, based on the number of positive balance bitcoin wallets, is estimated at about 34 million people worldwide (see www.

[1] Artykuł powstał w ramach realizacji projektu: *Postawy polityczne użytkowników kryptowalut w Polsce* finansowanego ze środków Narodowego Centrum Nauki, przyznanego w ramach konkursu Preludium 18 na podstawie decyzji numer 2019/35/N/HS5/02222. Kierownikiem projektu jest mgr Wojciech Mincewicz.

bitinfocharts.com)[2]. Steadily increasing both the number of new cryptocurrencies and users are growing steadily, as is interest in blockchain technology.

The emergence and development of cryptocurrencies creates, on the basis of science, an undeveloped space for representatives of many fields, including also political science. Cryptocurrencies have a number of properties that allow the elimination of state institutions, as well as other institutions, including, for example, central banks. They are generated on the basis of mathematical algorithms, not political decisions, and therefore are deflationary in nature. In addition, thanks to digital, digitized form and cryptographic security, they are resistant to forgery, ensure relative anonymity (pseudo-anonymous), are quick and direct in transferring. These properties make the in addition to the “desired” activities, cryptocurrencies facilitate the flows of funds in the range of financing terrorism, revolutionary, extremist or dissident movements. The example of Wikileaks, which collected over 4,000 bitcoins for its activities (Redman, 2020), confirms that even the world’s largest powers are not able to counteract the financing of specific projects using cryptocurrencies. Despite the dynamics of development and the growth of interest, as before no single universally recognized definition of the term has been developed so far. While cryptocurrencies are primarily an economic instrument, this has not been proposed by financial organizations, and most policymakers at all have refrained from defining the term. Most often, cryptocurrencies are treated as a form/type of virtual or digital currency (see Houben, Snyers, 2018). The aim of the article is a multidimensional analysis of the concept of “cryptocurrency,” based on a heuristic model used to recreate the characteristic features of the phenomenon by identifying and describing its main components, it means, aspects. Individual aspects have been identified on the basis of a review of the literature on the subject, where in quantitative terms the works of IT specialists, lawyers and economists are dominant. Understanding the term each time depends on the conditions of a specific field of knowledge, where the emphasis is appropriately on: the technical layer of cryptocurrencies; juristic challenges related to their development, and also analysis of their economic nature through the prism of the possibility of performing the basic functions of money.

The technical aspect of the functioning of cryptocurrencies – blockchain as a system innovation

In the IT and technical dimension, closely related to system security, the cognitive effort is focused on blockchain technology, the first implementation of which was made by S. Nakamoto. Bitcoin, like other cryptocurrencies, is based on the achievements of cryptography, including, in particular, Distributed Ledger Technology (DLT) (Piech, 2016; Olnes et al., 2017), by means of which is controlled and managed the trading of cryptocurrencies. Blockchain technology is to ensure the security and anonymity of trad-

[2] It is difficult to clearly estimate the number of people who participate in the world of cryptocurrencies. The socio-political characteristics are the subject of my research as part of the current project. The number of 34 million positive balance bitcoin wallets is only to a certain extent authoritative, since one user may have several wallets. This value, however, is only to illustrate to the reader how many cryptocurrency users in the world can be.

ing for its users. The simplified definition indicates that blockchain is an ever-expanding, secure, common maintain a register system in which each user keeps a copy of the data. The chain can only be updated if all parties involved in the transactions agree to it. The technical definition, in turn, prompts that blockchain is a distributed register operating in a peer to peer (P2P) network model, which is cryptographically secure, allows only adding data, is not modifiable and is updated only on the basis of consensus between its users (Bashir, 2017). To create an electronic payment system that would eliminate the need for an intermediary that would guarantee the correctness and security of financial transactions first-generation blockchains were used. Since Satoshi Nakamoto announced and implemented his idea, two more generations of blockchains have been created. Second-generation blockchain has found applications in economic, market and financial services that go beyond simple money transactions i.e. such as bonds, forward agreements, mortgage credit, title deeds, smart contracts. The emergence and development of the third generation blockchain means use other than economic, related to the use, for example, in the activities of state administration, health care, science (Swam, 2015).

The basis of the operation of cryptocurrencies is the mathematical hash function, i.e. the result of the action of the hash function. It is a function which to any large string of characters assigns any string of characters with a fixed size nonspecific value. In every case, it contains a fixed number of bits. The cryptographic hash function should additionally meet such properties as: be one-way, preimage resistance and the so-called “Collision” (Rodwald, 2013). Thanks to the above properties, computing the hash is an easy task and the opposite action is practically impossible. In the Bitcoin system uses the RIPEMD-160 and SHA-256 algorithms. RIPEMD in the blockchain is used to create Bitcoin addresses, and the SHA-256 algorithm is used to verify the computational effort generated by miners.

The hash function is also used to implement the second cryptographic tool, which is a digital signature. In the case of Bitcoin, he it adopts the Rivest Shamir Adleman (RSA) standard, which was one of the first implementations of a public key cryptography system. The history of public key cryptography dates back to the 1970s, when it was the mathematical basis of computer and information security. In the bitcoin world, asymmetric cryptography is used to generate a key pair public and a private. The public key is used to receive payments to the bitcoin wallet, and the private key is used to sign transactions and generate a “fingerprint” confirming possession of bitcoins. Public keys are in an open blockchain, so all users can access them. He it is generated from the private key due to the mathematical relationships between the key pair. When a transaction signed with a private key is sent out on the Bitcoin network, public keys are used by nodes to verify that the given transaction was actually signed with the appropriate private key. This process confirms ownership of bitcoins (Antonopoulos, 2014). Cryptocurrencies operate in a network with a peer-to-peer (P2P) architecture. It is a network made by users themselves who communicate directly with each other. The architecture model is based on the equivalence of all nodes. This means that, in contrast to the most widespread, classic client/server architecture, the this network does not include a control server like and centralized services. There is also no predetermined hierarchy and each user is part of the whole system. In practice, this means that it perform a function can act as a server as well as a client – download data from other machines and share its internal memory resources with all other computers (Schollmeier, 2001). When describing the IT aspect of the functioning of cryptocurrency systems, it is

often emphasized that they were designed as digital systems with a P2P architecture, which guarantees decentralization, which in turn makes the system resistant to failures, physical and IT attacks or collusion dishonest participants. The digital registry has been designed in such a way that the integrity of the data will be compromised when one entity or organization is able to obtain more than 50 percent of the computing power. Then a majority attack of 51% may occur, i.e. a situation where a group of system participants has the ability to change the blockchain record.

Although the nodes in the network are equal, depending on the functions they perform, they can have other roles such as: routing, service blockchain databases, mining and maintaining wallets. The most important element of Bitcoin’s infrastructure are miners, i.e. computers whose task is to: keep a blockchain register, verify transaction data updates and care their credibility. The main motivation for joining the system is the potential reward waiting for the miner, and theys themselves provide the computing power of their devices, necessary for the functioning of the network. When Bitcoin was started in 2009, the reward for generating a new block was 50 BTC. Every 210,000 blocks, this award is reduced by 50 percent. About 1,800 blocks are mined daily, and it takes an average of 10 minutes to generate one. In November 2012, the prize for mining the block dropped to 25 bitcoins, and in 2016 this amount was reduced from 25 to 12.5 bitcoins. Another reduction, i.e. halving, took place in May 2020 and from that moment on, the reward for generating a new block is 6.25 BTC. The mechanism of value change is permanently embedded in the system to regulate and control inflation and limit the supply of currency. Bitcoin’s operation is based on a system of blocks that are “mined” by miners. Mining is the process by which new blocks are added to the blockchain every day. The blocks contain transactions that are which are checked for correctness in mining process by nodes in the Bitcoin network. After generating and checking the blocks, they are added to the blockchain, thanks to which it is constantly growing. In practice, generating a new block consists in solving a cryptographic puzzle, which in the case of Bitcoin currently requires a large energy expenditure. Single computers are not able to generate enough computing power necessary to solve it. Hence, for mining specialized integrated circuits are used – Application-Specific Integrated Circuit (ASIC). The energy expenditure results from the need to calculate proof of work, where miners compete to finding a number that is smaller than the target set in the network. The difficulty in finding the right number serves to ensure that the appropriate resources are spent by miners before the new proposed block can be accepted. It also protects the system from fraud and attacks by double spending. Miners are rewarded with new bitcoins if they mine new blocks by obtaining a proof of work, which is used to ensure that the “miner” has done the required amount of work to find the new block. This process ensures decentralization, security and stability of the blockchain. Proof of work constitutes the so-called Nakamoto consensus, the achievement of which is the goal of miners involved in confirming transactions (Becker et al., 2013; Bentov et. al., 2014; Shi, 2016). Other algorithms that allow for reaching an agreement between network participants include: Proof of Stake, Delegated Proof-of-Stake, Proof of Importance, Proof of Activity, Proof of Elapsed Time (Dziambowski et. al., 2015; Li et. at., 2017). Reaching a consensus consists in carrying out a certain some kind of lottery for each new block and selecting a leader node that will be able to propose a new block designed to join the chain, and after this block has

been approved by other nodes, earn a win reward for adding this block. Proof of work is needed for obtain progress freeness. This means that the reward for sacrificing computing resources should be random and proportional to the miners’ contribution.

Legal aspect – cryptocurrencies as a virtual currency

With regard to cryptocurrencies, the following categories are used: virtual currency, digital currency, cyber currency, electronic currency or internet currency (Kirillova et al., 2018; Kochergin, 2017; Peters et al., 2015). Some authors take these terms as synonyms for the term cryptocurrency, which is a simplification and should not be practiced or reproduced. When considering the legal aspect, it is necessary to reflect on the essence of individual concepts, as well as to attempt to classify the issues and location and to compare cryptocurrencies in specifications to the category of money. The common feature of all the terms used above is their immaterial nature. The common element for these categories is the virtual space, without which their functioning would not be possible. Its meaning is to some extent explained by the virtual adjective (Latin virtualis), which is dictionary definition of: an object that does not exist physically, but by software. Therefore, it is created on a computer screen, but so realistic that it seems real (Dubisz, 2006).

The term “digital currency” is the broadest of the group indicated above and is often compared with the category of “electronic currency”. The simplest, descriptive, broad definition highlights its digital nature. Digital currency is created in the language of IT software and thanks to that it functions. Therefore, it is a digitally stored value that can be both a digital representation of the official means of payment and the virtual currency (Chuen, 2015). It constitutes a unified system of storing and transferring values (Tucker, 2009). Digital currencies is a concept different from electronic currencies, because it this last has a legal legal definition (Zacharzewski, Piech, 2017). In most cases, electronic currencies will mean: a monetary value stored electronically, including magnetically, issued, with the obligation to redeem it, for the purpose of making payment transactions, accepted by entities other than the issuer of electronic currency (Directive 2009/110/EC of the European Parliament and of the Council). The term electronic currency should be equated with the value recorded in a digitized form, which is a digital representation of a fiat currency. It is used to electronically transfer values. Electronic currency has an equivalent in the form of commonly used means of payment, has the status of legal tender and is accepted as a medium of exchange in the issuing country. While, digital currency will be anything that has a digitally recorded value, i.e. electronic currency and everything that isn’t him, and therefore has no monetary value, but is identified in virtual space. In the theoretical-cognitive dimension, it is worth considering what should be identified as digital currencies that is not electronic currency, because that is how cryptocurrencies should be classified? The collective category for this group is the already mentioned concept of virtual currency.

Determining one consistent definition of the term “virtual currency” is problematic due to the variety of systems based on them and the specific features of each of them. In many cases, the term “virtual” refers to a completely different state of affairs, which is caused by different interpretations of the vaguely defined term. In many cases, the term

“virtual” refers to a completely different state of affairs, which is caused by different interpretations of the vaguely defined term. Often the immateriality itself has been equated with a virtual creation one, hence the literature describes the term “virtual currency” as completely different types of non-cash money (see Ryfa, 2014). The first definitions referred to currencies functioning only in mass computer games, i.e. gaming money. They were then defined as: a means of payment not issued by any banking institution, being a unit of exchange between the issuer and a user or a group of users, playing the role of a universal equivalent in a given network, within strictly defined limits and mainly used to purchase virtual items (Chen, Wu, 2009). In such an approach, virtual currencies will be used to purchase virtual goods and services in a limited space, because they do not exist outside of it. Thus understood virtual currencies are not used to finalize transactions, the object of which is physical material goods, which limits the users themselves and makes them of little use on a global scale. In addition to gaming currency, in the first period of functioning of the concept, to the category of virtual currencies included, among others descriptions of point loyalty programs, air miles and gift cards (see pwc, 2014).

The development of the Internet and the ongoing process of digitization of finances implied the need to clarify the concept of virtual currency. The definition cited above excluded their use to purchase non-virtual goods outside the boundaries of a given virtual world. In 2012, the European Central Bank (ECB) determined that a virtual currency is a type of unregulated, digital money, issued and in principle controlled by creators, as well as used and accepted by users of a given community or virtual world (see European Central Bank, 2012). The term was specification three years later, when virtual currencies were defined as a digitally presented value that has not been issued by a central bank, credit institution or electronic money institution, which in some circumstances can be used as an alternative to money (see European Central Bank, 2015). In the same document, the ECB divides virtual currencies into three groups: closed virtual currency schemes, virtual currency schemes with unidirectional flow and virtual currency schemes with bidirectional flow. From the perspective of considering cryptocurrencies, it is worth paying attention to the last group of virtual currencies with two-way flow, which can be purchased with real money and exchanged for it. Therefore, they are used to purchase not only virtual, but also real goods and services (see European Central Bank, 2015).

The most extensive attempt to systematize and classify the concept of virtual currency two entities have made: Financial Action Task Force (FATF) and also European Banking Authority (EBA). In 2014, the FATF issued the *Virtual Currencies Key Definitions and Potential AML/CFT Risks* report, which indicates that the intensive development of virtual currencies creates the need for a definition that could be a starting point for national regulations. According to the FATF, a virtual currency is a digital equivalent of value that can be bought and sold in cyberspace, functioning as: a medium of exchange and/or a unit of account and/or a medium of hoarding, but not legally regulated (see 2014).

The proposed classification indicates two possibilities of dividing virtual currencies – convertible (open), corresponding to convertible currencies with two-way flow and non-convertible (closed), as well as centralized and decentralized, which include cryptocurrencies (see The Financial Action Task Force, 2014). The FATF definition was extended by the position of the European Banking Authority, which defines a virtual currency as a digital representation of value that can be transferred using IT technology and

used as a medium of exchange, unit of account or value storage medium, but it does not have the status of an official tender, i.e. its value it is not guaranteed by any government or the Central Bank, but may be regulated by the state (European Banking Authority, 2014). The issue of virtual currency was also raised on the European forum. The European Parliament, in its resolution of 26 May 2016 on virtual currencies, as a virtual currency recognized: digital cash, digital determinants of value that are not issued by a central bank or a public authority, are not linked to a fiat currency and are adopted by natural or legal persons as means of payment. As such, virtual currency can be transferred, stored or sold electronically (European Parliament resolution of 26 May 2016 on virtual currencies (2016/2007(INI)). In July 2016, the European Commission presented a draft amendment to Directive 2015/849 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing. In this draft, the Commission proposes extending the catalog of entities obliged to apply certain standards and procedures. In particular, it is about collecting information about transactions made and verifying users involved in these transactions. To the already existing list of entities they are to be added intermediaries in cryptocurrency trading, the so-called cryptocurrency exchanges and application providers (cryptocurrency wallets).

The economic aspect – cryptocurrencies and the functions of money

The last component of the model for analyzing the concept of cryptocurrencies is the economic aspect of their functioning. The key in this case is to find an answer to the question: *Can cryptocurrencies fulfill the functions of money and if so, to what extent?* In broad terms, money is all that is widely accepted as payment for goods and services, and also as a means of paying off debt (Mishkin, 2002). Therefore, one should agree with the thesis that defining money through the prism of its essence is wrong. Rather, one should focus on the functions it performs. Because it is the ability of a medium to act as money that depends on its ability to fulfill the basic functions of money. Consequently, the category of money includes means that fulfill his functions. Such thinking is characteristic of representatives of the Chicago school of economics. The most basic catalog is contained in three groups: money as a measure of value, money as a means of storing value, and money as a means of transferring value (Schaal, 1996). With the development of the commodity-money economy and the establishment of banks, another properties of money emerged. Two are attached to the above catalog: the resource hoarding function related to the storage of value and the weakest definition of the function of money as an international means of payment. It should be emphasized that the functions of money do not have a separate character, although some of them – the function of the measure of value and the medium of exchange, are prevail over the others. This means that they constitute a catalog of functions that constitute its meaning as exchange equivalents. The other two functions, i.e. the means of payment and the means of hoarding (the world money function is not included in this typology), are derivative from the former and are conditioned by them. In other words – if at a given time and place a specific measure is also a measure of value, a means of circulation, it should be considered as money. At the same time, this money has the potential to remain a means of hoarding and a means of payment. The basic functions of money

determined by the *sine qua non* attributes of money, and derivatives can also be realized by something other than money. However, this does not mean that they will also be a measure of value and a means of circulation. Thus, the essence of money is to measure value and to be a means of circulation (Zadora, 2015).

The first of the catalog of the function of money – a measure of value, allows expressing the value of a specific good. Thus, money becomes a unit of account in which prices are determined and settlements are made. In the function of money as a measure of value, it is essential to maintain its purchasing power, defined by the quantity of goods that can be purchased per unit of money. Expressing value in specific units gives you an opportunity to compare prices, as well as products and services with different characteristics and applications. Cryptocurrencies thus understood *explicate* fulfill the function in a broad sense. With their help, prices can be expressed and thus specific goods can be compared. However, this is only an apparent feature of cryptocurrencies. It should be noted that the value of individual bitcoins is determined not by their purchasing power, but by the rate against traditional currencies. Therefore, cryptocurrencies do not have value in themselves, and entities that make payments, e.g. in bitcoins, although they settle in cryptocurrency, it is done at the current exchange rate. Cryptocurrencies can therefore act as a measure of value only indirectly, as the traditional currency is always the benchmark. The function of the measure of value is then performed in a defective manner and different from traditional forms of money. Cryptocurrencies do not have purchasing power, they are characterized by large fluctuations in exchange rates, and the lack of stability makes it difficult to obtain information benefit from using to them as a measure of value.

The second of the basic functions – the medium of exchange, is related to the universal equivalence of means of payment and comes down to the role of an intermediary in exchange, a participant in the purchase and sale transaction. It also assumes *ex ante* that a given measure also functions as a measure of value and as a resource hoarding measure. In the case of cryptocurrencies, the level of social acceptance is the key when analyzing the possibility of fulfilling the intermediary function. It is a *sine qua non* condition for a given good to fulfill this function, because, as indicated above, universal acceptability is the starting point and the necessary *minimum*. According to coinmap.org, there are 19,300 places in the world where you can pay your liabilities with cryptocurrencies, most often bitcoin (see www.coinmap.org). While this figure is significant from a user perspective, it is a negligible percentage across society as a whole. Hence, it is difficult to confirm the thesis that cryptocurrencies outside of small social groups are generally acceptable. Nevertheless, the number of exchange sites is constantly growing, and as cryptocurrencies become more and more common, the possibility of their widespread use will increase (Beedham, 2020). The performance of the function of a medium of exchange depends, therefore, on the level of acceptance of a given payment equivalent in society. So far, therefore, the potential for application in this range is small, although it can be assumed that the ratio may change in the following years.

Due to its deflation properties, bitcoin, like most cryptocurrencies that have a limited number of coins, could be a very good means of storing value. The hoarding function is the accumulation of certain assets excluding them from economic circulation. It developed based on the value-measure function. The limited supply, due to the pre-programmed number of units, undoubtedly has a significant impact supporting the

strengthening of the scarcity feature, which, in line with market mechanisms, helps cryptocurrencies fulfill their hoarding function. However, cryptocurrencies do not have the capacity to store or transfer value because they have no value in themselves. Although the above “allegation” can also be attributed to fiat currency since August 1971, when Richard Nixon suspended the so-called the Bretton Woods agreement, to falsify the thesis that cryptocurrencies can perform the hoarding function, other arguments can also be cited. The first argument is related to the fluctuation of the exchange rates of cryptocurrencies in relation to fiat currencies, making it impossible to maintain a stable value of savings. Additionally, money performs a hoarding function only when its value does not change in relation to the price level. Second, money performs a hoarding function when its buyers trust that it stores value. The possibility of maintaining a constant purchasing power by a cryptocurrency has been contested many times, hence the fulfillment of the hoarding function by bitcoin or another coin is not possible at the moment.

The last function of money derivative, which was added to the above catalog at the latest, is the perception of money as a means of payment. This function of money is fulfilled when the sale of goods and services is separated in time from the transfer of the value of money. The function of the measure of payment of obligations is an extension of the function of the medium of exchange, although in this case money is a measure of payment of obligations. As in the case of the analysis of the cryptocurrency hoarding function, also in this case we are dealing with a kind of dualism. From a legal perspective, it is difficult to recognize that cryptocurrencies can be used as a means of payment, as their legal status still remains unregulated. It implies problems related to, for example, the lack of acceptance of the authorities in the use of cryptocurrencies to regulate basic obligations imposed by the state institution. On the other hand, the functionality of bitcoin and other coins should be pointed out, which makes it ideal for global transfers. Due to the relatively low cost and speed of the transaction compared to the transfer of traditional funds, it seems to be an ideal solution for this type of financial operations. This functionality is not even limited by large exchange rate fluctuations, because its usefulness is the same for each course.

Summary and conclusions

Cryptocurrencies are a global, supra-state characters product. The blockchain concept made digital records sparse and countable, and thus made them a representatives of value in the digital dimension. The technological solutions proposed in the Nakamoto Manifesto were known before in the field of cryptography. The implementation of individual solutions made it possible to solve two problems that the predecessors of the creators of bitcoin did not cope with – the problem of double-spending and Byzantine fault tolerance. The combination of asymmetric cryptography with other cryptographic solutions made it possible to create a safe, transparent, or relatively anonymous value exchange system, which is more and more common. A decentralized blockchain is a public distributed database that stores a record of digital transactions. The emergence and development of cryptocurrencies carries certain problems that should be identified when an attempt is made to conceptualize the concept. The first, basic, primary in relation to

the others, is to which category should they be assigned in the traditional classification of means of payment? Technological development, digitization of forms of means of exchange, resulted in the creation and development of the concept of “virtual currency” in the legal sociolect. This is how objects that fall into the category of digital money are defined, with the proviso that they are not electronic moneys. According to the above definitions, digital representation of value that can be transferred using IT technology and used as a medium of exchange without the status of official means of payment.

The reconstructed framework of the concept analysis indicates that for a broad approach to the problem, it is necessary to reflect on the economic aspect of the functioning of cryptocurrencies, which can be perceived as a kind of digital resource that functions as a currency based on cryptographic systems. This system may be similar to online banking, but it does not have a central authority to manage it. The means of payment created within the virtual community enables the exchange of goods and services. The means of exchange, from their most primitive form, have specific functions that make them universal and socially acceptable. Their evolution and their multiplication indicate that with the ongoing change, they also evolve. The comparison of these classic, known in economic theories with cryptocurrencies, indicates that so far he cannot implement them to the full extent. Nevertheless, it should be pointed out that in certain circumstances they can be used as a medium of exchange and a means of payment. Cryptocurrencies prove to be a defective measure of value, while a significant imperfection of bitcoin is its inability to treat it as a means of collecting or storing value. An important drawback that prevents them from being fully realized, despite the fact that cryptocurrencies have some features of money, e.g. portability, divisibility, is that they are not universal, and therefore not fully recognizable.

Based on the aspects distinguished and characterized above, based on the designed model of analysis, the author proposes to define cryptocurrencies as **decentralized register, operating in a network with a peer-to-peer architecture, cryptographically secured, based on trust and consensus, a type of virtual currency, incompletely fulfilling some functions of money**. This is the so-called broad definition, constructed on the basis of three dimensions. Narrowing the issues around only one of the areas of knowledge, i.e. referring to one aspect will constitute a narrow approach, focused only on the legal, economic or technical area of cryptocurrency functioning.

Bibliography

Antonopoulos A. M. (2014), *Mastering Bitcoin: unlocking digital cryptocurrencies*, “O’Reilly Media, Inc.”, Beijing–Cambridge.

Bashir I. (2017), *Mastering blockchain*, Packt Publishing Ltd., Birmingham

Becker J., Breuker D., Heide T., Holler J., Rauer H. P., Böhme R., (2013), *Can we afford integrity by proof-of-work? Scenarios inspired by the Bitcoin currency*, in: *The economics of information security and privacy*, pp. 135–156.

Beedham M. (2020), *People are obsessed with buing coffee with cryptocurrency – here’s why*, April 17, https://thenextweb.com/hardfork/2019/01/31/buying-coffee-bitcoin-cryptocurrency/.

Bentov I., Lee C., Mizrahi A., Rosenfeld M. (2014), *Proof of activity: Extending bitcoin’s proof of work via proof of stake [extended abstract] y*, “ACM SIGMETRICS Performance Evaluation Review”, 42(3), pp. 34–37.

Chaum D. (1983), *Blind signatures for untraceable payment*, “Advances in cryptology”, Springer MA, Boston, pp. 199–203.

Chaum D. (1985), *Security without identification: Transaction systems to make big brother obsolete*, “Communications of the ACM”, 28(10), pp. 1030–1044.

Chen L., Wu H. (2009), *The Influence of Virtual Money to Real Currency: A Case-based Study*, International Symposium on Information Engineer – ing and Electronic Commerce, Beijing University of Posts and Telecommunications.

Dai W. (1998), *B-money*, http://www.weidai.com/bmoney.txt.

Dubisz S. (ed.) (2006), *Uniwersalny słownik język polskiego PWN* [*The universal dictionary of the Polish language PWN*], vol. 4, Państwowe Wydawnictwo Naukowe, Warsaw.

Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC.

Dziembowski S., Faust S., Kolmogorov V., Pietrzak K. (2015), *August. Proofs of space*, in: “Annual Cryptology Conference” (pp. 585–605), Springer, Berlin–Heidelberg.

European Banking Authority (2014), *EBA Opinion on virtualcurrencies*, July 4, http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014 08+Opinion+on+Virtual+Currencies.pdf.

European Central Bank (2012), *Virtual Currency Schemes*, Frankfurt am Main.

European Central Bank (2015), *Virtual Currency Schemes – A futher analysis*, Frankfurt am Main.

European Parliament resolution of 26 May 2016 on virtual currencies (2016/2007(INI)), 26 May 2016– Brussels, https://www.europarl.europa.eu/doceo/document/TA-8-2016-0228_EN.html.

Houben R., Snyers A. (2018), *Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion*, European Parliament.

Kirillova E., Pavlyuk A. V., Mikhaylova I. A., Zulfugarzade T. E., Zenin S. S. (2018), *Bitcoin, lifecoin, namecoin: The legal nature of virtual currency*, “Journal of Advanced Research in Law and Economics”, 9(1 (31)), pp. 119–126.

Kochergin D. A. (2017), *The roles of virtual currencies in the modern payment system*, “St.Petersburg University Journal of Economic Studies” 33(1), pp. 119–140.

Lee Kuo Chien D. (ed.) (2015), *Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data*, Elsevier Academic Press.

Li W., Andreina S., Bohli J. M., Karame G. (2017), *Securing proof-of-stake blockchain protocols*, in: *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, Springer, Cham, pp. 297–315.

Mishkin F. S. (2002), *Ekonomia pieniądza, bankowości i rynków finansowych* [*Economics of money, banking and financial markets*], tran. A. Mincewicz, Wydawnictwo Naukowe PWN, Warsaw.

Nakamoto S. (2008), *Bitcoin: A peer-to-peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf.

Olnes S., Ubacht J., Janssen M. (2017), *Blockchain in government: Benefits and implications of distributed ledger technology for information sharing*, “Gov. Inf. Q.” 34: pp. 355–364.

Peters G., Panayi E., Chapelle A. (2015), *Trends in cryptocurrencies and blockchain technologies: A monetary theory and regulation perspective*, “Journal of Financial Perspectives” 3(3), arXiv preprint arXiv: 1508.04364.

Piech K. (2016) *Leksykon pojęć na temat technologii blockchain i kryptowalut* [*A lexicon of concepts on blockchain technology and cryptocurrencies*], Ministerstwo Cyfryzacji, Warsaw.

Pwc. (2014), *Virtual currencies: Out of the deep web, into the light*.

Redman J. (2020), *Wikileaks Gathers $37M in BTC Since 2010 – Over $400K Sent After Julian Assange’s Arrest*, February 25, https://news.bitcoin.com/wikileaks-gathers-37m-in-btc-since-2010-over-400k-sent-after-julian-assanges-arrest/.

Rodwald P. (2013), *Kryptograficzna funkcja skrótu* [*Cryptographic hash function*], “Zeszyt Naukowy Akademii Marynarki Wojennej” LIV nr 2 (193), pp. 91–102.

Ryfa J. (2014), *Waluty wirtualne – problem zdefiniowania i klasyfikacji nowego środka płatniczego* [*Virtual currencies – the problem of defining and classifying a new means of payment*], “Nauka o finansach – Financial Sciences” 2(19), pp. 138–147.

Schaal P. (1996), *Pieniądz i polityka pieniężna* [*Money and monetary policy*], tran. M. Rusiński, Państwowe Wydawnictwo Ekonomiczne, Warsaw.

Schollmeier R. (2001), *A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications*, “Proceedings First International Conference on Peer-to-Peer Computing”, pp. 101–102.

Shi N. (2016), *A new proof-of-work mechanism for bitcoin*, “Financial Innovation”, 2(1), p. 31.

Swam M. (2015), *Blockchain: Blueprint for a New Economy*, “O’Reilly Media, Inc.” Newton MA.

Szabo N. (1997), *The God Protocols*, https://nakamotoinstitute.org/the-god-protocols/.

The Financial Action Task Force (2014), *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, FATF/OECD.

Tucker P. C. (2009), *The digital currency doppelganger: Regulatory challenge or harbinger of the new economy*, “Cardozo J. Int’l & Comp. L.”, 17, p. 589.

Zacharzewski K., Piech K. (eds.) (2017), *Program „od papierowej do cyfrowej Polski” Strumień „Blockchain i kryptowaluty” – przegląd polskiego prawa w kontekście zastosowań technologii rozproszonych rejestrów oraz walut cyfrowych* [*Program „From paper to digital Poland” Stream „Blockchain and cryptocurrencies” – review of Polish law in the context of the application of distributed ledger technology and digital currencies*], https://www.gov.pl/documents/31305/52168/przeglad_polskiego_prawa_w_kontekscie_zastosowan_technologii_rozproszonych_rejestrow_oraz_walut_cyfrowych.pdf/f6e74ce0-09e5-776d-bd3b-c21fca96cce2.

Zadora H. (2015), *Podstawowe kategorie finansowe* [*Basic financial categories*], in: *Finanse: kategorie, zjawiska i procesy, podmioty*, eds. H. Zadora et. al., Publishing House “Difin”, Warsaw, pp. 39–59.

Nauki społeczne wobec powstania i rozwoju kryptowalut: analiza pojęcia

Streszczenie

Celem artykułu jest konceptualizacja, to znaczy wyjaśnienie, analiza znaczenia i wskazanie ram interpretacji pojęcia „kryptowaluty” na gruncie nauk społecznych, w tym politologii. Jako zagadnienie interdyscyplinarne, polisemiczne, a zarazem *novum* technologiczne, kryptowaluty stanowią wyzwanie dla przedstawicieli świata nauki. Zaproponowany heurystyczny model analizy pojęcia oparty o aspekt technologiczny, prawny oraz ekonomiczny wskazuje, że w szerokim ujęciu kryptowalut należy rozumieć jako: zdecentralizowany, funkcjonujący w sieci o architekturze peer-to-peer, zabezpieczony kryptograficznie, oparty na zaufaniu i konsensusie, typ waluty wirtualnej, spełniający w sposób niepełny niektóre funkcje pieniądza. Wyjaśnienie treści poprzez jeden z aspektów funkcjonowania kryptowalut stanowi jego zawężenie.

Słowa kluczowe: kryptowaluty, Satoshi Nakamoto, łańcuch bloków, rewolucja technologiczna, instrumenty finansowe

Article submitted: 06.05.2021; article accepted: 21.06.2021
Data przekazania tekstu: 06.05.2021; data zaakceptowania tekstu: 21.06.2021