UDC:

DOI: 10.5937/AnEkSub2300026T

Original scientific article

Анали Економског факултета у Суботици – The Annals of the Faculty of Economics in Subotica
Vol. XX, No. XX, pp. XX-XXX
Received: 12/06/2023
Accepted: 01/08/2023
Published online: 11/08/2023

Online First

Oligopoly structure in the cryptocurrency market

Олигополска структура на тржишту криптовалута

Nenad Tomić
Faculty of Economics, University of Kragujevac, Kragujevac, Republic of, Serbia, ntomic@kg.ac.rs,
https://orcid.org/0000-0003-1565-3197

Abstract: Blockchain technology has been announced as the driving force behind the democratization of digital business. Various interest groups believed that cryptocurrencies would enable fast, cheap and anonymous payments over the Internet. The absence of a central institution and the possibility of the participation of the wider community in the maintenance of the system should have created electronic money adapted to individuals, not the financial elite. However, the question arises whether cryptocurrencies really provide equal opportunities for all participants. The subject of the paper is the degree of centralization of the most famous cryptocurrency systems in terms of wealth distribution and the possibility of participation in their maintenance. The goal of the paper is to determine the degree of inequality in various aspects of the functioning of the cryptocurrency system. The results of the analysis indicate that cryptocurrencies function separately from the traditional financial system, but do not enable the financial inclusion of marginalized social groups. No current cryptocurrency community provides equality of participants, neither in terms of mining, nor in terms of wealth distribution. It can be concluded that the mining of cryptocurrencies and their secondary circulation show clear characteristics of oligopolistic structures.
Keywords: oligopoly, cryptocurrencies, mining pools, financial inclusion, market restrictions
JEL classification: D43, G32, O16

Сажетак: Блокчејн технологија је најављена као покретачка снага демократизације дигиталног пословања. Различите интересне групе су сматрале да ће криптовалуте омогућити брза, јефтина и анонимна плаћања путем интернета. Одсуство централне институције и могућност учешћа шире заједнице у одржавању система требало је да од криптовалута створи електронски новац прилагођен појединцима, а не финансијској елити. Међутим, поставља се питање да ли криптовалуте заиста пружају једнаке шансе за све учеснике. Предмет рада је степен централизације најпознатијих система криптовалута у погледу расподеле богатства и могућности учешћа у њиховом раду. Циљ рада је утврђивање степена неравноправности у различитим аспектима функционисања система криптовалуте. Резултати анализе указују да криптовалуте функционишу одвојено од традиционалног финансијског система, али не омогућавају финансијску инклузију маргинализованих друштвених група. Ни једна актуелна криптовалутна заједница не омогућава равноправност учесника, ни у погледу рударења, ни у погледу расподеле богатства. Може се закључити да рударење криптовалута и њихов секундарни промет показују јасне одлике олигополских структура.
Кључне речи: олигопол, криптовалуте, рударски пулови, финансијска инклузија, тржишна ограничења
ЈЕЛ класификација: D43, G32, O16

Introduction

Blockchain technology has been announced as the driving force behind the democratization of digital business (Chen, 2018). Its meaning is reflected in the decentralized management of large databases. Data entry is performed with the application of consensus protocols, which provide a chance for the inclusion of a large number of interested individuals and prevent the arbitrariness of malicious individuals and groups. Achieving a consensus on changing the state of the system involves voting by members. Thanks to the mentioned positive characteristics, blockchain is seen as a technological basis for the further evolution of electronic money, but also the development of contract applications, applications in healthcare, transport, political decision-making and for device communication in the Internet of Things.

Cryptocurrencies represent the first and best-known aspect of the application of blockchain technology. Since the emergence of Bitcoin in early 2009, interest in cryptocurrency business has been steadily growing. The high volatility of the most famous cryptocurrencies makes them unsuitable to be units of account and for storing value (Ammous, 2018). However, the number of cryptocurrencies and the number of market participants are increasing every year. From the very beginning, it was believed that cryptocurrencies would enable fast, cheap and anonymous payments over the Internet. Speculative investors have found in cryptocurrencies unregulated investment instruments, which can bring high returns on investments in a short period of time. The absence of a central institution and the possibility of wider community participation in maintaining the system should have created conditions adapted to individuals, not the financial elite.

The real question is whether cryptocurrencies really provide equal opportunities for all participants. In the literature, there are claims of pronounced inequality in the cryptocurrency community in terms of wealth distribution and access to the mining process (Cong, He & Li, 2019; Vaz & Brown, 2020). That is why the subject of the paper is the centralization of the most famous cryptocurrency systems in terms of wealth distribution and the possibility of participation in their maintenance. The goal of the paper is to determine the degree of inequality in various aspects of the functioning of the cryptocurrency system.

The paper is structured in three parts. In the first part, it will be explained how cryptocurrencies were supposed to contribute to the democratization of the financial system. In the second part, contradictions in the proclaimed goals and the technical design of the consensus protocol will be pointed out. The third part will bring conclusions about the forms of concentration in the cryptocurrency market, drawn on the basis of certain indicators.

1. Characteristics of cryptocurrencies

Electronic money was first mentioned in the work of Chaum (1983), who pointed out the absence of privacy in transactions with payment cards. He proposed the development of

ONLINE FIRST

electronic money based on a blind signature, which allows authentication and prevents double spending, but does not provide the ability to identify the payer. In further papers, it was proposed that the medium for the development of electronic money should be prepaid cards. With the commercial use of the Internet, attention is focused on the possibility of developing server-based electronic money. Theoretical considerations agreed that electronic money, regardless of the medium used for its disposal, should be as close as possible to cash in terms of its characteristics. Okamoto & Ohta (1991) defined the key features that electronic money must have in order to be acceptable for use, with anonymity and user security being considered the most important. Matonis (1995) supplemented the list, introducing the reduction of state influence as a necessary characteristic. The meaning of this feature is reflected in the possibility of electronic money being guided by market criteria, rather than the political ones. Despite the great efforts invested in the development of the electronic money system, not a single operational solution has attracted enough users. At the beginning of the XXI century, representatives of the first generation of electronic money lost the fight with electronic payment systems based on the existing payment infrastructure, such as Paypal.

Cryptocurrencies are a new class of electronic money, based on blockchain technology (Nakamoto, 2008). Bitcoin, as their first representative, offered an innovative concept of electronic money that does not have a central issuing institution. This money is automatically issued at a predetermined rate, which halves every four years. Newly created cryptocoins can be earned by community members, who help in maintaining the system. They use their computers to solve a complex calculation problem, which will enable the confirmation of transactions made in the previous period and prove that it is not a double spending of funds (Lee & Chuen, 2016, p. 19). The user who finds the solution first offers it to the other participants in the network for confirmation. If the solution turns out to be correct, the user gets a reward in the form of newly created cryptocoins. Confirmed transactions are then packed into memory units called blocks, which are linked to each other, creating a chain of blocks. That algorithmic process is called "mining" in cryptocurrency jargon, and the individuals who participate in it are "miners."

The fact that it is possible to earn money by engaging available computing resources in compliance with the rules has attracted a large number of technology enthusiasts. Contrary to expectations, after the first two years of stagnation, the value of Bitcoin began to rise, and a secondary market was created. Investors who are not engaged in mining but only in buying and selling Bitcoin on specialized exchanges, have appeared. Parallel to this process, other cryptocurrencies were emerging. A cryptocurrency community was created, which had both breadth and depth of offerings.

One should bear in mind that Bitcoin and other cryptocurrencies fulfilled two key expectations, defined in the nineties of the XX century. First, payments made with Bitcoin are pseudo-anonymous, in the sense that the individual making them cannot be personally identified. Since Bitcoin is stored in an electronic account that is unique to each user, payments can be tracked in terms of payer and payee account numbers, but it is not possible to link individuals to observed accounts beyond any doubt. Second, neither Bitcoin nor any other cryptocurrency is subject to government regulation in terms of supply control,

restrictions on disposition and use, or user tracking. Each cryptocurrency has its own payment infrastructure, which functions on a user-to-user basis, without the need for the participation of the state or financial intermediaries. In developing countries, a large number of adults who have access to mobile telephony and/or the Internet do not have the opportunity to use the services of financial institutions. Certainly, such persons also exist in developed countries, within marginalized groups. It is estimated that there are approximately 1.7 billion people in the world with access to the Internet and no access to financial services (Demirgüç-Kunt et al. 2018). Therefore, cryptocurrencies theoretically enable the financial inclusion of a large number of such individuals. In the literature, claims can be found that cryptocurrencies could also affect the reduction in the inequality of income distribution (Kamau, 2022). With this in mind, optimistic expectations have been created that cryptocurrencies will set the financial system free from state control and corporate aggressiveness.

In practice, the traditional financial system and the cryptocurrency community had no meeting points. Commercial banks have not started using cryptocurrencies in their business, investment banks and investment funds have only been marginally interested in including them in their portfolio. Many countries have also issued official warnings to institutions and citizens not to use cryptocurrencies, as they are unregulated and may expose them to the loss of funds. Therefore, the cryptocurrency community, although constantly growing, was formed practically separately from all traditional financial flows (Baker, 2022). As previously emphasized, cryptocurrencies do not fulfil any of the basic functions of money due to their volatility. Therefore, the expectation that cryptocurrencies will enable fast, cheap and anonymous payments over the Internet has not been fulfilled. Instead, a community of technology experts for mining and speculative investors was formed. The nature of the parties involved and the relationships within the community led to the rapid abandonment of the idea of democracy and free competition and the emergence of oligopolistic structures.

2. Restrictions on free competition in the mining process

Depending on access control and the availability of roles in the system, blockchain technology can be operationalized in one of two ways. For the development of cryptocurrencies, the public blockchain is most often used, that is, a blockchain where permission is not required to perform a certain role. Any stakeholder that meets the technical criteria can become a miner (Lin & Liao, 2017). Also, any interested individual can buy cryptocurrency from an online exchange and use it to send money. For the development of blockchain-based business applications, a private blockchain is most often used, that is, a blockchain that requires permission to participate. Such systems are accessed on the basis of invitations and it is known in advance which of the members can play the role of a miner, and who can only perform transactions. A permission-based blockchain is not applicable to cryptocurrencies, as it limits the number of potential users. However, some modifications are in use, in which the role of the miner is predetermined, while the

roles of payer and payee can be taken by anyone. Such are blockchains of cryptocurrencies Ripple, Stellar and NEM.

After choosing the type of blockchain, the choice of consensus protocol is crucial. These are mechanisms that automate the decision-making process in an environment where there is no mutual trust between the participants (Lamport, 1978). Confirmation of performed transactions is done on the basis of a consensus protocol. Due to the freedom of access and the unlimited number of members, miners cannot be sure whether there are malicious individuals or groups among them, who want to abuse the transaction confirmation process. That is why the mentioned mechanisms must be resistant to system crash errors and to the so-called Byzantine errors, where malicious individuals intentionally send false messages to cause confusion. The economic results achieved by the miners depend on the chosen consensus protocol.

The problem is that consensus protocols in public blockchains are competitive. A miner who wins or earns the right to mine the next block receives financial compensation for the work done. The compensation itself can be in the form of a commission charged for transactions included into the block, in the form of newly created cryptocoins, or in a combination of the two mentioned forms. In each of the above cases, there is a pronounced competition among miners to win the right to mine a block. With some protocols, competition occurs on a technical basis, because there is a criterion regarding the computer resources used for mining. In others, the competition is of a purely financial nature, as it is necessary to invest funds in a specific cryptocurrency in order to acquire the right to mine.

Bitcoin and the majority of other current cryptocurrencies, such as Ether, Monero, ZCash and others, use the proof-of-work (PoW) protocol. With this protocol, each miner generates a block of executed transactions, while solving a complicated mathematical problem of the reverse hash function. Namely, the hash value of the entire record of the block and an arbitrarily added number called nonce should have some given value (for example, start with the string 0000). To get the given value, the miner changes only the nonce, because small changes in the contents of the block lead to a large change in the hash value. Finding a solution is very computationally intensive, as it requires a huge number of calculations based on trials and failures. In contrast, checking the accuracy of the results is trivial (Narayanan et al. 2016, pp. 104-105).

Mining has become a very lucrative business since the rise in the price of Bitcoin in 2012. Since the graphics card in modern computer systems (graphical processing unit - GPU) is more capable of performing a large number of calculations in a unit of time than the processor, miners began to equip their computers with the most expensive models, creating market disturbances (Osbourne, 2018; Warren, 2018). One began with the assembly of special computer machines intended exclusively for mining, which can perform a greater number of calculations per second and thus increase the chances of mining a block. Also, miners started to join together in the so-called mining pools, which access mining together and share the obtained reward. Although PoW promised an equal chance for all participants, soon all miners who could not follow the race in technical equipment had to withdraw.

ОДЛОМЕНИ ДЕО

PoW creates huge costs for miners in terms of acquisition of technical equipment and electricity consumption. There are many academic papers on the topic of the economic unsustainability of the PoW protocol (de Vries, 2018; Todorović & Tomić, 2019). The pronounced cost component additionally contributes to the centralization of the mining process. Another protocol that creates competition on a technical basis is proof-of-capacity (PoC). Although it is not as computationally intensive as PoW, and therefore does not lead to high electricity consumption, PoC gives advantage to miners who have more available space on their hard disks. Thus, protocols that create competition on a technical basis require high initial investments in equipment, in order for miners to even engage in generating blocks.

Another large group of protocols requires initial investments in the chosen cryptocurrency before engaging in mining. The most popular among them is proof-of-stake (PoS), which is implemented in Peercoin and Cardano cryptocurrencies. Roughly speaking, each miner's stake is calculated, which depends on the amount of cryptocoins he owns and the length of time he holds them. The miner with the highest stake score gets the right to mine the block. After generating the block, the miner moves to the back of the list, and the next highest stake score assumes the role of a miner. However, not all users get their turn in this way, because when calculating, the length of tenure has an upper limit. Therefore, the PoS protocol favors rich miners. Although there are a large number of protocols (proof-of-importance - POI, proof-of-believability - PoBe) that modify the basic premises of PoS by introducing additional criteria for the selection of miners, practically all of them still favor rich miners (Tomić, Todorović & Jakšić, 2021, p. 372). An extreme example is the proof-of-burn protocol (PoB) where miners must first purchase some amount of a cryptocurrency and then send it to an irretrievable address (so that it is irrevocably alienated) in order to qualify for the selection. The problem is that each investment of this type is valid only for a certain period of time, after which the investment score is deleted. So not only does a miner have to invest a lot of money to be selected to mine a block, but he needs to do it continuously.

Although there was a promise that the blockchain would allow all interested parties to get involved in the maintenance and control of the system and earn money from it, this has not been achieved in practice. All public blockchain consensus protocols favor wealthy participants. With private blockchains, the roles are already predetermined, so ordinary users have no access. It can be concluded that regardless of the approach in the operationalization of the blockchain, there is no free competition for the role of the miner. The structure is oligopolistic, where the rich participants are in a situation to secure a privileged position in advance, or to buy it afterwards.

3. Formation of oligopolistic structures

Bitcoin is designed so that its supply increases over time, with miners receiving new cryptocoins as a reward. A small number of miners at the very beginning contributed to a large concentration of Bitcoins in the possession of the system's creators. The above applies to all cryptocurrencies that function according to the same principle. With the increase in

the number of miners and the creation of a secondary market, the number of Bitcoin owners has grown exponentially. This necessarily led to a dispersion of ownership and thus a reduction in inequality in the cryptocurrency community. However, the question arises as to how quickly inequality has decreased. At the end of 2013, after almost a full five years of operation, the 927 richest accounts contained more Bitcoins than all the rest (about a million at that time), which indicates a too slow reduction of centralization (Wile, 2013).

Several authors have tried to determine the centralization of the market through the comparative calculation of the GINI coefficient for the largest cryptocurrencies. The first comprehensive analysis was performed by Srinivasan & Lee (2017), which presented a cross-section of the state of the Bitcoin and Ether markets in July 2017. The authors emphasized that analyzing only the centralization of ownership is not enough, so they calculated GINI coefficients according to 6 parameters: centralization of miners who generate blocks, centralization of software used to manage cryptocurrencies (from the perspective of users and from the perspective of developers), centralization of cryptocurrency exchanges, centralization of users according to the countries of the world and the centralization of ownership. The results of their research are presented in Table 1.

Table 1: GINI coefficient for Bitcoin and Ether according to the given parameters

Parameters	Bitcoin	Ether
Mining	0.4	0.82
Software	0.915	0.92
Developers	0.79	0.91
Exchanges	0.83	0.85
Users' country of origin	0.84	0.85
Ownership	0.65	0.76

Source: Srinivasan & Lee (2017)

Based on the obtained results, it can be concluded that the Ether market is more centralized than the Bitcoin market according to all observed parameters. The conclusion supports the claim that the lower the market capitalization of a cryptocurrency, the more centralized its community is (Sedgwick, 2018). The drastic differences in the above analysis are manifested in terms of the miners who generate the block - while this segment is extremely centralized with Ether, Bitcoin shows a more even distribution of rewards. Such a result may be somewhat of a surprise, considering that at the time of analysis, both cryptocurrencies used the PoW algorithm. However, to fully understand the degree of centralization of the Bitcoin mining system, it is necessary to take into account the mining pools, which will be discussed later.

The key parameter in this analysis is the distribution of wealth, i.e. the dispersion of ownership. The balances on individual accounts were analyzed, because it is not possible to connect individuals with accounts, and therefore not to determine whether one individual actually possess funds on several accounts. Bitcoin's score of 0.65, although very high, is not as bad as expected and is comparable to the centralization of wealth in countries like Australia and El Salvador during the same period (Ventura, 2018). With a score of 0.76, Ether showed comparability with countries like Jordan and Panama. However, the above

results actually hide the true dimension of inequality in cryptocurrency communities. In order to exclude accounts with negligible amounts of cryptocurrencies, the authors set minimum amounts for both cryptocurrencies. Although this move made sense when it comes to low amounts on unused accounts, the authors set the minimum amounts unreasonably high at 185 Bitcoins, i.e. 2477 Ether. The market value of the set limits at the time was actually US$500,000. In other words, the GINI coefficient in terms of ownership is calculated only for the wealthy participants, who are called "whales" in the jargon, because of their size and influence in the market (Redman, 2020). Thus, both cryptocurrencies show extremely high inequality in the distribution of wealth even when looking only at wealthy participants. The authors admitted that including all individual accounts holding any amount of cryptocurrency would result in GINI coefficients of over 0.99 for both cryptocurrencies considered, which is unmatched by any country.

Suberg (2019) performed a wealth distribution analysis for Bitcoin, Ether, Bitcoin Cash and Litecoin. In doing so, he compares the GINI coefficients for 2018 and 2019, the percentage of each cryptocurrency held by the richest account and the top ten accounts, as well as the minimum number of miners needed to take majority control of the mining process. The results are presented in Table 2. They show that there was an increase in ownership concentration in 2019 for all observed cryptocurrencies, except for Bitcoin. Also, it has been confirmed that cryptocurrencies with lower market capitalization exhibit more pronounced inequalities and lower security. However, the author did not state whether he used any criteria when including accounts in the analysis of the GINI coefficient, although from the obtained values it can be concluded that he did.

Table 2: GINI coefficient for Bitcoin, Ether, Bitcoin Cash and Litecoin on given parameters

Parameters	Bitcoin	Ether	Bitcoin cash	Litecoin
Market capitalization in USD on 31.12.2019.	130.4 billion	14.1 billion	3.7 billion	2.6 billion
GINI 2018	0.66	0.69	0.73	0.83
GINI 2019	0.64	0.78	0.75	0.83
The percentage of wealth held by the richest account	0.62%	1.96%	2.79%	2.58%
Share of wealth held by the 10 richest accounts	3.84	7.27%	9.38%	10.36%
The number of users required to take over the network	4545	322	1109	189

Source: Suberg (2019)

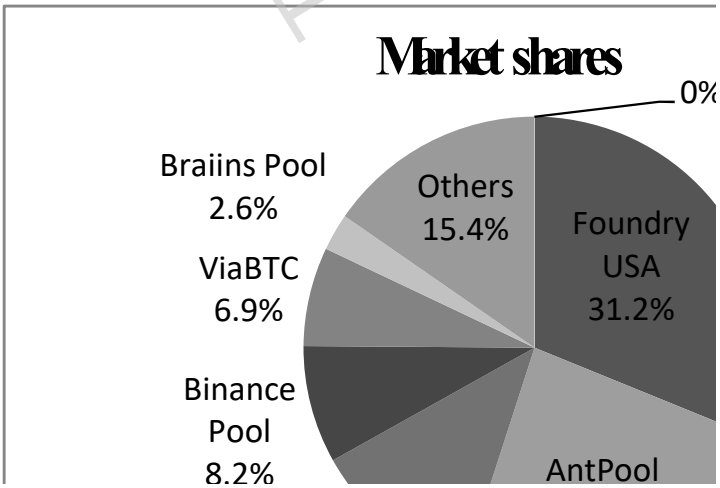
The last row of the table shows the minimum number of miners needed to achieve control over 51% of the mining power. With the mutual cooperation of the specified number of miners, transactions that did not actually happen can be written into the block, because the rest of the network has no way to prevent its adoption. Therefore, if a sufficient number of malicious individuals begin to cooperate, all funds can be fraudulently transferred to their accounts. Certainly, in theory such a move would be counterproductive,

as a cryptocurrency that suffers an attack would lose value practically instantly, making it expensive and unprofitable to take over. However, the fact that just over 4,500 users are enough to take control of the system of the most popular global cryptocurrency speaks of the low level of security of the whole concept.

Later research confirmed the results obtained by Srinivasan & Lee (2017) and Suberg (2019). Sai, Buckley & Gear (2021) concluded that 0.01% of the richest accounts hold about 58% of all Bitcoins, that is, that 0.16% of the richest accounts hold over 72% of Bitcoins.

Due to the number of cryptocurrencies based on the PoW concept, the competition between miners is most pronounced with this protocol. In the previous part, it was explained that the pronounced cost component puts a lot of pressure on independent miners, making individual mining unprofitable. This is why oligopolistic structures appear in the form of pools, which control large computing power (Eyal & Sirer, 2018, p. 96). Miners join together and perform as a team, where it does not matter which of the pool members first reached the solution and generated the block, because the reward is divided among the pool members according to the predetermined criteria. Pools increase the chance of individual miners to win a prize, but lead to deepening inequality and reduce the security of the system. Figure 1 shows the percentage share of the leading Bitcoin pools in the total generated blocks. The share was calculated on a sample of three days at the end of May 2023.

Figure 1: Shares of Bitcoin mining pools according to generated blocks, 3-day sample, May 2023



Source: btc.com

It can be seen that the structure of the mining pools is extremely centralized, with two largest pools mining over 50% of the blocks, while the four largest pools mining over 75% of the blocks. The fact that miners who are not members of the pool accounted for

only 0.42% of blocks in the observed period also speaks of the degree of centralization. The obtained results are not consistent with the analysis performed by Srinivasan & Lee (2017), which showed a relatively low concentration in the mining domain (GINI of 0.4). However, the aforementioned authors did not deal with the analysis of pools, but with the analysis of individual miners, where they did not determine whether the miner is a member of a pool or not. It can be concluded that individual miners have a statistically insignificant share, while the entire mining is organized according to the oligopoly principle. An additional problem is that pools do not provide an opportunity for their members to earn equally. The best example is Huobi.pool, which in the period before the pandemic was the sixth largest in the world. Within the pool, its own token called Huobi.pool Token (HPT) was developed as a unit of account for sharing mining rewards. As much as 70% of all HPTs were in just one account, which means that 70% of earnings were used by a single entity. Thus, while pools increase an individual's chance to successfully engage in mining, they also increase inequality within their own structure.

Before the COVID19 pandemic, it was estimated that about 65% of the total computing resources invested in Bitcoin mining came from China, while Russian and American miners each had a 7% share (Gogo, 2020). Numerous authors emphasize that a high concentration of miners in a non-democratic state could be a threat to the stability of the Bitcoin system. (Chester, 2019). However, in September 2021, China banned cryptocurrency trading and mining (Yu & Wallace, 2021), which led some miners to migrate to the US and Kazakhstan. Later data indicate that with or without the tacit consent of the state, the mining community in China continued to exist in a reduced form (Partz, 2022). Regardless of the political organization of the country where the miners come from, the real problem is that the vast majority of them, who are supposed to maintain a global network and make it safe, are actually centrally organized. During the year 2021, the American company Foundry created a disruption in the mining community by recruiting a large number of miners to the ranks of their newly established pool. Already at the end of 2021, Foundry became the largest pool and it holds that position to the mid-2023. Although one might think that it is good that the American pool has broken the dominance of Chinese miners, in fact the situation is even worse now than before the pandemic, because the two largest pools together have 55% of the total computing power. Regardless of the fact that at first glance they seem opposite, because AntPool's headquarters is in China, their size facilitates the potential coordination of joint action and possible cooperation in order to abuse the system.

Conclusion

The concept of cryptocurrencies theoretically enables the financial inclusion of marginalized social groups. Blockchain technology limits the political influence of the state and the corporate influence of financial institutions by decentralizing the management of issuing money and processing transactions. The cryptocurrency community offers chances for greater equality of participants compared to the traditional financial market. The aforementioned claims speak of the great potential of cryptocurrencies and the high

expectations placed before them. However, cryptocurrencies have not met any of these expectations up to this point.

Cryptocurrencies function in parallel with the traditional financial system, so theoretically they enable online payments for users who do not have access to financial services, but have telecommunication services. In practice, there is a problem of how such users can get possession of the first amount of cryptocurrency. If the user wants to buy them in secondary market, he needs first to invest fiat money. Therefore, some form of financial service is still necessary. Another way is to engage in mining. In the previous discussions, it was explained that mining cryptocurrencies that have a developed secondary market is actually a very expensive endeavor. The user would have to invest significant funds in equipment and become part of some global pool of miners. It is not clear which individuals do not have access to financial services and at the same time have significant amounts of money at their disposal, so that they can participate in the mining process and earn from it. A possible answer is wealthy individuals in countries that are excluded from international financial flows due to economic sanctions, but they were certainly not the primary target of inclusion. It can be concluded that cryptocurrencies currently do not enable the financial inclusion of marginalized social groups.

With the exception of few projects, such as the Petro token in Venezuela, all cryptocurrencies are actually private projects. Major international financial institutions have shown very little interest in investing in cryptocurrencies. Therefore, the influence of states and the corporate sector is very limited. However, it would be wrong to conclude that only thanks to these facts, blockchain technology has enabled decentralization. The basic premise, that all participants have an equal opportunity to participate in maintaining the system and making decisions, has not been fulfilled. Mining is run by large pools in which there is pronounced inequality. Almost all independent miners have been forced out of the market due to cost pressure. All consensus protocols favor rich miners and penalize those with limited resources. It is clear that blockchain has brought the same corporate pressure from the big players to the small ones, only in a seemingly altered form.

No single cryptocurrency community provides equality of participants. GINI coefficients, which are listed in the third part of the paper, speak in favor of an extremely uneven distribution of wealth. Inequalities are visible in the mining process, but also in secondary market. Large investors, known as whales, often use their position to create market disruptions to crowd out smaller investors. In the literature, one can find a large number of described situations during which a small number of investors led to a sudden change in the direction of the price movement through massive transactions. The difference with capital markets is that here there is no institution that can prevent such malicious market behaviour or the use of insider information. This is why inequality within cryptocurrency communities is even more pronounced than in traditional financial markets.

It can be concluded that oligopoly structures characterize both the mining process and the secondary market of all major cryptocurrencies. The examples given for Bitcoin apply to a greater or lesser extent to all other cryptocurrencies. Mining pools crowd out independent miners, while at the same time they establish a very unfavourable internal

hierarchical structure. Wealth is very unevenly distributed in favor of early adopters of cryptocurrencies and wealthy individuals who have invested large amounts in the mining process and secondary market. Increasing the number of participants does not lead to redistribution and does not reduce inequalities. On the contrary, it only increases the number of the "poor", that is, users with a minimum amount of funds. The institution of trust and regulation in traditional financial markets was created over a long period of time. Therefore, the situation in cryptocurrency communities cannot be expected to change quickly, especially without the existence of a consensus on the formation of institutions that will perform some form of supervision and control in order to create equal conditions for participants.

The availability of data and the method of their determination is the main limitation of the paper. It could be seen that different authors set their own criteria when determining the GINI coefficient of the cryptocurrency market, making cross-comparison of research impossible. Further research should monitor key indicators over a longer period of time and pay particular attention to disruptions that occur during sudden changes in the price of Bitcoin and other leading currencies, such as those that took place in late 2017 and early 2021.

References

Ammous, S. (2018). Can cryptocurrencies fulfil the functions of money? *The Quarterly Review of Economics and Finance*, *70*, 38-51. Doi: https://doi.org/10.1016/j.qref.2018.05.010

Baker, T. (2022). Let's stop treating crypto trading as if it were finance. *Columbia Law School blog on corporations and capital markets*, November 19. Retrieved May 5, 2023, from https://clsbluesky.law.columbia.edu/2022/11/29/lets-stop-treating-crypto-as-if-it-were-finance/

Chaum, D. (1983). Blind signatures for untraceable payments. *Advances in Cryptology Proceedings of Crypto '82*. 199-203.

Chen, Y. (2018). Blockchain tokens and the potential democratization of entrepreneurship and innovation. *Business horizons*, *61*, 567-575. Doi: https://doi.org/10.1016/j.bushor.2018.03.006

Chester, D. (2019). The dangers of mining pools: centralization and security issues. *Cointelegraph.com*, November 4, retrieved May 5, 2023, from https://cointelegraph.com/news/the-dangers-of-mining-pools-centralization-and-security-issues

Cong, L. W., He, Z., & Li, J. (2019). Decentralized mining in centralized pools. *The Review of Financial Studies,* *34*(3), 1191-1235. Doi: https://doi.org/10.1093/rfs/hhaa040

de Vries, A. (2018). Bitcoin's Growing Energy problem. *Joule*, *2*(5), 801-805. Doi: https://doi.org/10.1016/j.joule.2018.04.016

Demirgüc-Kunt, A., Klapper, L., Singer, D., Ansar, S., & Hess, J. (2018). *The Global Findex database 2017: Measuring financial inclusion and the fintech revolution*. World Bank Group

Eyal, I., & Sirer, E. G. (2018). Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM*, *61*(7), 95–102. Doi: https://doi.org/10.1145/3212998

Gogo, J. (2020). 65% of global bitcoin hashrate concentrated in China. *Bitcoin.com*, May 7. Retrieved May 5, 2023, from https://news.bitcoin.com/65-of-global-bitcoin-hashrate-concentrated-in-china/

Kamau, R. (2022). How Bitcoin can help solve the world's income inequality problem. *Forbes,* June 20. Retrieved May 4, 2023, from https://www.forbes.com/sites/rufaskamau/2022/06/20/how-bitcoin-can-help-solve-the-worlds-income-inequality-problem/?sh=4e9120885871

Lamport, L. (1978). Time, clocks and the ordering of events in a distributed system. *Communications of the ACM*. *21*(7), 558–565. Doi: https://doi.org/10.1145/359545.359563

Lee, D., & Chuen, K. (2016). *Handbook of digital currency*. London, UK: Elsevier

Lin, I.C., & Liao, T.C. (2017). A survey of blockchain security issues and challenges. *International Journal of Network Security*, *19*(5), 653-659. Doi: https://doi.org/10.6633/IJNS.201709.19(5).01

Matonis, J. (1995). Digital cash and monetary freedom. *INET'95 Internet society annual conference*, Honolulu, Hawaii.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Retrieved April 29, 2023, from http://Bitcoin.org/Bitcoin.pdf

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies*. Princeton, NJ, USA: Princeton university press.

Okamoto, T., & Ohta, K. (1991). Universal electronic cash. *Advances in cryptology CRYPTO'91*, Feigenbaum J. (ed.) Berlin: Springer-Verlag. 324-350

Osbourne, C. (2018). Cryptocurrency miners bought 3 million GPUs in 2017. *ZDNet*, March 1. Retrieved May 2, 2023, from https://www.zdnet.com/finance/blockchain/cryptocurrency-miners-bought-3-million-gpus-in-2017/

Partz, H. (2022). China returns as 2nd top Bitcoin mining hub despite the crypto ban. *cointelegraph.com*, May 17. Retrieved May 5, 2023, from

Online First

https://cointelegraph.com/news/china-returns-as-2nd-top-bitcoin-mining-hub-despite-the-crypto-ban

Redman, J. (2020). Onchain Data Shows Rising Bitcoin Whale Index Surpassing 4-Year High. *Bitcoin.com*, October 27. Retrieved May 4, 2023, from https://news.bitcoin.com/onchain-data-shows-rising-bitcoin-whale-index-surpassing-4-year-high/

Sai, A.R., Buckley, J., & Gear, A.L. (2021). Characterizing Wealth Inequality in Cryptocurrencies. *Frontiers in Blockchain 4,* article 730122, Doi: https://doi.org/10.3389/fbloc.2021.730122

Sedgwick, K. (2018). Most cryptocurrencies are more centralized than you think. *Bitcoin.com*, January 26. Retrieved May 5, 2023, from https://news.bitcoin.com/most-cryptocurrencies-are-more-centralized-than-you-think/

Srinivasan, B.S., & Lee, L. (2017). Quantifying decentralization. *News. Earn*, July 28, Retrieved May 3, 2023, from https://news.earn.com/quantifying-decentralization-e39db233c28e (18.11.2020.)

Suberg, W. (2019). Bitcoin wealth inequality drops in 2019 unlike Ether, Litecoin: Report. *Cointelegraph.com*, December 19, retrieved May 3, 2023, from https://cointelegraph.com/news/bitcoin-wealth-inequality-drops-in-2019-unlike-ether-litecoin-report (18.11.2020.)

Todorović, V., & Tomić, N. (2019). Unsustainability of cryptocurrency concept based on the Proof-of-work algorithm. *Bankarstvo*, *48*(1), 46-63. Doi: https://doi.org/10.5937/bankarstvo1901046T

Tomić, N., Todorović, V., & Jakšić, M. (2021). A survey on consensus protocols in permissionless blockchains. *Contemporary issues in economic, business and management, EBM 2020* – Kragujevac: Faculty of economics University of Kragujevac, 365-374.

Vaz, J., & Brown, K. (2020). Sustainable development and cryptocurrencies as private money. *Journal of Industrial and Business Economics*, *47*, 163-184. Doi: https://doi.org/10.1007/s40812-019-00139-5

Ventura, L. (2018). Wealth distribution and income inequality by country 2018, *Global Finance*, November 26. Retrieved May 3, 2023, from

Warren, T. (2018). Bitcoin mania is hurting PC gamers by pushing up GPU prices. *The Verge*, January 30. Retrieved May 2, 2023, from https://www.theverge.com/2018/1/30/16949550/bitcoin-graphics-cards-pc-prices-surge

ОКРУЖНЕЊ

Wile, R. (2013). 927 people own half of all bitcoins. *BusinessInsider*, December 10. Retrieved May 4, 2023, from https://www.businessinsider.com/927-people-own-half-of-the-bitcoins-2013-12

Yu, E., & Wallace, J. (2021). China declares cryptocurrency transactions illegal; Bitcoin price falls. *Wall Street Journal*, September 24. Retrieved May 5, 2023, from https://www.wsj.com/articles/china-declares-bitcoin-and-other-cryptocurrency-transactions-illegal-11632479288

ONLINE FIRST