FACTA UNIVERSITATIS
Series: **Electronics and Energetics** Vol. 37, Nº 1, March 2024, pp. 149 - 156
https://doi.org/10.2298/FUEE2401149S

Original scientific paper

BLOCKCHAIN: BALANCE OF ANONYMITY AND SECURITY

Elena E. Sharafanova, Marina I. Barabanova

International Banking Institute named after Anatoly Sobchak, Saint Petersburg, Saint Petersburg, Russia

ORCID iDs: Elena E. Sharafanova https://orcid.org/0000-0002-1331-5445
Marina I. Barabanova https://orcid.org/0000-0003-2232-6151

Abstract. *The purpose of the article is to summarize the problems of the relationship between anonymity and security when using blockchain technologies. The issue addressed in the article is to determine the conditions for the fundamental achievability of sustainable and secure use of the blockchain. Its inconsistency is shown: confidentiality and anonymity create security potential, protecting the user from identity theft and fraud. But the transparency of transactions allows data leakage about the identity of an anonymous user to create threats to the owner of the wallet. The opinions of experts on the possibility of ensuring security while maintaining the anonymity of users are presented, and data on the most common crimes against property associated with the use of blockchain are presented. Blockchain security is also considered in the context of the impact of its use on the environment, and impact statistics are presented. The directions of legal regulation that ensure a balance between anonymity and security are outlined. Results: directions for economic and legal support for the use of blockchain in the areas of sustainable development (in the field of ecology, social interaction, public administration) have been proposed.*

Key words: *blockchain, anonymity, security, confidentiality, crime, legal regulation*

1. INTRODUCTION

Blockchain is a group of technologies based on an algorithmic apparatus that made it possible to create a critical currency (bitcoin), eliminating the possibility of duplication or counterfeiting in the digital environment. The generally recognized advantages of blockchain technology are security, transparency, decentralization and confidentiality [1]. Providing enormous opportunities for the development of markets, including financial ones, these technologies are ambiguously assessed by major experts in the field of economics, whose opinions are summarized by D.V. Lipnitsky [2]. The advantages usually include a high degree of transaction security, anonymity, the ability to use it to optimize business operations,

Received December 1, 2023; revised January 30, 2024 and February 29, 2024; accepted March 03, 2024
Corresponding author: Sharafanova Elena Evgenevna
International Banking Institute named after Anatoly Sobchak, St. Petersburg, Russia
E-mail: el_siver@mail.ru

increased mobility of economic agents, faster transactions, and potentially the creation of a transparent public administration system. The disadvantages include the increased costs of maintaining the blockchain system, the high energy intensity of bitcoin mining, and the low rate of use in the process of reforming government bodies. The key properties of blockchain are security, privacy and associated anonymity. However, anonymity gives rise to a number of threats associated with the possibility of developing blockchain technologies in the field of cryptocurrencies for the organization of financial applications and the organization of monetary payments serving shadow activities, laundering proceeds from crime, and the financing of terrorism. The Federal Service for Financial Monitoring of the Russian Federation (Rosfinmonitoring), together with the Ministry of Internal Affairs and the Federal Security Service of Russia, as of March 2023, conducted about 400 investigations, and more than 20 criminal cases were initiated. Cryptocurrency turnover, reaching tens of billions of rubles, has been associated with the financing of terrorism, extremism, cybercrime and undermining the financial stability of the state [3].

The problems of the relationship between security (including the security of the individual, corporation, state) and anonymity, relevant for the effective use of blockchain, are the subject of this article. The fundamental achievability of sustainable and safe use of blockchain technologies is a hypothesis that is tested by the authors based on an analysis of publications by Russian and foreign authors.

The purpose of the article is to identify the determining conditions for ensuring a balance between anonymity and security in the use of blockchain technology to achieve sustainable development goals.

Structure of the article: The article contains an introduction, literature review, methodology including research questions, data sources and methods, results and conclusions.

2. Literature Review

The anonymity, confidentiality and security of blockchain are widely covered in the literature. Only in the Russian electronic scientific library e - library for the period from 2019 to 2-24, more than 34.5 thousand publications are available on the request “blockchain and security”. They are mainly devoted to issues of information security, problems of improving algorithms, including consensus algorithms (M.V. Sterzhanov) [4]. Some authors specialize in the specifics of using blockchain in certain industries. For example, E.S. Gerdt analyzes the possibilities of using blockchain technologies in housing and communal services [5] and in public administration; I.V. Sergeev and others consider the impact of blockchain on changes in logistics processes [6]; Bayramdurdyev D. and co-authors analyze the possibilities of using blockchain technologies in the computer industry [7], and this is not an exhaustive list. However, management mechanisms and methods for achieving a balance between security, on the one hand, and anonymity/confidentiality, on the other, are not widely represented. In particular, T. Faizov in his work focused on the possibilities of using technological innovations in the field of blockchain to improve public administration and enhance the dialogue between the government and citizens [8].

The development of Web3 is associated with a deepening problem of the balance between anonymity and security. A number of publications rightly note the difference between anonymity, which involves deliberately concealing the user’s identity, and confidentiality, which ensures the inaccessibility of his personal data from unauthorized access [9]. D. Preethi,

N., Khare, B., R. Tripathy defines blockchain security as the process of detecting and protecting against threats, and implementing appropriate responses to threats through the application of security tools, privacy policies, and information technology service regulations. Confidentiality in the blockchain implies the ability to make transactions without leaking user identification information [10]. Anonymity, which allows users to remain hidden when making transactions, provides a high level of protection against identity theft and fraud. Both confidentiality and anonymity create, on the one hand, the opportunity to use digital services that have great security potential [11], and on the other hand, the transparency of the block chain, as E.V. Bylinkina points out, allows "all participants to monitor the transactions of a specific anonymous user (his wallet). And if information about the identity of an anonymous user becomes known, then the entire transaction history of this wallet becomes available in connection with the identity of its owner" [12].

Anonymity is partially ensured by the fact that the blockchain protocol does not have a time stamp for each transaction, creates the possibility of hiding them (or hiding part of them) and increases the risks of abuse and violations in the field of economic security of companies. R.P. Bulyga and I.V. To solve this problem, Safonov propose to improve the standard methodology for auditing the efficiency of business processes by introducing an innovation, "consisting in the auditor's implementation of a special procedure for "moving funds between wallets" (public keys)" using blockchain technology" [13]. But P.S. Plotnikov, F.A. Neronov, V.V. Maklachkova argue that there is a fundamental opportunity to track transactions and obtain information about user transactions, so anonymity is still limited. They also emphasize that the ability to generate multiple addresses for storing and conducting transactions contributes to the growth of criminal activity due to the use of a second address for illegal activities [1].

3. METHODOLOGY

The study poses and outlines approaches to solving the following issues:

- how is the anonymity and security of the blockchain understood?
- does the anonymity of the blockchain affect the dynamics of cybercrimes?
- is there a connection between the use of blockchain technologies and damage to the environment?
- what conditions are decisive for achieving a balance between anonymity and security of the blockchain?

The data sources in the article are presented by materials of scientific articles published in the scientific electronic library e-library, articles by foreign researchers that are in the public domain, data from scientific reports and financial organizations: the Federal Service for Financial Monitoring of the Russian Federation (Rosfinmonitoring), the People's Bank of China, the Russian Association of Cryptoeconomics, Artificial Intelligence and Blockchain, Institute of Strategic Studies and Economics of Knowledge, National Research University Higher School of Economics (Russia).

Generalization and grouping, logical analysis and synthesis were used as research methods.

4. RESULTS

Anonymity is perhaps the most frequently mentioned advantage of blockchain, when using which, as Anwar K.S. writes, “transactions are anonymous until users themselves want to reveal their identity or personal data is revealed when purchasing this or that asset.” [14] The advantage, as often happens, gives rise to the main disadvantage: a high probability of using blockchain-based actions for fraud, money laundering, and terrorist financing. Realizing this, governments of various countries are making certain efforts to neutralize such threats. Thus, with fairly strict regulation of the use of cryptocurrencies in China, the government of the country is intensifying the use of blockchain for the public sector, introducing a single blockchain platform (RealDID) for personal identification, which allows verifying the user’s identity with minimal risk of leakage of personal information. The balance of anonymity and security is achieved by allowing users to register and log in anonymously using decentralized identifiers (DIDs) and private keys, and personal data is not directly linked to their financial information [15].

The need to develop a regulatory framework governing the use of blockchain is recognized by the governments of most countries in the world, but this process is proceeding unevenly. Some idea of it is contained in Table 1.

Table 1 Characteristics of the regulatory framework for blockchain regulation. Compiled using materials [9]

A country	Regulation status
UAE	Prohibition of foreign cryptocurrencies whose owners cannot be identified either through cryptocurrency providers or through the blockchain. (Zcash , Monero)
Salvador	As of 2021, Bitcoin is legal tender; foreign investors are exempt from paying taxes; Public digital wallet app released.
Brazil	Cryptocurrency as a means of payment has been legalized.
Central African Republic	Bitcoin is legal tender as of 2021.
Singapore	Transactions for paying for goods with cryptocurrency can be classified as barter trade, which removes them from taxation. No capital gains tax on trading profits.
USA	Regulation is provided by the Financial Crimes Enforcement Network (FinCEN), the US Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), and local regulators at the state level. 2022 – Responsible Financial Innovation Act passed.
Switzerland	Private investors are exempt from capital gains tax.
Russia	The Law on Digital Financial Assets has been adopted, but the concept of blockchain is not enshrined in it.

The People's Bank of China's 2023 report, the first to highlight the impact of cryptocurrencies on financial stability, calls on governments around the world to join forces to develop common approaches to blockchain-based business, risk definitions and supervisory conditions in order to eliminate regulatory arbitrage [16].

The risks are quite significant. However, there are also concerns that data obtained on the basis of blockchain solutions, in particular, information about transactions processed by the blockchain cluster launched in Beijing in February 2023, can also be used to manipulate users (both physical and legal entities) [17].

These fears are not unfounded. S.M. Mkrtchyan studied and identified the most common schemes of crimes against property associated with the use of blockchain:

- phone - porting: obtaining access codes to cryptocurrency wallets by replacing the SIM card identification number;
- obtaining insider information from employees of cryptographic organizations;
- phishing: sending emails with an invitation to go to fake sites;
- cyber attacks on open electronic wallets of cryptocurrency exchanges, the funds of which are necessary to ensure continuity of interactions [18].

The activities of miners in the absence of transparent accounting of their work can lead to the fact that, in case of collusion, a group of miners can gain the opportunity to control a significant part of the capacity and gain control over the ledger. This threat was described by I. Makarov and A. Shoar [19].

According to SlowMist Hacked total number of attacks in 2023 was 445; losses in value terms amounted to $2,384,140,525. The dynamics of losses from January to November 2018 are presented in Figure 1.

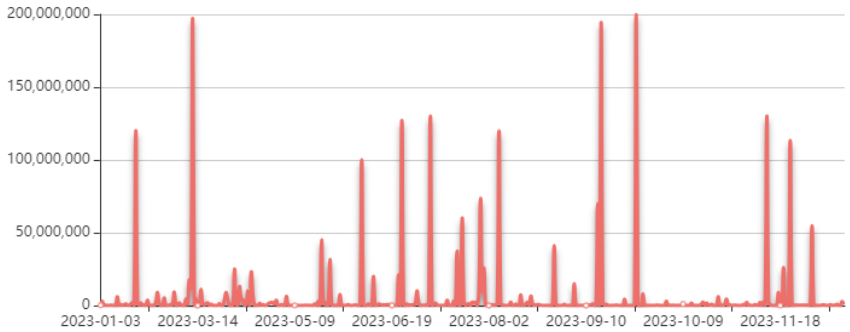

Fig. 1 Dynamics of losses from hacker attacks in 2023. Source: [https://hacked.slowmist.io/statistics/?c=all&d=2023]

According to the Russian Association of Cryptoeconomics, Artificial Intelligence and Blockchain, approximately 900 bitcoins are mined in the world every day, and income from the mining of the main cryptocurrency alone is estimated at $19.7 billion, with Russia's share in it being approximately $2.4 billion (about 12% from total production) [20]. Thus, with a hypothetically minimal tax burden, assuming that miners could pay tax on income as self-employed (6% of income) budget losses amount to more than $140 million. An indirect threat to the life safety of citizens and their quality of life is the high energy intensity of mining. According to experts from an industrial operator for the sale and maintenance of computing equipment, energy consumption by industrial miners in the Russian Federation by the end of 2023 will be up to 2.5 GW [21]. The number of miners in Russia in 2023 was estimated at about 100 thousand people, and, according to the Ministry of Energy, at the end of 2020, the average number of consumers for whom

the power supply was disrupted increased by 230%, the average duration of power outages increased by 19% [22]. Experts attribute this to the growth of shadow business activities for the extraction of cryptocurrency and, if the trend continues and the lack of legal regulation, can lead to a massive shortage of electricity. In particular, interesting information is contained in the works of S. Chamanara et al [23, 24]. According to the published results of a study by the United Nations University in the period 2020-2021. the global bitcoin mining network consumed 173.42 terawatt-hours of electricity, which is comparable to the energy consumption of Pakistan (whose population is 230 million people) [25].

Estimates of annual global carbon emissions from Bitcoin mining are 22.0 - 22.9 million tons of CO2, and this is comparable to emissions from Jordan, Sri Lanka and Kansas City. The CO2 equivalent from Bitcoin mining, according to researchers, is between 82 and 83 positions in the list of countries with the highest emissions [26]. Offsetting the carbon footprint of Bitcoin mining requires planting 3.9 billion trees in an area equal to 7% of the Amazon forests [27].

Summarizing the experience of using blockchain as a technology for carrying out business processes and financial transactions, the review of which is presented above, allows us to identify two groups of problems generated by the imbalance between security and anonymity:

- incomplete protection of digital assets from criminal activities;
- increased vulnerability of the global ecosystem due to increased energy intensity of mining, including shadow mining.

The solution to these problems lies in the field of economic and legal regulation. Blockchain and digital currency, a relatively new instrument of financial markets, have been outside the legal framework of the Russian Federation for quite a long period of time. But on January 1, 2021, the law “On digital financial assets, digital currency and on amendments to certain legislative acts of the Russian Federation” came into force, in which for the first time the very concept of digital currency was enshrined at the legislative level. as a set of “electronic data (digital code or designation) contained in an information system that is offered and (or) can be accepted as a means of payment that is not a monetary unit of a foreign state and (or) an international monetary or unit of account, and (or) as investments and in respect of which there is no person obligated to each owner of such electronic data, with the exception of operators and (or) nodes of the information system, who are obliged only to ensure compliance with the procedure for issuing these electronic data and carrying out actions in relation to them to introduce (change) entries into such an information system according to its rules” [28].

However, the law does not even mention mining, in essence and in the spirit of Russian civil legislation, which is a type of entrepreneurial activity. Recognizing mining as such will oblige miners not only to pay taxes, but also to set electricity tariffs according to the standards of persons engaged in business activities, and will also allow assessing real (or close to reality) activity in the field of mining and, on this basis, setting a fee for generating a carbon footprint for miners.

There should also be a clear distinction between blockchain (as a technology that provides a balance between security and anonymity) and cryptocurrencies (as a payment instrument that makes greater use of anonymity and potentially poses threats to the stability of national currencies). But the increasing use of stablecoins, which have significantly less volatility than cryptocurrencies issued by any entities that meet the conditions of issue. Stablecoins are issued by a specific organization on an already existing blockchain, and this helps to harmonize anonymity and security.

Despite the problems described above, blockchain technologies have good prospects for use in public administration, as well as in the management of regions and corporations, namely:

- NFT applications;
- IoT applications with decentralized data management;
- platforms for conducting and registering real estate transactions;
- personal identifiers;
- online voting, etc.

An interesting study conducted by the Institute of Strategic Studies and Economics of Knowledge of the National Research University Higher School of Economics [29] summarizes the most popular areas: non-fungible tokens (NFTs), crypto assets, decentralized applications, smart contracts, distributed hash tables, digital tokens, tokenized assets, smart property, decentralized autonomous organizations (DAO), blockchain platforms with open entry. The timing of mass implementation is estimated quite optimistically: from 1-2 years for the most significant NFT technology and 2-3 years for the next most important crypto-assets to 2-5 years for other technologies.

5. Conclusion

The analysis carried out allows us to accept the hypothesis that a balance between anonymity and security of the blockchain is fundamentally achievable. Its condition is strengthening government regulation in the issuance and circulation of digital assets. The development of economic and legal support for the use of blockchain should proceed in all three areas of sustainable development:

- in the field of ecology, acts are needed to remove bitcoin mining from shadow circulation, allowing not only to establish fair taxation for this essentially entrepreneurial activity, but also to create conditions for controlling increased energy consumption;
- development of cooperation between law enforcement agencies, public organizations, state and regional government bodies to identify and suppress actions related to the use of cryptocurrency for laundering proceeds from crime and financing terrorism;
- further implementation of blockchain 3.0 technology for the provision of social services, development of social infrastructure and public administration.

The most important, decisive condition for achieving a balance between anonymity and security of the blockchain is, of course, the consolidation of the actions of authorized government institutions in various countries to develop uniform regulatory rules that would ensure the secure integration of the blockchain into the national and global financial systems.

The authors of the article associate further development of the work with an in-depth analysis of the regulatory framework for the use of blockchain technologies in the financial sphere, highlighting general principles and specific features, as well as identifying the best legislative and law enforcement practices that contribute to increasing legal business activity and the growth of national economies.

References

[1] P.S Plotnikov, F.A. Neronov, V.V. Maklachkova, "Analysis of vulnerabilities of blockchain technology", *DSPA: Issues of application of digital signal processing*, vol. 12, no 3, pp. 33-38, 2022.

[2] D.V. Lipnitsky, "Opportunities and challenges for blockchain in the new industrialization", *Industrial Economics*, vol. 85, no. 1, pp. 82-100, 2019.

[3] Rosfinmonitoring. URL: https://fedsfm.ru/search?searchText=blockchain
[4] M.V. Sterzhanov, "Blockchain system consensus algorithms", *Modern means of communication*, vol. 1, no. 1, pp. 67-68, 2022.
[5] E.S. Gerdt, "Possibilities of using blockchain technology for housing and communal services management", *Modern Science*, vol. 11, no. 2, pp. 138-143, 2022.
[6] I.V.Sergeev, R.A. Kornienko, R.I. Ivenin, "Digital transformation of supply chains using blockchain technologies and big data analytics", *RISK: Resources, Information, Supply, Competition*, no. 3, pp. 34-45, 2019.
[7] D. Bayramdurdyev, Sh. Dzhumabaeva, V. Orazgeldiev, L. Allanazarova, "Blockchain technologies in the computer industry: prospects and opportunities", In Situ, no. 1, pp. 24-26, 2023.
[8] T. Faizov. "Problems of legal application of blockchain technology in the activities of government agencies". URL: https://www.advgazeta.ru/mneniya/problemy-pravovogo-primeneniya-tekhnologii-blokcheyn-v-deyatelnosti-gosorganov/
[9] Anonymity and privacy in crypto. URL: https://blog.1inch.io/anonymity-and-privacy-in-crypto/
[10] D. Preethi, N. Khare, B.R. Tripathy, "Security and Privacy Issues in Blockchain Technology", in book *Blockchain Technology and the Internet of Things*, pp.245-263, 2020.
[11] Blockchain privacy and anonymity. URL: https://bitcoal.io/blockchain-privacy-and-anonymity/
[12] E.V. Bylinkina, "Blockchain : legal regulation and standardization", *Law and Politics*, no. 9, 2020..
[13] R.P. Bulyga, I.V. Safonova, "Transformation of audit methodology in connection with the use of blockchain and DLT technologies", *Accounting. Analysis. Audit.*, vol. 8, no. 5, pp. 6-13, 2021.
[14] K.S. Anwar, "Blockchain technology as a tool for strengthening the economies of developing countries", *News of the Issyk-Kul Forum of Accountants and Auditors of Central Asian Countries*, vol. 38, no. 3-1, pp. 425-429, 2022.
[15] RealDID (blockchain platform for identification). URL: https://www.tadviser.ru/index.php/Product:RealDID_(blockchain-platform_for_identification)
[16] China's Cryptocurrency Regulation: The Central Bank urges the world to jointly regulate cryptocurrencies. URL: https://blockbar.io/finance-and-law/chinese-central-bank-urges-the-world-to-jointly-regulate-crypto/
[17] ChainMaker (blockchain cluster). URL: https://www.tadviser.ru/index.php/Article:ChainMaker(blockchaincluster)
[18] S.M. Mkrtchyan, "Crimes against property committed in the sphere of blockchain functioning: new criminal schemes and their criminal legal assessment", *All-Russian Criminological Journal*, vol. 14, no. 6, pp. 845-854, 2020.
[19] I. Makarov, A. Shoar, "Blockchain analysis of the bitcoin market", *Scientific and technical libraries*, no. 11, pp. 135-152, 2022.
[20] Miner in law: the authorities advocated recognizing miners as entrepreneurs. URL: https://iz.ru/1242907/evgenii-kuznetcov/dobytchik-v-zakone-vlasti-vystupili-za-priznanie-mainerov-predprinimateliami
[21] The shortage of mining capacity in Russia began in the spring and will last 1.5-2 years - expert. URL : https://mfd.ru/news/view/?id=2585515
[22] So it mines: energy consumption in Russia may increase by 2.5 times due to crypto miners. URL: https://iz.ru/1261597/valerii-voronov/tak-i-mainit-energopotreblenie-v-rossii-mozhet-vyrasti-v-25-raza-iz-za-dobytchikov-kripty
[23] S. Chamanara, S.A. Ghaffarizadeh, K. Madani, "The environmental footprint of Bitcoin mining across the globe: Call for urgent action", *Earth's Future*, vol. 11, 2023.
[24] S. Chamanara, K. Madani, "The Hidden Environmental Cost of Cryptocurrency: How Bitcoin Mining Impacts Climate, Water and Land", United Nations University Institute for Water, Environment and Health (UNU-INWEH), Hamilton, Ontario, Canada, 2023.
[25] UN Study Reveals the Hidden Environmental Impacts of Bitcoin: Carbon is Not the Only Harmful By-product. URL: https://unu.edu/press-release/un-study-reveals-hidden-environmental-impacts-bitcoin-carbon-not-only-harmful-product
[26] C. Stoll, L. Klaaßen, U. Gallersdörfer, "The Carbon Footprint of Bitcoin", *Joule*, vol. 3, no. 7, pp. 1647-1661, 2019.
[27] UN Study Reveals the Hidden Environmental Impacts of Bitcoin: Carbon is Not the Only Harmful By-product. URL: https://unu.edu/press-release/un-study-reveals-hidden-environmental-impacts-bitcoin-carbon-not-only-harmful-product
[28] Federal Law "On digital financial assets, digital currency and on amendments to certain legislative acts of the Russian Federation" dated July 31, 2020 N 259-FZ (latest edition). URL: https://www.consultant.ru/document/cons_doc_LAW_358753/
[29] Top 10 blockchain technologies: developments and applications. URL: https://issek.hse.ru/news/844587804.html