

## DATA SCIENCE В УПРАВЛЕНИИ ОБРАЗОВАТЕЛЬНЫМ ПРОСТРАНСТВОМ

### State data security in the context of sanctions and economic pressure


#### **Milana G. Uspayeva**

Candidate of Economic Sciences, Associate Professor of the Department of Finance, Credit and Antimonopoly Regulation

Kadyrov Chechen State University

Grozny, Russia

mguspaeva@mail.ru

 0000-0000-0000-0000

#### **Ahmed M. Gachaev**

Head of the Department of Higher and Applied Mathematics, Associate Professor


Grozny State Petroleum Technical University named after M.D. Millionshchikova,

Leading Researcher of the Department of Physical, Mathematical and Chemical Sciences

Academy of Sciences of the Chechen Republic

Grozny, Russia


Gachaev-chr@mail.ru

 0000-0000-0000-0000

Поступила в редакцию 19.03.2023

Принята 07.04.2023

Опубликована 15.06.2023

 10.25726/w9269-5289-1129-g

#### **Аннотация**

Today, there is a rapid development of information and telecommunications systems and technologies and, as a result, their wide application in various spheres of society's activities. A significant number of modern public and private institutions use information and telecommunications systems to manage production processes, support decision-making, store and process information, search for necessary data, and so on. Almost all of these systems work on the principle that processes are managed centrally and full control over the system can be obtained by accessing the main central server. This increases the risk of compromising the entire system, the number of its vulnerabilities and threats. As blockchain technology continues to gain popularity and usage worldwide, the issue of state data security has become increasingly important, particularly in the context of economic sanctions and pressure. This article examines the implications of economic pressure and sanctions on state data security within blockchain technology. The article first discusses the fundamentals of blockchain technology, including its security features and potential vulnerabilities. It then explores the various ways in which economic pressure and sanctions can impact the security of state data within blockchain, including the use of blockchain technology to circumvent sanctions, the risk of data breaches, and the potential for data manipulation. The article also examines various measures that can be taken to enhance state data security within blockchain, including the development of robust encryption protocols, the implementation of multi-factor authentication, and the use of decentralized data storage. Overall, the article highlights the importance of addressing state data security concerns within the context of economic pressure and sanctions, and provides recommendations for policymakers and blockchain practitioners to enhance the security of state data within blockchain technology.

#### **Ключевые слова**

blockchain, AI, machine learning, security, government.

### **Введение**

The term Blockchain partly describes the principle of operation of the technology itself. "Block "is a block," chain " is a chain. It follows that a Blockchain is a chain of blocks. But not just a chain. It has a strict sequence defined by complex cryptographic functions (Cryptomathic, 2015).

Blocks are data about transactions, transactions, and contracts within the system presented in cryptographic form. All blocks are lined up in a chain, that is, they are sequentially connected to each other. To add(write) a new block, you need to check the sequence of previous blocks (Yang, 2018).

Let's take a more detailed look at how the Blockchain works. (Noe, 2017).

Each block has its own hash and the hash of the previous block. Block 3 points to block 2, Block 2 to block 1. the first block is special, it can't point to the previous block because it doesn't exist, this block is called the genesis block.

Let's try to break the integrity and make unauthorized changes to block 2. Changing even one SIM in the data of Block 2 will change its hash, which will automatically lead to changes in all subsequent blocks and make them invalid. But using hashing itself to prevent the creation of fake blocks is not enough.

Computers today have a lot of power and can calculate thousands of hashes per second. Therefore, there is a high probability of spoofing the block and listing all subsequent blocks to make the blockchain valid again.

To prevent such cases, the blockchain has a Proof of Work algorithm. Its essence is to find the hash of a function whose result starts with a certain number of zeros. This mechanism slows down the creation of new blocks and protects against DDoS attacks. In the case of bitcoin, it takes about 10 minutes to calculate a new block and add it to the overall sequence of network blocks. Proof of Work significantly complicates the possibility of forging blocks, since after forging one block, all subsequent blocks must also be recalculated through Proof of Work. Sharing this mechanism together with block hashes is the foundation of Blockchain security (Elisa, 2018).

There is another way that the Blockchain protects itself, and this is decentralization. Instead of using a centralized object to manage the entire sequence, each node has its own copy of the registry and uses a peer-to-peer network to communicate with other nodes. Anyone can join the network, get a full copy of the registry, and participate in verifying the validity of a sequence of blocks. After creating a new block, it is sent to all nodes connected to the network to verify the hash (authenticity of the block). If the check is passed, each node adds a new block to its copy of the Blockchain. All nodes reach consensus by agreeing on which blocks are valid and which are not. Fake blocks will be rejected by other network nodes. Therefore, to successfully falsify a block in the blockchain, it is necessary to recalculate its hash and hash of all subsequent blocks using the Proof of Work algorithm, as well as have access to more than 50% of network nodes, which is almost impossible.

According to the principle of its operation, Blockchain has such advantages as:

1. Decentralization. The main storage server is missing. All records are stored for each network member.
2. Transparency of work. Any of the participants can check all transactions that take place in the system
3. Security. All operations are securely protected by cryptographic functions
4. Reliability. Any attempt to make unauthorized changes will be rejected by other network members.

### **Материалы и методы исследования**

The blockchain network does a good job of ensuring data integrity. Due to the existence of many copies of the database and making changes to it only after confirming the correctness of the information by other network participants, the information remains protected from intentional, unauthorized or accidental changes, as well as any changes in the process of storing processing or transmitting. Information becomes impossible to change due to technical failures in the network node or due to the human factor, since operations are confirmed due to complex mathematical functions (Elisa, 2018).

As a result, the information remains unchanged and correct. Ensuring this category of information security makes it possible to conduct stable operations, make the right decisions, and save data in the form in which it was created (Yang, 2019).

According to the principle of accessibility, information must be available to authorized persons at the right time. In the blockchain network, each participant is considered authorized and can read or write data at any time and participate in the verification of data that other participants add (Zeng, 2021).

Confidentiality of information is achieved by providing the ability to access it with the least privileges, that is, an authorized person should have access only to those data that are defined for him by access rights. Each network member can get a full copy of the database on their device and read all the data in it, which is fundamentally contrary to the principle of data confidentiality. Storing data in the blockchain in encrypted form in the database will not solve the problem of privacy, since in most cases confidential data does not lose its relevance over time, such as personal data. And decrypting the received data becomes a matter of time and depends on the computing power of the attacker trying to gain access to the information (Zeng, 2021).

### **Результаты и обсуждение**

Several projects and initiatives have been undertaken to address state data security concerns in the context of economic pressure and sanctions in blockchain technology. One such project is the Digital Dollar Project, which aims to develop a digital version of the US dollar that incorporates blockchain technology and enables secure and efficient financial transactions. The project is designed to enhance the security of state data by leveraging blockchain's decentralized and tamper-resistant nature, which can help prevent data manipulation and breaches.

Another example is the use of blockchain technology in supply chain management, where it has the potential to enhance the security of state data related to trade and commerce. For instance, the IBM Food Trust project uses blockchain technology to track and verify the origin, quality, and safety of food products throughout the supply chain. This enables state actors to securely share data related to trade and commerce, while also ensuring the integrity and authenticity of the data.

In addition to these projects, several data-driven studies have been conducted to assess the impact of economic pressure and sanctions on state data security within blockchain technology. For instance, a study by the Institute for Security and Technology (IST) found that the use of blockchain technology to circumvent economic sanctions has become increasingly prevalent, particularly in countries such as Iran, North Korea, and Venezuela. The study also found that such practices pose significant risks to state data security, as they can enable malicious actors to manipulate data and evade detection.

At the same time, in some theories, a people are primarily a community of a united culture (tradition, language, or religion) that can function without a state. Therefore, the English definitions of "national security" and "state security" are understood as the security of the state. Although this concept is a broader category because it applies equally to both the territory and the people who live on it. In the social sciences, state security is understood primarily as a system of values, which include: survival (of the people and the state), political (structure, sovereignty) independence, quality of life (at the social, economic and cultural levels). However the number of values that are the basis of security can be much broader and cover such issues as: the prestige of the state or the affairs of citizens outside its borders. Thus, national security, as a category, is narrower than the security of the state, and is associated with the protection of values that guarantee the survival of the people, for example, during the loss of statehood or outside their territory. Therefore, it is considered that national security protects the internal values of the state, that is, those that have an existential character. This means that national security can also be understood as a type of State Security. Researchers of this problem point out that national security is gaining new features, since in the era of globalization it goes beyond the interests of states but does not become part of international security.

Another study by the Blockchain Research Institute (BRI) found that the use of decentralized data storage can significantly enhance the security of state data within blockchain technology. The study examined the potential benefits of decentralized data storage, such as increased data privacy, enhanced data security,

and reduced risk of data breaches. It also highlighted the need for robust encryption protocols and multi-factor authentication to further enhance the security of state data within blockchain.

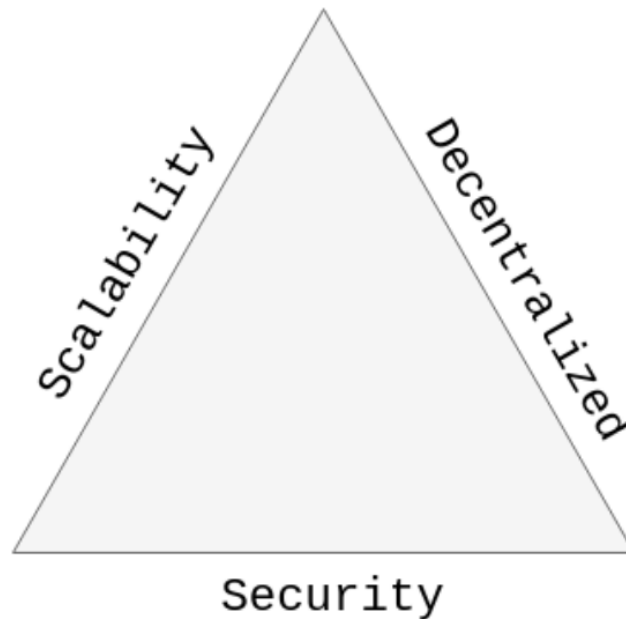


Figure 1. Blockchain trilemma in e-government system

These projects and studies demonstrate the importance of addressing state data security concerns within the context of economic pressure and sanctions in blockchain technology. While blockchain technology has the potential to enhance the security of state data, it is important to develop and implement robust security measures to mitigate potential risks and ensure the integrity and authenticity of state data (Li, 2018).

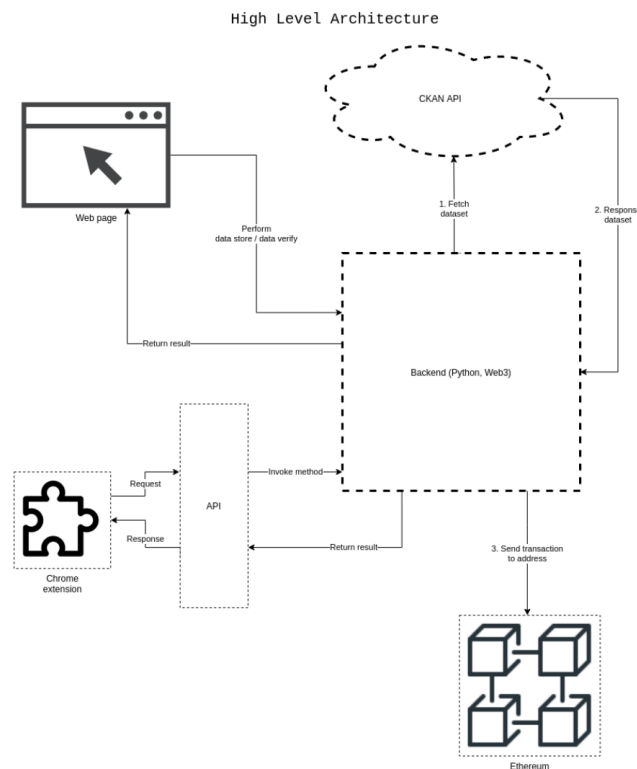


Figure 2. High level architecture blockchain system for e-government security

Blockchain technology has unique features that make it well-suited for state data security in the context of economic pressure and sanctions. One such feature is the tamper-resistant nature of blockchain, which enables the secure and transparent storage and transfer of data (Yang, 2018). Another feature is the decentralized nature of blockchain, which distributes data across a network of nodes, making it more difficult for malicious actors to manipulate or corrupt data (Cryptomathic, 2015).

In addition to these features, blockchain technology has several use cases that can enhance state data security. For instance, blockchain can be used to securely store and share identity information, such as passport information and social security numbers, which can help prevent identity theft and fraud (Huh, 2017). Blockchain can also be used to securely store and share health information, such as medical records, which can improve patient privacy and data security (Turkanović, 2018).

Furthermore, the use of blockchain technology can enhance the security of state data in the context of trade and commerce. For instance, blockchain can be used to securely track and verify the origin, quality, and safety of products throughout the supply chain, which can help prevent fraud and ensure compliance with trade regulations (Noe, 2017). Blockchain can also be used to securely store and share financial data, such as transaction records, which can improve the transparency and accuracy of financial reporting (Clavin, 2019).

However, while blockchain technology has the potential to enhance state data security, it is not without its challenges. One challenge is the potential for data breaches and cyber attacks, which can compromise the security and integrity of state data stored on the blockchain (Zeng, 2021). Another challenge is the potential for data manipulation, particularly in the context of economic pressure and sanctions, where malicious actors may seek to circumvent restrictions and manipulate data to evade detection (Elisa, 2018).

To address these challenges, it is important to implement robust security measures, such as encryption protocols, multi-factor authentication, and decentralized data storage (Li, 2018). It is also important to ensure that all stakeholders in the blockchain ecosystem, including state actors, developers, and users, are educated about the potential risks and best practices for maintaining state data security within blockchain technology (Tshering, 2020).

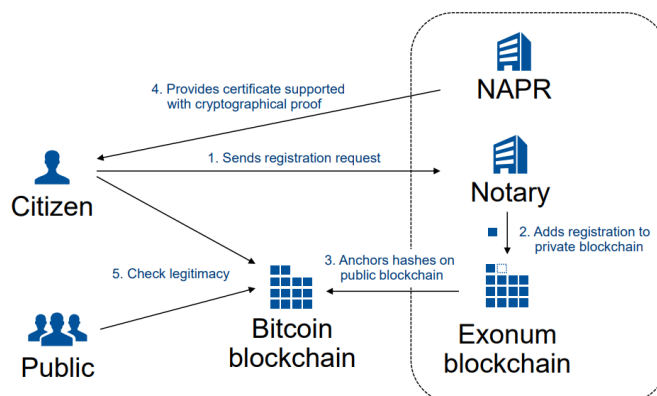


Figure 3. Registration process in e-government blockchain

Several definitions of national security should be given, none of which claim to be complete. In the encyclopedic version, national security is "the ability of a country to preserve sovereignty, political, economic, social and other foundations of public life and act as an independent subject of International Relations" (Tshering, 2020). Or national security is "the protection of vital interests of a person, state and society, state borders, territorial integrity, socio-political structure, cultural values and everything that forms the basis of the material and spiritual life of the country from internal and external threats" (Yang, 2019). In the latter case, attention is drawn to the use of the term "threat" in the singular, which contradicts the social realities of any country.

The legislative version is too overloaded with details, but it is necessary to quote it in view of the demonstration of the ability of State forces to outline a nation-safe issue: national security – this is "the protection of vital interests of a person and citizen, society and the state, which ensures the sustainable development of society, timely detection, prevention and neutralization of real and potential threats to national interests in the

areas of law enforcement, anti-corruption, border activities and defense, migration policy, health, child protection, education and science, scientific, technical and innovative policy, cultural development of the population, ensuring freedom of speech and information security, interests" (Addo, 2021).

Problems of blockchain application development. The introduction of blockchain technology is hindered by many factors. Let's list the main ones.

The inertia of market players and the need to reach consensus between many participants, the lack of a legislative framework significantly hinders the development of the market. The lack of a legislative framework leads to uncertainty in many issues. For a technology to gain trust, it must meet standards (for example, state standards). No standards – no compliance. The technology does not have a governing body and it is unclear who will determine the ways of its development.

The complexity of existing prototypes of blockchain solutions for understanding the mass business consumer. Today, businesses interested in the practical application of the technology are wondering what investments are needed to implement a blockchain project in the corporate sector. In this case, there is no clear answer. The order of numbers largely depends on the scope of application; the complexity of business logic that needs to be created for a specific project; the number of connections with third-party services; the key storage infrastructure used; the number of roles and users in the system, and so on. The company will also need a full-time security specialist who will lead the project, even if a specialized blockchain developer takes over the entire construction of the system. On average, the cost of building an accounting system for an enterprise can be estimated at tens or hundreds of thousands of dollars.

The main problems include "scalability". Currently, all blockchain protocols are built in such a way that each computer on the network must process each transaction – this property provides maximum fault tolerance and security at the cost of the fact that the computing power of the network is limited to the computing power of a single computer. It is necessary to overcome these limitations and reach a level sufficient for its mass distribution.

There is also the problem of integrating new and existing private systems with an open blockchain. One solution to this problem is to create a blockchain-based authentication service to implement a global level of security. Such a service can become a standard security infrastructure for new models of mixed private and public systems, which will benefit all stakeholders in various sectors of the economy. An example of this approach is the Hydro Raindrop blockchain (Li, 2018).

According to the site Statista.com global spending on blockchain solutions is projected to reach 6.6 billion USD in 2021. Forecasts suggest that they will continue to grow in the coming years, reaching almost 19 billion USD by 2024.

There is no doubt that the blockchain technology itself is widely known and associated with cryptocurrencies, although in fact, it is an electronic list of created records (blocks of information) with the possibility of verifying them through public access and a distributed storage base. The main advantage of this electronic "registration book" is that it is protected from unauthorized access and can be effectively updated online due to its nature as a decentralized network on many devices. These features make the technology ideal for verifying data, accessing data, and protecting it. Companies around the world have started using blockchain for internal purposes, such as recording internal transactions, as well as in their payment processes.

Given the potential of the technology and the broad interest of businesses in the opportunities it provides, blockchain itself has become a huge market, even at an early stage of technology development. Promising blockchain startups regularly accumulate hundreds of millions of dollars in investment, which indicates a high level of trust in the technology.

In 2021, interethnic payments and settlements were considered the largest area of use of blockchain technology, accounting for about 16 percent of the global blockchain technology market, see fig. 4.

The use of blockchain technology in the field of international payments and settlements is becoming increasingly popular, as they allow you to make money transfers around the world quickly and easily, avoiding expensive banking services and currency conversion. However, recently, the banking industry has also become active and open to blockchain technology, which opens prospects for consumers and businesses to transfer funds internationally with the possibility of lower costs and at the same time compete with the capabilities of

cryptocurrencies. Since banks themselves use blockchain technology, they eliminate the "intermediary", which in this case is cryptocurrencies. Expanding the use of the technology leads to an improvement in the quality of the competitive market environment for international payments and the expected increase in the volume of the global blockchain technology market in the coming years.

Another popular use case that occupies a significant part of the blockchain technology market is the storage, reproduction, and research of the origin of data related to the necessary business processes of organizations specializing in B2B software, in particular, IT businesses and Computer Services. Such technologies allow you to verify the origin and authenticity of product components in the value chain management system, in other words, it acts as a family tree of the product. In this area, blockchain technology becomes a guarantee of compliance with regulatory requirements and prevents forgery of components of the final product.

As you can see, the areas of use of blockchain technology are quite wide and all of them are fully or partially related to the accounting system, that is, accountants and auditors.

Let's outline the areas in which leading companies already use blockchain technology and which still have prospects for using it:

- 1) International Settlements and settlements with counterparties;
- 2) payment of taxes, fees and other types of debt;
- 3) work with documents and distributed data warehouses;
- 4) prompt recording of business activity facts and real-time reporting;
- 5) working with state registers and obtaining official information.

Undoubtedly, by influencing the accounting system, the technology under study does not significantly change it (Tshering, 2020).

### **Заключение**

Pricewaterhouse Coopers predicts that technology investments will reach 25 billion by 2025. Today in Australia, many projects are implemented using blockchain technologies. The loudest and last, perhaps, is the e-money.

The prospects of blockchain technology are changing the various areas in which they are used, and this confirms the opinion that this state of affairs opens up a new round in the development of the digital economy. Following the dynamics of research in this area in leading scientific journals included in the Scopus scientometric database, we can conclude that since 2015, interest in blockchain technologies has been constantly growing and in the first months of 2022 has significantly exceeded the indicators of previous years. Blockchain technology, which gained popularity after being introduced to the world in 2008 in the Bitcoin white paper, was launched on January 3, 2009, when the first block in the Bitcoin network was signed. Today, the opportunities that the use of blockchain can provide are being explored by leading states, banks and corporations. A decentralized technology that allows you to register information, track the path of transactions, and reduce transaction costs can change our daily lives, and this is happening today openly and securely.

Accounting and the field of Finance will undoubtedly change under the influence of the widespread use of the latest technologies, but these changes will concern only the tools with which the system of Organization of accounting and audit will be implemented, without changing the very essence of the process and their methodological techniques.

For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation (Clavin, 2019).

### **Список литературы**

1. Yang L., Elisa N., & Eliot N. (2018). Privacy and security aspects of E-government in smart cities. New York: Elsevier Press.
2. Cryptomathic. (2015). A key component for e-government security. <https://www.cryptomathic.com/news-events/blog/key-for-egovernment-security-central-signing-authentication/>

3. Huh S., Cho S., & Kim S. (2017). Managing iot devices using blockchain platform. In 2017 19th international conference on advanced communication technology (ICACT) (pp. 464–467). IEEE.
4. Turkanović M., Hölbl M., Košič K., Heričko M., & Kamišalić A. (2018). Eductx: A blockchain-based higher education credit platform. *IEEE Access*, 6, 5112–5127.
5. Noe E. (2017). Usability, accessibility and web security assessment of e-government websites in tanzania. *International Journal of Computer Applications*, 164(5), 42–48.
6. Clavin J., Sisi D. (2019) Global Transformation with Blockchain: From Lab to App: Workshop Summary. Retrieved October 21, 2020 from <https://carta.umbc.edu/workshops/workshopsblockchain-workshop2018/>.
7. Zeng J., Yu Liu. (2021). Government Data Sharing based on Blockchain. In 2021 The 3rd International Conference on Blockchain Technology (ICBCT '21), March 26-28, 2021, Shanghai, China. ACM, New York, NY, USA, 9 Pages. <https://doi.org/10.1145/3460537.3460562>
8. Elisa N., Yang L., Naik N. (2018). Dendritic cell algorithm with optimised parameters using genetic algorithm. In *IEEE world congress on computational intelligence* (pp. 1–8). IEEE
9. Li J., Yang L., Qu Y., & Sexton G. (2018). An extended Takagi–Sugeno–Kang inference system (tsk?) with fuzzy inter-polation and its rule base generation. *Soft Computing*, 22(10), 3155–3170
10. Tshering G. and Gao S. (2020), "Understanding security in the government's use of blockchain technology with value focused thinking approach", *Journal of Enterprise Information Management*, Vol. 33 No. 3, pp. 519-540. <https://doi.org/10.1108/JEIM-06-2018-0138>
11. Yang L., Elisa N. and Eliot N., (2019). Privacy and security aspects of E-government in smart cities. In *Smart cities cybersecurity and privacy* (pp. 89-102). Elsevier.
12. Addo A., & Senyo P. K. (2021). Advancing E-governance for development: Digital identification and its link to socioeconomic inclusion. *Government Information Quarterly*, 38(02), 101568. <https://doi.org/10.1016/j.giq.2021.101568>.
13. Bouras M. A., Lu Q., Zhang F., Wan Y., Zhang T., & Ning H. (2020). Distributed ledger technology for eHealth identity privacy: State of the art and future perspective. *Sensors (Switzerland)*, 20(02), 1–20.
14. Di Porto F., & Zuppetta M. (2021). Co-regulating algorithmic disclosure for digital platforms. *Policy and Society*, 40(02), 272–293. <https://doi.org/10.1080/14494035.2020.1809052>.
15. Gilani K., Bertin E., Hatin J., & Crespi N. (2020). A survey on blockchain-based identity management and decentralized privacy for personal data. *2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)* pp. 97–101. <https://doi.org/10.1109/BRAINS49436.2020.9223312>.

### Безопасность государственных данных в условиях санкций и экономического давления


#### Милана Гумкиевна Успаева

Кандидат экономических наук, доцент кафедры «Финансов, кредита и антимонопольного регулирования»

Чеченский государственный университет им. А.А. Кадырова


Грозный, Россия

[mguspaeva@mail.ru](mailto:mguspaeva@mail.ru)

 0000-0000-0000-0000




**Ахмед Магомедович Гачаев**

Заведующий кафедрой «Высшая и прикладная математика», доцент,  
Грозненский государственный нефтяной технический университет им. акад. М.Д. Миллионщикова  
ведущий научный сотрудник отдела физико-математических и химических наук  
Академия наук Чеченской республики  
Грозный, Россия  
Gachaev-chr@mail.ru  
 0000-0000-0000-0000

Received 19.03.2023

Accepted 07.04.2023

Published 15.06.2023

 10.25726/w9269-5289-1129-g

**Abstract**

Сегодня наблюдается стремительное развитие информационных и телекоммуникационных систем и технологий и, как следствие, их широкое применение в различных сферах жизнедеятельности общества. Значительное число современных государственных и частных учреждений используют информационные и телекоммуникационные системы для управления производственными процессами, поддержки принятия решений, хранения и обработки информации, поиска необходимых данных и так далее. Почти все эти системы работают по принципу централизованного управления процессами, и полный контроль над системой можно получить, обратившись к главному центральному серверу. Это увеличивает риск компрометации всей системы, количество ее уязвимостей и угроз. Поскольку технология блокчейн продолжает набирать популярность и использоваться во всем мире, вопрос безопасности государственных данных становится все более важным, особенно в контексте экономических санкций и давления. В этой статье рассматриваются последствия экономического давления и санкций для государственной безопасности данных в рамках технологии блокчейн. Сначала в статье рассматриваются основы технологии блокчейн, включая ее функции безопасности и потенциальные уязвимости. Затем в нем исследуются различные способы, с помощью которых экономическое давление и санкции могут повлиять на безопасность государственных данных в блокчейне, включая использование технологии блокчейн для обхода санкций, риск утечки данных и потенциал для манипулирования данными. В статье также рассматриваются различные меры, которые могут быть приняты для повышения безопасности государственных данных в рамках блокчейна, включая разработку надежных протоколов шифрования, внедрение многофакторной аутентификации и использование децентрализованного хранилища данных. В целом, в статье подчеркивается важность решения проблем безопасности государственных данных в контексте экономического давления и санкций, а также даются рекомендации для политиков и практиков блокчейна по повышению безопасности государственных данных с помощью технологии блокчейн.

**Keywords**

блокчейн, искусственный интеллект, машинное обучение, безопасность, правительство.

**References**

1. Yang L., Elisa N., & Eliot N. (2018). Privacy and security aspects of E-government in smart cities. New York: Elsevier Press.
2. Cryptomathic. (2015). A key component for e-government security. <https://www.cryptomathic.com/news-events/blog/key-for-egovernment-security-central-signing-authentication/>

3. Huh S., Cho S., & Kim S. (2017). Managing iot devices using blockchain platform. In 2017 19th international conference on advanced communication technology (ICACT) (pp. 464–467). IEEE.
4. Turkanović M., Hölbl M., Košič K., Heričko M., & Kamišalić A. (2018). Eductx: A blockchain-based higher education credit platform. *IEEE Access*, 6, 5112–5127.
5. Noe E. (2017). Usability, accessibility and web security assessment of e-government websites in tanzania. *International Journal of Computer Applications*, 164(5), 42–48.
6. Clavin J., Sisi D. (2019) Global Transformation with Blockchain: From Lab to App: Workshop Summary. Retrieved October 21, 2020 from <https://carta.umbc.edu/workshops/workshopsblockchain-workshop2018/>.
7. Zeng J., Yu Liu. (2021). Government Data Sharing based on Blockchain. In 2021 The 3rd International Conference on Blockchain Technology (ICBCT '21), March 26-28, 2021, Shanghai, China. ACM, New York, NY, USA, 9 Pages. <https://doi.org/10.1145/3460537.3460562>
8. Elisa N., Yang L., Naik N. (2018). Dendritic cell algorithm with optimised parameters using genetic algorithm. In *IEEE world congress on computational intelligence* (pp. 1–8). IEEE
9. Li J., Yang L., Qu Y., & Sexton G. (2018). An extended Takagi–Sugeno–Kang inference system (tsk?) with fuzzy inter-polation and its rule base generation. *Soft Computing*, 22(10), 3155–3170
10. Tshering G. and Gao S. (2020), "Understanding security in the government's use of blockchain technology with value focused thinking approach", *Journal of Enterprise Information Management*, Vol. 33 No. 3, pp. 519-540. <https://doi.org/10.1108/JEIM-06-2018-0138>
11. Yang L., Elisa N. and Eliot N., (2019). Privacy and security aspects of E-government in smart cities. In *Smart cities cybersecurity and privacy* (pp. 89-102). Elsevier.
12. Addo A., & Senyo P. K. (2021). Advancing E-governance for development: Digital identification and its link to socioeconomic inclusion. *Government Information Quarterly*, 38(02), 101568. <https://doi.org/10.1016/j.giq.2021.101568>.
13. Bouras M. A., Lu Q., Zhang F., Wan Y., Zhang T., & Ning H. (2020). Distributed ledger technology for eHealth identity privacy: State of the art and future perspective. *Sensors (Switzerland)*, 20(02), 1–20.
14. Di Porto F., & Zuppetta M. (2021). Co-regulating algorithmic disclosure for digital platforms. *Policy and Society*, 40(02), 272–293. <https://doi.org/10.1080/14494035.2020.1809052>.
15. Gilani K., Bertin E., Hatin J., & Crespi N. (2020). A survey on blockchain-based identity management and decentralized privacy for personal data. *2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)* pp. 97–101. <https://doi.org/10.1109/BRAINS49436.2020.9223312>.