УДК 004.056
https://www.doi.org/10.47813/dnit.4.2025.3019

EDN
ZCXMZK

Технология Blockchain как метод защиты данных в современных условиях

А.А. Грейс[1,2*], В.В. Калитина[2], Д.Р. Идрисова[1], Д.М. Скрябин[1], К.П. Лукьянов[1], А.П. Энгель[2]

[1]Сибирский федеральный университет, пр. Свободный, 79, Красноярск, 660041, Россия
[2]Красноярский государственный аграрный университет, пр. Мира, 90, Красноярск, 660049, Россия

*E-mail: alena.yabl@yandex.ru

Аннотация. В статье рассматривается технология блокчейн как перспективный инструмент обеспечения информационной безопасности в условиях нарастающих киберугроз и увеличения объёмов цифровых данных. Проведен анализ ключевых принципов блокчейна, включая децентрализацию, криптографическую защиту, неизменяемость данных и прозрачность, а также их влияние на устойчивость систем хранения и передачи информации. Выявлены основные киберугрозы, такие как вредоносное ПО, фишинг, DDoS-атаки и SQL-инъекции, а также рассмотрены традиционные методы защиты. Особое внимание уделено преимуществам блокчейна перед централизованными подходами к безопасности, в частности его способности снижать риски несанкционированного доступа и манипуляций с данными.

Ключевые слова: блокчейн, информационная безопасность, киберугрозы, децентрализация, криптографическая защита.

Blockchain technology as a method of data protection in modern conditions

A.A. Grace[1,2*], V.V. Kalitina[2], D.R. Idrisova[1], D.M. Skryabin[1], K.P. Lukyanov[1], A.P. Engel[2]

[1]Siberian Federal University, 79 Svobodny pr., Krasnoyarsk, 660041, Russia
[2]Krasnoyarsk State Agrarian University, 90 Mira Avenue, Krasnoyarsk, 660049, Russia

*E-mail: alena.yabl@yandex.ru

Abstract. This article examines blockchain technology as a promising tool for ensuring information security amid growing cyber threats and increasing volumes of digital data. The study analyzes the key principles of blockchain, including decentralization, cryptographic protection, data immutability, and transparency, as well as their impact on the resilience of data storage and transmission systems. Major cyber threats such as malware, phishing, DDoS attacks, and SQL injections are identified, alongside an overview of traditional security measures. Particular attention is given to the advantages of blockchain over centralized security approaches, specifically its ability to mitigate risks associated with unauthorized access and data manipulation.

Keywords: blockchain, information security, cyber threats, decentralization, cryptographic protection.

1. Introduction

In the era of rapid digitalization across all sectors of society, information security has become a top priority. While modern technologies enhance convenience and efficiency in data management, they simultaneously introduce new challenges related to data protection. Cyber threats such as malware, phishing, and DDoS attacks pose significant risks to the confidentiality, integrity, and availability of information. Traditional security measures, including antivirus software, firewalls, and encryption systems, remain essential components of cybersecurity. However, their effectiveness is increasingly compromised due to their reliance on centralized structures, which can serve as vulnerable entry points for malicious actors [1].

This growing threat landscape necessitates the development of innovative solutions that can enhance the resilience of information systems. One such solution is blockchain technology, initially designed to support cryptocurrency transactions but now recognized for its potential as a robust data protection tool. Blockchain's key advantages include decentralization, immutability of records, cryptographic security, and transaction transparency. Despite the rising interest in this technology, its integration with conventional cybersecurity measures and the overall effectiveness of such an approach require further investigation.

Existing academic studies primarily focus on specific aspects of blockchain, such as cryptographic algorithms, smart contracts, and consensus mechanisms. However, a comprehensive analysis of its potential applications in information security remains underexplored. This paper examines the fundamental principles of blockchain, its key characteristics, and its integration with traditional security methods. Particular emphasis is placed on decentralization, transparency, and the resilience of blockchain-based systems, allowing for a thorough evaluation of their viability in safeguarding information across various industries, including finance, logistics, and government administration [2-3].

2. Materials and methods

The key components of information security are confidentiality, integrity, and availability of information. Confidentiality refers to protecting data from unauthorized access, integrity ensures the data remains unaltered and prevents unauthorized modifications, and availability ensures that the information is accessible when and where needed. These three components form the foundation of any information security system, and their protection is crucial for organizations and individuals.

In the context of rapid digital transformation, cyber threats have become one of the most serious issues for safeguarding these components. Malicious software, system attacks, and data breaches represent significant risks to the confidentiality, integrity, and availability of information. The history of information security is full of examples of attacks that have left a significant mark globally, disrupting the operations of companies, banks, government institutions, and individual users.

One of the most well-known threats is viruses and malicious software, which, over the decades, have posed a serious danger to users and organizations. Viruses, trojans, worms, spyware, and ransomware infect computers and networks, causing irreparable damage. Malicious programs are often accompanied by spam, which is not only a source of annoyance for users but also a channel for spreading viruses. Spam can contain fake offers, links to malicious websites, or attachments with viruses, posing a significant security threat.

Phishing is another serious threat that continues to evolve with increasingly sophisticated forms. This social engineering method targets users with deceptive messages designed to steal confidential information, such as passwords, logins, and credit card details. DDoS attacks, aimed at overloading a server or network, also leave a significant mark in history. These attacks use a large number of infected devices to overwhelm a server, making it temporarily unavailable.

SEO infections, which allow malicious sites to rank highly in search engine results, also present a major threat. SQL injections, which involve embedding malicious SQL code into database queries, are also among the most common and dangerous attacks. Data breaches, which have become particularly prevalent in recent decades, have led to several large-scale leaks.

Cyber attack methods such as social engineering are also becoming increasingly widespread. In these cases, cybercriminals manipulate individuals to gain access to confidential information. Exploitation of vulnerabilities in software, brute-force attacks, and the spreading of malicious attachments via email or social media – these all affect information security, undermining the confidentiality, integrity, and availability of data.

3. Discussion

Modern data protection systems incorporate a variety of methods and tools aimed at ensuring the confidentiality, integrity, and availability of information. Traditional protection measures include antivirus software, firewalls, regular software updates, the use of strong passwords and two-factor authentication, as well as regular data backups. These measures provide basic protection against a range of cyber threats such as viruses, phishing, and unauthorized access; however, their effectiveness is increasingly questioned in the face of growing threats.

Antivirus programs and firewalls play an essential role in maintaining security by blocking malicious software and monitoring network traffic. However, for these tools to remain effective, it is necessary to regularly update threat databases and monitor the health of the software. The problem lies in the fact that these protective tools rely on centralized systems, which can be vulnerable to attacks if the system itself is not updated promptly.

Regular software updates are also crucial for closing vulnerabilities that may be exploited by cybercriminals. However, despite numerous patches and updates, neglecting these processes can lead to serious consequences. Automating the update process can help mitigate such risks, but it is impossible to completely eliminate vulnerabilities, as new types of attacks are constantly emerging.

The use of strong passwords and two-factor authentication is an important step in securing data. Implementing two-factor authentication significantly complicates account hacking, but even so, the system may still be vulnerable to social engineering methods or attacks on the channels through which confirmation codes are transmitted.

Regular data backups help protect against data loss in the event of a malware attack, such as ransomware. However, this protection method is not always a guarantee of complete security, as infected systems may destroy backup copies if they are not stored in secure, remote locations.

In contrast, modern data protection systems that require a high level of reliability, transparency, and resilience tackle data protection challenges differently. Reliable protection systems must ensure constant data availability, safeguard against unauthorized access and alterations, and enable rapid data recovery in the event of an attack or failure.

Blockchain, with its unique structure, serves as an example of a modern technology that meets these requirements. One of the key features of blockchain is decentralization, which prevents dependence on a single point of failure and ensures data availability even when faced with external threats. Unlike traditional protection methods, blockchain uses a distributed data storage system where information is recorded in blocks and stored across multiple nodes, making it more secure against manipulation and loss.

Transparency is another crucial advantage of blockchain, as all transactions are recorded on the network and can be verified by every participant. This significantly enhances trust and eliminates the possibility of data tampering. In contrast to centralized systems, where changes to data may occur covertly, blockchain allows every alteration to be tracked in real-time.

The resilience of blockchain systems is ensured through their distributed architecture and ability to self-recover. Even if some nodes fail, the remaining ones continue to operate, ensuring uninterrupted system functionality. Blockchain systems possess high adaptability and can respond swiftly to new threats, making them an essential component for building long-term, secure infrastructures.

4. Results: On the concept of blockchain technology

Blockchain represents an innovative technology that fundamentally transforms concepts of data protection and security in the digital world. Unlike traditional centralized systems, blockchain operates based on a distributed ledger, where data is not stored in one location but is spread across multiple network nodes. This eliminates the possibility of centralized attacks, such as DDoS attacks, which can overload a server in centralized systems. Even if one of the nodes fails, the network continues to function without interruption, making blockchain highly resilient to various threats [4].

A key feature of blockchain is the use of cryptographic methods to protect data. Each transaction is recorded in the blockchain with a unique digital signature and hash value, ensuring the integrity and authenticity of the information. The connection of each block to the previous one through cryptographic algorithms makes the data virtually immutable, preventing tampering or manipulation. This property of blockchain significantly enhances the security and reliability of data storage.

Blockchain also provides transparency and traceability of all transactions. In open networks, all records are stored in a publicly accessible ledger, allowing any user to verify the history of operations and identify any suspicious activity. This transparency minimizes the risks of fraud and data manipulation, as any attempts to alter the information are immediately detectable by network participants.

The blockchain technology eliminates the need for intermediaries and centralized governing bodies, further contributing to enhanced security. In traditional systems, administrators can become vulnerable if their credentials are compromised. In blockchain, all network participants are equal, and the system operates without centralized control, reducing the potential for attacks on a single point.

Another important aspect of blockchain is its protection against spam and counterfeit data. Blockchain networks often charge a fee for registering transactions, making mass generation of fake records economically unfeasible. Additionally, each transaction is verified by the network, which prevents the introduction of suspicious or malicious data.

The blockchain system also provides reliable protection against data theft. In some cases, data can be encrypted and divided into fragments, which are stored across different nodes. This makes it impossible to steal all the information even if one of the nodes is compromised. Furthermore, blockchain enables the implementation of digital identity systems that use unique keys or biometric data instead of traditional passwords. This significantly reduces the risk of credential theft, which is often targeted in phishing attacks.

Finally, blockchain supports smart contracts that automatically execute predefined conditions. This allows, for example, the automatic blocking of suspicious transactions or notifications to users about potential breaches, further enhancing the security of the system.

Thus, blockchain represents a technology that significantly outperforms traditional data protection methods, offering unique mechanisms of security, resilience to attacks, and transparency, making it an indispensable tool in the era of digitalization and cyber threats.

5. Conclusion

Blockchain technology can be effectively used in conjunction with traditional data protection methods, such as antivirus software, firewalls, intrusion detection systems, encryption, and others, to create a multi-layered and more reliable defense mechanism. It is important to recognize that blockchain does not replace existing security measures, but rather complements and enhances their capabilities while addressing some of their vulnerabilities. This integration of blockchain with traditional security technologies creates a more resilient and robust system.

Encryption remains one of the most effective traditional technologies for data protection. Blockchain can be used to enhance the security of encrypted data exchanges. For instance, blockchain can provide a secure repository for cryptographic keys and records, making them accessible only to authorized users. When data is encrypted and access is controlled through blockchain, it offers an additional layer of protection that is tamper-resistant, as any attempt to modify encrypted data will be logged in the blockchain.

Antivirus programs and intrusion detection systems (IDS) detect and block viruses, malware, and suspicious activity. Blockchain can be leveraged to create more reliable security logs and track the behavior of software. Records of actions performed on a device or within a network can be stored in the blockchain, ensuring an immutable and tamper-proof event log. In the event of a threat, such as a hack or intrusion, all information related to the actions of the attackers will be available for analysis and verification.

Multi-factor authentication employs multiple layers of verification, such as a password and a one-time code via SMS, to protect against unauthorized access. Blockchain can improve this protection by providing a more secure and reliable form of authentication using cryptographically protected digital identifiers and keys. Unlike traditional methods, which may be vulnerable to phishing or hacking, blockchain-based digital identifiers make the falsification of authentication data impossible.

Firewalls protect networks from unauthorized access and attacks. Blockchain can be used to manage access at the network infrastructure level. For example, blockchain can track and record all access attempts to a network, including information on who and when tried to connect, creating a transparent view of network activity. Recording these events in the blockchain ensures that they cannot be tampered with or deleted, providing a higher level of control.

DDoS attacks aim to overload servers and render them inaccessible. In combination with traditional DDoS protection measures, blockchain can be employed to defend against such attacks by distributing traffic and data across multiple nodes in the network. Blockchain can also be used to create distributed applications and infrastructures that automatically redirect traffic, improving fault tolerance. It also helps build systems for analyzing and preventing attacks based on transparent and immutable data.

Digital signatures are widely used to secure transactions and documents in the digital space. Blockchain can enhance these processes by providing unforgeable verification of signatures and documented agreements. Smart contracts on blockchain automatically execute contract conditions, reducing the risk of fraud and errors. For example, if a contract specifies that data should only be transferred under certain conditions, a smart contract will check their fulfillment and record the transaction, eliminating human errors.

Monitoring and auditing systems track activities within a network and on devices. Blockchain can be used to store audit trails, ensuring complete transparency and immutability of records. This is particularly important when investigating security incidents. Blockchain creates an accessible log of all actions that cannot be altered or deleted, which greatly increases the reliability and accuracy of investigations.

The research confirms that blockchain technology holds significant potential to enhance data protection in the face of modern cyber threats. One of the key findings is the high resilience of blockchain to various types of attacks, including DDoS and phishing. This is achieved through the decentralized network structure, which eliminates the presence of a single point of failure, and the use of cryptographic methods that ensure data integrity and confidentiality. For example, in the financial and logistics industries, where blockchain is actively deployed, the number of successful attacks on such systems is significantly lower compared to traditional centralized solutions.

An important aspect of blockchain is its ability to ensure data immutability and transparency. Each transaction recorded in the blockchain becomes part of a chain that cannot be altered or deleted without the consensus of the majority of network participants. This property is especially valuable in industries where a high degree of trust is required, such as healthcare and government administration. For instance, in blockchain-based electronic voting systems, every vote is recorded and can be verified, which eliminates the possibility of manipulation and enhances confidence in the process.

The research also shows that blockchain effectively complements traditional data protection methods, such as antivirus software, firewalls, and multi-factor authentication. A combined approach enables the creation of a multi-layered security system that significantly complicates the task for attackers. For example, using blockchain to store cryptographic keys enhances the security of data encryption, while integrating with monitoring and auditing systems ensures the transparency and immutability of event logs.

Blockchain also demonstrates high efficiency in reducing the risks of data leakage. Due to the distributed nature of data storage, information is divided into fragments and stored across multiple network nodes. This makes it impossible to steal all the information even in the event of a breach of one node. An example of this can be seen in blockchain-based medical data storage systems, where confidential patient information is reliably protected from unauthorized access.

Finally, blockchain enables the automation of data protection processes through the use of smart contracts. These programmable conditions automatically perform predefined actions, such as blocking suspicious transactions or notifying users of attempted breaches. This reduces reliance on human intervention and improves responsiveness to threats.

The results of the study confirm that blockchain offers a fundamentally new approach to data protection, which can be integrated with traditional methods to create more resilient systems. Unlike previous studies, this paper proposes a comprehensive approach to integrating blockchain with existing technologies, thereby addressing the key vulnerabilities of centralized systems. However, there are limitations, such as the significant computational resources required for blockchain implementation, which may be economically burdensome. Furthermore, scalability issues in blockchain systems remain unresolved and require further investigation.

The research has confirmed that blockchain is an effective method for data protection in the context of modern cyber threats. Its key advantages – decentralization, transparency, and cryptographic security – make it an attractive tool for use across various sectors, including finance, logistics, and government administration. The results of this work can be used to develop more reliable data protection systems and for further research in the integration of blockchain with traditional technologies.

References

1. Shakhsuvarova, I.Z. Information security: theoretical foundations of the concept / I.Z. Shakhsuvarova // Alley of Science. – 2022. – T. 1. – No. 7 (70). – P. 209-214.
2. Borisov, R.S. Information security / R.S. Borisov // MODERN SCIENCE. – 2019. – No. 4-3. – P. 151-154.
3. Sukhov, A.N. Information security: theoretical and practical aspect / A.N. Sukhov // Psychological and pedagogical search. – 2021. – No. 1 (57). – P. 183-191.
4. Yakushkin, S.A. Blockchain technology: meaning, categories, legal perspective / S.A. Yakushkin // Bulletin of Science and Practice. – 2019. – No. 5(8). – P. 134-139.