

TECHNICAL SCIENCES

РОЛЬ ТЕХНОЛОГИИ БЛОКЧЕЙН В КИБЕРБЕЗОПАСНОСТИ: ПРИМЕНЕНИЕ, ВЫЗОВЫ И ПЕРСПЕКТИВЫ

Ахмедова А.

Нахчыванский Государственный Университет
ORCID ID: <https://orcid.org/0009-0004-9657-5649>

Асадова Ш.

Нахчыванский Государственный Университет

THE ROLE OF BLOCKCHAIN TECHNOLOGY IN CYBERSECURITY: APPLICATIONS, CHALLENGES AND PERSPECTIVES

Ahmadova A.

Nakhchivan State University
ORCID ID: <https://orcid.org/0009-0004-9657-5649>

Asadova S.

Nakhchivan State University

АННОТАЦИЯ

В данной работе рассматривается трансформирующая роль технологии блокчейн в укреплении современных основ кибербезопасности перед лицом усложняющихся угроз. Исследование подчеркивает, как децентрализованная и криптографическая природа блокчейна снижает системные уязвимости, в частности, устраняя риски, связанные с едиными точками отказа и DDoS-атаками. Кроме того, интеграция блокчейна с искусственным интеллектом и облачными вычислениями анализируется как проактивная стратегия для обнаружения угроз в реальном времени. Особое внимание уделяется обеспечению безопасности экосистемы Интернета вещей (IoT) с помощью протоколов децентрализованной идентификации и аутентификации. В заключение рассматриваются критические вызовы внедрения, такие как энергоэффективность и нормативно-правовая база, что определяет блокчейн как фундаментальный стандарт цифровой целостности в будущем.

ABSTRACT

This paper examines the transformative role of blockchain technology in enhancing modern cybersecurity frameworks against increasingly sophisticated threats. The study highlights how the decentralized and cryptographic nature of blockchain mitigates systemic vulnerabilities, specifically addressing the risks associated with Single Points of Failure and DDoS attacks. Furthermore, the integration of blockchain with artificial intelligence and cloud computing is explored as a proactive strategy for real-time threat detection and autonomous response. Special emphasis is placed on securing the Internet of Things (IoT) ecosystem through decentralized identification and authentication protocols. Finally, the research addresses critical implementation challenges such as energy efficiency and regulatory frameworks, positioning blockchain as a fundamental standard for future digital integrity.

Ключевые слова: технология блокчейн, кибербезопасность, целостность данных, децентрализованные системы.

Keywords: blockchain technology, cybersecurity, data integrity, decentralized systems.

Introduction

In the technological paradigm of the modern era, the acceleration of digitalization processes has fundamentally transformed the entire spectrum of human activity. While digital communication channels in previous decades were characterized solely by simple text exchange and limited data transmission, the current landscape features generative artificial intelligence platforms, complex banking-financial ecosystems, and integrated e-government infrastructures. While ensuring high efficiency in data management, this evolution has also increased the complexity of critical information systems, rendering them vulnerable to larger-scale external interventions.

In this context, the insufficiency of traditional cybersecurity architectures against contemporary threats necessitates the development of more innovative and

resilient defense mechanisms. The integration of blockchain technology into the cybersecurity ecosystem offers strategic security solutions by enabling a transition to decentralized structures. The technology in question serves as an effective methodological framework for preserving data integrity, increasing the transparency of authorization processes, and eliminating potential security vulnerabilities.

The evolution of cyber-threats and traditional defense mechanisms

The extensive expansion of the digital ecosystem has, in turn, created a fertile environment for the proliferation of complex and high-risk cyber-threats. Conventional protection methods demonstrate insufficient effectiveness in countering modern organized cyber-attacks, particularly in cases involving unauthorized data acquisition, manipulation of confidential information, and the total paralysis of critical infrastructure systems.

These deficiencies are directly related to the fact that centralized management models possess a Single Point of Failure and remain structurally weak against external interventions.

Strategic solution: Blockchain technology and the security paradigm

The gaps emerging in the current cybersecurity landscape render the implementation of fundamentally more reliable, transparent, and cryptographically grounded technologies inevitable for the protection of digital assets. In this context, blockchain solutions offer an innovative defense paradigm by ensuring data integrity and availability through Distributed Ledger Technology (DLT). In such an environment, blockchain emerges not merely as a means of data storage, but as a strategic tool for enhancing cyber resilience and establishing a decentralized trust model.

Blockchain applications in cybersecurity

Initially implemented exclusively within the cryptocurrency sphere, blockchain has now evolved into one of the fundamental pillars of cybersecurity. This technology ensures data integrity and immutability [8]. Due to its decentralized architecture, data is not stored on a single server but is distributed among network participants.

The Bitcoin ecosystem serves as a primary example. While an attack on a central server in traditional banking systems jeopardizes the entire system, in blockchain-based systems, data is synchronized across thousands of nodes. Consequently, unauthorized interventions by hackers at several points do not compromise the overall security of the network. Furthermore, this technology accelerates processes while reducing the costs associated with digital identification.

DDoS threats in digital infrastructure and their consequences

The rapid expansion of the global digital infrastructure has significantly increased both the frequency and the destructive scale of Distributed Denial of Service (DDoS) attacks. These types of cyber interventions paralyze the availability of critical services by overwhelming centralized server architectures with excessive malicious request traffic [5]. Consequently, for organizations, these attacks are not limited to direct financial losses but also create serious strategic risks, leading to the undermining of corporate reputation and the long-term degradation of user trust.

Blockchain architecture: Cryptographic resilience and Anti-DDoS mechanisms

In countering such sophisticated threats, blockchain technology establishes a fundamental protective barrier through the principle of storing data in a cryptographic chain structure. In this system, each block references the hash value of the preceding block, forming a digital sequence characterized by a chain-like succession that is virtually impossible to manipulate [3]. The decentralized nature of blockchain, particularly in distributed Domain Name System (DNS) solutions, ensures the absence of a single target point (Single Point of Failure), thereby maximizing the network's immunity to DDoS attacks and its overall **cyber resilience**.

Technological synergy: Integration of artificial intelligence, cloud computing, and blockchain

In the near future, the convergence of blockchain technology with Artificial Intelligence (AI) and cloud computing systems will initiate a qualitatively new phase in cyber-threat monitoring and preventive defense strategies. This triple integration will facilitate the intelligent analysis of anomalies in real-time and the immutable recording of such data on the blockchain, thereby creating conditions for the formation of autonomous and high-speed response mechanisms against cyber incidents. Such an ecosystem will fundamentally strengthen corporate and state-level security architectures by making data management in the digital environment more transparent and resilient to manipulation.

IoT security and institutional regulatory perspectives

The implementation of decentralized security protocols for the identification and authentication of devices, particularly within the Internet of Things (IoT) ecosystem, is considered one of the priority directions of modern cybersecurity science [1, 2]. Blockchain-based distributed identification models will not only ensure secure interactions among billions of heterogeneous devices within the network but also minimize the risks inherent in centralized management systems. With the enhancement of energy efficiency, optimization of technical complexity, and the establishment of international legal regulatory frameworks, blockchain is poised to become a fundamental standard providing absolute transparency and integrity in the global digital environment.

Conclusion

Blockchain technology, through its decentralized architecture and principles of cryptographic security, is paving the way for revolutionary transformations in the field of cybersecurity [7]. Despite current technical challenges, the implementation of this technology is indispensable for the establishment of a more resilient, efficient, and attack-resistant digital ecosystem [6].

References

1. Seyyar, Y. E. (2021). Cybersecurity in IoT systems for the transportation sector: Threats, attacks, and protection strategies. *Journal of Engineering and Technology*.
2. Ahakonye, L. A. C., Nwakanma, C. I., & Kim, D. S. (2022). Tides of Blockchain in IoT Cybersecurity. *IEEE Access*.
3. Goel, A., & Rahulamathavan, Y. (2020). A Comparative Survey of Centralised and Decentralised Identity Management Systems: Analysing Scalability, Security, and Feasibility. *Future Internet*.
4. Yacan, İ. (2021). Endüstri 4.0 Teknolojileri ve Toplum 5.0 Kavramı. *Yeni Fikir Dergisi*, 13(27), 31–39.
5. Aydın, Ö., & Yükçü, S. (2019). Assessment of Blockchain Technology in terms of Benefit-Cost in Cyber Attack Prevention. *Journal of Business Research*.

6. Ahmadova, A. (2022). The Potential Of Blockchain Technology In Education: Reliability, Efficiency And Future Strategies. *International Journal of Educational Technology*.

7. Shaik, I. A. (2023). Security applications of blockchain: Emerging research and innovations. *Journal of Cyber Security*.

8. Ceylan, O., & Işık, A. H. (2020). Blokzincir Teknolojisi ve Uygulama Alanları. *Bilişim Teknolojileri Dergisi*.