BULLETIN of Cherkasy State Technological University

Journal homepage: https://bulletin-chstu.com.ua/en

Vol. 29 No. 4. 2024

UDC 004.056.55:004.75
DOI: 10.62660/bcstu/4.2024.43

Integration of blockchain technologies into cybersecurity systems for critical infrastructure facilities: Prospects and challenges

Viktor Danchuk[*]

Doctor of Physical and Mathematical Sciences, Professor
National Transport University
01010, 1 M. Omelianovych-Pavlenko Str., Kyiv, Ukraine
https://orcid.org/0000-0003-4282-2400

Mariia Danchuk

PhD in Economic Sciences, Associated Professor
National Transport University
01010, 1 M. Omelianovych-Pavlenko Str., Kyiv, Ukraine
https://orcid.org/0009-0007-3033-3227

Abstract. The purpose of the study was to analyse the potential and main problems of integrating blockchain technologies into the processes of ensuring cybersecurity of critical infrastructure facilities in Ukraine. As part of the work, the potential of blockchain technologies in improving the security of critical infrastructures was analysed, the existing challenges of scaling and performance of such systems were assessed, and the possibilities of international cooperation for implementing innovative solutions in the field of cybersecurity were explored. The paper provided a comprehensive analysis of the prospects for integrating blockchain technologies into cybersecurity systems for critical infrastructure facilities. To ensure the relevance of the study, the technical features of the blockchain, such as consensus mechanisms, data distribution models, and cryptographic methods, were considered. It was found that blockchain technologies provide increased transparency, resistance to cyber threats, and optimisation of access control to critical data. At the same time, the main challenges remain low scalability of systems, limited transaction speed, and high energy costs, which complicates their large-scale implementation. The study also showed that there is a need to adapt regulatory requirements to improve the efficiency of blockchain integration into infrastructure facilities. The study demonstrated the significant potential of blockchain technologies as one of the key components in building sustainable cybersecurity systems. The conclusions of the paper emphasise the need for an interdisciplinary approach to the implementation of technologies, including technical, economic, and regulatory aspects, to increase the level of security of critical infrastructure facilities in the context of growing cyber threats. In addition, the paper highlights the importance of international cooperation, which will combine resources and expertise to create more effective and innovative solutions in the field of cybersecurity

Keywords: distributed ledgers; data management; regulatory aspects; cryptography; digital trust

INTRODUCTION

The development of modern technologies and their integration into critical infrastructure systems create not only new opportunities, but also increase the vulnerability of such objects to cyber threats. Industrial control systems, energy complexes, transport networks, and medical facilities are becoming targets for

Article's History: Received: 08.07.2024; Revised: 25.10.2024; Accepted: 16.12.2024.

Suggested Citation:
Danchuk, V., & Danchuk, M. (2024). Integration of blockchain technologies into cybersecurity systems for critical infrastructure facilities: Prospects and challenges. *Bulletin of Cherkasy State Technological University*, 29(4), 43-52. doi: 10.62660/bcstu/4.2024.43.

[*]Corresponding author

intruders, threatening national security and stability. In the face of increasing complexity of cyber-attacks, traditional protection methods are often insufficient for the security of such facilities. This highlights the need to apply innovative solutions, among which blockchain technology occupies a special place. Blockchain, originally developed as the foundation of cryptocurrencies, demonstrates potential in a wider range of applications, including cybersecurity. Its key features – decentralisation, immutability of records, and a high level of transparency and reliability – make it a promising tool for protecting data and infrastructure systems. In the context of critical infrastructure, blockchain can be used to improve the security of access control systems, monitor networks, and prevent unauthorised interference. However, the process of integrating blockchain into cybersecurity systems involves a number of challenges. Among them, the high power consumption of some blockchain solutions, limited scalability and the need to ensure compatibility with existing systems stand out. In addition, there are still issues of regulatory regulation and standardisation of such technologies, which complicates their widespread implementation.

The analysis of studies by various researchers demonstrated a wide range of approaches to integrating blockchain technologies into cybersecurity systems. For example, A. Iskryzhytskii & A. Zadorozhnii (2024) emphasised the benefits of decentralised data storage, stressing that the use of blockchain technologies reduces the risk of successful attacks on centralised access points. In turn, N. Mohamed & A.A. Ahmed (2024) investigated the effectiveness of the technology in preventing "man-in-the-middle" attacks and concluded that the use of smart contracts significantly reduced the risks of unauthorised interference. E. Barka *et al.* (2022) focused on using blockchain to control access to critical infrastructure resources. The researchers noted that the introduction of decentralised identifiers improved the reliability of user identification and authentication systems. On the other hand, A. Ali *et al.* (2023) analysed the scalability and power consumption issues of blockchain systems, offering solutions based on hybrid architectures that combine the advantages of blockchain and conventional databases.

Q. Wang & M. Su (2020) studied examples of successful blockchain applications in the energy sector. Their findings showed that the use of technology in energy distribution and smart grid management reduces the likelihood of disruptions due to cyber-attacks. The study by J. Horner & P. Ryan (2019) focused on the regulatory aspects of blockchain implementation, pointing out the need for international standardisation to ensure technology compatibility. D. Kobets & O. Runov (2024) explored the potential of blockchain in medical infrastructure, emphasising its ability to guarantee a high level of protection of medical data, preventing their falsification or unauthorised disclosure. L. Koh *et al.* (2020) analysed the technology's capabilities in transport systems, where blockchain has increased the transparency and reliability of logistics operations. A.A. Zainuddin *et al.* (2024) investigated the synergistic effect of sharing blockchain and artificial intelligence technologies in threat detection systems. Their results highlight that integrating these approaches improves the analysis capabilities and performance of cybersecurity systems. In addition, K. Košťál *et al.* (2019) considered the use of blockchain in the field of monitoring network events. In their study, they argued that a decentralised logging system prevented the possibility of changing or deleting suspicious activity records, which increased the overall level of cybersecurity.

Despite significant advances in blockchain technology applications, several key issues remained unresolved. Methods for integrating blockchain with traditional cybersecurity systems have not been sufficiently studied, especially in conditions of limited computing resources. They also required additional analysis of the issue of scaling blockchain solutions for large-scale critical infrastructure facilities. There were also no comprehensive studies on the cost-effectiveness and profitability of implementing blockchain in such systems. The purpose of the study was to analyse the potential and limitations of using blockchain technologies in cybersecurity systems of critical infrastructure facilities, with an emphasis on their integration, scalability, and cost-effectiveness. The objectives of the study were: to conduct a comparative analysis of existing approaches to the integration of blockchain technologies into the cybersecurity system; to assess the limitations and scalability of blockchain solutions for large infrastructure facilities; to investigate the economic efficiency of using blockchain in the context of improving the sustainability of critical infrastructure.

MATERIALS AND METHODS

Critical infrastructure ensures the functioning of society, economic stability and national security. Therefore, the development of effective methods of its protection has become a key task of modern cybersecurity. The approach to studying this issue was based on the analysis of traditional security methods and innovative technologies, in particular blockchain. At the first stage of the study, an overview of existing solutions was made. Conventional methods, such as multi-level protection, remain the foundation of modern cybersecurity systems. These include the use of firewalls, intrusion detection and prevention systems (IDS/IPS), antivirus software, and data encryption. Such systems are effective against many threats, but face limitations in the face of complex attacks such as "zero-day" or Advanced Persistent Threats (APT).

The main focus was on the analysis of conventional security methods and innovative technologies, in particular blockchain. The territorial boundaries of the study covered Ukraine in order to assess specific challenges and implement technologies in Ukrainian critical infrastructure. The experience of Ukraine was compared with the leading practices of countries that actively use blockchain in the field of cybersecurity, such as: Israel, the EU countries and the USA (Chowdhury & Gkioulos, 2021; Yu *et al.*, 2021; Joint Statement on…, 2023). Among the areas of implementation of blockchain technologies in Ukraine were considered: energy, financial systems, healthcare, and cybersecurity. The Ukrainian experience was compared with innovations in these countries, which helped to identify common trends and specific challenges (Implementation of blockchain…, 2023; Kozhemiakin, 2023; Shevchuk *et al.*, 2024).

Exploring a multi-level architecture that combines multiple security mechanisms has been key to understanding how different technologies can interact to maximise efficiency. The study also focused on analysing mechanisms such as access control, network segmentation, and artificial intelligence-based solutions for detecting anomalies. Such systems create backup mechanisms that can be activated in the event of an attack, but their implementation often requires significant resources. Further, the potential of the latest technologies, in particular blockchain, was investigated. This technology offers unique cybersecurity solutions due to its decentralised nature, which ensures a high level of data integrity. The study examined ways to use blockchain to control access, monitor threats, and ensure transparency in system management. For example, saving a history of changes and transactions on the blockchain allows quickly identifying possible threats and violations.

Another important stage was the study of the limitations and challenges of implementing blockchain in the Ukrainian critical infrastructure. In particular, attention was paid to regulatory issues, high implementation costs, and the need to adapt to existing management systems. Special attention was paid to the problems of scalability and performance of blockchain technologies. These aspects were critical for applications in infrastructures that require real-time processing of large amounts of data. The analysis focused on solutions such as layer architectures, sharding, and the use of Proof-of-Stake consensus mechanisms. The final stage of the study was based on the limitations and challenges of blockchain implementation.

RESULTS

Ensuring the cybersecurity of critical infrastructure is a key challenge to prevent economic damage, social consequences, and possible threats to national security. In this context, various security approaches are based on the use of both conventional methods and the latest technologies, in particular blockchain. Conventional approaches include the use of multi-level security systems that involve the use of firewalls, IDS/IPS systems, antivirus software, and data encryption tools. These methods provided a basic level of protection, but were not always effective in more complex attacks, such as zero-day attacks or APTs. Centralised architectures often faced problems controlling large amounts of data simultaneously, which made it difficult to detect and neutralise threats in real time. One of the approaches that was actively used was multi-level protection, which combined several types of tools. This included access control, network segmentation, an information security management system that collects, analyses, and responds to incidents in real time, and artificial intelligence-based solutions for predicting and detecting anomalies. A multi-level security system created backup mechanisms that could be activated in the event of an attack on one of the levels, but the implementation of such systems was often expensive and complex.

With the development of technology, it became possible to integrate the latest solutions to improve the effectiveness of protection. Among them were systems based on machine learning and artificial intelligence, which allowed automating the processes of analysing large amounts of data and quickly identifying potential threats. However, the implementation of such solutions required significant investment and a high level of technical training (Ullah *et al.*, 2020). Blockchain technologies offered a new approach to security based on decentralised data storage and management, which allowed changing or deleting them without the consent of all network participants. This provided a high level of data integrity and increased resistance to cyber-attacks. In particular, the blockchain was used to create access control systems, monitor and detect threats, and to save the history of changes and transactions in systems, which increased transparency and control over access to data. Despite all the advantages, the use of blockchain technologies in cybersecurity had its limitations. These included high implementation costs, the need for significant computing resources, and the potential vulnerability to new types of attacks targeting the blockchain technology itself. In addition, the regulation of blockchain systems remained insufficiently clear in many countries, which made it difficult to implement them in existing critical infrastructure frameworks. Consequently, modern approaches to ensuring the cybersecurity of critical infrastructure required a combination of conventional methods with the latest technologies, in particular blockchain, which created new opportunities for strengthening protection, but also posed new challenges that needed to be addressed (Habib *et al.*, 2022).

Scalability and performance are key factors that determine the effectiveness of using blockchain technologies in cybersecurity systems, especially for critical infrastructure facilities. These aspects relate to the ability of blockchain systems to process large amounts of data and the number of transactions in real time, which is important for ensuring their functionality at the level of modern industrial systems (Smith & Dhillon, 2020). The scalability of blockchain technologies was related to their ability to process a large number of transactions in a certain period of time without losing performance. The blockchain worked on the principle of adding blocks with transactions to the chain using a consensus mechanism, which ensured data security and integrity, but often led to transaction delays, especially in high-load systems.

In addition, technologies can be used to reduce the load on the main blockchain. This included solutions such as a layered architecture, where transaction processing takes place at a second level (for example, a solution based on the Lightning Network in Bitcoin or a solution based on the Polygon platform for Ethereum). Other methods include sharding, which involves splitting data into separate parts, which reduces the load on each individual network node. In this approach, each node processes only a fraction of transactions, which significantly increases the overall network bandwidth. In addition, Proof-of-Stake, instead of the traditional Proof-of-Work, which uses significantly less computing power, allows reducing energy costs and improving performance.

The performance of blockchain systems is measured by the number of transactions they can process per unit of time and the time required to verify transactions (Shapovalova *et al.*, 2024). For critical infrastructure applications, high performance is a prerequisite for smooth system operation. Performance lags lead to delays, which can affect the speed of response to cyber threats (Pacheco *et al.*, 2023). Modern blockchain platforms work to optimise performance using various approaches. For example, platforms that support the concept of hybrid consensus combine various transaction verification mechanisms to ensure fast processing and high security. This allows reducing the cost of processing transactions and increasing the overall speed of the system.

Challenges that arise when implementing scalable and productive blockchain systems include the need for powerful computing resources, which may be economically impractical for some organisations. In addition, the security of these systems can be compromised due to various vulnerabilities associated with new integration methods, which requires detailed testing and additional measures to ensure their sustainability. Thus, issues of scalability and performance of blockchain systems remain important for the implementation of these technologies in critical infrastructure, and require a comprehensive approach, including the development of new technological solutions and optimisation of existing protocols (Nasir *et al.*, 2022).

The protection of critical infrastructure is a particularly important task, as these facilities provide the main functions that support the life of society, economic stability, and national security. Given the growth of cyber-attacks and the complexity of modern threats, the integration of blockchain technologies opens up new prospects for strengthening the cybersecurity of critical objects. Blockchain can become a powerful tool for data protection, access control, and ensuring the transparency and integrity of information systems (Radvanovsky & McDougall, 2023). One of the key advantages of blockchain technologies is decentralisation. In critical infrastructure systems, this means that data is not stored in a single centralised location, which can become the target of a cyberattack. The decentralised structure of the blockchain provides distributed storage of information on many nodes of the network, which makes it difficult to change or delete it without authorisation. This significantly reduces the risks associated with a single-node attack and makes the system more resistant to large-scale cyber-attacks, including DDoS attacks.

Blockchain technologies guarantee data integrity due to cryptographic transaction protection and a hashing mechanism that eliminates unauthorised information changes. This is especially important for critical infrastructure, where ensuring the reliability of data is a prerequisite for proper functioning. In addition, the blockchain provides transparency by being able to track all changes in the system, which allows conducting audits and identifying potential violations in real time. This creates a new level of trust between system participants and makes it difficult to fake or conceal important information (Wei *et al.*, 2020).

Integration of blockchain technologies allows creating effective access control systems for critical infrastructure objects. Smart contracts allow automating the process of granting or revoking access based on certain conditions. Such systems can use decentralised identifiers to authenticate users, which provides a high level of protection against fraud and abuse. If necessary, access can only be restricted to a certain circle of authorised persons, and All Access changes are automatically recorded in the blockchain, which makes the system transparent and controlled. Blockchain-based systems have the potential to detect and prevent cyber-attacks due to their decentralised nature and ability to process data in real time. Blockchain integration with monitoring systems allows creating dynamic anomaly detection mechanisms that help to track unauthorised changes and respond to potential threats in time. Smart contracts can automatically block or restrict access if suspicious activity is detected, which increases the overall level of infrastructure security.

Despite the great potential, the introduction of blockchain technologies in critical infrastructure protection systems is accompanied by some problems. These include the high cost of implementation, the need for significant computing resources, and compatibility issues with existing systems. In addition, the blockchain may have restrictions on the speed of transaction processing, which may affect its application in large systems with high speed requirements (Wisniewski *et al.*, 2022). In general, the integration of blockchain technologies into cybersecurity systems for critical infrastructure facilities opens up new opportunities for strengthening data protection, access control, and transparency. However, for widespread implementation, it is necessary to overcome certain technical and economic barriers and ensure that new solutions comply with regulatory requirements and safety standards.

In the modern world, technological innovations are becoming the driving force behind development. This is especially relevant for critical infrastructure, which, in the context of global digitalisation and growing cyber threats, requires a radical approach to security and efficiency (Safitra *et al.*, 2023). Blockchain is one of these technologies that, despite its relatively recent emergence, has already proven its ability to change the functioning of many industries. In the energy sector of Ukraine, blockchain opens up new horizons for decentralising network management (Semenenko *et al.*, 2024).

In transport and logistics, blockchain is becoming a key tool for ensuring transparency in supply chains. The use of smart contracts for cargo tracking not only minimises bureaucratic delays, but also creates conditions for combating corruption in customs processes (Pournader *et al.*, 2020). This is especially important for Ukraine, which is an important transport hub in Europe. Healthcare also benefits from blockchain integration. Storing patients' medical data in decentralised systems minimises the risk of loss or theft, while providing quick access for authorised users. Such initiatives contribute to the development of e-health, which is becoming relevant in the context of crises and pandemics. Despite the obvious advantages, the implementation of blockchain faces a number of challenges. These include high initial costs, the need for high technical competence, and insufficient legislative regulation. The issue of cybersecurity of the blockchain infrastructure itself is also important, because errors in smart contracts can become a source of vulnerabilities.

The integration of blockchain technologies into Ukraine's critical infrastructure is a challenge that simultaneously opens up significant prospects. Energy, transportation, healthcare, and finance are already demonstrating the effectiveness of this technology in combating cyber threats, corruption, and inefficiency. The success of this process depends on the interaction of the state, business and society, and on the willingness to invest in training, infrastructure and legislative support. For Ukraine, this is an opportunity not only to strengthen its infrastructure, but also to become a leader in innovation in the region. Table 1 shows the prospects for implementing blockchain technologies in the critical infrastructure of Ukraine.

Table 1. Implementation of blockchain technologies in critical infrastructure of Ukraine: key areas and opportunities

Scope of application	Research/Projects in Ukraine	Quantitative data/Results
Energy	Pilot project of blockchain systems for energy consumption accounting	Reducing energy losses in a pilot project
Healthcare	Development of a system for storing medical data on the blockchain	Medical records are more protected from unauthorised access as part of testing
Financial sector	Blockchain integration for banking transactions	Reducing the time of international transfers
Transport and logistics	Implementation of blockchain solutions for cargo tracking	Delivery efficiency increased transparency of customs procedures
Electoral systems	Pilot project of electronic voting on the blockchain	Participants rated system security as high
Government infrastructure management	Using blockchain in the land cadastre	Cadastre records are stored in a decentralised system

Source: developed by the authors based on Implementation of blockchain technology in healthcare in 2023 (2023), S. Kozhemiakin (2023), M. Shevchuk *et al.* (2024)

Table 1 shows that blockchain technologies have significant potential in modernising Ukraine's critical infrastructure. Due to its decentralised nature, blockchain can provide transparency and security in industries such as energy, transportation, healthcare, and the financial sector. Significant steps have already been taken in the implementation of this technology in 2024, in particular, in projects to decentralise energy networks and pilot initiatives to use the e-Hryvnia. Such examples indicate prospects for improving the efficiency of resource management and the resilience of systems to cyber-attacks.

However, for the widespread adoption of blockchain in critical infrastructure, a number of challenges must be overcome. These include insufficient funding, the need for high technical competence, and imperfect legislative regulation. Solving these problems requires coordinated efforts by the state, business, and educational institutions. Ukraine has every chance to become an innovator in the use of blockchain in critical industries, which will increase its competitiveness and ensure greater reliability of national systems. Ukraine is actively developing international cooperation in the field of blockchain technologies to ensure cybersecurity of critical infrastructure facilities. The main areas of this interaction are the exchange of experience, implementation of advanced technical solutions and joint development of the latest security systems.

Despite significant prospects, Ukraine faces numerous challenges. This includes instability of domestic funding and insufficient legal framework to support innovation. For example, the lack of uniform standards and regulations in the field of blockchain solutions complicates their implementation at the national level. In addition, the need for harmonisation with international law requires time and considerable resources. However, cooperation with international partners allows to overcome these barriers, gradually strengthening the cyber defence of critical facilities in the country. Table 2 shows Ukraine's international cooperation in the implementation of blockchain technologies for cybersecurity of critical infrastructure.

Table 2. International cooperation of Ukraine in the implementation of blockchain technologies for cybersecurity of critical infrastructure

Country	Area of cooperation	Prospects	Challenges
USA	Exchange of experience, training of experts, support of Ukrainian initiatives	Access to innovative solutions, joint projects in the field of cybersecurity	Unstable political situation in Ukraine, restrictions on funding
EU	Technological assistance, implementation of blockchain solutions for public administration	Use of Estonia's best practices, integration with European standards	Differences in legislation and infrastructure readiness levels
Israel	Joint research in the field of cybersecurity, exchange of analytical data on threats	Development of advanced technologies to protect critical systems	Maintaining a stable level of security in the face of global threats
Poland	Development of regional cooperation programmes in the field of cybersecurity of critical infrastructure	Strengthening regional security, creating compatible solutions for blockchain platforms	Lack of a unified system of standards in the region

Source: developed by the authors based on Israel and Ukraine face shared cyber threats (2023), Joint Statement on the United States-European Union 9th Cyber Dialogue in Brussels (2023)

Ukraine has a significant potential for using blockchain technologies in cybersecurity, because these technologies provide decentralised, transparent, and reliable data exchange. Due to partnership with leading countries in this area, such as the United States and Israel, Ukraine gets access to the latest solutions. In particular, the use of blockchain can improve the protection of state registers, monitor data in real time, and optimise the management of critical infrastructure. The integration of these technologies helps to ensure the continuity of systems even during cyber-attacks, which is a key task for the country in modern conditions.

An important aspect is the development of the regulatory framework for blockchain implementation. Ukraine is actively working to harmonise its laws with international standards, which makes it possible to simplify cooperation with other countries. For example, the adoption of laws on digital assets and regulation of blockchain technologies creates a favourable environment for attracting foreign investment and technology. Moreover, it helps to increase the level of trust in Ukrainian cybersecurity projects.

However, to achieve success, it is necessary to overcome significant challenges. Ukraine needs more funding for the development of blockchain infrastructure and training of specialists in this field. In addition, it is necessary to strengthen cooperation with regional partners, such as Poland, to create common protection systems. Strengthening these relations and utilising international experience will allow Ukraine to integrate blockchain into its systems and become one of the leaders in this field in Eastern Europe.

DISCUSSION

Ensuring the cybersecurity of critical infrastructure is crucial for preventing economic losses, social consequences, and threats to national security. The presented results confirm that the integration of conventional approaches with modern technologies, such as blockchain, allows creating more effective security systems. The main elements of multi-level protection are firewalls, IDS/IPS systems, antivirus software, and data encryption tools. Despite their basic effectiveness, such methods are not always able to counteract complex attacks, such as APT or zero-day attacks. Centralised architectures often face problems handling large amounts of data, which makes it difficult to detect threats in real time. K. Yu *et al.* (2021) investigated the effectiveness of conventional methods of protecting critical infrastructure, in particular the use of multi-level security systems. Their results confirm that firewalls and IDS/IPS provide a basic level of protection, but are not always effective against modern threats, such as zero-day attacks. This is consistent with current results, but the researchers emphasise a greater reliance on the human factor in incident response, which was not the main focus of the current study. This creates the need to introduce new technologies to improve security efficiency. N. Chowdhury & V. Gkioulos (2021) investigated the effectiveness of conventional critical infrastructure security tools, such as multi-level security systems. They noted that while firewalls and IDS/IPS provide a basic level of protection, they are not always effective enough against the latest threats, especially zero-day attacks. This correlates with current results, but the researchers emphasise the greater role of the human factor in Incident Response, which was not the main focus of this study. This highlights the need to introduce innovative technologies to improve the effectiveness of protection.

C. Große *et al*. (2021) conducted a study of conventional approaches to protecting critical infrastructure, in particular, the use of firewalls, IDS/IPS systems, and antivirus software. They note that while these methods provide a basic level of protection, they are not effective enough to deal with more complex threats, such as APT or zero-day attacks. In addition, centralised architectures face difficulties when processing large amounts of data, which makes it difficult to quickly detect threats. The researchers also emphasise that the human factor plays an important role in responding to incidents, which increases the need to introduce new technological solutions to improve security. The current results describe in more detail the practical implementation of blockchain technologies in Ukraine, in particular, in the energy, healthcare, and transport sectors, and focus on international cooperation.

Blockchain technologies offer a decentralised approach to data storage and management, which significantly increases their resistance to cyber-attacks. The immutability of data in the blockchain creates a high level of integrity and transparency, which is critical for monitoring and managing access to information systems. D. Berdik *et al*. (2021) investigated cybersecurity and blockchain technologies, namely, the use of blockchain to ensure the protection of information systems in real time. They focused on the benefits of a decentralised approach to data storage and management, improving the integrity and transparency of information, and automating access processes through smart contracts. The implementation of the blockchain allows automating access processes using smart contracts that ensure the accuracy of meeting specified conditions. The current results also identified the advantages of a decentralised architecture, in particular, in the context of reducing the risks of attacks on a single data storage point, which coincides with the authors' results. However, the current study focuses more on the use of blockchain specifically for critical infrastructure, while the researchers focus more on general aspects of cybersecurity.

The main challenges remain high implementation costs, the need for significant computing resources, and unresolved compatibility issues with existing systems. In addition, the regulation of blockchain technologies in many countries is still at an early stage, which can make it difficult to integrate them into critical infrastructure. Performance limitations of blockchain systems, such as slow transaction processing, also affect their applicability in large-scale systems with high speed requirements. I. Tibrewal *et al*. (2022) analysed the use of blockchain technologies in critical infrastructure. They argued that the main advantage is transparency and the inability to change data, but noted that blockchain is too expensive and difficult to implement in small organisations. This is consistent with current findings, although the researchers do not focus on scalability issues, which are considered critical in the current paper. T.R. Vance & A. Vance (2019) investigated the application of blockchain technologies in critical infrastructure, focusing on their ability to provide transparency and protect data from changes. However, they also emphasised the high cost and complexity of integrating these technologies into small organisations. This is consistent with the current results, but the researchers did not address the scalability issues that are key in the current study. M.K. Hasan *et al*. (2022) investigated the implementation of blockchain technologies in the field of protecting critical infrastructure, paying attention to their ability to guarantee data openness and protection against unauthorised changes. However, they noted that the significant costs and complexity of implementation limit the use of these technologies in small organisations. In contrast to this approach, the current paper focuses on scalability, which is crucial for a successful blockchain application.

The success of using a blockchain largely depends on its ability to process large amounts of data in real time. Second-tier technologies, such as the Lightning Network or sharding, offer solutions to reduce the load on the underlying blockchain. Replacing the Proof-of-Work consensus mechanism with Proof-of-Stake reduces energy costs and improves productivity. C.T. Nguyen *et al*. (2019) investigated the performance of blockchain systems and proposed the use of hybrid approaches, such as Proof-of-Stake. They concluded that these methods can significantly improve the speed of real-time transaction processing. The current study also considered this approach, but focused more on implementation issues due to the complexity of settings and compatibility with existing systems. However, critical infrastructure requires careful testing of these solutions to ensure that they are resistant to new types of attacks.

M. Warkentin & C. Orgeron (2020) explored the legal aspects of implementing blockchain technologies in developing countries, in particular, in the context of national security. They noted that insufficiently regulated legislation creates serious barriers to the widespread adoption of these technologies in critical infrastructure. This coincides with the current conclusions, which pointed out the need to develop a regulatory framework for regulating the use of blockchain. However, the researchers focused more on the legal aspects, while the current study focused on the technical and economic problems of implementation. R. Zambrano (2020) considered the legal challenges that arise when implementing blockchain technologies in developing countries, with a focus on national security. He emphasised that the lack of developed legislation is a serious barrier to the integration of blockchain into critical infrastructure, as countries must create appropriate regulations for the successful implementation of these technologies. The current results focused more on the severity of the barriers created by insufficient legislative development, while the researcher focused on the fact that countries should create the necessary regulations for the implementation of technologies.

Ensuring the cybersecurity of critical infrastructure requires combining traditional approaches with modern technologies, such as blockchain, to create more sustainable and effective security systems. The analysis shows that although conventional methods provide a basic level of security, their limitations in countering modern threats, centralised architecture and dependence on the human factor emphasise the need for innovative solutions. Blockchain shows significant potential through transparency, data immutability, and decentralisation, but its integration into critical infrastructure faces scalability, cost, and compatibility challenges. Effective application of these technologies requires both technological improvement and adaptation of the regulatory framework.

CONCLUSIONS

In the course of the study, a comprehensive analysis of modern approaches to ensuring cybersecurity of critical infrastructure facilities was carried out, with an emphasis on the integration of blockchain technologies. It was established that ensuring cybersecurity is a key task for preventing economic losses, social consequences, and potential threats to national security. Conventional methods, such as multi-level security systems using firewalls, IDS/IPS systems, antivirus software, and data encryption tools, provide a basic level of protection. However, their effectiveness is often limited in the face of complex attacks, such as zero-day attacks or APTs. Centralised data management systems have also been vulnerable to scalability and real-time issues.

With the development of technology, it became possible to implement the latest solutions, in particular, based on machine learning, artificial intelligence, and blockchain technologies. Blockchain allows creating decentralised data storage and management systems, which ensures their integrity, transparency and increases resistance to cyber-attacks. In particular, the technology has found application in access control, monitoring and detecting threats, and in maintaining the history of changes and transactions. However, the introduction of blockchain is accompanied by challenges. These include high implementation costs, significant computing resource requirements, compatibility issues with existing systems, and limited transaction processing speed in large-scale systems. It was noted that solutions such as multi-layer architectures, sharding, and hybrid consensus mechanisms are being actively developed to overcome these limitations.

The analysis revealed that the integration of blockchain technologies into the critical infrastructure of Ukraine has significant potential. The implementation of pilot projects in the fields of energy, transport, healthcare, and finance confirmed the effectiveness of blockchain in the fight against cyber threats, corruption, and inefficiency. In particular, blockchain helped to increase the level of data protection, reduce transaction processing time, and increase the transparency of processes. Limitations of the study were the complexity of fully evaluating the effectiveness of blockchain technologies due to the lack of large-scale practical implementations and limited data on their impact on real cyber threats. Further research should focus on developing solutions to improve the scalability and performance of the blockchain, and adapting these technologies to the specifics of critical infrastructure.

ACKNOWLEDGEMENTS

None.

CONFLICT OF INTEREST

None.

REFERENCES

[1] Ali, A., Ali, H., Saeed, A., Ahmed Khan, A., Tin, T.T., Assam, M., Ghadi, Y.Y., & Mohamed, H.G. (2023). Blockchain-powered healthcare systems: Enhancing scalability and security with hybrid deep learning. *Sensors*, 23(18), article number 7740. doi: 10.3390/s23187740.

[2] Barka, E., Kerrache, C.A., Benkraouda, H., Shuaib, K., Ahmad, F., & Kurugollu, F. (2022). Towards a trusted unmanned aerial system using blockchain for the protection of critical infrastructure. *Transactions on Emerging Telecommunications Technologies*, 33(8), article number e3706. doi: 10.1002/ett.3706.

[3] Berdik, D., Otoum, S., Schmidt, N., Porter, D., & Jararweh, Y. (2021). A survey on blockchain for information systems management and security. *Information Processing & Management*, 58(1), article number 102397. doi: 10.1016/j.ipm.2020.102397.

[4] Chowdhury, N., & Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, 40, article number 100361. doi: 10.1016/j.cosrev.2021.100361.

[5] Große, C., Olausson, P.M., & Wallman-Lundåsen, S. (2021). Left in the dark: Obstacles to studying and performing critical infrastructure protection. *Electronic Journal of Business Research Methods*, 19(2), 58-70. doi: 10.34190/ejbrm.19.2.2509.

[6] Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. (2022). Blockchain technology: Benefits, challenges, applications, and integration of blockchain technology with cloud computing. *Future Internet*, 14(11), article number 341. doi: 10.3390/fi14110341.

[7] Hasan, M.K., Alkhalifah, A., Islam, S., Babiker, N.B.M., Habib, A.K.M.A., Aman, A.H.M., & Hossain, M.A. (2022). Blockchain technology on smart grid, energy trading, and big data: Security issues, challenges, and recommendations. *Wireless Communications and Mobile Computing*, 2022(1), article number 9065768. doi: 10.1155/2022/9065768.

[8] Horner, J., & Ryan, P. (2019). Blockchain standards for sustainable development. *Journal of ICT Standardization*, 7(3), 225-248. doi: 10.13052/jicts2245-800X.733.

[9] Implementation of blockchain technology in healthcare in 2023. (2023). Retrieved from https://stfalcon.com/uk/blog/post/implementation-of-blockchain-technology-in-healthcare.

[10] Iskryzhytskii, A., & Zadorozhnii, A. (2024). Study of available methods and technologies for decentralized storing and administration of public data. *Technical Sciences and Technologies*, 2(36), 137-150. doi: 10.25140/2411-5363-2024-2(36)-137-150.

[11] Israel and Ukraine face shared cyber threats. (2023). Retrieved from https://www.fdd.org/analysis/2023/11/13/israel-and-ukraine-face-shared-cyber-threats/.

[12] Joint Statement on the United States-European Union 9th Cyber Dialogue in Brussels. (2023). Retrieved from https://surl.li/ooyrtk.

[13] Kobets, D., & Runov, O. (2024). Integration of blockchain technologies in the personnel potential management system of medical institutions. *Innovation and Sustainability*, 4(1), 112-119. doi: 10.31649/ins.2024.1.112.119.

[14] Koh, L., Dolgui, A., & Sarkis, J. (2020). Blockchain in transport and logistics – paradigms and transitions. *International Journal of Production Research*, 58(7), 2054-2062. doi: 10.1080/00207543.2020.1736428.

[15] Košťál, K., Helebrandt, P., Belluš, M., Ries, M., & Kotuliak, I. (2019). Management and monitoring of IoT devices using blockchain. *Sensors*, 19(4), article number 856. doi: 10.3390/s19040856.

[16] Kozhemiakin, S. (2023). *Blockchain in Ukraine is used at the state level: 4 main areas are named*. Retrieved from https://hub.obozrevatel.com/ukr/blokchejn-dlya-ukraintsiv-yak-zastosue-kriptotehnologiyu-mintsifru.htm.

[17] Mohamed, N., & Ahmed, A.A. (2024). AI in combatting man-in-the-middle attacks: A comprehensive review. In *Proceedings of the 15th international conference on computing communication and networking technologies* (pp. 1-6). Kamand: IEEE. doi: 10.1109/ICCCNT61001.2024.10725789.

[18] Nasir, M.H., Arshad, J., Khan, M.M., Fatima, M., Salah, K., & Jayaraman, R. (2022). Scalable blockchains – a syste matic review. *Future Generation Computer Systems*, 126, 136-162. doi: 10.1016/j.future.2021.07.035.

[19] Nguyen, C.T., Hoang, D.T., Nguyen, D.N., Niyato, D., Nguyen, H.T., & Dutkiewicz, E. (2019). Proof-of-stake consensus mechanisms for future blockchain networks: Fundamentals, applications and opportunities. *IEEE Access*, 7, 85727-85745. doi: 10.1109/ACCESS.2019.2925010.

[20] Pacheco, M., Oliva, G., Rajbahadur, G.K., & Hassan, A. (2023). Is my transaction done yet? An empirical study of transaction processing times in the Ethereum blockchain platform. *ACM Transactions on Software Engineering and Methodology*, 32(3), article number 59. doi: 10.1145/3549542.

[21] Pournader, M., Shi, Y., Seuring, S., & Koh, S.C.L. (2020). Blockchain applications in supply chains, transport and logistics: A systematic review of the literature. *International Journal of Production Research*, 58(7), 2063-2081. doi: 10.1080/00207543.2019.1650976.

[22] Radvanovsky, R., & McDougall, A. (2023). *Critical infrastructure: Homeland security and emergency preparedness*. Boca Raton: CRC Press. doi: 10.4324/9781003346630.

[23] Safitra, M.F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, 15(18), article number 13369. doi: 10.3390/su151813369.

[24] Semenenko, O., Nozdrachov, O., Chernyshova, I., Melnychenko, A., & Momot, D. (2024). Innovative technologies to improve energy efficiency and security of military facilities. *Machinery & Energetics*, 15(4), 147-156. doi: 10.31548/machinery/4.2024.147.

[25] Shapovalova, N., Dotsenko, I., Trachuk, A., & Skrynnikov, I. (2024). Applying artificial intelligence tools for time series analysis. *Journal of Kryvyi Rih National University*, 22(1), 46-51. doi: 10.31721/2306-5451-2024-1-58-46-52.

[26] Shevchuk, M., Zhulinskyi, M., Kupchok, V., Mykhailiv, A., & Kukoreno, M. (2024). Using blockchain technology to increase the efficiency of energy industry enterprises. *Scientific Notes of Lviv University of Business and Law*, 40, 704-709. doi: 10.5281/zenodo.10637407.

[27] Smith, K.J., & Dhillon, G. (2020). Assessing blockchain potential for improving the cybersecurity of financial transactions. *Managerial Finance*, 46(6), 833-848. doi: 10.1108/MF-06-2019-0314.

[28] Tibrewal, I., Srivastava, M., & Tyagi, A.K. (2022). Blockchain technology for securing cyber-infrastructure and internet of things networks. In A.K. Tyagi, A. Abraham & A. Kaklauskas (Eds.), *Intelligent interactive multimedia systems for e-healthcare applications* (pp. 337-350). Singapore: Springer. doi: 10.1007/978-981-16-6542-4_17.

[29] Ullah, Z., Al-Turjman, F., Mostarda, L., & Gagliardi, R. (2020). Applications of artificial intelligence and machine learning in smart cities. *Computer Communications*, 154, 313-323. doi: 10.1016/j.comcom.2020.02.069.

[30] Vance, T.R., & Vance, A. (2019). Cybersecurity in the blockchain era: A survey on examining critical infrastructure protection with blockchain-based technology. In *Proceedings of the IEEE international scientific-practical conference problems of infocommunications, science and technology* (pp. 107-112). Kyiv: IEEE. doi: 10.1109/PICST47496.2019.9061242.

[31] Wang, Q., & Su, M. (2020). Integrating blockchain technology into the energy sector – from theory of blockchain to research and application of energy blockchain. *Computer Science Review*, 37, article number 100275. doi: 10.1016/j.cosrev.2020.100275.

[32] Warkentin, M., & Orgeron, C. (2020). Using the security triad to assess blockchain technology in public sector applications. *International Journal of Information Management*, 52, article number 102090. doi: 10.1016/j.ijinfomgt.2020.102090.

[33] Wei, P., Wang, D., Zhao, Y., Sah Tyagi, S.K., & Kumar, N. (2020). Blockchain data-based cloud data integrity protection mechanism. *Future Generation Computer Systems*, 102, 902-911. doi: 10.1016/j.future.2019.09.028.

[34] Wisniewski, M., Gladysz, B., Ejsmont, K., Wodecki, A., & Van Erp, T. (2022). Industry 4.0 solutions impacts on critical infrastructure safety and protection – a systematic literature review. *IEEE Access*, 10, 82716-82735. doi: 10.1109/ACCESS.2022.3195337.

[35] Yu, K., Tan, L., Mumtaz, S., Al-Rubaye, S., Al-Dulaimi, A., Bashir, A.K., & Khan, F.A. (2021). Securing critical infrastructures: Deep-learning-based threat detection in IIoT. *IEEE Communications Magazine*, 59(10), 76-82. doi: 10.1109/MCOM.101.2001126.

[36] Zainuddin, A.A., Sairin, H., Mazlan, I.A., Muslim, N.N., & Wan Sabarudin, W.A.S. (2024). Enhancing IoT security: A synergy of machine learning, artificial intelligence, and blockchain. *Data Science Insights*, 2(1), 9-19.

[37] Zambrano, R. (2020). Taming the beast: Harnessing blockchains in developing country governments. *Frontiers in Blockchain*, 2, article number 27. doi: 10.3389/fbloc.2019.00027.

Інтеграція блокчейн-технологій у системи забезпечення кібербезпеки для об'єктів критичної інфраструктури: перспективи та виклики

Віктор Данчук

Доктор фізико-математичних наук, професор
Національний транспортний університет
01010, вул. М. Омеляновича-Павленка, 1, м. Київ, Україна
https://orcid.org/0000-0003-4282-2400

Марія Данчук

Кандидат економічних наук, доцент
Національний транспортний університет
01010, вул. М. Омеляновича-Павленка, 1, м. Київ, Україна
https://orcid.org/0009-0007-3033-3227

Анотація. Дослідження було спрямоване на аналіз потенціалу та основних проблем інтеграції блокчейн-технологій у процеси забезпечення кібербезпеки об'єктів критичної інфраструктури в Україні. У рамках роботи здійснювалися аналіз потенціалу блокчейн-технологій у підвищенні рівня захищеності критичних інфраструктур, оцінка існуючих викликів масштабування та продуктивності таких систем, а також вивчення можливостей міжнародної співпраці для впровадження інноваційних рішень у сфері кібербезпеки. У роботі проведено всебічний аналіз перспектив інтеграції блокчейн-технологій у системи забезпечення кібербезпеки для об'єктів критичної інфраструктури. Для забезпечення релевантності дослідження враховувалися технічні особливості блокчейну, такі як механізми консенсусу, моделі розподілу даних та криптографічні методи. Було виявлено, що блокчейн-технології забезпечують підвищення рівня прозорості, стійкості до кіберзагроз та оптимізацію управління доступом до критичних даних. Водночас основними викликами залишаються низька масштабованість систем, обмежена швидкість транзакцій і високі енергетичні витрати, що ускладнює їх широкомасштабне впровадження. Дослідження також показало, що існує потреба в адаптації регуляторних вимог для підвищення ефективності інтеграції блокчейну в інфраструктурні об'єкти. Дослідження продемонструвало значний потенціал блокчейн-технологій як одного з ключових компонентів у побудові стійких кібербезпекових систем. Висновки роботи акцентують на необхідності міждисциплінарного підходу до впровадження технологій, що включає технічні, економічні та регуляторні аспекти, для підвищення рівня захищеності об'єктів критичної інфраструктури в умовах зростання кіберзагроз. Крім того, у роботі підкреслено важливість міжнародної співпраці, яка дозволить об'єднати ресурси та експертизу для створення більш ефективних та інноваційних рішень у сфері кібербезпеки

Ключові слова: розподілені реєстри; управління даними; регуляторні аспекти; криптографія; цифрова довіра