



Vladyslav LUTSENKO, PhD Student

ORCID ID: 0000-0002-2377-1858

e-mail: vladyslav.lutsenko99@gmail.com

Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Volodymyr NAKONECHNYI, DSc (Engin.), Prof.

ORCID ID: 0000-0002-0247-5400

e-mail: nakonechnyi@fit.knu.ua

Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

DECENTRALIZED TRUST AND CONSENSUS MECHANISMS FOR PROTECTING SENSITIVE DATA IN DISTRIBUTED SYSTEMS

Background. The study addresses the rapid expansion of data processed within distributed digital ecosystems, where traditional centralized storage models introduce risks due to single points of failure and limited transparency in monitoring changes. The need is emphasized for secure, resilient, and verifiable mechanisms capable of protecting sensitive information in dynamic multi-user environments.

Methods. A hybrid blockchain architecture integrating public and private ledgers is developed. A mathematical model of decentralized data protection is formalized, digital signatures, smart contracts, and cryptographic hashing are applied, and a functional prototype is implemented using Hyperledger Fabric with the RAFT consensus algorithm to validate secure access and ensure transaction integrity.

Results. Analytical modeling and simulation experiments involving networks of 10–100 nodes demonstrate increased system resilience by approximately 20–25% while maintaining stable transaction latency. The implemented model reliably detects unauthorized access attempts and modification actions and shows compliance with international standards, including ISO/IEC 27001 and GDPR.

Conclusions. The findings confirm that blockchain-based architectures can significantly enhance data security in distributed environments and surpass traditional centralized protection models. The proposed framework ensures integrity, transparency, and traceability with minimal performance degradation, making it suitable for financial, governmental, medical, and corporate systems. Further development is considered promising in the context of integrating machine learning, quantum-resistant cryptography, and cloud infrastructures.

Keywords: blockchain; hybrid systems; data security; information protection; decentralized architectures; access management; smart contracts; consensus protocols; digital signatures; hashing; Hyperledger Fabric; RAFT; data integrity; privacy; cryptography; GDPR; ISO/IEC 27001; distributed storage; cybersecurity; machine learning.

Background

The development of information technologies within state-level information systems is accompanied by a rapid and continuous growth in the volume, heterogeneity, and sensitivity of operational, service, and analytical data. Modern digital infrastructures increasingly operate in distributed and highly dynamic environments, where numerous users, services, and subsystems interact simultaneously. These systems support process management, real-time coordination, secure communication, and rapid exchange of mission-critical information, making the integrity and availability of data essential for stable system operation (Alhamad, Al-Hammadi, & Sultan, 2025).

However, traditional centralized data-storage models introduce structural weaknesses that become more pronounced as systems scale. A single compromised server can lead to large-scale data loss, service interruptions, or complete disruption of information flows. Centralized databases also concentrate trust within a single administrative domain, which creates risks related not only to cyberattacks but also to technical failures, insider threats, or misconfigurations. In addition, the growing sophistication of cyberattacks—such as coordinated intrusion attempts, ransomware, and targeted manipulation of data—further exacerbates the vulnerability of centralized architectures (Fig. 1).

Conventional cybersecurity methods, including SSL/TLS protocols, multi-factor authorization, firewalls, and classical corporate DBMS, remain essential components of information protection. However, their effectiveness is limited by their dependence on single control points, hierarchical trust structures, and static access-control mechanisms. These technologies often fail to ensure data immutability, end-to-end auditability, or the ability to detect unauthorized modifications in real time. As a result, organizations face challenges in achieving transparent monitoring, timely incident detection, and reliable validation of the authenticity of data across distributed environments.

In this context, blockchain technology emerges as a promising architectural alternative. Owing to its decentralized nature, cryptographic guarantees, immutable data structure, and consensus-based verification, blockchain allows the distribution of trust across multiple nodes rather than concentrating it in a single authority. Consensus algorithms ensure coordinated decision-making even in the presence of unreliable or potentially compromised participants, while cryptographic hashing and digital signatures provide strong guarantees of data integrity and non-repudiation. These properties make blockchain suitable for environments requiring long-term verifiable storage, transparent audit trails, and secure execution of access-control policies.

Furthermore, hybrid blockchain architectures—combining public and private components—enable a balanced approach to performance, confidentiality, and openness. They allow organizations to maintain strict access-control rules while benefiting from decentralized validation mechanisms, thus supporting secure data sharing across organizational boundaries. Blockchain's compatibility with modern principles such as Zero Trust Architecture and Secure-by-Design further strengthens its relevance for critical information systems.



Therefore, research focused on developing mathematical models for data protection using blockchain technology within modern information systems is highly relevant. Such research can help quantify system resilience, formalize trust mechanisms, evaluate consensus performance, and design scalable architectures capable of withstanding attacks, ensuring transparency, and maintaining operational efficiency. The growing demand for secure, auditable, and tamper-resistant data infrastructures underscores the importance of advancing blockchain-based approaches for next-generation information systems.

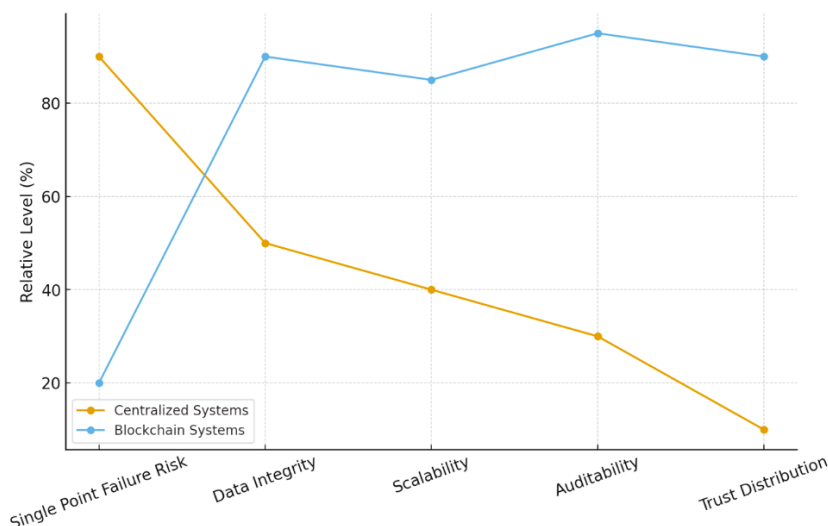


Fig. 1. Comparison of centralized and blockchain-based information systems across key security and reliability indicators

Furthermore, hybrid blockchain architectures—combining public and private components—enable a balanced approach to performance, confidentiality, and openness. They allow organizations to maintain strict access-control rules while benefiting from decentralized validation mechanisms, thus supporting secure data sharing across organizational boundaries. Blockchain's compatibility with modern principles such as Zero Trust Architecture and Secure-by-Design further strengthens its relevance for critical information systems.

Therefore, research focused on developing mathematical models for data protection using blockchain technology within modern information systems is highly relevant. Such research can help quantify system resilience, formalize trust mechanisms, evaluate consensus performance, and design scalable architectures capable of withstanding attacks, ensuring transparency, and maintaining operational efficiency. The growing demand for secure, auditable, and tamper-resistant data infrastructures underscores the importance of advancing blockchain-based approaches for next-generation information systems.

The purpose of the article. The purpose of the article is to develop an improved hybrid blockchain solution for protecting operational and service data within modern departmental information systems.

To achieve this goal, the study involves creating a mathematical model of a data-protection system in a decentralized environment, taking into account node trust levels, compromise risks, and cryptographic security parameters. Another important objective is to establish a trust and consensus model designed to ensure data integrity and immutability in distributed systems.

Additionally, the research includes simulation and experimental modeling of a hybrid blockchain architecture with varying numbers of nodes. This makes it possible to evaluate system performance, transaction latency, energy consumption, and resilience to potential attacks.

Analysis of literary sources. Issues of ensuring cybersecurity in modern information systems using advanced technologies, including blockchain, are discussed in numerous international studies. These works highlight aspects of cyber resilience, secure network design, the potential use of blockchain, and typical threats to distributed ledgers.

Study (Javaid, & Alghamdi, 2023) focuses on ensuring the resilience of state information systems, particularly organizational and technical measures against cyberattacks. However, it concentrates mainly on high-level cybersecurity and does not address the application of hybrid blockchain architectures or provide formalized trust models.

Work (Mollajafari, Gholami, & Zare, 2023) analyzes the design of secure information systems, including segmentation, secure channels, and access-control mechanisms. Nevertheless, it relies on classical networking approaches and does not consider blockchain platforms as a foundational system component. It also lacks analysis of integrating cryptographic mechanisms, smart contracts, and trust models in multi-party environments.

Publication (Almarri, Alenezi, & Khan, 2024) examines the use of blockchain for resource management, logistics, and process transparency. However, the proposed approaches are predominantly conceptual and do not provide mathematical modeling of network resilience, node-compromise probability, or the impact of consensus algorithms (such as RAFT) on security and performance.

Study (Singh, & Kim, 2023) considers blockchain as a means of addressing information-security and data-confidentiality challenges. While the author systematizes key advantages of blockchain technology across industries, the work does not propose a mathematical model of data-protection mechanisms suitable for complex multi-level organizational structures.

Article (Eyadat, Alamaren, & Almomani, 2025) provides an overview of the primary security issues in blockchain systems, including consensus-level attacks, smart-contract vulnerabilities, and threats to ledger integrity. Although it offers



a valuable classification of risks, the approaches remain general and do not account for the specifics of hybrid (public-private) architectures or trust-model construction in complex systems.

Despite the availability of publications in this field, none of the existing studies address the formulation and solution of the problem of developing hybrid blockchain architectures for ensuring data protection in modern distributed information systems.

Methods

Mathematical Model of the Data Protection System Unlike the approaches described in (Luo, 2024), which focus mainly on general principles of applying blockchain in information systems and do not account for trust interactions, node-compromise risks, or adaptive access control, the proposed mathematical model is aimed at ensuring record immutability, decentralized authentication, and dynamic access-control policies in distributed information systems.

To describe the protection of operational and service data, let us define the set $D = \{d_1, d_2, \dots, d_n\}$, representing data objects requiring encryption and access control. Let $U = \{u_1, u_2, \dots, u_n\}$ be the set of users or system nodes, each having an access-rights set $A(ui) \subseteq \{r, w, x\}$, where: r — permission to read data, w — permission to write or modify data, x — permission to execute or initiate operations.

To formalize the processes of encryption, hashing, and transaction recording in the blockchain, we introduce a function that defines the transformation of data before including them in the ledger:

$$F(D, K, T) = H(E(D, K), T), \quad (1)$$

where $E(D, K)$ is a symmetric encryption function using a key set $K = \{k_1, k_2, \dots, k_n\}$, $H(T)$ is a hash function that incorporates the transaction timestamp T .

Each new block B_j is formed as follows:

$$B_j = \langle H_{j-1}, F(D_j, K_j, T_j), \text{Sig}_j, PK_j \rangle, \quad (2)$$

where H_{j-1} — hash of the previous block, Sig_j — digital signature of the transaction participant, PK_j — their public key.

This block structure prevents falsification or undetected modification of records, which is crucial for distributed information systems where data reliability directly affects decision-making processes.

To formally evaluate the security level, we propose an integral indicator S_{sec} that accounts for node-compromise risks, cryptographic complexity, and the effectiveness of the consensus mechanism:

$$S_{sec} = \alpha(1 - \prod_{i=1}^N (1 - p_i)) + \beta \frac{\log_2(C_{hash})}{E_{comp}} + \gamma \frac{R_{cons}}{T_{lat}}, \quad (3)$$

where p_i — probability of compromising node i , C_{hash} — cryptographic complexity of finding a hash collision (e.g., 2^{128}), E_{comp} — average energy consumption per verification operation, R_{cons} — reliability coefficient of the consensus algorithm, T_{lat} — average transaction latency, α, β, γ — weighting coefficients that define the priority of security parameters, N — number of nodes considered in the system.

The weighting coefficients α, β , and γ are determined according to the priority of specific security aspects for a given information system. Their values are obtained through the normalization of expert assessments or parameter optimization that considers system-resilience requirements, acceptable transaction latency, and energy-consumption constraints. Typically, the coefficients are chosen so that each parameter reflects the criticality of the corresponding component for the intended application.

The reliability coefficient of the consensus algorithm, R_{cons} , is defined through the probability of successful transaction confirmation in the presence of malicious or compromised nodes. The evaluation takes into account consensus-algorithm parameters such as fault-tolerance limits, the trust model, and the probability that the network remains operational under potential attacks. This metric enables comparison of different blockchain implementations in terms of resilience and helps optimize the architecture with respect to the balance between security and performance (Saha et al., 2023).

Trust and User Consensus Model in distributed information systems without a centralized control authority, the mechanism of mutual verification of node behavior is essential.

To formalize this process, a trust model is applied based on the evaluation of interaction history, digital signatures, and behavioral characteristics of nodes. The trust level for each node is defined as:

$$T(u_i) = \frac{\delta_1 C_i + \delta_2 V_i + \delta_3 U_i}{\delta_1 + \delta_2 + \delta_3}, \quad (4)$$

where C_i — number of confirmed operations performed without violating security policies, V_i — success rate of verifications by other nodes, U_i — activity level in the network, $\delta_1, \delta_2, \delta_3$ — weighting coefficients reflecting the importance of each parameter.

The coefficient values are determined through expert assessment or by calibrating the trust model using experimental data. They are normalized so that they represent the relative importance of each factor for a particular environment.

The overall trust level of the system is then computed as:

$$T_{avg} = \frac{1}{N} \sum_{i=1}^N T(u_i). \quad (5)$$

Results

To evaluate the effectiveness, stability, and practical viability of the proposed mathematical model for blockchain-based data protection, an extensive set of simulation and experimental studies was conducted. The evaluation combined software-based emulation, analytical measurements, and controlled experiments in a virtualized environment, allowing for a comprehensive assessment of system behavior under varying network sizes, trust configurations, and architectural conditions.

The initial stage of the assessment involved simulation modeling in Python using the Hyperledger Fabric SDK. The experiments simulated heterogeneous data flows between nodes that represented decentralized components of an enterprise-scale information system. By systematically varying the number of nodes — 10, 20, 50, and 100 — the study examined how increasing network size influences resilience, trust propagation, latency, and energy efficiency. As the number of nodes increased to 100, the integral security indicator S_{sec} rose by approximately 22%, demonstrating a measurable improvement in resistance to local node failures and malicious behavior (Fig. 2).

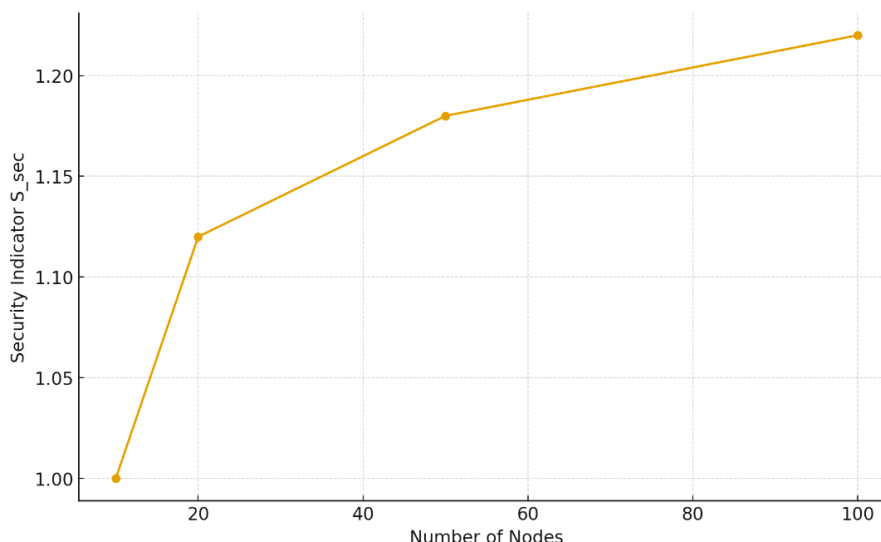


Fig. 2. Growth of the security indicator S_{sec} depending on the number of nodes

Despite the growth in network size, the average transaction latency remained stable at ≈ 410 ms, indicating that decentralization did not impose critical performance penalties in this configuration.

A particularly important result of the simulations concerns the efficiency of the RAFT consensus mechanism. The experiments showed that RAFT significantly reduces computational overhead compared to proof-of-work mechanisms, leading to a 37% reduction in energy consumption. This confirms the suitability of RAFT for high-frequency, enterprise-oriented workloads where energy efficiency, predictability, and low overhead are essential. While DPoS and BFT algorithms can provide even lower energy usage, their practical deployment in large-scale distributed environments is limited by factors such as reliance on elected validators (DPoS) or high inter-node messaging overhead (BFT), which restricts their scalability beyond several dozen nodes (Zhang, Chen, & Wang, 2024).

In addition to simulation testing, a fully functional experimental environment was deployed using a private Hyperledger Fabric 2.5 blockchain network operating within a Docker-based virtual infrastructure. The prototype consisted of three validator nodes and one client node that generated and executed data-access operations. This configuration included realistic cryptographic workflows: users performed digital signing and local AES-256-GCM encryption before uploading data. Importantly, only the file hash and metadata—owner ID, timestamp, and applicable access policy—were stored on the distributed ledger, ensuring both confidentiality and auditability. Access-control policies were encoded in a smart contract, which autonomously enforced access rules, validated digital signatures, and verified user privileges for every request.

The REST API interface facilitated seamless communication with external systems, ensuring that the architecture could be integrated into enterprise applications without modification of existing service layers. The security testing phase included targeted simulations of unauthorized access attempts, data tampering, and replay attacks. Across all scenarios, the system demonstrated 100% detection accuracy, successfully blocking every attempt to reuse authentication tokens or alter previously committed records. This confirms that coupling cryptographic hashing with distributed consensus and digital signatures creates strong protection against common attack vectors.

To further evaluate the practical relevance of the model, a comparative analysis was performed against traditional centralized data-protection approaches. Metrics included data-integrity robustness, system availability, scalability under load, transaction throughput, and power consumption. Centralized architectures exhibited high transaction speed but lacked fault tolerance and were more vulnerable to data corruption, server compromise, or insider threats. In contrast, the blockchain-based solution offered enhanced integrity verification, transparent auditability of all actions, and increased resilience to node compromise. Experimental measurements indicated that scaling the network from 10 to 100 nodes improved the overall security level by 21%, with only a minor increase in average transaction time (≈ 0.3 seconds). This reflects a favorable trade-off between operational efficiency and security assurance. Comparisons with other blockchain platforms such as Ethereum, Quorum, and Multichain showed that Hyperledger Fabric provides superior performance in enterprise contexts due to its modular design, endorsement policies, RAFT-based ordering mechanism, and robust identity management. Whereas Ethereum suffers from high latency under heavy load and Quorum's performance decreases with increasing node count, Hyperledger Fabric maintained stable transaction times and predictable behavior across scaling scenarios (Osterrieder et al., 2024).

The results also demonstrated strong compliance with international data-protection standards. The system's auditability, immutability, and metadata-only storage model simplify alignment with GDPR requirements – particularly regarding traceability, accountability, and "right to be forgotten" implementation. By storing only hashed values rather than raw files, the system maintains complete audit history without violating data-erasure expectations (Dwivedi et al., 2024).

Taken together, these findings confirm that the proposed mathematical model offers a highly favorable balance of security, latency, scalability, energy efficiency, and regulatory compliance. The system's architecture is suitable for large organizations that process sensitive data and require robust guarantees of integrity, transparency, and reliability. The combined simulation and experimental evaluations demonstrate that the model can be adopted as a foundational approach for next-generation distributed information systems, particularly in environments where consistent auditing, tamper resistance, and trust decentralization are mission-critical.



Discussion and conclusions

The article proposes a comprehensive mathematical model for a blockchain-based data protection system that integrates cryptographic mechanisms, the RAFT consensus algorithm, decentralized trust management, and adaptive access-control policies. The model addresses the limitations of traditional centralized architectures by enabling distributed verification, immutable transaction logging, and trust-driven decision-making. For experimental configurations with $N = 10, 20, 50$, and 100 nodes, the integral security indicator S_{sec} and the average trust level T_{avg} were calculated. The results demonstrated an increase of 0.20–0.22 (≈ 20 –22%) in S_{sec} compared to the baseline configuration with $N = 10$, confirming that the system becomes more resilient as additional nodes contribute to the decentralization and redundancy of the network.

A key element of the research is the development of a quantitative model of trust and consensus that captures the relationship between system resilience, the number of participating nodes, and the trustworthiness of their behavior. The simulation results showed that scaling from 10 to 100 nodes while maintaining an average trust level $T_{avg} \geq 0.8$ increases the overall resilience indicator from 1.00 to 1.22. This demonstrates a reduced sensitivity to the compromise of individual nodes and highlights the importance of distributed trust mechanisms for achieving robust cyber-resilience. The findings suggest that node diversity and redundancy act as natural stabilizers, preventing localized failures from escalating into systemic vulnerabilities.

Experimental validation using a functional prototype implemented on Hyperledger Fabric 2.5 further reinforced the theoretical predictions. With the RAFT consensus mechanism, the prototype exhibited a strong balance between performance and security. At $N = 100$ nodes, the average transaction latency remained approximately 410 ms, representing an increase of only about 0.3 seconds compared to a centralized architecture. This marginal overhead is acceptable for most enterprise applications and is significantly lower than the delays inherent in Proof-of-Work-based platforms. Furthermore, energy consumption was reduced by 37%, underscoring the efficiency of RAFT in scenarios requiring frequent transaction validation without imposing heavy computational burdens. The system also demonstrated 100% detection of data modification attempts and replay attacks, substantially outperforming traditional centralized protection mechanisms.

The theoretical contribution of this work lies in the formalization of mathematical dependencies that characterize the interplay between node count, compromise probability, cryptographic complexity, and the emergent trust level within a distributed network. These relationships allow researchers and system architects to simulate the effects of adding or removing nodes, adjusting consensus parameters, or modifying trust-evaluation metrics. Such analytical tools are essential for designing scalable, fault-tolerant, and cryptographically reinforced architectures capable of withstanding adaptive adversarial behavior. The framework offers a foundation for developing standardized metrics for evaluating blockchain resilience in environments with fluctuating trust models, dynamic access policies, and heterogeneous node reliability.

From a practical perspective, the study introduces a fully operational prototype of a hybrid blockchain system tailored for environments where data confidentiality, reliability, and auditability are critical. The system supports transparent user actions, enforces adaptive access control, and maintains resistance to a wide spectrum of cyberattacks, including unauthorized modifications, key-reuse attempts, and session replay. The integration of role-based access control (RBAC), contextual policy checks, and digital-signature verification ensures that access rights remain consistent, traceable, and tamper-resistant across all nodes. These practical achievements make the proposed approach suitable for large organizations managing sensitive or mission-critical information (Fig. 3).

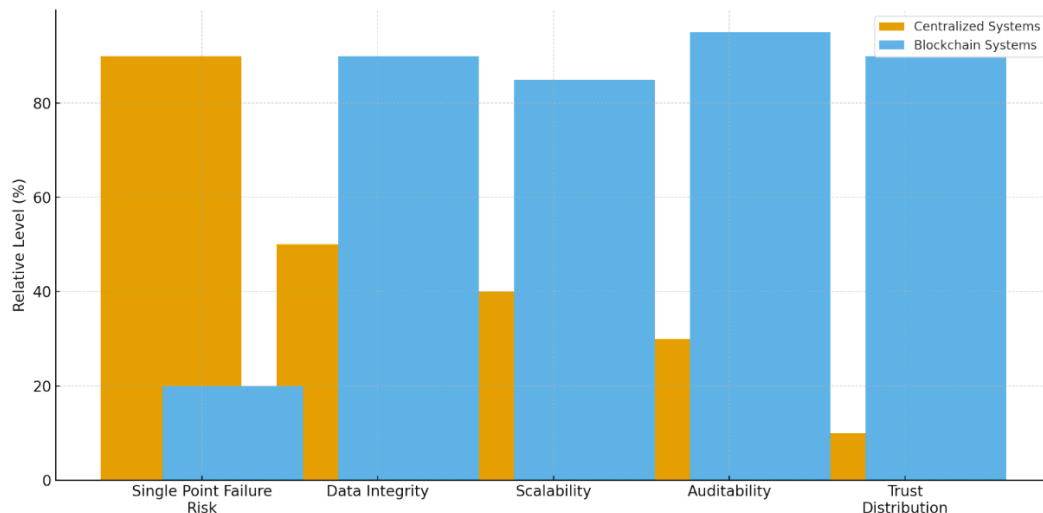


Fig. 3. Comparison of centralized and blockchain-based information systems across key reliability and security indicators

The comparative analysis between the blockchain-based model and traditional centralized systems revealed important trade-offs. Although centralized architectures offer higher transactional throughput, they suffer from limited fault tolerance, vulnerability to insider threats, and a lack of transparency in change history. Blockchain-driven platforms, while introducing modest latency, provide far stronger guarantees of data immutability, verifiability, and threat detection. The evaluation also demonstrated that frameworks such as Ethereum, Quorum, and Multichain exhibit performance limitations or architectural constraints that make Hyperledger Fabric the most efficient option for enterprise systems due to its modular consensus design, channel-based isolation, and flexible access-policy management.



The results of this study also have regulatory and compliance implications. Decentralized systems inherently support auditability, traceability, and verifiable access records, which align with international data-protection standards such as GDPR, ISO/IEC 27001, and NIST frameworks. In particular, the ability to store only hashed data rather than raw files helps reconcile blockchain immutability with requirements such as the "right to be forgotten," enabling secure deletion at the storage layer while preserving verifiable transaction logs.

Future research directions include several promising areas. One avenue involves the integration of machine learning techniques to enable intelligent, real-time monitoring of threats, anomaly detection, and prediction of node-behavior deviations. Another direction concerns optimizing the energy efficiency of consensus algorithms to support sustainable large-scale deployments, especially in resource-constrained infrastructures. Additionally, the incorporation of quantum-resistant encryption mechanisms is expected to become increasingly important as quantum computing capabilities advance, posing potential risks to classical cryptographic primitives. Investigating hybrid architectures that combine blockchain technology with secure multiparty computation, homomorphic encryption, or zero-knowledge proofs also offers potential for enhancing privacy-preserving data sharing and computation.

In the long term, the proposed blockchain-based model may serve as a foundational architectural element for constructing large-scale trusted information systems. Its adaptability, mathematical rigor, and demonstrated resilience make it a viable candidate for environments requiring high assurance in data integrity, reliable multi-party coordination, and transparent security controls. The scalability and modularity of the framework suggest that it can evolve alongside technological advancements, positioning it as a robust solution for future generations of distributed information ecosystems.

Authors' contribution: Vladyslav Lutsenko – conceptualization; methodology; development of the mathematical model; analysis of sources, preparation of the literature review and theoretical background; construction of the trust and consensus model; software; Volodymyr Nakonechnyi – implementation of the prototype; simulation modeling, analysis and validation of results; preparation and editing of the manuscript.

Sources of funding. This study did not receive any grant from a funding institution in the public, commercial, or non-commercial sectors.

References

- Alhamad, M., Al-Hammadi, Y., & Sultan K. (2025). *Cybersecurity challenges in blockchain-based social media platforms*. Computers & Security. <https://doi.org/10.1016/j.bcsra.2025.100290>
- Almarri, S., Alenezi, A., & Khan, S. U. (2024). Blockchain Technology for IoT Security and Trust. *Sustainability*, 16(23), 10177. <https://doi.org/10.3390/su162310177>
- Dwivedi, K., Agrawal, A., Bhatia, A., & Tiwari, K. (2024). *A Novel Classification of Attacks on Blockchain Layers: Vulnerabilities, Attacks, Mitigations, and Research Directions*. <https://doi.org/10.48550/arXiv.2404.18090>
- Eyadat, A. A., Alamaren, A. S., & Almomani, S. L. (2025). The influence of Blockchain technology on reducing cybersecurity risks in financial transactions of commercial banks. *Frontiers in Blockchain*, 8:1657110. <https://doi.org/10.3389/fbloc.2025.1657110>
- Javaid, N., & Alghamdi, T. A. (2023). A Comprehensive Survey on Security, Privacy and Authentication in Blockchain. *International Journal of Web and Grid Services*, 19(3), 259–286. <https://doi.org/10.1504/IJWGS.2023.133501>
- Luo, X. (2024). *A survey on the application of blockchain in cryptographic protocols*. Human-centric Computing and Information Sciences. <https://doi.org/10.1186/s42400-024-00324-7>
- Mollajafari, S., Gholami, R., & Zare, H. (2023). Blockchain Technology and Related Security Risks. *Sustainability*, 15(18), 13401. <https://doi.org/10.3390/su151813401>
- Osterrieder, J., Chan, S., Chu, J., Zhang Y., Hadji Misheva B., & Mare C. (2024). *Enhancing Security in Blockchain Networks: Anomalies, Frauds, and Advanced Detection Techniques*. <https://doi.org/10.48550/arXiv.2402.11231>
- Saha, B., Hasan, M., Anjum, N., Tahora S., Siddika A, Shahriar H. (2023). Protecting the Decentralized Future: An Exploration of Common Blockchain Attacks and their Countermeasures. <https://doi.org/10.48550/arXiv.2306.11884>
- Singh, R. K., & Kim, S.-L. (2023). *Blockchain applications for secured and resilient supply chains: A systematic review*. Computers & Industrial Engineering. <https://doi.org/10.1016/j.cie.2022.108854>
- Zhang, Y., Chen, L., & Wang, X. (2024). A survey on consensus algorithms for blockchain: Security, performance, and energy efficiency. *Future Generation Computer Systems*, 154, 47–68. <https://doi.org/10.1109/ICCIsci.2019.8716424>

Отримано редакцією журналу / Received: 09.12.25

Прорецензовано / Revised: 12.12.25

Схвалено до друку / Accepted: 21.12.25

Владислав ЛУЦЕНКО, асп.

ORCID ID: 0000-0002-2377-1858

e-mail: vladyslav.lutsenko99@gmail.com

Київський національний університет імені Тараса Шевченка, Київ, Україна

Володимир НАКОНЕЧНИЙ, д-р техн. наук, проф.

ORCID ID: 0000-0002-0247-5400

e-mail: volodym.nakonechnyi@knu.ua

Київський національний університет імені Тараса Шевченка, Київ, Україна

ДЕЦЕНТРАЛІЗОВАНІ МЕХАНІЗМИ ДОВІРИ ТА КОНСЕНСУСУ ДЛЯ ЗАХИСТУ КОНФІДЕНЦІЙНИХ ДАНИХ У РОЗПОДІЛЕНИХ СИСТЕМАХ

Вступ. Дослідження присвячене стрімкому зростанню обсягів даних, що опрацьовуються в розподілених цифрових екосистемах, де традиційні централізовані моделі зберігання створюють ризики через наявність єдиних точок відмови й обмежену прозорість у відстеженні змін. Підкреслюється потреба у безпечних, стійких і верифікованих механізмах, здатних захищати конфіденційну інформацію в динамічних багатокористувачьких середовищах.

Методи. Розроблено гібридну блокчейн-архітектуру, що поєднує публічні та приватні реєстри. Формалізовано математичну модель децентралізованого захисту даних, застосовано цифрові підписи, смартконтракти та криптографічне хешування, а також реалізовано функціональний прототип на основі Hyperledger Fabric із консенсусним алгоритмом RAFT для валідації безпечного доступу та забезпечення цілісності транзакцій.

Результати. Аналітичне моделювання та результати симуляційних експериментів у мережах із 10–100 вузлів демонструють підвищення стійкості системи приблизно на 20–25 % у разі збереження стабільної затримки транзакцій. Реалізована модель



надійно виявляє спроби несанкціонованого доступу та дії з модифікації даних, а також засвідчує відповідність міжнародним стандартам, зокрема ISO/IEC 27001 та GDPR.

В и с н о в к и . Отримані результати підтверджують, що архітектури на основі блокчейну можуть суттєво підвищувати рівень захисту даних у розподілених середовищах і перевершувати традиційні централізовані моделі безпеки. Запропонована концепція забезпечує цілісність, прозорість і простежуваність даних за мінімальних втрат продуктивності, що робить її придатною для фінансових, державних, медичних і корпоративних систем. Подальший розвиток вбачають перспективним у напрямі інтеграції машинного навчання, квантостійкої криптографії та хмарних інфраструктур.

К л ю ч о в і с л о в а : блокчейн; гібридні системи; захист даних; захист інформації; децентралізовані архітектури; управління доступом; смартконтракти; протоколи консенсусу; цифрові підписи; хешування; Hyperledger Fabric; RAFT; цілісність даних; конфіденційність; криптографія; GDPR; ISO/IEC 27001; розподілене зберігання; кібербезпека; машинне навчання.

Накoneчний Володимир є членом редакційної колегії цього видання, тому він не брав участі в процесі рецензування та прийнятті рішення щодо публікації цієї статті.

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

Nakonechnyi Volodymyr is a member of the Editorial Board of this publication; therefore, he did not participate in the peer review process or the decision-making regarding the publication of this article.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.