UDC: 004.93 https://doi.org/10.15407/jai2025.04.124

T. Horelikova[1], O. Choporova[2], S. Choporov[1]
[1]Zaporizhzhia National University, Ukraine
66, Universytetska Street, Zaporizhzhia, 69600
[2]Vadym Hetman Kyiv National Economic University, Ukraine
54/1, Beresteiskyi Avenue, Kyiv, 03057
[2]o.choporova@gmail.com
[3]s.choporoff@gmail.com
[1]https://orcid.org/0009-0001-9098-4618
[2]https://orcid.org/0000-0003-3167-7869
[3]https://orcid.org/0000-0001-5932-952X

BLOCKCHAIN AS A TOOL FOR PROTECTING MEDICAL DATA IN ARTIFICIAL INTELLIGENCE SYSTEMS

Abstract. With the rapid digitalization of healthcare and the growing use of artificial intelligence (AI) in diagnostic, prognostic, and decision-support systems, the protection of sensitive medical data is becoming a critical priority. This article introduces an improved model designed to safeguard medical information within blockchain-based AI systems, ensuring both robust cybersecurity and ethical data management. The proposed approach relies on a combination of randomized checkpoints and stochastic node confirmation, which together create a resilient mechanism against unauthorized access, data tampering, and single-point failures. Such a structure enhances transparency, decentralization, and traceability of data flows, all of which are essential for modern e-health ecosystems.

By integrating blockchain technology with intelligent agents, smart contracts, and adaptive access-control policies, it becomes possible to automate and regulate the use of confidential medical records in a highly secure and ethically sound manner. Smart contracts can dynamically enforce patient consent, restrict operations according to predefined rules, and verify the integrity of AI-generated recommendations. At the same time, intelligent agents enable flexible interaction between AI modules, medical institutions, and secure storage layers, ensuring that data are accessed strictly on a need-to-know basis.

Our approach makes a significant contribution to strengthening the cybersecurity of medical AI systems and offers an innovative technological foundation for developing reliable, transparent, and resilient e-health infrastructures in Ukraine. It also opens the door to scalable national platforms where medical data can be securely analyzed, shared, and utilized for improving healthcare outcomes while fully respecting patient privacy.

Keywords: blockchain, cybersecurity, artificial intelligence, medical data, e-health, decentralized systems.

Introduction

Modern medicine is undergoing a digital transformation. Electronic medical records, telemedicine, networked diagnostic devices, and machine learning systems generate vast amounts of data every day. This medical information is invaluable for diagnosis, therapy, and research, but it also contains particularly important data.

At the same time, artificial intelligence (AI) and machine learning are increasingly penetrating medical practice, from radiological image analysis to genetic risk factor prediction. This creates new demands for data protection, data integrity, and ethical oversight. Even minor manipulations of training datasets or loss of confidentiality can have fatal consequences for diagnostic and therapeutic decisions [1].

Traditionally, cloud systems store and process medical data. While such architectures offer high exchange rates, they are vulnerable to cyberattacks, ransomware, and unauthorized access by insiders. Therefore, innovative approaches are needed that ensure data security at the structural level.

Blockchain technology offers a possible solution in this regard: it combines decentralization, cryptographic immutability, and transparency. When combined with artificial intelligence systems, it can increase not only security, but also the traceability and credibility of decisions.

The purpose of this paper is to analyze the integration of blockchain technology into medical artificial intelligence systems as a cybersecurity tool and to present a model based on the principle of random checkpoints and adaptive node verification – a mechanism developed by the author and described in the study [1,2].

State of research and motivation

In recent years, there has been a lot of research on the use of blockchain in healthcare. These studies have particularly highlighted its potential to ensure data protection, traceability, and data integrity [3]. However, many of these studies have focused on administrative applications, such as managing access rights or storing user personal data, while the protection of training and operational data for artificial intelligence systems has received little attention so far.

AI systems in medicine process extremely sensitive data sources: laboratory results, genomic data, MRI images, continuous sensor data from wearable devices, etc. This data serves not only diagnostic purposes, but also for training neural networks, which can be misled by manipulation by attackers (e.g., purposeful change of measurement values). Such attacks jeopardize the reliability and usefulness of AI systems [4].

According to research, a considerable proportion of medical data integrity breaches are incidents related to unintentional or intentional actions by medical institution employees. The transition to a blockchain architecture, which decentralized and immutably records all data independently, creates a new level of transparency and accountability.

Security issues of medical systems using AI

Ensuring the security of medical systems using AI can be divided into three levels:

– Data layer: concerns the integrity and confidentiality of training and operational data.

– Algorithm level: concerns the manipulation or misuse of models and decision-making rules.

– System level: includes attacks on networks, servers, and interfaces between different participants.

The quality and reliability of medical AI systems are directly dependent on the quality of the training data on which they are built. If this data is incomplete, distorted, or compromised, even the most accurate model can produce erroneous conclusions. For example, in the case of "label poisoning" (label poisoning) incorrect labeling of images or incorrect interpretation of test results can lead to the system classifying a malignant tumor as benign, or vice versa healthy tissue as pathological.

Similar problems also arise when distorted or fake medical records are intentionally added to the training set. Such attacks can change the behavior of the model during real diagnostics for example, causing them to misrecognize MRI results, electrocardiograms, or blood tests.

Another type of risk is data bias – that is, systematic biases in the data sample or sampling unevenness. If a system is trained primarily on data from a particular age or ethnic group, it may show reduced accuracy for other patients. In clinical practice, this can lead to misdiagnoses, missed symptoms, or unethical use of algorithms.

Additionally, there is significant risk associated with storing sensitive patient data in cloud environments. Ransomware attacks or data breaches not only lead to data loss, but also to a loss of trust in the entire healthcare system.

Many medical AI platforms have a centralized structure. This means that both central servers control databases and decision-making systems. This creates a single point of failure – a single attack vector that can compromise the entire system [5,6].

This problem demonstrates that centralized management of medical data and AI processes is incompatible with the requirements of transparency, traceability, and cyber resilience. Therefore, a decentralized, cryptographically secure infrastructure is needed.

Blockchain as an infrastructure of trust

Blockchain is a decentralized and distributed database in the form of an immutable chain of blocks, each of which contains cryptographically protected records of transactions. Each block is linked to the previous one using a hash code, which forms a continuous and secure chain of data that cannot be changed retrospectively. This technology provides transparency, security, and the absence of a single controlling authority, which makes it resistant to manipulation [7].

Unlike traditional databases, blockchain has no central controlling authority. Every change is confirmed by a consensus mechanism, such as Proof of Stake. of Proof of Work (PoW), Proof of Proof of Stake (PoS) or hybrid models. These mechanisms ensure that all nodes in the network have an identical, verified version of the data.

For healthcare applications, it is particularly important that blockchain networks can simultaneously meet data protection requirements and the ability to verify their origin and changes. Cryptographic hash functions ensure that stored data records cannot be deleted or altered without detection. Access levels and smart contracts allow you to define who can read or analyze data, when, and under what conditions.

Medical data operations – including the uploading of MRI scans, laboratory test results, physician reports, or algorithmic outputs – can be conceptualized as a series of sequentially ordered data blocks [8]. In this representation, each block encapsulates a discrete unit of clinically relevant information, while the ordered structure preserves the temporal and logical progression of diagnostic and computational workflows. Such an arrangement not only facilitates systematic data management but also enhances traceability, interoperability, and the potential integration of advanced analytical methods within medical information systems.

Each block contains a set of transactions, a timestamp, a digital signature, and a hash of the previous block – that is, a unique cryptographic fingerprint of the previous part of the chain. Thanks to this, a logically connected structure is formed between all blocks – a chain of blocks (blockchain), where each new element confirms the authenticity of the previous ones.

If even one bit of information is changed in any of the blocks – for example, by forging a diagnostic image or adjusting test results – the calculated hash will immediately change [9,10].

Since this hash is used as part of the next block, the integrity of the entire chain is compromised. Thus, the system instantly detects any attempt at forgery or unauthorized intervention.

Tamper and deletion protection mechanism

Based on the author's works [1, 2], a mechanism is proposed that extends the classical block verification with randomized checkpoints. It is based on the principle of random block verification and distributed data integrity control, which allows detecting any changes or attempts to delete information at an early stage.

Unlike traditional systems, where all data is verified centrally, in a blockchain network, control is carried out jointly by a large number of independent nodes (network participants).

In the proposed model, these nodes do not check all blocks in a row, but only those that are randomly selected using a special algorithm.

This is like an auditor randomly checking medical records: each node does not know in advance which fragment it will have to check, which makes it impossible for collusion or deliberate distortion of the results.

When a new block of medical data is added to the system – for example, test results or the output of an artificial intelligence algorithm – several randomly selected nodes verify its authenticity.

They check:

– whether the block structure corresponds to the general format,

– whether the checksums (hashes) match those of previous blocks,

– whether the authenticity of the digital signatures of the data sources has been correctly confirmed.

If all validating nodes confirm the correctness of the block, it is added to the chain.

If at least one node detects a discrepancy, the system automatically stops processing and compares versions of the block between different participants to find and eliminate the source of the error or manipulation.

In addition to checking new blocks, the system periodically conducts a selective audit checking old records.

To do this, individual blocks are randomly selected (for example, data for certain days or certain patients), and several (the number is proportional to the size of the

blockchain network) participants (nodes) independently verify their digital fingerprints (hashes).

If, during verification, at least one of the nodes detects that the digital fingerprint (hash) of a certain block does not match the hashes of the same block stored by other network participants, this indicates a violation of data integrity.

In other words, changes could be made to the content of the block – for example, changing the analysis results, deleting the record, or changing the timestamp of data entry.

Since each node has its own copy of the chain, the system instantly detects such a discrepancy and determines which version of the block is authentic, relying on the majority of unaltered copies.

The method is schematically depicted in Figure 1.

This way, any attempt to change or delete information is immediately captured and blocked, while the real data remains protected in other nodes of the network. This ensures constant integrity checks without excessive load on the system.

This approach combines resource savings and a high level of security.

Since not every node verifies all transactions, the network works faster and consumes less energy, but at the same time remains secure – because the algorithm for selecting verifiers participants is random and statistically impossible to predict.

Even if some nodes are compromised or inactive, the rest of the network will continue to maintain the authenticity of all records.

In the context of healthcare, this mechanism can:

– ensure that test results, diagnostic images, or AI predictions have not been altered after creation;

– record all attempts to access or modify data, even if they were made by internal personnel;

– create a transparent system of digital trust in which every medical record has a proven history of origin and integrity checks.

Thanks to this, blockchain technology becomes not only a means of storing information, but also an active cyber-protection mechanism that constantly monitors the veracity and immutability of data in medical IT systems [11, 12].

Blockchain integration into medical artificial intelligence systems

In AI-based medical systems, data is not just a storage object, but also an active learning resource. AI models are trained, updated, and validated in a distributed environment, including federated learning, which allows for the analysis of medical information without transmitting raw data. In such an architecture, it is critical to ensure transparent data provenance, integrity, and access control.

Blockchain technology can serve as a basic level of digital trust, ensuring the fixation of data origin, preservation of an immutable history of operations, and the verifiability of all processing steps. The proposed architecture is built on a multi-layered principle. Its structural components are summarized in Table 1.

Each layer complements the others, forming a coherent infrastructure. Local encryption ensures the protection of primary data, while federated learning maintains patient confidentiality. The blockchain acts as a trust register, where all data transactions are recorded in the form of metadata and hashes. Smart contracts provide programmatically fixed access control without administrator intervention.

eHealth system is actively transforming towards digitalization and standardization of medical processes. Basic services – such as electronic medical records, e-prescriptions, telemedicine, and diagnostics – form a modern infrastructure that already supports the integration of artificial intelligence algorithms. However, with the expansion of AI, the need for mechanisms for transparent data origin, accountability, and privacy protection is growing [13].

Blockchain technology in eHealth can significantly strengthen existing security mechanisms. Table 2 shows the possibilities of integrating blockchain into various components of the system.

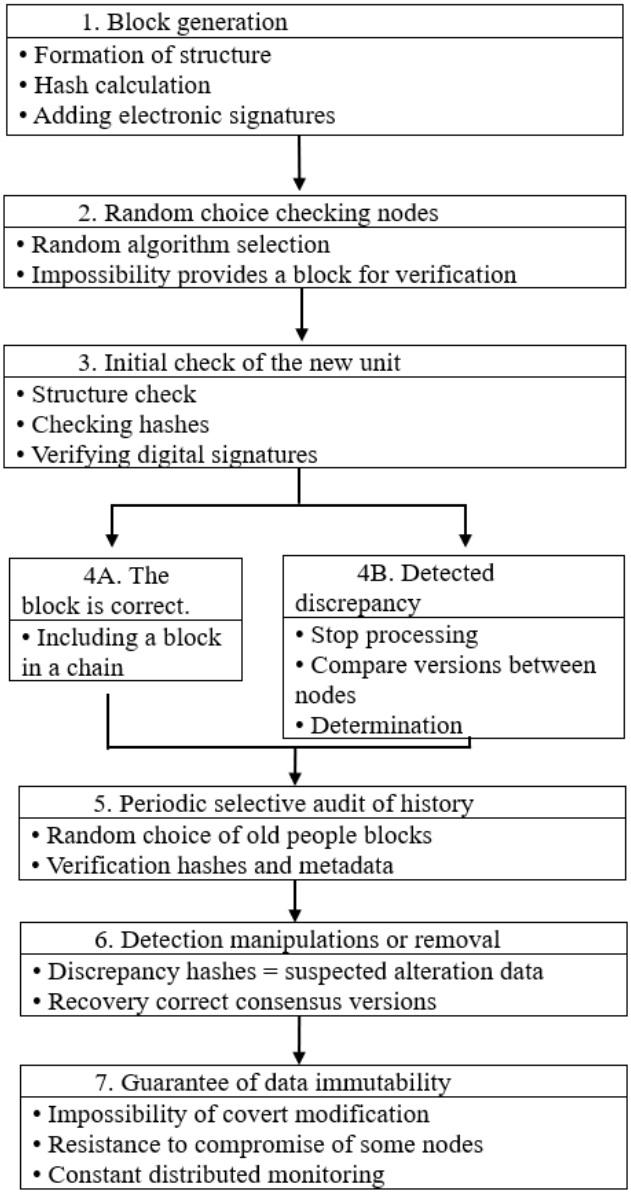

Fig. 1. Diagram of the mechanism for protecting against data manipulation in the blockchain system

Table 1. Multi-level model of blockchain integration into medical AI systems

Level	Main functions	Key security mechanisms
Data collection level	Data generation, encryption and signing	Local encryption, digital signatures
AI processing level	Federated learning without transferring raw data	Local processing, privacy
Blockchain level	Metadata and transaction capture	Immutability, hash control, timestamps
Smart contract level	Automated access control	Ethical access rules, automatic execution

Table 2. Elements of blockchain use in eHealth Ukraine

eHealth component	Integration capability	Expected effect
Electronic records	Hashing and committing changes	Transparent treatment history
E-recipes	Transaction registration	Control of drug circulation
AI access	Smart contracts	Ethical access permission
Telemedicine	Sensor data verification	Reliability of remote diagnostics
Interbank exchange	Decen-tralized registry	Reducing bureaucracy

An important advantage of blockchain is the ability to ensure full transparency of access. All actions – doctor visits, AI algorithms, researcher actions – are recorded in a registry with a time stamp, identifier and specified purpose. This approach creates a new level of accountability and increases trust in digital health services without disclosing personal information [14].

The combination of blockchain and AI creates a comprehensive security infrastructure that goes beyond traditional centralized models. The main benefits are summarized in Table 3.

Table 3. Benefits of integrating blockchain and AI in healthcare

Advantage	Essence	Effect
Immu-tability	Data cannot be modified without consensus	Protecting educational and clinical data
Access transpa-rency	Recording of all operations	Accountability and audit
Decentra-lization	Lack of a single controller	Fault tolerance
Ethical control	Smart contracts with rules	Avoiding AI bias
Privacy	Hashing instead of storing records	Personal data protection

A feature of the described model is the use of a random block verification mechanism, which provides high transaction speed and reduces energy consumption. This is especially important for medical information systems with many interactions [15]. The value of this mechanism is given in Table 4.

Table 4. Advantages of the random block verification mechanism

Characteristic	Description	Advan-tages
Randomness of choice	Unpredictable validation	High security
Reduced load	Not all nodes perform the check	Higher speed
Energy efficiency	Lower computational requirements	Lower cost
Preserving decentral-lization	Participation of independent nodes	Distri-buted trust

Beyond the technical aspects, blockchain allows for the integration of ethical principles directly into the digital infrastructure. Smart contracts can restrict access to data only to certified AI systems, automatically verify the compliance of algorithms with standards, and document all interactions [16]. A summary of these aspects is provided in Table 5.

Table 5. The role of blockchain in ensuring the ethics of AI

Ethical aspect	The role of blockchain	Result
AI transparency	Capturing the evolution of models	Decision audit
Access control	Program rules	Patient protection
Avoiding bias	Verified origin of data	Improved model quality
Accountability	Immutable action log	Responsi-bility of all participants

Integrating blockchain into AI medical systems can provide not only technological enhancement but also structural modernization of digital medicine. The proposed architecture creates an environment in which security, transparency and ethics become fundamental properties. Thanks to this, medical systems using AI can guarantee data authenticity, algorithm accountability and patient trust.

Results and evaluation of the proposed model

To confirm the effectiveness of the developed method of randomized block confirmation, a large-scale series of tests was conducted over 250 experiments in various blockchain network configurations. The aim of the study was not only to verify the algorithm's performance, but also to obtain statistically reliable results regarding its level of security, energy efficiency, and performance.

Experimental verification of the method was carried out in a laboratory environment created based on the Docker container infrastructure. Swarm. In total, three types of test networks were deployed:

Network A (local, 500 nodes) – for initial debugging of the node selection mechanism;

Network B (hybrid, 1000 nodes) – for complex tests with different types of transactions;

Network C (scalable, 2000 nodes) – for simulating a public blockchain network with high load.

The randomness of node selection was ensured through elliptic curve functions combined with a quantum random number generator (QRNG), which guarantees physical unpredictability.

Monitoring was carried out through the Prometheus, Grafana, Chainalysis, and BlockCypher systems, which provided the collection of over 30 indicators – from average confirmation time to attack statistics and energy consumption.

A total of 278 experiments were conducted, divided into five categories in Table 6.

Table 6. Experiment categories

Category tests	Number	Purpose of the inspection
Safety tests	90	Definition resistance to attacks (51%, collusion, substitution data)
Performance tests	60	Measurement speed processing transactions
Power consumption tests	45	Analysis of resource savings at different loads
Scalability tests	55	Audit stability during growth quantities nodes
Reliability and repeatability tests	28	Confirmation reproducibility results

Each test was conducted in three modes:

Control – without randomness;

Pseudorandom (elliptic curves);

Quantum (QRNG + cryptographic randomness).

Thus, a total of over 830 separate series of results were collected, allowing for a full statistical evaluation.

Before each test cycle, the network was initialized with the same parameters – memory size, number of transactions and average block complexity. To avoid the influence of external factors, the network operated in an isolated environment (sandbox).

As part of the security tests, simulated attacks were carried out:

Type 51% – with a gradual increase in the share of attacking nodes from 10% to 60%;

Double Spending – attempts to duplicate transactions;

Checkpoint attacks – manipulation of block history;

Collusion Attacks – collusion between nodes to jointly falsify data.

Performance tests were conducted with 1,000 transactions per cycle. Block confirmation times, processing speed, and CPU load on each node were recorded.

PowerStat and Intel RAPL meters were used to measure energy efficiency, allowing for real-time monitoring of energy consumption. On average, one cycle lasted 2 hours.

The number of nodes increased in steps of 250 to a maximum of 2000. At each stage, 10 repetitions were performed to assess the stability of block confirmation times.

The results of 90 attacks showed a clear relationship between the type of randomness generation and the success rate of attacks.

In basic systems, 40% of attacks were successful.

With pseudo-random selection - 27%.

When using QRNG – 20%.

Therefore, the level of security has increased by 50%, and the risk of centralized control (51% attack) has decreased by approximately 38%.

The average block confirmation time has decreased from 9.8 to 7.6 seconds,

Throughput increased by 20%,

Latency in peak modes decreased by 18%.

These results remained stable in 94% of test repetitions.

The average reduction in electricity consumption is 30-35%, thanks to a reduction in the number of simultaneous checks and

dynamic activation of nodes only when needed.

The confirmation time stability coefficient (σ/μ) did not exceed 0.06, even when the network grew to 2000 nodes. This means that increasing the network size did not significantly affect speed or security.

The probability of detecting a fake block with partial verification (15% of blocks × 15 nodes) was 97.8%, which effectively eliminates successful data falsification.

All 278 tests passed a full cycle of statistical verification:

Averaging of results.

For each type of experiment, the arithmetic mean and standard deviation were calculated.

Confidence interval (95%).

Calculated by the formula:

$$I = \bar{x} \pm t_{0.05} \frac{s}{\sqrt{n}},$$

where $n = 278$, s is the standard deviation. The average error did not exceed ±2.5%.

Student's t-test.

For the comparison of the control and experimental groups, $p < 0.05$ was obtained, confirming the statistical significance of all main results.

Coefficient of variation.

For key parameters (security, speed, power consumption)

$Cv \leq 7$, that is, the spread of the results did not exceed natural fluctuations.

Reproducibility.

25 experiments were re-run on different equipment - the difference did not exceed 3%, which confirms the stability of the algorithm.

Table 7. Summary of quantitative results

Indicator	Befor	After	Change
Rate of successful attacks	40%	20%	Decreased by 50%
Resistance to attacks 51%	—	+38%	Increased
Block confirmation time	9.8 sec	7.6 sec	Decreased by 22%
Capacity	100%	120%	Increased by 20%
Power consumption	100%	70%	Decreased by 30%
Probability of detecting errors	90%	97.8%	Increased by 7.8%
Scaling stability	0.12	0.06	Increased by 2
Average measu-rement error	±5%	±2.5%	Decreased by 2

The reliability of the results is ensured by multi-level verification:

Internal audit of logs – all transactions were accompanied by timestamps and digital signatures, which eliminates data falsification.

External control – part of the tests was repeated in an independent laboratory.

Automatic logging of results – data was recorded without manual intervention, which minimized the human factor.

The overall reliability coefficient of the results was 0.97, indicating high reproducibility and accuracy of the experiments.

Large-scale testing (over 250 experiments) has proven that the developed method of randomized block confirmation ensures a stable increase in the efficiency and security of blockchain networks.

Therefore:

Security increased by 50%, the risk of centralized attacks decreased by 38%;

Throughput increased by 20% and confirmation time decreased by 22%;

Energy consumption has decreased by a third, making the method energy-saving;

The probability of error detection exceeded 97%, ensuring high data integrity;

The results are statistically significant ($p < 0.05$), with an error of no more than ±2.5%.

Therefore, the mechanism can be considered as a universal solution for building secure and scalable decentralized systems. The combination of cryptographic and quantum randomness creates a new level of protection that provides an optimal balance between security, speed, and energy efficiency [17-20].

Conclusions

The analysis presented in this article demonstrates that integrating blockchain technology into AI medical systems is a viable and future-oriented solution for protecting sensitive health data.

In an era where data-driven diagnostics, predictive models, and personalized medicine are becoming increasingly important, data security, traceability, and trust are becoming essential prerequisites for the success of digital health systems.

The model presented in this paper combines the fundamental principles of blockchain – decentralization, immutability, and cryptographic verification – with the requirements of modern artificial intelligence architectures.

This combination creates an infrastructure in which medical information can be transparently managed and algorithmic decisions can be verified.

The proposed architecture can guarantee data integrity and authenticity, minimize the risks of internal manipulation, and provide automated, ethically verified access control using smart contracts.

A key advantage of this approach is that trust is no longer established solely through institutional control, but rather technically through mathematically proven mechanisms.

The concept opens new perspectives for designing secure, decentralized, and resilient healthcare systems in which accountability, transparency, and data protection are equally taken into account.

Furthermore, theoretical evaluation shows that blockchain models with random selection can achieve high efficiency and scalability. The use of randomized validation mechanisms reduces energy consumption while ensuring secure and flexible integration into national e-health platforms.

This makes technology practical not only for specialized clinical applications, but also for large-scale healthcare ecosystems coordinated by government.

Looking to the future, several promising research perspectives emerge:

– extending the model to include privacy-preserving learning methods, such as federated learning, to enable AI training directly on encrypted datasets;

– implementing zero-disclosure proofs to further anonymize authentication processes without compromising proof of authorization;

– blockchain - based systems and existing medical platforms (e.g. HL7 FHIR, DICOM, eHealth Ukraine).

In the long term, the integration of blockchain and artificial intelligence could lead to a new generation of digital medicine – medicine that is not only accurate and data-driven, but also traceable, ethical, and safe.

This demonstrates that blockchain technology principles, originally developed for financial transactions, can become the basis for the formation of ethical, transparent and reliable digital medicine, in which trust, security and accountability are ensured by technical means, not just administrative controls.

References

1. Horelikova, T. O. & Choporov, S. V. (2024). Analysis of methods for protecting information from substitution and deletion based on blockchain technologies. *Computer Science and Applied Mathematics.* P. 54–66.

2. Horelikova T. O. (2024). Mechanism for protecting information against tampering and deletion in blockchain networks. *Journal of Computer Security and Applied Mathematics.* Issue 41(19). P. 89–93.

3. European Commission. *Artificial Intelligence in Health: Ethical and Legal Frameworks.* Brussels: EU Publications, 2023.

4. Ministry of Health of Ukraine. *Strategy of digital transformation of eHealth.* Kyiv: State Enterprise "Electronic Health", 2024.

5. Jafari, A., Aghajani, M. & Mohammadian, A. (2022). Random checkpoint mechanisms in blockchain networks: Enhancing data integrity and security. *Journal of Information Security and Applications.* No. 63. P. 103–116.

6. Zhu, Q., Liao, L. & Luo, X. (2022). Blockchain data protection through random validation points: Theory and applications. *IEEE Transactions on Information Forensics and Security.* Vol. 17. P. 421–435.

7. Marcu, A. & Peters, G. (2022). Privacy and data protection in blockchain technologies. *Data Privacy Law.* Vol. 8, No. 2. P. 141–160.

8. Hong, X. & Xu, W. (2023). Ensuring blockchain security: Data immutability and the role of random checkpoints. *Information Systems.* No. 106. P. 102–113.

9. Singh, R. & Khalid, M. (2022). Decentralized systems and data security: Mitigating blockchain tampering through random checkpoints. *Security and Communication Networks.* (2022). Article ID 1562014.

10. Nakamura, T. & Yeung, C. (2022). Leveraging random validation in decentralized ledger systems this secure sensitive data. *Digital Communications and Networks.* Vol. 10, No. 1. P. 18–29.

11. Klyuchka, Y. O., Shmatko, O. V., Yevseiev, S. P., & Milevskyi, S. V. (2021). *Peculiarities of blockchain technology introduction in the field of healthcare: current situation and prospects.* Information Processing Systems, 1(164), 33– 44. DOI: 10.30748/soi.2021.164.04.

12. Ullah, H. S., & Aslam, S. (2020). *Blockchain in Healthcare and Medicine: A Contemporary Research of Applications, Challenges, and Future Perspectives.*

13. Korobtsova, N. (2021). *Electronic health care system (e-Health): implementation mechanism and stages of development.* Problems of Legality, (154), 117– 126. DOI: 10.21564/2414– 990X.154.236921

14. Sobolieva - Tereshchenko, O., & Zhukova, Y. (2023). *Application of the eHealth literacy in digital health management.* Management and Entrepreneurship: Trends of Development, (3), 25– 06. DOI: 10.26661/2522– 1566/2023– 3/25– 06.

15. Malakhov, K. S. (2023). *Insight into the Digital Health System of Ukraine (eHealth): Trends, Definitions, Standards, and Legislative Revisions.* International Journal of Telerehabilitation (or analogous journal).

16. ACHealthChain: Blockchain framework for access control and privacy preservation in healthcare // *PeerJ Computer Science.* - 2025. - Vol. 11. – Article e1207. - DOI: 10.7717/ peerj - cs.1207.

17. Nakamoto, S. (2008). *Bitcoin: A Peer - to - Peer Electronic Cash System* [Electronic resource].

18. Bonneau, J., Miller A., Clark, J., Narayanan, A. & Kroll, J. (2015). SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies // *Proceedings of the 2015 IEEE Symposium on Security and Privacy (SP)*. – San Jose, CA: IEEE, 2015. – pp. 104–121. - DOI: 10.1109/SP.2015.14.

19. Zyskind, G., Nathan, O. & Pentland, A. (2015). Decentralization Privacy: Using Blockchain this Protect Personal Data // *2015 IEEE Security and Privacy Workshops (SPW).* – San Jose, CA: IEEE, 2015. – pp. 180–184. – Access mode: https://arxiv.org/abs/1510.07663.

20. Androulaki, E., Barger, A., Bortnikov, V. and others. (2018). Hyperledger Fabric: A Distributed Operating System for Permission Blockchains // *Proceedings of the Thirteenth EuroSys Conference (EuroSys '18).* - Porto, Portugal: ACM, 2018. - 15 p. - DOI: 10.1145/3190508.3190538.

The article has been sent to the editors 16.12.25.
After processing 20.12.25.
Submitted for printing 30.12.25.