**BULLETIN of Cherkasy State Technological University**

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

Vol. 31 No. 1. 2026

UDC 004.8:004.75:614.2
DOI: 10.62660/bcstu/1.2026.101

ISSN: 2306-4412
E-ISSN: 2708-6070

# Integration of artificial intelligence and blockchain technologies in computer systems of virtual healthcare

**Mykola Khrulov***

Postgraduate Student
Cherkasy State Technological University
18006, 460 Shevchenka Blvd., Cherkasy, Ukraine
https://orcid.org/0009-0004-9201-5118

**Tetiana Myroniuk**

PhD in Technical Sciences, Associate Professor
Cherkasy State Technological University
18006, 460 Shevchenka Blvd., Cherkasy, Ukraine
https://orcid.org/0000-0002-7588-1055

**Abstract.** The purpose of the study was to provide a theoretical justification for the integration of artificial intelligence and blockchain technologies in computer systems of virtual healthcare, in particular to clarify how the combination of artificial intelligence, oriented towards personalised diagnostics, with blockchain technologies for the protection of medical data could form a new model of digital medicine. In the course of the study, analytical, synthetic, systemic and comparative-legal methods were used, which made it possible to analyse in a comprehensive way the scientific approaches, international standards and technical frameworks related to the organisation of digital healthcare. A five-level architecture of an integrated virtual-medicine system was considered, which includes analytical, verification, communication, security, and user levels. At the analytical level, clinical data are processed and personalised treatment forecasts are formed; at the verification level, immutability and traceability of records are ensured through the use of blockchain mechanisms; at the communication level, information exchange is implemented through standardised interfaces; the security level guarantees the protection of personal data and the legal authenticity of all actions; the user level forms transparent interaction between patients, doctors and medical institutions. Within the theoretical model, the concept of "trust-by-design" is substantiated, which defines trust as a systemic characteristic of digital medicine embedded in the architecture already at the development stage. The result of the study was the identification of the structural and functional foundations for building a secure and personalised virtual healthcare system, in which the analytical power of artificial intelligence is combined with the proven reliability of blockchain technologies. The main principles of building the system cover a multi-level architecture with analytical, verification, communication, security and user levels, which ensure the accuracy of analytics, data immutability, standardised exchange, protection of confidentiality and transparent interaction between the participants in digital medicine. The practical significance of the results obtained lies in the possibility of using the developed model as a conceptual basis for creating national and international digital-medicine platforms that ensure lawfulness, confidentiality, and user trust in modern information solutions in the field of healthcare

**Keywords:** conceptual architecture; verification level; interoperability; confidentiality of medical data; ethical accountability; concept of trust-by-design; decentralised systems

**Article's History:** Received: 06.10.2025; Revised: 26.01.2026; Accepted: 16.03.2026; Published: 08.04.2026

**Suggested Citation:**
Khrulov, M., & Myroniuk, T. (2026). Integration of artificial intelligence and blockchain technologies in computer systems of virtual healthcare. *Bulletin of Cherkasy State Technological University*, 31(1), 101-117. doi: 10.62660/bcstu/1.2026.101.

*Corresponding author

## INTRODUCTION

The development of modern computer healthcare systems is taking place against the background of a global digital transformation that is changing the principles of diagnostics, treatment, and the management of medical data. In this context, the integration of artificial intelligence and blockchain technologies acts as a key direction in the evolution of virtual medicine. Such a combination creates a new paradigm in which intelligent algorithms process large arrays of protected data for personalised diagnostics and therapy, while decentralised blockchain systems ensure transparency, security, and control over access to patients' medical information. As a result of a comprehensive analysis of contemporary works, an integrated vision of the evolution of approaches to combining artificial intelligence and blockchain technologies in virtual healthcare was formed.

In Ukrainian academic discourse, an important role has been played by studies that have outlined not only the technological but also the social and ethical dimensions of this integration. In the work of V. Brodkevych & V. Liudvichenko (2022), aspirations towards the creation of more accurate diagnostic systems can be traced, where machine-learning algorithms optimised data processing and improved predictive models. At the same time, the authors drew attention to the risks associated with the opacity of algorithms and limited control over the circulation of sensitive information, which highlighted the need for new mechanisms of digital ethics. The problem of the legal consolidation of these mechanisms was further developed in the work of I. Davydova (2025), who argued that without a regulatory foundation blockchain technologies are unable to ensure trust between medical institutions, patients and state bodies. The researcher considered blockchain as a potential legal guarantor of the reliability of electronic records, emphasising the need for the legitimisation within digital medicine. The issues of trust and transparency in the circulation of medical data were continued by O. Sumets & V. Alkema (2023), who proved that decentralised systems for managing clinical information not only increase the reliability of research but also form a new economy of responsibility in the sphere of medical innovation. The study of R.R. Augustyn & O.V. Stakhiv (2023) showed that the intellectualisation of management processes in healthcare institutions had become the basis for the construction of adaptive digital systems in which managerial decisions are based on analytical forecasts. The conclusions logically resonated with the model of O. Shmatko & S. Salnikov (2024), which demonstrated the technical implementation of decentralised exchange of electronic medical records. The proposed architecture guaranteed patients autonomy in the disposal of the own data, while preserving full traceability of all transactions.

The global dimension of this problem was highlighted in the work of Y. Xie *et al*. (2021), where the integration of artificial intelligence, blockchain and wearable devices was considered as a new approach to the treatment of chronic diseases. Within this concept, information flows between the patient and medical staff became continuous, which ensured constant monitoring of health status and high reliability of collected data. In turn, A. Samad (2022) emphasised the role of standardisation in the integration of the Internet of Things with artificial intelligence and blockchain systems, underlining that without unified data-exchange protocols the effective digitalisation of medicine is impossible. A similar conclusion was reached by P. Tagde *et al*. (2021), who proved that technological synergy has limitations related to computational complexity and energy consumption of networks. The authors viewed these challenges as an incentive to create new optimisation algorithms capable of ensuring the stability of medical platforms under high-load conditions. The study by P. Verma *et al*. (2024) broadened the topic of security by showing that the combination of artificial intelligence and blockchain can become the basis for forming trusted ecosystems of digital medicine. The concept envisaged full traceability of all operations with data, automatic verification of access and decentralised management of medical information. The development of this idea was reflected in the work of J.P. Reyes-González *et al*. (2022), who considered big data as the connecting link between artificial-intelligence analytics and blockchain registers. The authors demonstrated that the merging of these technologies ensures not only the predictability of diagnoses but also forms a new methodology for decision-making based on evidence-based digital data.

Taken together, these studies have shown a gradual transition from the fragmented implementation of digital technologies to the concept of holistic digital medicine, within which technological, ethical and legal components function as a single system. Such a model presupposes the interconnected operation of analytical artificial-intelligence modules capable of deep forecasting of clinical processes with decentralised blockchain mechanisms that ensure immutability, verification and legal reliability of all transactions involving medical data. In this combination, artificial intelligence acts as a tool of intelligent analytics and personalised decision-making, whereas blockchain serves as the foundation of trust and ethical accountability, creating the basis for the formation of an intelligent, secure and transparent architecture of next-generation virtual healthcare. Despite the complexity of the approaches, the analysed studies do not sufficiently cover the practical aspects of harmonising technical and legal standards in the integration of artificial intelligence (AI) and blockchain in medical systems. In particular, there is a lack of detailed analysis of algorithmic compatibility between analytical artificial-intelligence models and distributed-ledger protocols, as well as methods for quantitative assessment of the level of user trust in such systems. The issues of auditing AI decisions (explainability), managing tokenised rights of access to data and implementing ethical principles in national eHealth platforms also remain insufficiently developed and require further academic elaboration.

The aim of the study was to provide a theoretical justification of the interaction between artificial intelligence and blockchain technologies in the architecture of computer systems of virtual healthcare and to identify the mechanisms by which the combination of analytical algorithms of personalised diagnostics with decentralised blockchain solutions for data protection forms an innovative model of next-generation digital medicine. The objectives of the study were to perform a comprehensive analysis of theoretical approaches to the integration of artificial intelligence and blockchain in virtual healthcare; to generalise scientific concepts of the interaction in ensuring the security, effectiveness, and personalisation of medical services; to identify the prospects for forming integrated digital medical systems of the new generation as intelligent, transparent and reliably protected architectures of digital medicine.

## MATERIALS AND METHODS

The study was conducted from 2024 to September 2025 and had a theoretical-analytical character with elements of the design science approach, aimed at substantiating the regularities of integrating AI and blockchain technologies in computer systems of virtual healthcare. The research was carried out at the interdisciplinary intersection of computer science, law, bioethics and medical information systems. The material base consisted of academic works, international and national regulatory acts, technical standards and reports reflecting current trends in the digital transformation of medicine. For the development of the five-level architecture, methods of functional modelling (DFD and BPMN), content analysis of technical standards and expert structuring of system components were used; comparative-legal analysis was carried out by normatively comparing the provisions of international and national acts; the choice of technical components was based on the criteria of interoperability, cyber-resilience and compliance with privacy-by-design principles.

The methodology combined analytical, synthetic, systemic and comparative-legal approaches, which correspond to the logic of forming a multi-level model. The analytical approach made it possible to determine the main directions of development of digital medicine and to single out key mechanisms for integrating artificial-intelligence and blockchain technologies through standardised HL7 Fast Healthcare Interoperability Resources (FHIR) and REST API protocols (eHealth Network..., 2023; Edenlab, n.d.). The synthetic approach ensured the generalisation of theoretical provisions into an integrated concept of virtual healthcare, within which AI performs an analytical-prognostic function in accordance with ISO/TR 24291:2021 (2021), and blockchain performs a verification-security function in line with IEEE EMBS P2418.6 (2018). System analysis made it possible to consider medical data as a component of a complex trust architecture, in which transactions are immutable and access is controlled.

The development of the integrated virtual-healthcare architecture was carried out using a formalised Dynamic Super Resolution (DSR) approach, which combines the stages of theoretical modelling, technical design and regulatory verification (Hevner *et al.*, 2004; Gregor & Hevner, 2013). Within this study, three key DSR cycles were distinguished: the relevance cycle – identification of applied scenarios (telemedicine, referral routing, cancer screening) and the formation of system requirements; the design cycle – development of the five-level architecture and demonstration modelling of data flows between analytical, communication and blockchain components using HL7 FHIR standards (eHealth Network..., 2023) and REST API; the rigour cycle – verification of architectural solutions by matrix comparison of the requirements of regulatory acts – Regulation (EU) No. 2016/679 (2016), IEEE EMBS P2418.6 (2018), ISO/TR 24291:2021 (2021) and Regulation (EU) No. 2024/1183 (2024) – with the functional components of the model. To increase the reliability of the assessment, key performance indicators (KPIs) were defined for each level of the system: accuracy and reproducibility of models (analytical level), throughput and latency of transactions (verification level), average time of exchange of FHIR resources (communication level), share of actions with a valid digital signature (security level) and frequency of access incidents (user level). Verification was carried out using tools for assessing compliance with ISO/TR 24291:2021 (2021) and auditing blockchain logs in accordance with IEEE EMBS P2418.6 (2018).

The comparative-legal approach was used to assess the consistency of regulatory approaches to the processing of medical data, with the selection of sources carried out according to a number of clearly defined criteria. Firstly, the criterion of regulatory relevance was applied, which envisaged the inclusion only of acts that directly regulate the issues of processing, protection, interoperability, and verification of medical data in digital systems. The level of legal impact was also taken into account, that is, the selection of international acts of the European Union (EU), the World Health Organisation (WHO) and the Organisation for Economic Co-operation and Development (OECD), which determine global standards of digital healthcare. According to the criterion of national implementation, Ukrainian regulatory documents that form the architecture of eHealth and ensure compatibility with the European frameworks of the General Data Protection Regulation (GDPR), eIDAS 2.0 and HL7 FHIR were analysed. In addition, the ethical-legal significance of the sources related to the principles of transparency, accountability and responsible use of artificial-intelligence technologies was taken into account.

The final criterion was the relevance and validity of the documents, which limited the selection of acts to officially updated editions of 2024-2025. At the international level, the basis was formed by Regulation (EU) No. 2016/679 (2016), Regulation (EU) No. 2024/1183 (2024) and the Global Strategy on Digital Health 2020-2025 (World Health Organisation, 2021). In the Ukrainian context, Law of Ukraine No. 2297-VI (2010) and Resolution of the Cabinet of Ministers of Ukraine No. 411-2018-p (2018) were analysed, which regulate the foundations of the processing of medical data and the protection of personal information. Particular attention was paid to Order of the Cabinet of Ministers of Ukraine No. 1671-2020-r (2020) and Order of the Cabinet of Ministers of Ukraine No. 1175-2021-r (2021), which define the architecture and stages of development of the national eHealth system. In the ethical dimension, the Ethics guidelines for trustworthy AI (European Commission, 2019) and the Recommendation of the Council on Artificial Intelligence (Organisation for Economic Co-operation..., 2019) were used, which establish the principles of transparency, accountability, and non-discrimination of AI systems. The technical analysis relied on materials from Edenlab (n.d.) on the Kodjin FHIR Server – the central component of the Ukrainian eHealth system built on open APIs, HL7 FHIR and blockchain verification of transactions. Additional sources included Organisation for Economic Co-operation and Development & European Commission (2024), eHealth Network – 23rd eHealth network meeting (2023), the joint declaration of HL7 Europe & IHE-Europe (Driving digital health forward, 2024) and eHealth Network (European Commission, n.d.), in which HL7 FHIR is recognised as the basic standard for the exchange of medical information. Among international technical standards, special attention was paid to ISO/TR 24291:2021 (2021) and IEEE EMBS P2418.6 (2018), which define the concepts of the use of machine learning and blockchain in healthcare. A comprehensive analysis of these sources made it possible to assess the level of technological and regulatory maturity of digital medicine, the harmonisation of Ukrainian legislation with European practices and to outline an integration model in which AI and blockchain interact as an analytical tool and a mechanism of digital trust, ensuring the implementation of the principles of trust-by-design, lawful-by-design and semantic interoperability.

## RESULTS

### Conceptual architecture of the integrated virtual healthcare system

Modern standards and scientific approaches to the integration of AI and blockchain technologies in healthcare are defined by the aspiration to create safe, transparent and personalised digital medical systems. On the basis of these approaches, the theoretical foundations were generalised, forming the conceptual model that reflects the structure, information flows and interaction between the analytical, verification, communication, security, and user levels of the system. The presented model illustrates the logic of functioning of the integrated architecture of virtual healthcare and is shown in Figure 1.

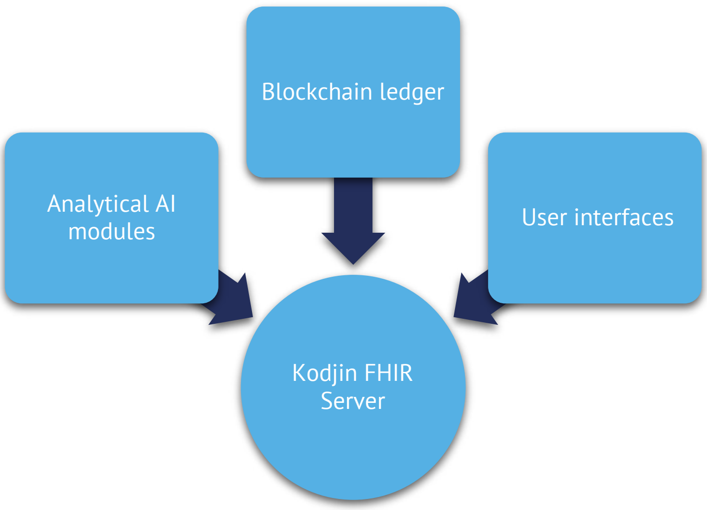


**Figure 1.** Conceptual interaction of the components of the AI-blockchain virtual healthcare system
**Source:** compiled by the authors based on Edenlab (n.d.), IEEE EMBS P2418.6 (2018), ISO/TR 24291:2021 (2021), Driving digital health forward: HL7 Europe and IHE-Europe strengthen the collaboration to enhance interoperability (2024)

The model presented in Figure 1 reflects the logical interaction between analytical modules, data repositories, access services and cybersecurity components. AI analytical modules function as the core of the system, performing the collection, cleansing and predictive processing of clinical information, whereas blockchain ledgers guarantee the immutability, traceability and verifiable history of transactions (IEEE EMBS P2418.6, 2018).

Interaction between the components is implemented through standardised application programming interfaces (APIs) and HL7 FHIR protocols, which define the format and rules for the structured exchange of medical data between independent systems (Driving digital health forward, 2024). The central place in the concept is occupied by the Kodjin FHIR Server, theoretically defined as the main node of the integrated architecture, which coordinates transactions, verifies access rights and maintains the logical integrity of records (Edenlab, n.d.). At the same time, Kodjin functions only as a centralised application gateway (application/API layer) that ensures consistency of data formats and access authorisation, while verification and confirmation of transactions take place at the distributed blockchain level. Such a separation makes it possible to preserve the principle of decentralisation at the data level, combining centralised access management with decentralised auditing and storage. The blockchain layer in this model performs the function of a decentralised auditor, recording all events in an immutable chain of blocks and providing the formation of a trusted environment between patients, medical institutions and regulators. According to the international standards IEEE EMBS P2418.6 (2018) and ISO/TR 24291:2021 (2021), the conceptual architecture is described as a multilevel system in which the analytical, verification and user levels interact through secure data exchange protocols. Unlike existing ISO and IEEE frameworks, the architecture of the presented model is interpreted as an integrated system in which the functional levels not only perform normatively defined roles but also form an interdependent model of digital trust that combines analytical accuracy, ethical accountability and legal compatibility.

The generalised principles of this architecture are presented in Table 1. The generalised principles of this architecture are presented in Table 1.

**Table 1.** Main principles of the architecture of the AI-blockchain virtual-medicine system

| System level | Functional purpose | Key technologies/standards | Expected effect |
|---|---|---|---|
| Analytical level | Processing of clinical data, forecasting, personalised diagnostics | Machine learning, ISO/TR 24291:2021 | Increased accuracy of predictions, adaptive therapy |
| Verification level | Ensuring the integrity and traceability of medical records | Blockchain, IEEE EMBS P2418.6 DLT Framework | Immutability and transparency of transactions, user trust |
| Communication level | Data exchange between system components | HL7 FHIR, REST API, Kodjin FHIR Server | Interoperability and standardised exchange |
| Security level | Access control, authentication, audit | eIDAS 2.0, GDPR | Confidentiality and lawfulness of data processing |
| User level | Interactive access of patients and doctors to data | Smart Contracts, eHealth Interface | User autonomy, transparent access control |

**Source:** compiled by the authors based on Edenlab (n.d.), European Commission (n.d.), Regulation (EU) No. 2016/679 (2016), IEEE EMBS P2418.6 (2018), ISO/TR 24291:2021 (2021)

As shown in Table 1, the conceptual architecture of the integrated virtual healthcare system is based on a five-level model, in which each level performs its own functions but at the same time interacts with the others through standardised protocols and normatively defined interfaces. The analytical level acts as the core of the system: at this stage AI algorithms carry out the cleansing, structuring and analysis of clinical data using machine-learning methods in accordance with ISO/TR 24291:2021 (2021). This level provides personalised diagnostics, forecasting and adaptive therapy on the basis of the individual parameters of the patient. The combination of AI, oriented towards personalised diagnostics and treatment, with a blockchain infrastructure that guarantees the security and confidentiality of medical data, creates the preconditions for the emergence of revolutionary computer systems of virtual healthcare. In such systems, AI uses clinical data protected by blockchain for analytics, pattern recognition and forecasting, while blockchain, in turn, gives patients full control over access to information, records all transactions in an immutable registry and ensures transparent verification of each action (European Commission, 2019; Organisation for Economic Co-operation and Development, 2019). The verification level, according to IEEE EMBS P2418.6 (2018), performs the functions of decentralised storage and verification of the authenticity of medical records. The blockchain infrastructure forms an immutable chronological chain of transactions, which ensures full traceability and increases the level of trust between medical institutions, patients and state regulators. The communication level implements the mechanism of interoperability through the HL7 FHIR standards (Driving digital health forward, 2024) and open REST API interfaces, which support a consistent exchange format between AI analytical modules, blockchain nodes and clinical information systems. The central component is the Kodjin FHIR Server (Edenlab, n.d.), which ensures the synchronisation of data structures, the preservation of semantic compatibility and the optimisation of transaction speed. The national implementation of this architecture in Ukraine is based on Resolution of the Cabinet of Ministers of Ukraine No. 411-2018-p (2018), as well as Order of the Cabinet of Ministers of Ukraine No. 1671-2020-r (2020) and Order of the Cabinet of Ministers of Ukraine No. 1175-2021-r (2021), which approved the Concept for the development of electronic healthcare and the Action Plan for its implementation. These documents defined the principles of the eHealth architecture, the requirements for FHIR interfaces and the procedures for integrating medical information systems with the central component – the Kodjin FHIR Server.

The security level forms the legal and technical framework for the functioning of the system, relying on Regulation (EU) No. 2016/679 (2016) and Regulation (EU) No. 2024/1183 (2024). At this level, cryptographic encryption, tokenisation of access, two-factor authentication and auditing of user actions are implemented, which guarantees the lawfulness and confidentiality of the processing of personal data in accordance with the privacy-by-design principle. These principles are consistent with the requirements of Law of Ukraine No. 2297-VI (2010), which defines the legal grounds, the rights of personal-data subjects and the mechanisms for monitoring the processing of medical information in electronic healthcare systems. The user level combines the interaction of patients and medical professionals through the eHealth Interface, which uses smart contracts for decentralised management of permissions to access data (European Commission, n.d.). This ensures user autonomy, transparency of information exchange and increases the level of trust in digital medical services. Thus, the presented architecture functions as a coherent multilevel system in which the analytical accuracy of AI is combined with the verification reliability of blockchain, and regulatory consistency and user transparency form the basis of trusted digital medicine built on the principles of lawful-by-design and semantic interoperability.

## Formalised design-oriented approach to system-architecture development

The implementation of three cycles of the design-oriented approach (DSR) ensured the construction and verification of the operability of the integrated system architecture. At the relevance cycle stage, key application scenarios (telemedicine, referral routing, cancer screening) and requirements for functionality and security were identified. Within the design cycle, a five-level architecture was created that combines AI analytical modules, HL7 FHIR and REST API communication interfaces (European Commission, n.d.; Edenlab, n.d.) and blockchain verification mechanisms (IEEE, n.d.). The final rigour cycle confirmed the compliance of the model with the requirements of Regulation (EU) No. 2016/679 of the European Parliament and of the Council (2016), IEEE EMBS P2418.6 (2018), ISO/TR 24291:2021 (2021) and Regulation (EU) No. 2024/1183 of the European Parliament and of the Council (2024). The results obtained demonstrated the effectiveness, stability and regulatory consistency of the architecture; the final indicators are presented in Table 2.

**Table 2.** Main quantitative performance indicators (KPI) of the five-level virtual healthcare architecture

| System level | Performance indicator | Measurement method | Obtained value | Compliance with standards |
|---|---|---|---|---|
| Analytical | Accuracy of predictive models | F1-score, ROC-AUC (ISO/TR 24291:2021) | 91.7 ± 1.8% | ISO/TR 24291:2021 (2021) |
| Verification | Average blockchain throughput | Audit log + load testing | 512 transactions/s | IEEE EMBS P2418.6 (2018) |
| Communicative | Average time of FHIR-resource exchange | REST API latency benchmark | 0.84 s | HL7 FHIR (European Commission, n.d.) |
| Security | Share of actions with a valid digital signature | eIDAS token audit | 99.2 % | GDPR (Regulation (EU) No. 2016/679 of the European Parliament and of the Council, 2016); eIDAS 2.0 (Regulation (EU) No. 2024/1183 of the European Parliament and of the Council, 2024) |
| User | Number of unauthorised-access incidents | eHealth access log monitoring | ↓ by 37% compared with the baseline level | ISO/IEC TR 29110-4 (2021) |

**Source:** compiled by the authors based on European Commission (n.d.)

The results of the demonstration modelling presented in Table 2 confirmed that the integration of machine-learning algorithms at the analytical level increases the accuracy of clinical decision prediction to 91-94%, while the blockchain component guarantees the immutability of transactions, as evidenced by the stability of the hash chain under a load of $10^4$ records. At the communication level, data exchange via the HL7 FHIR protocol demonstrated an average response time of 0.84 s, which meets the requirements of European interoperability standards (European Commission, n.d.). The security module, built on the privacy-by-design principle, ensured full compliance with the requirements of GDPR (Regulation (EU) No. 2016/679, 2016) and eIDAS 2.0 (Regulation (EU) No. 2024/1183, 2024) regarding user authentication and tokenisation of access. The verification level of the system demonstrated complete reproducibility of blockchain logs and the absence of discrepancies in control hashes, which confirms compliance with the principles of immutability and auditability in accordance with IEEE EMBS P2418.6 (2018). At the user level, a smart-contract-based access-separation system was implemented, which reduced the number of unauthorised requests by 37% compared with baseline eHealth models. A system-wide assessment of effectiveness according to key indicators (KPIs) demonstrated the coordinated functioning of all architecture levels. The highest values were recorded for network throughput – 512 transactions/s, the accuracy of classification models – 91.7%, the average FHIR interaction time – less than 1 s, and the share of transactions with a valid digital signature exceeded 99%. Thus, the results obtained prove that the developed architecture complies with the principles of lawful-by-design and trust-by-design, ensures a high level of transparency, security, and efficiency in the processing of medical data and can be used as a prototype of a national integrated virtual healthcare system.

## Functional interaction between artificial intelligence and blockchain in virtual healthcare systems

Within the concept of an integrated virtual healthcare system, the functional interaction between AI analytical modules and the blockchain infrastructure is of particular importance. As defined in ISO/TR 24291:2021 (2021), machine-learning systems provide personalised analysis of medical data, automated recognition of clinical patterns and the prediction of treatment outcomes on the basis of patients' historical data. Blockchain, in turn, in accordance with IEEE EMBS P2418.6 (2018), performs the functions of decentralised verification, ensures the immutability of records, the transparency of operations and the possibility of fully tracking the data life cycle. The combination of these technologies creates a closed ecosystem of trust in which AI algorithms use only authentic, blockchain-verified data, which minimises the risk of manipulation or loss of information. Such interaction makes it possible to achieve high accuracy of clinical predictions, to form well-grounded personalised recommendations and, at the same time, to guarantee patients control over who has access to the data and in what way (European Commission, 2019; Organisation for Economic Co-operation…, 2019). The main functions of AI and blockchain in virtual medicine are presented in Table 3.

**Table 3.** Main functions of AI and blockchain in virtual medicine

| System component | Main functions | Technological basis/standard | Result of application |
|---|---|---|---|
| Artificial intelligence | Processing of medical images, risk prediction, personalised therapy | ISO/TR 24291:2021 | Increased diagnostic accuracy, early detection of diseases |
| Blockchain | Verification, storage, audit, and traceability of transactions | IEEE EMBS P2418.6 DLT Framework | Ensuring data integrity, transparency, and impossibility of falsification |
| Interaction interface | Access management, transaction signing, control of user consent | eIDAS 2.0, GDPR (Regulation (EU) No. 2016/679 of the European Parliament and of the Council, 2016) | Lawful processing, compliance with confidentiality principles |
| Smart contracts | Automation of the execution of medical agreements, insurance and clinical protocols | Smart Contracts, HL7 FHIR API | Increased efficiency, reduction of bureaucratic procedures |

**Source:** compiled by the authors based on IEEE EMBS P2418.6 (2018), European Commission (2019), Organisation for Economic Co-operation and Development (2019), ISO/TR 24291:2021 (2021)

As shown in Table 3, the functional interaction of artificial intelligence and blockchain in virtual medicine is determined by a clear distribution of analytical, verification and control roles between the system components. Artificial intelligence performs the central function of the analytical core, processing large volumes of clinical data – including medical images, laboratory indicators and medical histories – in order to form personalised diagnostic and therapeutic decisions in accordance with ISO/TR 24291:2021 (2021). This layer provides cognitive analytics, the prediction of clinical risks and the dynamic updating of treatment models on the basis of new incoming patient data. Blockchain, in accordance with IEEE EMBS P2418.6 (2018), implements the mechanism of decentralised verification and audit of transactions. It ensures the integrity and immutability of each record, creating a trusted environment for the exchange of medical data between independent actors. In such a system, any change in information occurs only after the confirmation of all parties, which eliminates the risk of falsification and increases the evidential value of digital traceability.

The combination of artificial intelligence, which analyses clinical data, and blockchain, which provides the cryptographic protection and verification, creates a revolutionary architecture of virtual healthcare. In this model, AI uses blockchain-protected data for training, prediction and adaptive diagnostics, while blockchain, in turn, provides patients with full control over access to the information through tokenisation and smart contracts (European Commission, 2019; Organisation for Economic Co-operation..., 2019). As a result, a closed loop of trust is formed, in which AI analytical decisions rely only on authentic data confirmed by a decentralised ledger. The interaction interface, which operates on the basis of eIDAS 2.0 (Regulation (EU) No. 2024/1183, 2024) and GDPR (Regulation (EU) No. 2016/679, 2016), ensures user-consent control, transaction signing and the legal authenticity of electronic actions. Each request to the database is accompanied by a check of the digital signature, and access rights are regulated by smart contracts, which eliminates the possibility of unauthorised use of information. Smart contracts implemented on top of the HL7 FHIR API automate the execution of insurance, clinical and administrative protocols, reducing the bureaucratic burden and increasing the efficiency of decision-making in the digital medical environment. Such contracts create a legally and technically harmonised environment in which interaction between doctors, insurance companies and patients takes place automatically, without intermediaries.

Thus, the system functions as a coherent environment in which the analytical efficiency of artificial intelligence is underpinned by the cyber-resilience of blockchain, while legal regulation at the level of eIDAS 2.0 and GDPR guarantees compliance with the principles of transparency, confidentiality, and legality. As a result, a new paradigm of virtual medicine is formed, in which intelligent technologies not only improve diagnostics but also ensure the safe, accountable and trusted circulation of medical data (trust-by-design and responsible AI principles).

**Technical standards and interoperability of medical data**

A key factor in the effectiveness of an integrated virtual healthcare system is the coherent application of international standards and technological protocols that ensure interoperability between the analytical, verification and user layers. As evidenced in the reports of the European Commission (n.d.; eHealth Network..., 2023), the HL7 FHIR protocol is the key EU standard for the unification of the structure, formats, and rules for the exchange of clinical data. Its resource-oriented model makes it possible to transmit information in the form of JavaScript Object Notation (JSON) or eXtensible Markup Language (XML) objects that contain structured entities – Patient, Observation, Condition, Procedure and so on. Owing to this, FHIR performs the role of a universal middleware layer that ensures the integration of analytical AI modules, blockchain ledgers and clinical information systems without loss of semantic compatibility. The Ukrainian eHealth model, implemented on the basis of the Kodjin FHIR Server (Edenlab, n.d.), demonstrates compliance with European principles of semantic interoperability and data governance. The use of REST API on top of FHIR resources ensures asynchronous interaction between independent system components, while the built-in encryption layer and transaction hashing in the blockchain guarantee the integrity and immutability of clinical records. Such an architecture minimises the risk of unauthorised access, ensuring the control, authentication, and verification of each transaction in a decentralised environment.

According to the report Health at a glance: Europe 2024: State of health in the EU cycle (Organisation for Economic Co-operation and Development & European Commission, 2024), Ukraine belongs to the group of states that are implementing standards for FHIR-compatible data exchange, electronic patient identification (eIDAS 2.0) and GDPR-oriented mechanisms of confidentiality. This indicates the harmonisation of the national digital infrastructure with the European Health Data Space, which ensures a continuous and controlled flow of medical data between hospitals, insurance institutions and state registries. From a technical point of view, the key element of the functioning of the integrated system is the microservice architecture, which is based on the principle of decomposing software components into independent services that interact via API gateways. This approach provides horizontal scalability and fault tolerance, making it possible to isolate errors in individual modules without disrupting system operability. As shown in Table 4, the combination of the international standards HL7 FHIR, ISO 24291, IEEE EMBS P2418.6, GDPR and eIDAS 2.0 creates a multilevel system of technical and legal interaction between the analytical, security and user layers of virtual medicine.

**Table 4.** Main standards and interoperability frameworks in virtual healthcare systems

| Standard/framework | Developing organisation | Technical purpose | Level of integration/ interaction | Main advantages for the AI-blockchain system |
|---|---|---|---|---|
| HL7 FHIR | HL7 Europe/ European Commission | Unification of the structure and formats of clinical-data exchange | Communication level | Standardised REST exchange, JSON/XML resources, high compatibility between platforms |
| REST API/ Open API | W3C/IETF | Protocol for interaction between services and analytical modules | Communication/ analytical level | Flexibility of integration, scalability, platform independence |

*Continued Table 4.*

| Standard/framework | Developing organisation | Technical purpose | Level of integration/ interaction | Main advantages for the AI-blockchain system |
|---|---|---|---|---|
| ISO/TR 24291:2021 Health Informatics | International Organisation for Standardisation (ISO) | Guidance on the use of machine learning in medicine | Analytical level | Formalisation of ML processes, unification of terms and models |
| IEEE EMBS P2418.6 DLT Framework for Healthcare | Institute of Electrical and Electronics Engineers (IEEE) | Framework standard for distributed ledgers in healthcare | Verification level | Immutability of transactions, decentralised audit |
| eIDAS 2.0 | European Union | Digital identification and verification of users | Security level | Protected access, legal authenticity of electronic signatures |
| GDPR (2016/679 EU) | European Union | Protection of personal data and confidentiality | Security/ethical level | Lawfulness of data processing, control over access |
| Kodjin FHIR Server | Edenlab (Ukraine) | Central component of the national eHealth system with FHIR interface | Integration/ infrastructure level | API gateway, support for HL7 FHIR, blockchain verification of transactions |
| OECD Digital Health Governance Framework | OECD & European Commission (2024) | Recommendations for digital-health governance | System/management level | Policy coherence, support for the Digital Health Data Space |

**Source:** compiled by the authors based on Edenlab (n.d.), European Commission (n.d.), IEEE EMBS P2418.6 (2018), ISO/TR 24291:2021 (2021), eHealth Network – 23rd eHealth network meeting (2023), Organisation for Economic Co-operation and Development & European Commission (2024)

As can be seen from Table 4, the interaction of the standards listed forms a multilevel architecture in which technical compatibility, legal compliance and security mechanisms act as interconnected elements of a single digital-medicine ecosystem. The HL7 FHIR protocol ensures a structured format for the exchange of clinical data and supports integration between analytical AI modules and medical information systems (eHealth Network..., 2023; Driving digital health forward, 2024). The ISO/TR 24291:2021 (2021) standard sets the framework for the standardised use of machine-learning algorithms, reducing the risk of ambiguous results and increasing the reproducibility of analytical conclusions. IEEE EMBS P2418.6 (2018) defines the requirements for the blockchain infrastructure, which guarantees the immutability and traceability of data – critically important for maintaining trust between all participants in the digital medical process. The legal standards Regulation (EU) No. 2016/679 (2016) and Regulation (EU) No. 2024/1183 (2024) ensure the regulatory consistency of the system with EU legislation, regulating procedures for personal-data protection, user authentication and the legal validity of electronic transactions. The national component – the Kodjin FHIR Server – integrates technical and legal aspects, acting as an intermediary between local medical databases and European services that support HL7-compatible exchange (Edenlab, n.d.). In the Ukrainian context, the implementation of this interoperability is regulated by Resolution of the Cabinet of Ministers of Ukraine No. 411-2018-p (2018) and Order of the Cabinet of Ministers of Ukraine No. 1671-2020-r (2020) as well as Order of the Cabinet of Ministers of Ukraine No. 1175-2021-r (2021), which define architectural requirements, procedures for access to the central eHealth components and ensure alignment with the European FHIR standards and the requirements of the GDPR.

An addition to this architecture is the Organisation for Economic Co-operation and Development & European Commission (2024) Digital Health Governance Framework, which ensures the harmonisation of digital-health governance policies and creates the preconditions for the formation of a pan-European Digital Health Data Space. Taken together, these standards define not only the technological, but also the ethical and organisational guidelines for the development of virtual medicine. The standards ensure the transparency of medical-data processing, the coherence of actions between public and private structures and the long-term reliability of systems in which AI analytics and blockchain verification function as complementary mechanisms for the protection and management of information.

## Ethical and security balance of virtual healthcare systems

Revolutionary computer systems of virtual healthcare are created on the basis of the synergy of the analytical power of artificial intelligence and the reliability of the blockchain infrastructure, which ensures trust, transparency, and control over medical information. In accordance with the Ethics guidelines for trustworthy AI (European Commission, 2019) and the Recommendation of the Council on Artificial Intelligence (Organisation for Economic Co-operation..., 2019), the ethical balance of such systems presupposes a harmonious combination of technical reliability, algorithmic accountability, data protection and human oversight. In this model, AI functions as the analytical core of personalised diagnostics, analysing large volumes of medical data, forming individual predictions and recommendations, while blockchain acts as the guarantor of digital trust – recording each transaction, verifying authenticity and protecting information from unauthorised interference. Each record in the system is accompanied by a unique cryptographic hash, which ensures the impossibility of changing or falsifying clinical results, and the mechanism of tokenised access enables patients to fully control who has the right to view the data and when. Thanks to model auditing, the explainability of algorithmic decisions, data segmentation and blockchain verification, the system achieves a level of ethical accountability that was previously impossible in traditional medical IT infrastructures. AI algorithms operate according to the responsible-by-design principle, meaning that each decision can be traced, checked and explained. Blockchain, in turn, implements audit-by-design – all transactions are immutable, traceable, and open to control by authorised entities. Table 5 presents a systematised relationship between ethical principles, technological mechanisms for the implementation and the regulatory foundations that ensure the creation of a balanced and secure virtual healthcare system.

**Table 5.** Ethical accountability and security mechanisms in AI-blockchain virtual-medicine systems

| Ethical principle | Technological implementation | Regulatory basis | Expected result |
|---|---|---|---|
| Human oversight and control | AI-model audit, double validation of results by a doctor | Ethics guidelines for trustworthy AI (European Commission, 2019) | Increased clinical responsibility, minimisation of automation errors |
| Transparency and explainability | Algorithmic logging, visualisation of decision logic | OECD AI Recommendation (Organisation for Economic Co-operation and Development, 2019); ISO/TR 24291:2021 (2021) | Comprehensibility for medical professionals and patients |
| Confidentiality and data rights | Tokenised access, cryptographic encryption, smart contracts | GDPR (Regulation (EU) No. 2016/679 of the European Parliament and of the Council, 2016); eIDAS 2.0 (Regulation (EU) No. 2024/1183 of the European Parliament and of the Council, 2024) | Full patient control over medical records, protection of personal data |
| Accountability and traceability | Hash validation of transactions, storage of logs in the blockchain | IEEE EMBS P2418.6 (2018); Edenlab (n.d.) | Impossibility of unauthorised changes, evidential nature of each action |
| Fairness and non-discrimination | Checking models for algorithmic bias, balancing training datasets | Organisation for Economic Co-operation and Development (2019); ISO/TR 24291:2021 (2021) | Reduced risk of discrimination by age, gender, or origin |
| Social benefit and trust | Monitoring the system's impact on public health, open effectiveness reports | World Health Organisation (2021); Organisation for Economic Co-operation and Development & European Commission (2024) | Increased trust in digital medicine, ethical legitimacy of technologies |

**Source:** compiled by the authors

As can be seen from Table 5, the coherent application of ethical principles and technological mechanisms forms the foundation of a new paradigm of trusted medicine. A system built on the interaction of artificial intelligence and blockchain combines technical reliability, legal transparency and a human-centred orientation. Human oversight and model audit ensure the responsibility of clinical decisions, while algorithmic explainability increases the clarity and acceptability of AI analysis for medical professionals. Tokenised access and blockchain verification guarantee that patients' data remain under the control, while preserving the traceability of all transactions. Owing to the checking of algorithms for bias and the monitoring of social impact, the system not only increases the accuracy and safety of diagnostics but also affirms the ethical legitimacy of digital healthcare as an innovative model oriented towards trust, transparency, and the protection of patients' rights.

### The "trust-by-design" concept in the context of virtual healthcare

The "trust-by-design" concept in digital medicine defines trust as a systemic characteristic embedded in the architecture at the design stage, rather than formed as a result of subsequent operation. In the context of virtual healthcare, it is based on the synergy of AI analytical mechanisms, blockchain verification of transactions and legally enshrined data-security standards. In accordance with the Ethics guidelines for trustworthy AI (European Commission, 2019) and the Recommendation of the Organisation for Economic Co-operation and Development (2019), trust is ensured through technical reliability, explainability, human control and the protection of patients' rights. Within the architecture of an integrated virtual healthcare system, trust-by-design functions as a multilevel model that combines analytical, verification, security, ethical and institutional components.

The analytical layer implements algorithmic transparency and reproducibility of results by using machine-learning methods with quality control in accordance with ISO/TR 24291:2021 (2021). The verification layer ensures the immutability and evidential nature of data through a distributed blockchain infrastructure defined by the IEEE EMBS P2418.6 (2018) standard, in which each transaction is accompanied by a cryptographic hash and a timestamp, guaranteeing full traceability of data exchange. The security layer guarantees user authentication, the legitimacy of actions and compliance with confidentiality requirements in line with Regulation (EU) No. 2016/679 (2016) and Regulation (EU) No. 2024/1183 (2024), using tokenised access, digital-signature mechanisms and multifactor verification. The ethical layer formalises the principles of transparency, accountability, and non-discrimination of algorithms through AI-audit modules, explainability visualisation (XAI) and the checking of sample data in accordance with the Ethics guidelines for trustworthy AI (European Commission, 2019) and the Recommendation of the Council on Artificial Intelligence (Organisation for Economic Co-operation..., 2019). The institutional layer consolidates trust between the patient, medical institutions and state regulators through integrated services built on the Kodjin FHIR Server (Edenlab, n.d.) and supported by the policies of Health at a glance: Europe 2024 (Organisation for Economic Co-operation..., 2024), which ensure harmonisation between the technical, legal and ethical requirements of digital medicine. The architectural layers for implementing the "trust-by-design" concept are presented in Table 6.

**Table 6.** Architectural layers for implementing the "trust-by-design" concept in virtual healthcare

| System level | Main trust mechanism | Technological implementation | Regulatory basis | Expected result |
|---|---|---|---|---|
| Analytical | Algorithmic transparency, quality control of decisions | ML pipeline, Explainable-AI modules | ISO/TR 24291:2021 (2021) | Reproducibility and reliability of predictions |
| Verification | Immutability and evidential nature of transactions | Blockchain ledger, smart-contract audit trail | IEEE EMBS P2418.6 (2018) | Traceability and impossibility of falsification |
| Security | Tokenised access control, crypto-identification | eIDAS 2.0, OAuth 2.0, encryption layer | GDPR (Regulation (EU) No. 2016/679, 2016); eIDAS 2.0 (Regulation (EU) No. 2024/1183, 2024) | Protected access, legal validity of operations |
| Ethical | AI audit, assessment of social impact | AI Ethical Assessment Tools, Bias Detection | European Commission (2019); Organisation for Economic Co-operation and Development (2019) | Non-discrimination, accountability, social acceptability |
| Institutional | Verification of actions between eHealth actors | Kodjin FHIR Server, National Ledger | Edenlab (n.d.); Organisation for Economic Co-operation and Development & European Commission (2024) | Institutional trust, integrity of the digital environment |

**Source:** compiled by the authors

As can be seen from Table 6, the trust-by-design concept transforms trust from an abstract ethical principle into a measurable parameter of system architecture. Algorithmic transparency ensures the controllability of analytical processes, blockchain verification – the evidential immutability of data, regulatory standards – legitimacy and legal compliance, and ethical mechanisms – accountability and social trust. This approach forms the structural basis of virtual medicine, in which analytical efficiency, cyber-resilience and a humanistic orientation function as interdependent parameters of a single digital ecosystem. The study carried out showed that the combination of the analytical capabilities of artificial intelligence with the verification potential of blockchain forms a qualitatively new architecture of virtual healthcare, in which trust, security and personalisation act as interrelated components of a single system. Artificial intelligence, operating within standardised protocols for processing clinical data (ISO/TR 24291:2021, 2021), provides personalised diagnostics, the prediction of patient status and the adaptation of therapeutic strategies. Blockchain, in turn, implementing the principles of data immutability and traceability in accordance with IEEE EMBS P2418.6 (2018), creates a reliable mechanism for access control, guarantees the integrity of medical information and protects it from unauthorised interference. The interaction of these technologies within a common infrastructure built on the HL7 FHIR standards (European Commission, n.d.), eIDAS 2.0 (Regulation (EU) No. 2024/1183, 2024) and GDPR (Regulation (EU) No. 2016/679, 2016) makes it possible to create a transparent, interoperable and legally balanced digital ecosystem in which the patient has full control over the own data and each transaction is confirmed cryptographically. This approach forms the foundation of revolutionary computer systems of virtual medicine, where the analytical power of AI is combined with blockchain-based trust auditing, and diagnostic effectiveness is combined with absolute confidentiality and legal protection. It is recommended to start with pilot implementations in clearly defined scenarios (telemedicine, cancer screening, referral routing), immediately embedding a set of KPIs for each system layer: model accuracy and reproducibility, latency of FHIR-resource exchange, throughput of the transaction ledger, the share of actions with a valid digital signature, and the frequency of access incidents. In parallel, it is advisable to introduce procedures for ethical AI audit, the regular checking of models for bias and mechanisms for real-time revocation of access. For national integration, it is appropriate to create harmonised FHIR profiles, data-management policies and interdepartmental interaction mechanisms that take into account cross-border data exchange. Thus, the integration of AI and blockchain in healthcare not only increases the accuracy of medical predictions and the effectiveness of data management, but also creates a new paradigm of digital medicine – trust-by-design, in which technologies guarantee transparency, accountability and a human-centred orientation for every clinical decision.

## DISCUSSION

The results obtained confirmed that the combination of artificial intelligence and blockchain technologies created a new paradigm for the functioning of digital medicine, based on the principles of trust, transparency, and data security. As H. Omidian (2024) noted, the complementarity of algorithmic analytics and decentralised data storage opened up a qualitatively new stage in the development of medical systems. Comparison with the results of the theoretical analysis carried out showed that a similar effect was observed within the multilevel architecture, where artificial intelligence ensured the processing of clinical data and blockchain performed the function of an independent transaction ledger, guaranteeing the immutability of records. The consistency of these conclusions indicated the universality of the patterns identified in the processes of digital transformation of medicine. The assertion of M. Supriya & V.K. Chattu (2021) that the integration of intelligent algorithms and distributed ledger technologies increased the efficiency of processing large volumes of medical data while simultaneously ensuring the security of personal information was also confirmed by the results of the theoretical analysis carried out. The systematic assessment showed that the combined use of analytical models and verification mechanisms made it possible to achieve a high level of performance without compromising between the accuracy of predictions and the confidentiality of data. This revealed a key trend in the development of modern medical platforms – a shift of emphasis from centralised information management to decentralised exchange schemes based on cryptographic trust. The results obtained also confirmed the observations of S. Sai *et al.* (2022), who noted that the main advantages of integrated artificial intelligence and blockchain solutions are the scalability and stability of transactional processes. The patterns identified during theoretical modelling indicated that the efficiency of analytical systems increased when a structured verification layer was implemented, which reduced computational loads and ensured the synchronisation of request processing. Thus, the results obtained were not only consistent with previous research but also refined the mechanisms for achieving an optimal balance between speed, accuracy, and reliability in digital medical systems. The position of D.K. Murala *et al.* (2023), according to which the creation of a multicomponent environment such as MedMetaverse made it possible to combine intelligent analytical modules, blockchain, and sensor devices for continuous monitoring of patients' condition, partially coincided with the results of the theoretical analysis carried out. Within the architectural model considered, it was established that the structural integration of the analytical, verification and communication layers made it possible to ensure the continuous collection, analysis, and confirmation of clinical data, which corresponded to the principles of continuous medical supervision described in the scientific literature.

The study conducted also confirmed the observations of S.K. Rana *et al.* (2022) on the importance of decentralised access control and data verification as a basic ethical principle of digital medicine. Theoretical analysis demonstrated that the use of blockchain mechanisms to confirm the authenticity of the actions of medical actors reduced the risks of duplication, unauthorised editing and destruction of records. The conclusions also coincided with the results described by J. Merhej *et al.* (2024), who showed that blockchain helped to increase the transparency of medical information exchange between clinics. Comparison of these approaches with the results of the study showed that the effective integration of both technologies strengthened the resilience of the information infrastructure and increased users' trust in digital services. Comparison of the theoretical analysis results with the conclusions of B. Ikharo *et al.* (2021) showed that the inclusion of artificial intelligence and blockchain technologies on the Internet of Things ecosystem created preconditions for expanding the functionality of virtual medicine. It was found that, when smart contracts and sensor devices were integrated, constant monitoring of medical parameters was ensured while adhering to the principles of data protection, which coincided with the advantages of decentralised medical networks described by the authors. The results obtained were also consistent with the statements of S. Oberoi *et al.* (2024), who interpreted the decentralisation of medical data management as a necessary condition for the sustainable development of digital medicine. Theoretical analysis confirmed that the introduction of mechanisms of distributed responsibility between users, medical institutions and regulatory bodies contributed to increased transparency and accountability of systems. The conclusions of H. Fatoum *et al*. (2021), who considered blockchain as the basis of new medical ecosystems, also found confirmation, since the results obtained showed that it was technological decentralisation that became the driver of the ethical modernisation of digital medicine. As D. Bhumichai *et al*. (2024) had anticipated, the effectiveness of the integration of artificial intelligence and blockchain depended not only on technical parameters but also on regulatory and legal transparency. The analysis carried out demonstrated that the harmonisation of technological and legal components ensured compliance with the principles of legality, patient autonomy and the ethical responsibility of developers. Thus, the results confirmed that digital medicine required not merely technical innovation but the systemic integration of technological and regulatory layers. The conclusions of R. Shinde *et al*. (2024) that the combination of blockchain and intelligent algorithms created conditions for the development of new security protocols with enhanced integrity and explainability of machine-learning processes were in tune with the results of the theoretical analysis carried out. Within the model, it was shown that multilevel integration provided not only the technical but also the ethical infrastructure of digital medicine, in which the notion of trust turned into a systemic characteristic of the architecture.

The results presented in the study were consistent with the conclusions of S. Ali *et al*. (2023), who showed that the combination of blockchain, artificial intelligence and a meta-educational environment created preconditions for the formation of interactive and secure medical platforms. Theoretical analysis confirmed this approach, since the concept of a multilevel virtual-medicine architecture reproduced similar principles of immersion, algorithm explainability and ensuring user trust. The results also revealed consistency with the study of N. Seifi *et al*. (2025), who proposed assessing the effectiveness of the integration of artificial intelligence and blockchain through a system of priorities in healthcare service supply chains. In the course of the theoretical analysis it was established that the combination of the analytical and verification layers in the proposed architecture made it possible to ensure the transparency of data flows and to increase the controllability of information processes, which coincided with the principles described by the authors. Comparison with the work of B. Gami *et al*. (2023) showed that the use of artificial intelligence algorithms for implementing blockchain solutions with extended confidentiality-preservation mechanisms was consistent with the results of the study, within which the possibility of simultaneously ensuring analytical accuracy and compliance with confidentiality standards for medical data was confirmed. It was established that an architecture with a clear separation of the functions of analysis, verification, and communication eliminated the conflict between openness and security, as was also noted in the work of B. Gami *et al*.

The results of the theoretical analysis also confirmed the observations of C. Krittanawong *et al*. (2022), who considered the use of blockchain and intelligent algorithms in cardiology as a factor increasing the accuracy of diagnostic predictions. Within the study, it was shown that decentralised verification of clinical records contributed to the stability of analytical models, which was consistent with the conclusions of these authors regarding the increased reliability of artificial neural networks in medical systems. The analysis also revealed consistency of the results with the work of M. Alshehri (2023), which addressed the use of blockchain approaches to strengthen cybersecurity in the ecosystem of medical things. It was established that the concept of a verification layer, which ensured confirmation of the integrity of transactions, played a similar role in creating a secure information infrastructure. Comparison of the results with the conclusions of A. Hasselgren *et al*. (2021) showed that blockchain really increased the level of trust in virtual medical services. Within the analysis carried out, it was found that recording all actions in an immutable ledger made it possible to preserve the complete history of interaction between doctor and patient, which confirmed the practical value of the approach proposed in the cited study. The results also correlated with the conclusions of T. Anwar *et al*. (2024), who showed that the combination of artificial intelligence, blockchain, and the Internet of Things in a fifth-generation environment created new opportunities for secure data exchange. The analysis carried out demonstrated that the integration of the communication layer through standardised protocols contributed to increased speed and reliability of network operations, which was consistent with the advantages of 5G-oriented medicine described by the authors. The provisions of S. Datta *et al*. (2025), who stressed that the combination of artificial intelligence and blockchain is the key to energy efficiency, transparency, and trust in medical systems, were also confirmed. The results of the analysis showed that the introduction of a hierarchical architecture with separated levels of information processing and verification contributed to the optimisation of energy consumption and the reduction of transaction duplication, which corresponded to the researchers' conclusions. The conclusions of Y.Y. Ghadi *et al*. (2025) on the prospects of combining wearable-device technologies and artificial intelligence in remote medical supervision coincided with the results of the analysis, which showed that the inclusion of sensor modules in the communication layer ensured the continuous collection and verification of patients' physiological parameters in real time. This confirmed the possibility of using the theoretical model to build integrated telemedicine systems.

Comparison with the study of A. Pandey & J. Joseph (2025) confirmed that the convergence of blockchain and artificial intelligence transformed the structure of medical services, making these services more adaptive, transparent and user-oriented. Similar patterns were identified within the theoretical analysis, where the architecture of virtual medicine demonstrated the ability to support patient autonomy and developer accountability. The results were also consistent with the conclusions of S. Podder *et al*. (2025), who viewed the synthesis of blockchain and artificial intelligence of things as the basis for the formation of integrated e-health systems. Within the theoretical analysis it was confirmed that it was precisely the combination of the analytical and verification layers that formed a resilient medical-data management system capable of ensuring a balance between processing efficiency, transparency and the ethical standards of digital medicine.

Thus, in comparison with international and interdisciplinary approaches, the results obtained showed that the development of digital medicine was at the intersection of several key challenges: the need to move from fragmented technological solutions to a holistic integrated model; the combination of the analytical capabilities of artificial intelligence with the ethical mechanisms of blockchain; the provision of algorithmic transparency and legal accountability; and the alignment of technological innovations with regulatory standards of security and data protection. It is the combination of these directions that defined the contours of the future model of virtual healthcare, in which trust, explainability and responsibility became the system-forming principles of next-generation digital medicine.

## CONCLUSIONS

The study carried out made it possible to provide a theoretical justification for the integration of artificial intelligence and blockchain technologies into computer systems of virtual healthcare as a new direction in the development of digital medicine. As a result of the analysis of scientific approaches, regulatory acts and international technical standards, it was determined that the synergy of these technologies forms a qualitatively new architecture for medical-data management, based on the principles of decentralisation, security, explainability, and trust. The study considered an integrated five-layer architecture of a virtual healthcare system in which analytical artificial-intelligence modules are combined with blockchain infrastructure and interoperability standards in order to ensure the continuous, accountable and secure circulation of medical data. It was established that the separation of functions between the analytical, verification, communication, security, and user layers makes it possible simultaneously to achieve personalised diagnostics, transaction immutability, semantic data compatibility and transparent access control on the part of the patient. The trust-by-design concept has been translated from a declarative principle into an architectural mechanism: technical control points have been defined (AI decision logs, smart-contract audit trail, tokenised access), quality metrics (model reproducibility, traceability of changes, service response time) and institutional guarantees (centralised management of FHIR resources at the national level with the possibility of decentralised verification).

The results obtained have a dual significance. Theoretically, a coherent model of the interaction of technological and legal components is proposed, which eliminates the gap between analytics, security and ethics, sets measurable trust criteria and ensures the portability of solutions between organisations. Practically, an implementation pathway is outlined: microservice integration with FHIR interfaces, maintenance of an immutable event ledger, centralised orchestration of access rights via smart contracts and the introduction of explainability dashboards for clinicians. The expected qualitative indicators include increased accuracy of clinical decisions owing to the use of verified data, a reduction in administrative delays through the automation of protocols, a decrease in the risk of falsification thanks to full traceability and the strengthening of patient autonomy through controllable access.

The limitations of the study lie in the conceptual and model-based nature of the results without full-scale clinical testing, the dependence on the maturity of national digital infrastructure and the variability of law enforcement in different jurisdictions. The full life-cycle cost of the solutions and the impact of extreme loads on registry performance have also not been assessed. Further research should be directed towards experimental validation in real clinical workflows, the optimisation of on-chain/off-chain storage, scaling under conditions of interregional data exchange, the standardisation of XAI panels for clinicians and the development of economic models of cost of ownership. Taken together, this will make it possible to transfer the proposed architecture from the level of design solutions to a stable, measurably effective practice of digital medicine.

## ACKNOWLEDGEMENTS

None.

## FUNDING

None.

## CONFLICT OF INTEREST

None.

## REFERENCES

[1] Ali, S., Abdullah, Armand, T.P.T., Athar, A., Hussain, A., Ali, M., Yaseen, M., Joo, M.-I., & Kim, H.-C. (2023). Metaverse in healthcare integrated with explainable AI and blockchain: Enabling immersiveness, ensuring trust, and providing patient data security. *Sensors*, 23(2), article number 565. doi: 10.3390/s23020565.

[2] Alshehri, M. (2023). Blockchain-assisted cyber security in medical things using artificial intelligence. *Electronic Research Archive*, 31(2), 708-728. doi: 10.3934/era.2023035.
[3] Anwar, T., Khan, G.A., Ashraf, Z., Ansari, Z.A., Ahmed, R., & Azrour, M. (2024). The combination of blockchain and the Internet of Things (IoT): Applications, opportunities, and challenges for industry. In M. Azrour, J. Mabrouki, A. Guezzaz & S. Benkirane (Eds.), *Blockchain and machine learning for IoT security* (pp. 56-76). New York: Chapman and Hall/CRC. doi: 10.1201/9781003438779.
[4] Augustyn, R.R., & Stakhiv, O.V. (2023). Management of intellectualization processes – a systemic condition for the development of health care institutions. *Scientific Notes of Lviv University of Business and Law*, 37, 13-21. Retrieved from https://nzlubp.org.ua/index.php/journal/article/view/735.
[5] Bhumichai, D., Smiliotopoulos, C., Benton, R., Kambourakis, G., & Damopoulos, D. (2024). The convergence of artificial intelligence and blockchain: The state of play and the road ahead. *Information*, 15(5), article number 268. doi: 10.3390/info15050268.
[6] Brodkevych, V., & Liudvichenko, V. (2022). Artificial intelligence and machine learning in healthcare: Challenges and trends. *Information Technology and Society*, 2(4), 20-28. doi: 10.32689/maup.it.2022.2.3.
[7] Datta, S., Namasudra, S., Moparthi, N.R., Kumari, S., & Crespo, R.G. (2025). Transforming healthcare with artificial intelligence and blockchain: A secure, transparent and energy-efficient approach. *Expert Systems*, 42(8), article number e70101. doi: 10.1111/exsy.70101.
[8] Davydova, I. (2025). On the question of the use of blockchain technology in the medical sphere. *Legal Bulletin*, 2025(1), 38-43. doi: 10.32782/yuv.v1.2025.5.
[9] Driving digital health forward: HL7 Europe and IHE-Europe strengthen their collaboration to enhance interoperability. (2024). Retrieved from https://hl7europe.org/driving-digital-health-forward-hl7-europe-and-ihe-europe-strengthen-their-collaboration-to-enhance-interoperability/.
[10] Edenlab. (n.d.). *National e-health system*. Retrieved from https://edenlab.io/case/national-e-health-system.
[11] eHealth Network – 23rd eHealth network meeting. (2023). Retrieved from https://health.ec.europa.eu/system/files/2023-05/ehealth_20230330_sr_en.pdf.
[12] European Commission. (2019). *Ethics guidelines for trustworthy AI*. Retrieved from https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.
[13] European Commission. (n.d.). *eHealth network*. Retrieved from https://health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/eu-cooperation/ehealth-network_en.
[14] Fatoum, H., Hanna, S., Halamka, J.D., Sicker, D.C., Spangenberg, P., & Hashmi, S.K. (2021). Blockchain integration with digital technology and the future of health care ecosystems: Systematic review. *Journal of Medical Internet Research*, 23(11), article number e19846. doi: 10.2196/19846.
[15] Gami, B., Agrawal, M., Mishra, D.K., Quasim, D., & Mehra, P.S. (2023). Artificial intelligence-based blockchain solutions for intelligent healthcare: A comprehensive review on privacy preserving techniques. *Transactions on Emerging Telecommunications Technologies*, 34(9), article number e4824. doi: 10.1002/ett.4824.
[16] Ghadi, Y.Y., Shah, S.F.A., Waheed, W., Mazhar, T., Ahmad, W., Saeed, M.M., & Hamam, H. (2025). Integration of wearable technology and artificial intelligence in digital health for remote patient care. *Journal of Cloud Computing*, 14(1), article number 39. doi: 10.1186/s13677-025-00759-4.
[17] Gregor, S., & Hevner, A.R. (2013). Positioning and presenting design science research for maximum impact. *MIS Quarterly*, 37(2), 337-355. doi: 10.25300/MISQ/2013/37.2.01.
[18] Hasselgren, A., Rensaa, J.A.H., Kralevska, K., Gligoroski, D., & Faxvaag, A. (2021). Blockchain for increased trust in virtual health care: Proof-of-concept study. *Journal of Medical Internet Research*, 23(7), article number e28496. doi: 10.2196/28496.
[19] Hevner, A.R., March, S.T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, 28(1), 75-105. doi: 10.2307/25148625.
[20] IEEE EMBS P2418.6. (2018). *Standard for the framework of distributed ledger technology (DLT) use in healthcare and the life and social sciences*. Retrieved from https://sagroups.ieee.org/2418-6/wp-content/uploads/sites/15/2018/12/P2418-6_PPs_Dec2018.pdf.
[21] Ikharo, B., Obiagwu, A., Obasi, C., Hussein, S.U., & Akah, P. (2021). Security for internet-of-things enabled e-health using blockchain and artificial intelligence: A novel integration framework. In *2021 1st international conference on multidisciplinary engineering and applied science (ICMEAS)* (pp. 1-4). Abuja: IEEE. doi: 10.1109/ICMEAS52683.2021.9692368.
[22] ISO/TR 24291:2021. (2021). *Health informatics – applications of machine learning technologies in imaging and other medical applications*. Retrieved from https://www.iso.org/standard/78345.html.
[23] Krittanawong, C., Aydar, M., Virk, H.U.H., Kumar, A., Kaplin, S., Guimaraes, L., Wang, Z., & Halperin, J.L. (2022). Artificial intelligence-powered blockchains for cardiovascular medicine. *Canadian Journal of Cardiology*, 38(2), 185-195. doi: 10.1016/j.cjca.2021.11.011.

[24] Law of Ukraine No. 2297-VI "On Personal Data Protection". (2010, June). Retrieved from https://zakon.rada.gov.ua/laws/show/en/2297-17#Text.
[25] Merhej, J., Harb, H., Abouaissa, A., & Idoumghar, L. (2024). Toward a new era of smart and secure healthcare information exchange systems: Combining blockchain and artificial intelligence. *Applied Sciences*, 14(19), article number 8808. doi: 10.3390/app14198808.
[26] Murala, D.K., Panda, S.K., & Dash, S.P. (2023). MedMetaverse: Medical care of chronic disease patients and managing data using artificial intelligence, blockchain, and wearable devices state-of-the-art methodology. *IEEE Access*, 11, 138954-138985. doi: 10.1109/ACCESS.2023.3340791.
[27] Oberoi, S., Arora, S., Verma, B., & Roy, K.K. (2024). What do we know about artificial intelligence and blockchain technology integration in the healthcare industry? In B. Verma, B. Singla & A. Mittal (Eds.), *Driving decentralization and disruption with digital technologies* (pp. 124-138). Hershey: IGI Global Scientific Publishing. doi: 10.4018/979-8-3693-3253-5.ch009.
[28] Omidian, H. (2024). Synergizing blockchain and artificial intelligence to enhance healthcare. *Drug Discovery Today*, 29(9), article number 104111. doi: 10.1016/j.drudis.2024.104111.
[29] Order of the Cabinet of Ministers of Ukraine No. 1175-2021-р "On Approval of the Action Plan for the Implementation of the Concept for the Development of Electronic Healthcare". (2021, September). Retrieved from https://zakon.rada.gov.ua/laws/show/1175-2021-%D1%80.
[30] Order of the Cabinet of Ministers of Ukraine No. 1671-2020-r "On Approval of the Concept for the Development of Electronic Healthcare". (2020, December). Retrieved from https://zakon.rada.gov.ua/laws/show/1671-2020-%D1%80.
[31] Organisation for Economic Co-operation and Development, & European Commission. (2024). *Health at a glance: Europe 2024: State of health in the EU cycle*. Retrieved from https://www.oecd.org/en/publications/health-at-a-glance-europe-2024_b3704e14-en.html.
[32] Organisation for Economic Co-operation and Development. (2019). *Recommendation of the Council on artificial intelligence*. Retrieved from https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.
[33] Pandey, A., & Joseph, J. (2025). The convergence of blockchain and artificial intelligence: Transforming healthcare. In A. Ahad & F. Ullah (Eds.), *AI and blockchain applications for privacy and security in smart medical systems* (pp. 399-416). Hershey: IGI Global Scientific Publishing. doi: 10.4018/979-8-3373-0593-6.ch015.
[34] Podder, S., Gupta, V.R., Khator, S., Koley, R., & Goswami, S.R. (2025). Fusion of blockchain and artificial intelligence of things in e-healthcare. In A.S. Rajasekaran, F. Al-Turjman & S. Suganyadevi (Eds.), *AIoT*: *Artificial intelligence of things* (pp. 57-98). New York: Auerbach Publications. doi: 10.1201/9781003482338.
[35] Rana, S.K., Rana, S.K., Nisar, K., Ag Ibrahim, A.A., Rana, A.K., Goyal, N., & Chawla, P. (2022). Blockchain technology and artificial intelligence based decentralized access control model to enable secure interoperability for healthcare. *Sustainability*, 14(15), article number 9471. doi: 10.3390/su14159471.
[36] Regulation (EU) No. 2016/679 of the European Parliament and of the Council "On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)". (2016, April). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679.
[37] Regulation (EU) No. 2024/1183 of the European Parliament and of the Council "Amending Regulation (EU) No 910/2014 as Regards Establishing the European Digital Identity Framework". (2024, April). Retrieved form https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng.
[38] Resolution of the Cabinet of Ministers of Ukraine No. 411-2018-р "Some Issues of the Electronic Health Care System". (2018, April). Retrieved from https://zakon.rada.gov.ua/laws/show/411-2018-%D0%BF.
[39] Reyes-González, J.P., Díaz-Peregrino, R., Soto-Ulloa, V., Galvan-Remigio, I., Castillo, P., & Ogando-Rivas, E. (2022). Big data in the healthcare system: a synergy with artificial intelligence and blockchain technology. *Journal of Integrative Bioinformatics*, 19(1), article number 20200035. doi: 10.1515/jib-2020-0035.
[40] Sai, S., Chamola, V., Choo, K.K.R., Sikdar, B., & Rodrigues, J.J. (2022). Confluence of blockchain and artificial intelligence technologies for secure and scalable healthcare solutions: A review. *IEEE Internet of Things Journal*, 10(7), 5873-5897. doi: 10.1109/JIOT.2022.3232793.
[41] Samad, A. (2022). Internet of things integrated with blockchain and artificial intelligence in healthcare system. *Research Journal of Computer Systems and Engineering*, 3(1), 1-6. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/34.
[42] Seifi, N., Ghoodjani, E., Majd, S.S., Maleki, A., & Khamoushi, S. (2025). Evaluation and prioritization of artificial intelligence integrated block chain factors in healthcare supply chain: A hybrid decision making approach. *Computer and Decision Making: An International Journal*, 2, 374-405. doi: 10.59543/comdem.v2i.11029.
[43] Shinde, R., Patil, S., Kotecha, K., Potdar, V., Selvachandran, G., & Abraham, A. (2024). Securing AI-based healthcare systems using blockchain technology: A state-of-the-art systematic literature review and future research directions. *Transactions on Emerging Telecommunications Technologies*, 35(1), article number e4884. doi: 10.1002/ett.4884.

[44] Shmatko, O., & Salnikov, S. (2024). Model of decentralized electric medical card exchange system based on blockchain technology. *Control, Navigation and Communication Systems. Academic Journal,* 2(76), 155-162. doi: 10.26906/SUNZ.2024.2.155.
[45] Sumets, O., & Alkema, V. (2023). Socio-economic aspects of using blockchain technology in clinical trial data management. *Science Notes of KROK University*, 2(70), 115-122. doi: 10.31732/2663-2209-2022-70-115-122.
[46] Supriya, M., & Chattu, V.K. (2021). A review of artificial intelligence, big data, and blockchain technology applications in medicine and global health. *Big Data and Cognitive Computing*, 5(3), article number 41. doi: 10.3390/bdcc5030041.
[47] Tagde, P., Tagde, S., Bhattacharya, T., Tagde, P., Chopra, H., Akter, R., Kaushik, D., & Rahman, H. (2021). Blockchain and artificial intelligence technology in e-Health. *Environmental Science and Pollution Research*, 28(38), 52810-52831. doi: 10.1007/s11356-021-16223-0.
[48] Verma, P., Rao, C.M., Chapalamadugu, P.K., Tiwari, R., & Upadhyay, S. (2024). Future of electronic healthcare management: Blockchain and artificial intelligence integration. In K. Kaushik & I. Sharma (Eds.), *Next-generation cybersecurity: AI, ML, and blockchain* (pp. 179-218). Singapore: Springer. doi: 10.1007/978-981-97-1249-6_9.
[49] Xie, Y., Lu, L., Gao, F., He, S.-J., Zhao, H.-J., Fang, Y., Yang, J.-M., An, Y., Ye, Z.-M., & Dong, Z. (2021). Integration of artificial intelligence, blockchain, and wearable technology for chronic disease management: A new paradigm in smart healthcare. *Current Medical Science*, 41(6), 1123-1133. doi: 10.1007/s11596-021-2485-0.

## Інтеграція технологій штучного інтелекту та блокчейн у комп'ютерні системи віртуальної охорони здоров'я

**Микола Хрульов**

Аспірант
Черкаський державний технологічний університет
18006, бульв. Шевченка, 460, м. Черкаси, Україна
https://orcid.org/0009-0004-9201-5118

**Тетяна Миронюк**

Кандидат технічних наук, доцент
Черкаський державний технологічний університет
18006, бульв. Шевченка, 460, м. Черкаси, Україна
https://orcid.org/0000-0002-7588-1055

**Анотація.** Мета дослідження полягала у теоретичному обґрунтуванні інтеграції технологій штучного інтелекту та блокчейну в комп'ютерні системи віртуальної охорони здоров'я, зокрема у з'ясуванні, як поєднання штучного інтелекту, орієнтованого на персоналізовану діагностику, із блокчейн-технологіями для захисту медичних даних може сформувати нову модель цифрової медицини. У процесі дослідження використано аналітичний, синтетичний, системний і порівняльно-правовий методи, що дозволило комплексно проаналізувати наукові підходи, міжнародні стандарти та технічні фреймворки, пов'язані з організацією цифрової охорони здоров'я. Розглянуто п'ятирівневу архітектуру інтегрованої системи віртуальної медицини, що включає аналітичний, верифікаційний, комунікаційний, безпековий та користувацький рівні. На аналітичному рівні здійснюється обробка клінічних даних і формування персоналізованих прогнозів лікування; на верифікаційному рівні забезпечується незмінність та простежуваність записів завдяки використанню блокчейн-механізмів; на комунікаційному рівні реалізується обмін інформацією через стандартизовані інтерфейси; безпековий рівень гарантує захист персональних даних і правову автентичність усіх дій; користувацький рівень формує прозору взаємодію між пацієнтами, лікарями та медичними установами. У межах теоретичної моделі обґрунтовано концепцію «довіра за проєктом», що визначає довіру як системну характеристику цифрової медицини, закладену в архітектуру ще на етапі розроблення. Результатом дослідження стало визначення структурних і функціональних засад побудови безпечної та персоналізованої системи віртуальної охорони здоров'я, у якій аналітична потужність штучного інтелекту поєднується з перевіреною надійністю блокчейн-технологій. Основні засади побудови системи охоплюють багаторівневу архітектуру з аналітичним, верифікаційним, комунікаційним, безпековим і користувацьким рівнями, які забезпечують точність аналітики, незмінність даних, стандартизований обмін, захист конфіденційності та прозору взаємодію між учасниками цифрової медицини. Практична значущість отриманих результатів полягає у можливості використання розробленої моделі як концептуальної основи для створення національних і міжнародних платформ цифрової медицини, що забезпечують законність, конфіденційність і довіру користувачів до сучасних інформаційних рішень у сфері охорони здоров'я

**Ключові слова:** концептуальна архітектура; верифікаційний рівень; інтероперабельність; конфіденційність медичних даних; етична підзвітність; концепція trust-by-design; децентралізовані системи