International Journal of Latest Engineering and Management Research (IJLEMR)
ISSN: 2455-4847
www.ijlemr.com || Volume 08– Issue 12 || December 2023 || PP. 45-61

Data Integrity and Auditing in Healthcare using .NET Blockchain: An Analytical Study

Maksym Tytarenko[1]
[1]*Bachelor, Lumighost Ltd., London, 71-75 Shelton Street Covent Garden WC2H 9JQ*

Abstract: Blockchain technology, together with decentralised networks, is proving to be a promising solution for improving the performance, security, and resilience of information networks, especially in the context of healthcare support. This paper presents the results of a study on the use of .NET Blockchain in the development of decentralised networks for information support in healthcare services. Several key findings are demonstrated through modelling and analysis. First, the decentralised network model significantly improves data transfer capabilities compared to a centralised topology. Secondly, the decentralised network shows a long-term high level of performance and low latency, which indicates its advantage in the efficient processing of medical data. In addition, it was found that decentralised networks are inherently resistant to DDoS attacks due to their distributed nature, the use of smart contracts, and the asymmetry of node importance. The findings highlight the benefits of using .NET Blockchain technology in creating decentralised networks for information support in healthcare services. Improved data transfer, resistance to DDoS attacks, and efficient information processing make this approach appropriate in ensuring the integrity and security of medical data in information systems. This study contributes to the expansion of knowledge in the field of practical applications of blockchain in critical industries such as healthcare.

Keywords: Blockchain, .NET, Decentralized Networks, Medical Services, Security

I. INTRODUCTION

In today's healthcare context, the need to ensure data integrity and compliance with security standards is crucial. The healthcare industry has been heavily influenced by technological innovations, and the reliability and security of patient information has become a crucial aspect in this context. The introduction of blockchain technology in the healthcare sector is carried out in accordance with modern requirements for data security and integrity [1]. A study analysing the use of .NET Blockchain technology in the context of data integrity and auditing in healthcare is worthy of attention.

The healthcare sector faces many challenges, including illegal access to medical information, fraudulent activities, and the need for continuous data exchange between healthcare facilities. These challenges require the implementation of innovative solutions that not only guarantee data integrity but also provide an effective audit mechanism. The means offered by .NET Blockchain technology is a powerful tool for achieving these goals [2].

According to Mordor Intelligence [3], the global use of Blockchain technology in the healthcare industry is estimated at USD 2.37 billion by the end of 2023. At the end of the five-year forecast period (2028), the global healthcare blockchain market is estimated to grow to USD 19.52 billion. (an increase of 8.237 times / CAGR - 52.48 %). At the same time, one of the significant drivers for the greater involvement of blockchain technology in the medical field is the significant falsification of medicines: 30 % of the total production, according to WHO estimates, and according to the Pharmaceutical Security Institute, the rate of crimes in the pharmaceutical sector has increased 30.6 times over twenty years (2002 - 196 / 2022 - 6000) [3]. Other analytical companies expect a similar increase in investment in the development of Blockchain technologies for medical applications: Allied Market Research [4] - $ 16.3 billion. USD in 2031 (CAGR - 40.8 %), Precedence Research [5] - USD 14.25 billion in 2032 (CAGR - 40.8 %). In 2032 (CAGR - 34.02 %), Grand View Research [6] - USD 21.14 billion. USD 21.14 billion in 2030 (CAGR - 68.40 %). Thus, the average growth rate of the Blockchain technologies market in the healthcare industry is CAGR - 48.93 %, which indicates a significant interest of stakeholders in ensuring information security and related problems of protecting relevant healthcare data.

The above circumstances actualise the chosen research vector and indicate the practical need to ensure information security in the healthcare sector, in particular, using Blockchain technology.

II. LITERATURE REVIEWS

Blockchain technology has a practical application in the medical field, which is confirmed by the experts' opinion - Table 1.

Table1

Analysis of expert opinions on the application of Blockchain technology in the medical industry

Expert organisation	Areas of application of Blockchain technology in the medical industry	Link
Mordor Intelligence	Clinical Data Exchange, Billing Management and Claims Adjudication, Supply Chain Management	[3]
Allied Market Research	Supply Chain Management, Data Exchange and Interoperability, Claims Adjudication and Billing, Others	[4]
Precedence Research	Claims Adjudication & Billing, Clinical Data Exchange & Interoperability, Clinical Trials &eConsent, Supply Chain Management, Others	[5]
Grand View Research	Clinical Data Exchange & Interoperability, Claims Adjudication & Billing, Supply Chain Management, Clinical Trials &eConsent, Others	[6]
MarketsandMarkets	Supply Chain Management, Clinical Data Exchange and Interoperability, Claims Adjudication & Billing Management, Others	[7]
P&S Intelligence	Clinical Data Exchange and Interoperability, Claims Adjudication and Billing Management, Drug Supply Chain Management, Drug Discovery and Clinical Trials, Prescription Drug Abuse	[8]
Verified Market Research	Claims Adjudication & Billing, Clinical Data Exchange & Interoperability	[9]
Vantage Market Research	Clinical Data Exchange, Billing Management and Claims, Supply Chain Management, Adjudication	[10]
Business Wire	Clinical Data Exchange & Interoperability, Claims Adjudication & Billing	[11]
Polaris Market Research	Clinical Data Exchange & Interoperability, Claims Adjudication & Billing, Supply Chain Management, Clinical Trials &eConsent, Others	[12]

Source: author's development

Based on the data presented in Table 1, the following comparative conclusions can be drawn:

- According to several expert sources, the main applications of blockchain technology in the healthcare industry include clinical data exchange, billing and insurance claims management, and medical supply chain management. These areas are common to most sources.
- Some expert sources also point to specific applications, such as supporting clinical trials, countering prescription abuse and medication misuse. This indicates the diversity of possibilities for the use of blockchain technology in the medical field.
- Some application areas, such as clinical data exchange and supply chain management, are found in most expert sources, indicating their high level of relevance and popularity in the context of blockchain technology implementation in the medical sector.
- Many expert organisations point out that blockchain technology helps to ensure data security and build trust between participants in the healthcare system. This demonstrates the importance of these aspects in the areas of application under consideration.
- Experts cite various applications of blockchain technology in the healthcare industry, which indicates a wide range of opportunities and potential benefits of this technology for healthcare.

Thus, based on the analysis of information from various expert sources, it can be concluded that blockchain technology offers broad prospects for application in the healthcare industry and can help in various aspects, including data security, invoice and supply chain management, research support, and other areas.

Experts also highlight certain tools for applying blockchain technology in the medical industry - Table 2.

Table2

Analysis of experts' opinions on the use of Blockchain technology tools in the medical industry

Expert organisation	Variations in the application of Blockchain technology tools in the medical industry	Link
STL Advisory Limited	Supply Chain Transparency, Patient-Centric Electronic Health Records, Smart Contracts for Insurance and Supply Chain Settlements, Medical Staff Credential Verification, IoT Security for Remote Monitoring	[13]
Geekflare	Patient Data Management, Medical Data Security Assurance, Improving Communication between Providers and Patients, Genomic Data	[14]

Expert organisation	Variations in the application of Blockchain technology tools in the medical industry	Link
	Protection, Smart Contracts for Insurance and Supply Chain Settlements, Healthcare Transactions Control, Drug Supply Chain Counterfeit Management, Tracking Medical Credentials, Integration with Wearable IoT Devices	
Softermii Inc.	Patient Data Management, High-Security Standards in Data Encryption, Healthcare Transactions Control, Drug Supply Chain Management, Clinical Trials and Healthcare Research Improvement, Medical Paperwork Management, Integration with Wearable IoT Devices, Tracking Medical Credentials, Smart Contracts for Insurance	[15]
Analytics Steps Infomedia LLP	Providing Accommodation in a Variety of Sectors, Improved Patient treatment that is Faster, Less Expensive, and More Effective, Genomic Data Protection, Insurance and Supply Chain Settlements using Smart Contracts, Medical Data Security Assurance, Improving Communication Between Providers and Patients,	[16]
Itrex Group	Transparent Supply Chain, Faster Medical Credentialing, Patient-Centered EHRs, Manageable Medical Trials, Enhanced Security, Commitments Enforced Via Smart Contracts, Genomic Research	[17]
Cointelegraph	Medical Record Management, Clinical Trials, Prescription Brug Traceability, Supply Chain Management, Medical Device Management, Telemedicine, Drug Development, Personalized Medicine, Health Insurance	[18]
News-Medical.Net	Managing Electronic Medical Record (EMR) Data, Protection of Healthcare Data, Personal Health Record Data Management, Point-of-care Genomics Management, Electronics Health Records Data Management, Mobile Health Apps and Remote Monitoring, Tracing and Securing Medical Supplies, Health Insurance Claims, Tracking Diseases and Outbreaks, Safeguarding Genomics	[19]
GeeksforGeeks	Securing Patient Data, Medical Drugs Supply Chain Management, Single Longitudinal Patient Records, Supply Chain Optimization, Drug Traceability, Cryptocurrency Payments, Decentralized Storage of Medical Records, Update Medical Supply Chain Management, Improves Electronic Health Record Systems, Improved Recruitment for Clinical Trials	[20]
101 Blockchains	Supply Chain and Drug Counterfeit, Data Segmentation and No Proper Management, Healthcare Data Storage and Security, Drug Traceability, Clinical Trials, Patient Data Management, Claim and Billing,	[21]
PixelCrayons	Electronic Health Records, Drug Supply Chain Integrity, Against Counterfeit Drugs, Tracking Medical Credentials, Enhancing Data Security	[22]

Source: author's development

Comparing the conclusions of various expert organisations on the application of Blockchain technology in the healthcare sector (Table 2), we can identify some common and distinctive trends:

- The vast majority of expert sources point to clinical data exchange, supply chain management, and healthcare data security as key areas of Blockchain application in healthcare;
- Almost all expert organisations emphasise the importance of Blockchain as a tool to ensure the security and integrity of medical data;
- A significant number of expert sources point to the management of the supply chain of medical products as a critical area of application that helps to avoid counterfeiting and ensure the quality and safety of medicines.
- Expert opinions indicate that Blockchain improves cooperation between medical institutions and patients by facilitating data exchange and reducing bureaucratic procedures;
- According to expert organisations, smart contracts are actively used to automate insurance payments and supply chain management in healthcare;

- The expert community believes that Blockchain supports clinical and genomics research by facilitating data collection and analysis;
- According to experts, integration with IoT devices and wearables helps to expand the possibilities of remote patient monitoring and medical data management.
- Some expert sources, such as Cointelegraph and News-Medical.Net, provide a list of various application areas, including disease monitoring, drug development, telemedicine, etc.

In summary, Blockchain technology is proving to be a powerful tool for improving healthcare, ensuring data security, and optimising many aspects of the healthcare sector. The variety of applications and their overall impact on improving efficiency and trust in healthcare make Blockchain technology an important asset for the healthcare industry.

At the same time, the focus of the current study is to identify the potential of Blockchain technology to ensure data integrity and audit of medical services and related operations. To this end, let us consider relevant and up-to-date studies - Table 3.

Table 3
Analysis of studies on the use of Blockchain technology in healthcare to ensure data integrity and audit of medical services and related operations

Researchers	Key aspects of the study	Link
Jabbar et al. (2020)	Researchers emphasise that the electronic health record (EHR) exchange system is an important tool in the medical industry, capable of predicting treatment outcomes and ensuring the effectiveness of therapy. However, ensuring the integrity and interoperability of data remains a challenge due to the large amount of information, security issues, and diversity of systems. In this context, the researchers propose BiiMED: a blockchain framework to improve EHR exchange. It includes an access management system for sharing EHRs between healthcare providers and a decentralised Trusted Third-Party Auditor (TTPA) to ensure data integrity. This work sets the stage for further research into interoperability and data integrity in a fully decentralised environment, improving the delivery of healthcare and reducing the risk of errors.	[23]
Dai et al. (2018)	Data management for biomedical research and clinical trials is critical. To improve the quality and reliability of data analysis, the blockchain-based TrialChain platform was developed. It allows you to verify the integrity of data from large-scale studies. The platform uses a private blockchain based on MultiChain, integrates with a data science platform, and has a web-based administration application. TrialChain is integrated into the data collection process and provides public verification of results. The use of a combined private/public blockchain platform allows for data authentication and efficient verification of results through the Trial Chain API. The platform provides a solution for verifying the collection and analysis of biomedical research data, ensuring the security and reliability of information.	[24]
Barbaria, Mahjoubi& Rahmouni (2023)	The paper proposes a blockchain model for ensuring the integrity of medical data in the context of AI-based research. The HL7 FHIR data structure is used for interoperability with existing systems. The model has four components: integration with FHIR, blockchain for access control and data auditing, distributed architecture for privacy, and APIs for the network.	[25]
Zhang et al. (2022)	This study proposes a blockchain-based data sharing model (BHDSF) to provide fine-grained access control and efficient retrieval of encrypted personal health records (PHRs) in remote healthcare. BHDSF takes into account the risks of unreliable cloud services and malicious auditors and provides reliable PHR integrity checking and metadata verification using blockchain technology. In addition, BHDSF enables effective aggregate authentication to verify source records from H-IoT devices, which is lacking in most existing data exchange systems.	[26]
Zaabar et al.	Researchers are proposing to improve the security and privacy of	[27]

Researchers	Key aspects of the study	Link
(2021)	electronic health records (EHRs) using blockchain technology. The proposed architecture uses decentralised databases to avoid the problems of centralised storage. The decentralised OrbitDB database is used to store EHRs using the Hyperledger Fabric network and Hyperledger Composer to store data hashes and control access. The proposed architecture is designed to improve the reliability of healthcare management systems and avoid security limitations typical of conventional systems for smart healthcare. The results of the performance evaluation and benchmarking have proven the reliability and benefits of the proposed system in terms of security and privacy, key characteristics of healthcare blockchain systems, and performance metrics including throughput and latency.	
Benil & Jasper (2020)	This study proposes a new scheme, called EC-ACS (Elliptical Curve Certificateless Aggregate Cryptography Signature scheme), to ensure the security and privacy of electronic health records (EHR) in a cloud environment using blockchain technology. The scheme uses elliptic curve cryptography (ECC) to encrypt medical data and generate a digital signature for data exchange and storage in the cloud. The use of blockchain technology guarantees the integrity, traceability, and secure storage of medical records. This scheme ensures the security, confidentiality, and protection of information from unauthorised access in the medical data storage system in the cloud environment.	[28]
Shen, Guo & Yang (2019)	This study proposes an efficient health data exchange scheme, named MedChain, which combines blockchain, digest chain, and structured P2P network technologies to overcome the inefficiencies of existing approaches to sharing different types of health data. Based on MedChain, a session-based medical data exchange scheme has been developed that provides flexibility in data exchange. The evaluation results show that MedChain can achieve higher efficiency and meet the security requirements of healthcare data exchange.	[29]
Lee, Kim & Kim (2019)	This study proposes a framework for health data exchange called SHARE Chain. SHARE Chain uses blockchain technology to improve data reliability and includes two features to address reliability and interoperability issues between institutions. The first enhancement is to improve reliability through data integrity in the blockchain ledger and the creation of a Consortium Blockchain Network for data exchange between authenticated institutions. The second feature improves interoperability on healthcare data exchange standards: Fast Healthcare Interoperability Resources and Cross-Enterprise Document Sharing.	[30]
Shae & Tsai (2017)	The study proposes the architecture of a blockchain platform for clinical trials and precision medicine. It identifies 4 new system architecture components to be developed on top of the traditional blockchain and discusses their technological challenges: (a) a new blockchain parallelisation component for analysing large amounts of data, (b) a data management component for integrating large amounts of data, (c) an anonymity management component for protecting the privacy of individuals and IoT devices and secure data access, and (d) a data exchange management component for creating a trusted healthcare data ecosystem.	[31]
Choudhury et al. (2019)	This study proposes a novel data management system for multi-site clinical trials based on blockchain technology. We demonstrate how our system, using smart contracts and private channels, provides confidential data communication, protocol execution, and an automated audit trail. We compare this system to a traditional approach to data management and evaluate its effectiveness in meeting the key requirements of multi-site clinical trials. Our system ensures compliance with research ethics regulatory bodies (IRBs) across sites and participants.	[32]

Source: author's development

Based on the analysis (Table 3), we note that researchers are focusing on several key aspects when developing solutions that ensure data integrity and audit of medical services and related operations:

- to ensure the integrity of medical data, researchers are developing architectural solutions that use blockchain technology to protect data from unauthorised changes and keep it unchanged;
- the use of smart contracts in blockchain technology allows automating the audit and tracking of medical operations and services. This helps to increase the safety and reliability of medical operations;
- researchers are developing solutions to ensure the confidentiality of medical data and restrict access to it only to authenticated users;
- the use of healthcare data exchange standards, such as HL7 FHIR, helps to improve interoperability between different systems and ensure the quality of data exchange.
- researchers also pay attention to the efficiency and productivity of the developed solutions to make them suitable for widespread use in healthcare.

To summarise, research in the field of Data Integrity and Auditing in Healthcare using .NET Blockchain addresses the issues of protecting the integrity of medical data, auditing medical operations, and ensuring confidentiality in healthcare. Researchers emphasise the importance of using blockchain technology to create reliable and secure medical systems.

Proposed solutions include the creation of consortial blockchain networks for the exchange of medical data, the use of smart contracts to automate the audit and tracking of transactions, and the application of healthcare data exchange standards to improve interoperability and quality of data exchange.

The studies reviewed are aimed at ensuring the security and reliability of healthcare data exchange and make a significant contribution to improving healthcare systems and ensuring patient protection.

At the same time, we note that currently, a relatively small number of scientific papers contain information on the performance of networks that use security systems based on .NET Blockchain technology. Given the above circumstances, it is advisable to perform comparative modelling with the establishment of substantive indicators to determine the effectiveness of centralised and decentralised network topological solutions.

III. PURPOSE AND OBJECTIVES

The purpose of the study is to test the technical capability of a medical service information support network built on the principles of .NET Blockchain decentralisation to ensure high performance with unconditional data integrity.

Research Objectives:

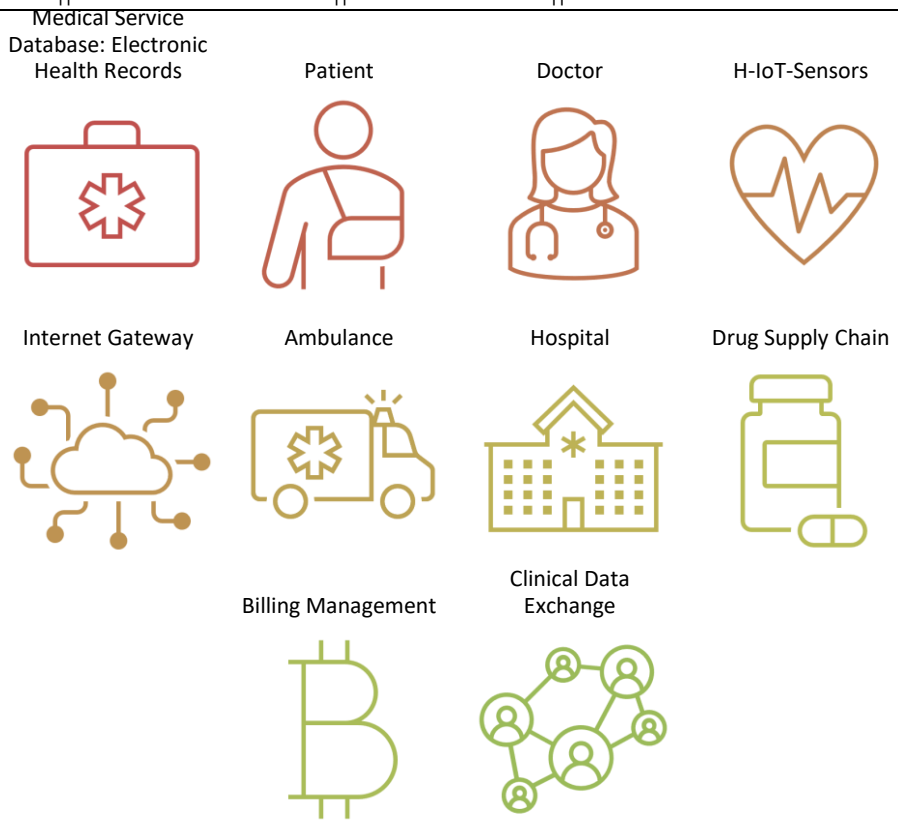
1. Identify a typical scheme of a modern healthcare network that requires ensuring the integrity of operational data.
2. Perform modelling of a centralised and decentralised information network for medical service support.
3. Perform a comparative analysis of the modelling results.
4. Determine the effectiveness of the information network for the support of medical services, formed on the principle of decentralisation of .NET Blockchain.
5. Formulate analytical conclusions based on the results of the study.

IV. METHODOLOGY

Based on the capabilities of modern electronic medical services, we will form a diagram of the nodes of the modelled .NET Blockchain network - Fig. 1.

In accordance with the above concept (Fig. 1), in the modelled network based on the principles of decentralisation and the use of smart contacts in the context of ensuring a closed cycle of medical services, it is advisable to consider a minimum set of elements (9 units), in which the main ones are the patient, the doctor, and the database, and the other components depend on the decisions of the leading participants in the blockchain network.

The modelling of the above scheme (Fig. 1) is performed to determine the key parameters of the network's capacity. The main characteristic of the modelled .NET Blockchain network is the time of data transfer between elements.



Source: author's development

Figure 1 Elementary diagram of nodes of the modelled .NET Blockchain network

The process of data transmission in the form of indivisible blocks (store-and-forward routing (SFR)) is described by the equation – (1):

$$t_{SFR} = t_l + \left(\frac{m}{R}\right) \times l, \tag{1}$$

Where t_l – network latency: the initial preparation time is the time that characterises the duration of message preparation for transmission, route search in the network, etc. This time is taken into account when calculating the total time of data transfer between processors and determining the communication component of the duration of a parallel algorithm in multiprocessor computing systems; m – block size; R – Network throughput: Throughput is the maximum amount of data that can be transmitted per unit time over a single data link. This characteristic is measured, for example, by the number of bits transmitted per second; and – the length of the data transmission route.

When describing the modelling of a .NET Blockchain network, the point-to-point technology is used, where the element that has the source block prepares the entire amount of data to be transferred, determines the transit element through which the data can be delivered to the target element, and starts the data transfer operation. The element to which the block is directed first receives all the transmitted data and then starts transmitting the received block further along the route.

The second method of communication involves dividing the original block into smaller data blocks (packets), which reduces the amount of information transmitted. With this method of transmission (MPP), a transit element can send data packets to subsequent elements after receiving the first packet, without waiting for the entire block to be received. This method of communication is called "cut-through routing" or CTR.

Data transmission time for CTR – (2):

$$t_{CTR} = t_{SFR} + \frac{V}{R} \times \left(l + \left\lceil \frac{m}{V - V_0} \right\rceil \right) = t_{SFR} + \frac{V}{R} \times (l + n - 1), \tag{2}$$

Where V – data packet size; V_0 – the amount of service information defined in each data packet – "packet header"; n – the number of data packets to be transferred – (3):

$$n = \left\lceil \frac{m}{V - V_0} \right\rceil + 1, \tag{3}$$

Where $\lceil \ \rceil$ – parentheses denoting the operation of casting to an integer with excess.

We assume the size of the medical data block is in the form of a matrix A, with dimension $m \times n$. The sequential block transfer algorithm for a centralised topology has the following complexity – (4):

$$T_1 = n^2 \tag{4}$$

In the case of a decentralised .NET Blockchain network with parallel processes of sending blockchain packets, the complexity is determined by the expression – (5):

$$T_p = \frac{n^2}{p}, \tag{5}$$

Where $\frac{n}{p}$ – block splitting into packets marking.

Taking into account this estimate, the acceleration and efficiency indicators of the parallel data transfer algorithm in the .NET Blockchain network are as follows –(6), (7):

$$S_p = \left\lceil \frac{n^2}{n^2 / p} \right\rceil = p, \tag{6}$$

$$E_p = \left\{ \frac{n^2}{[p \times (n^2 / p)]} \right\} = 1. \tag{7}$$

When transferring data, you should also take into account the time spent on calculating related processes, in particular, determining the block packet – (8):

$$T_{p(calc)} = \frac{n}{p} \times (2n - 1) \times \tau. \tag{8}$$

An estimate of the labour intensity of the general data collection operation can be determined byiterations. At the first iteration, the interacting pairs of .NET Blockchain network elements exchange packets of a volume $w[n / p]$ (w (the size of one packet element in bytes), at the second iteration, this volume is doubled and becomes equal, etc. As a result, the duration of the data collection operation when using the Hockney model can be determined using the following expression – (9):

$$T_{p(comm)} = \sum_{i=1}^{\log_2 p} (\alpha + 2^{i-1} w[n / p] / \beta) = \alpha \log_2 p + w[n / p](2^{\log_2 p} - 1) / \beta, \tag{9}$$

Where α – latency of the data transmission network; β – network throughput.

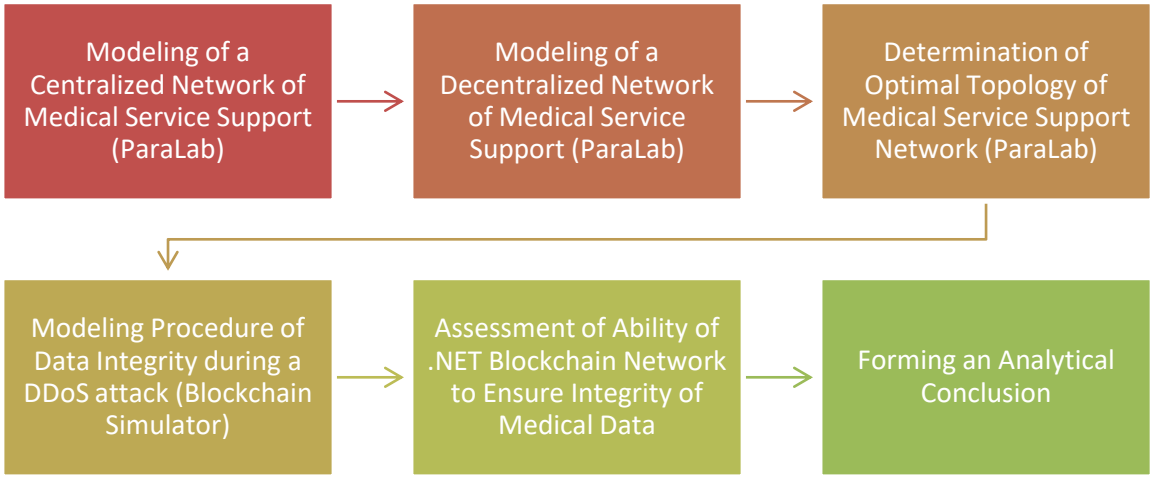
Thus, the total execution time of the parallel decentralised data transfer algorithm (taking into account expressions (8) and (9)) is – (10):

$$T_p = (n / p) \times (2n - 1) \times \tau + \alpha \log_2 p + w(n / p)(p - 1) / \beta. \tag{10}$$

The modelling of topological solutions of centralised and decentralised .NET Blockchain networks is performed in ParaLab [33].

According to the results of the literature review (Table 3), it is confirmed that Blockchain technology can ensure the integrity of medical data. With the help of the Blockchain Simulator [34], this study made it possible to simulate the process of data protection in the case of the most common type of digital attack - DDoS attack [35]-[40].

Thus, the research procedure is as follows - Fig. 2.



Source: author's development

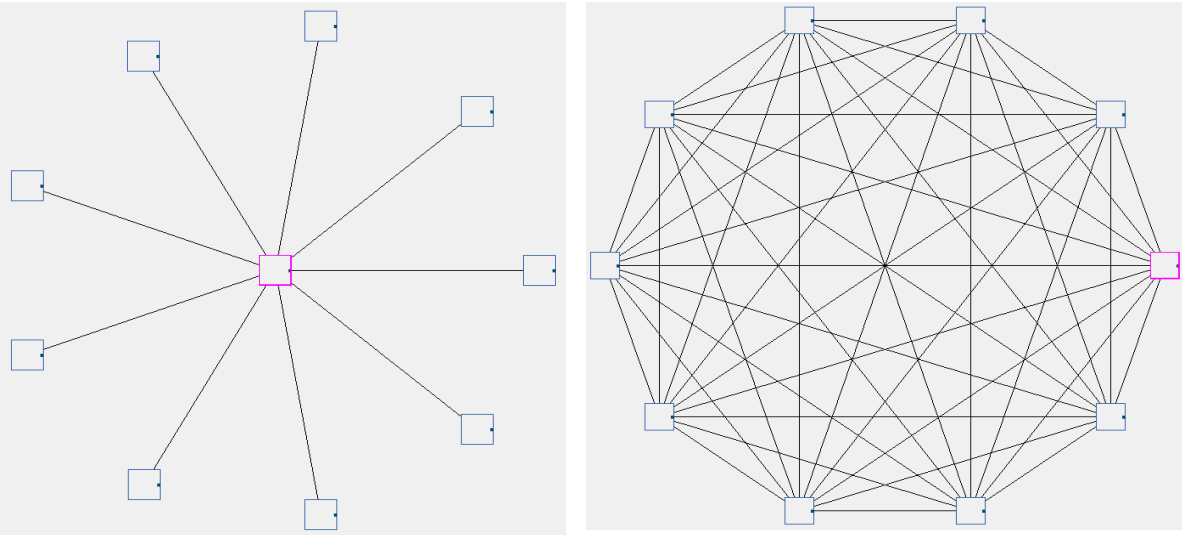
Fig. 2 Research procedure

The proposed research procedure allowed us to extend the parametric analysis of .NET Blockchain networks for medical service support, which are described in the overview section (Table 3).

V. RESULTS

In accordance with the proposed methodology and research procedure, using the ParaLab PC software environment [33], we model a centralised (typical) and decentralised .NET Blockchain network for medical service support, taking into account the number of nodes indicated in the conceptual diagram (Fig. 1) - Fig. 3.

The differences between these schemes are that participants (elements) in a typical topological solution access medical data centrally, while in a decentralised topology (typical for .NET Blockchain networks used on cryptocurrency exchanges), each of the elements can access the necessary data in batches of information blocks from other elements.



a. Centralized Topology b. Decentralized Topology

Source: author's development в ПК ParaLab[33]

Fig. 3 Topology model of the .NET Blockchain network for medical service support

In a centralised system, all data is typically stored on one central server or on multiple centralised servers managed by a single organisation or service provider. All requests for access to the data are directed to the central server. In a decentralised network, the data is distributed among various nodes that are connected to the network. Each node has its own copy of the data and can participate in confirming and processing transactions.

In centralised systems, the integrity and security of data depends on a central server. If the server is vulnerable or under attack, all data can be compromised. Blockchain ensures high data integrity and security

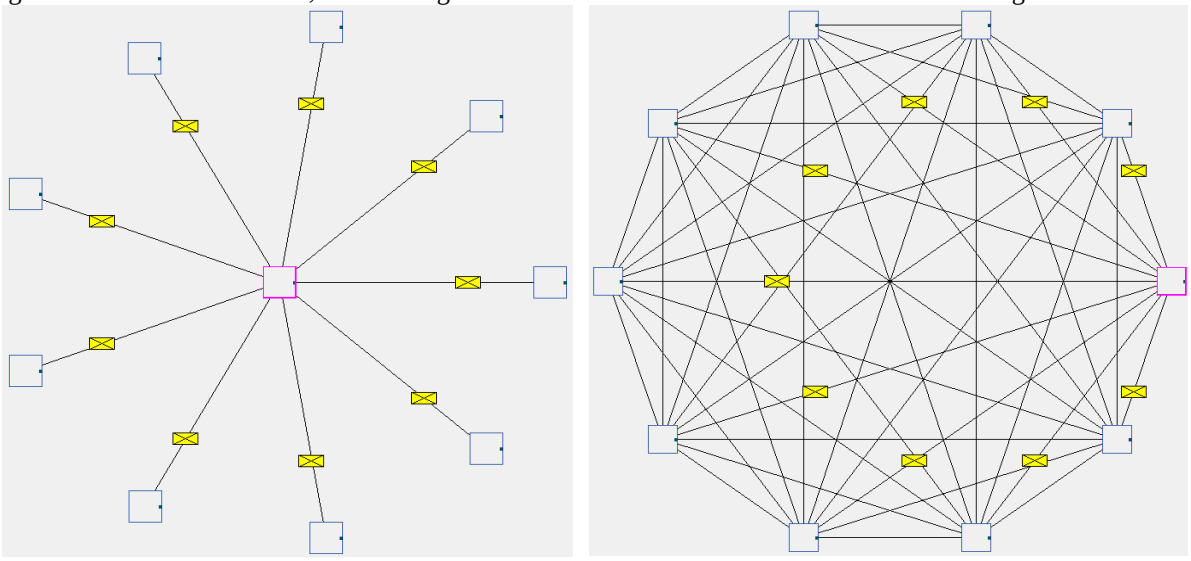
through distributed storage and cryptographic protection. Data in the network cannot be changed without a pre-confirmed transaction, and each node verifies the validity and integrity of the data.

In centralised systems, auditing and tracking of transactions may be limited and dependent on the capabilities of the central server. The system may be less transparent to users. In a blockchain network, all transactions are recorded in the blockchain, allowing for the audit and tracking of each transaction. This makes the network more transparent and reliable.

Access to centralised systems may be more restricted and require multi-formal authorisation and identification procedures. Blockchain can simplify access to data, especially when using smart contracts that automate access control.

In general, decentralised .NET Blockchain networks provide greater security, integrity, and transparency for healthcare information, and can simplify the processes of accessing and sharing data in healthcare.

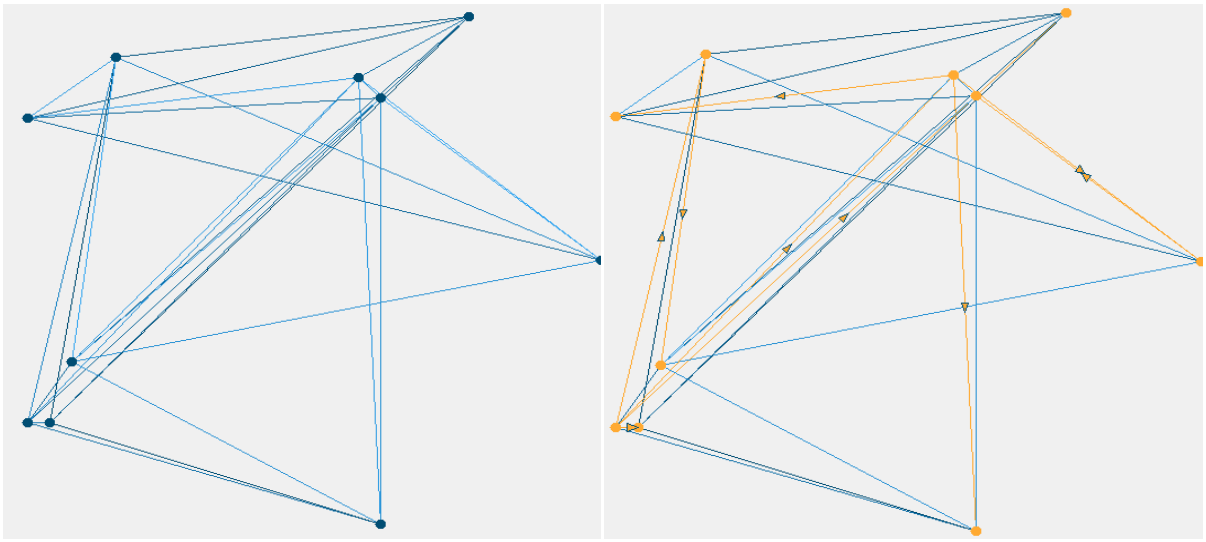
ParaLab [33] allows visualisation of the process of exchanging blocks and packets of information - Fig. 4. It also demonstrates the procedure of transferring information units between all nodes, the location of which is generated in a random order, which brings the modelled situation closer to real conditions - Fig. 5.



a. Centralized Topology b. Decentralized Topology

Source: author's development в ПІК ParaLab[33]

Fig. 4 Visualisation of the process of exchanging blocks and packets of information in modelled .NET Blockchain networks



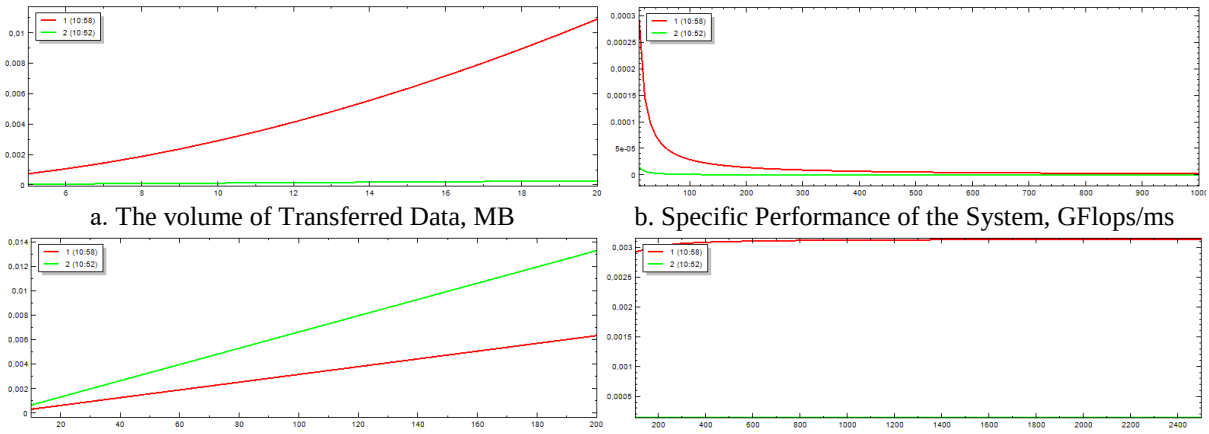
a. Randomly Generated Network b. Visualization of the Longest Contact

Source: author's development в ПІК ParaLab[33]

Fig. 5. Visualisation of the process of exchanging blocks and packets of information in modelled .NET Blockchain networks

According to the results of modelling the .NET Blockchain network of information and service support for medical services, the following aspects have been established (Fig. 6):

- the decentralised network model demonstrates a significantly higher data transfer capacity for the same period of time (Fig. 6, a);
- the specific performance of the decentralised network maintains high parameters for a longer period of time compared to the network arranged according to the centralised topology (Fig. 6, b);
- the centralised system has higher latency values, which indicates the greater efficiency of the decentralised network, since the nodes of this blockchain system need less time to perform preparatory and technological operations (Fig. 6, c);
- at the same time, the decentralised blockchain network demonstrates a stable provision of high throughput of the modelled system, which is explained by the absence of the need for each node to constantly contact the central service when requesting information and passing the corresponding data transaction (Fig. 6, d).



a. The volume of Transferred Data, MB

b. Specific Performance of the System, GFlops/ms

c. System Latency, ms

d. Network Bandwidth, MB/ms

1 – Decentralized Topology; 2 – Centralized Topology

Source: author's development в ПК ParaLab[33]

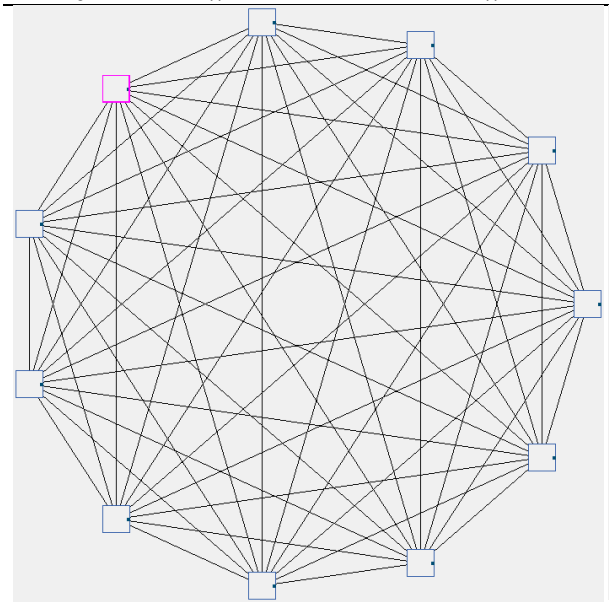
Fig. 6. Results of modelling.NET Blockchain networks

The following analytical conclusions can be drawn from the relevant results of modelling the .NET Blockchain network (Fig. 6):

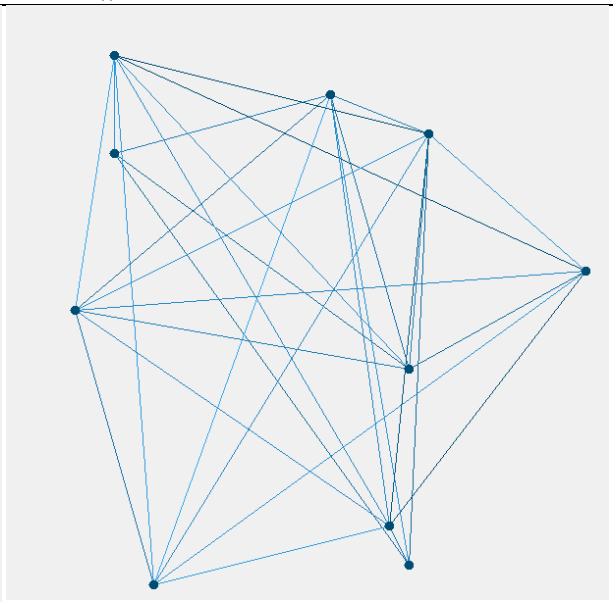
- decentralised blockchain networks allow medical data to be transferred more efficiently and quickly compared to centralised systems. This is especially important in cases of urgent emergencies, when quick access to information can save lives;
- the use of blockchain allows to ensure reliable integrity of medical data. Each transaction is recorded and protected cryptographically, making it impossible for unauthorised access or modification of information;
- blockchain provides transparency of operations and the ability to audit medical transactions in real-time. This helps to reduce the risk of errors and misunderstandings between the elements of the medical service;
- decentralised blockchain networks reduce waiting times for access to medical data. This improves the quality of patient care and helps to avoid delays in the provision of medical care;
- blockchain can be used to ensure the confidentiality of medical data, leaving control over access to it in the hands of patients and medical professionals.

Thus, a decentralised .NET Blockchain network proves to be a more productive and reliable system for information and service support of medical services, which can be important for ensuring data integrity and efficient data exchange in the healthcare sector.

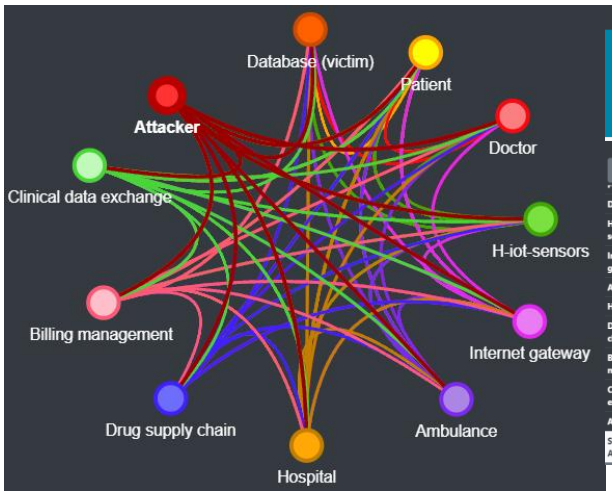
In accordance with the proposed methodology and research procedure, using the PC Blockchain Simulator [34], we will simulate a DDoS attack on a decentralised .NET Blockchain network during information-block and information-packet transactions between model nodes. To do this, let's introduce the eleventh element - the attacker (Fig. 7) - into the formed model (Fig. 3, b).



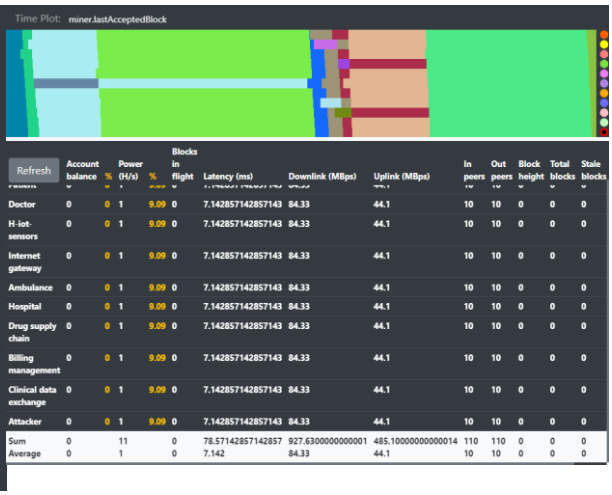
a. Decentralized Model with the integration of DDoSAttack



b. Randomly Generated Network with the integration of DDoS Attack



c. Counterpart of the Model Built in Blockchain Simulator [34]



d. Modeling of Information Transactions During DDoS Attack

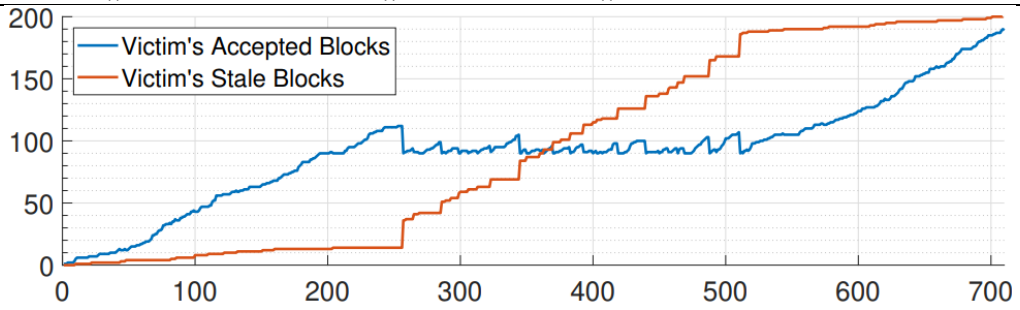
Source: author's development в ПК ParaLab[33]та в ПКBlockchain Simulator [34]

Figure 7 Modelling a DDoS attack on a decentralised .NET Blockchain network

According to the modelling results (Fig. 8), it was found that after a DDoS attack on node 1 in the blockchain network, an interesting impact on the system's functioning was observed. The attack disables the victim's ability to transfer blocks to the network and leads to an increase in the number of stale blocks in the network. At the same time, the number of received blocks remains unchanged.

During a DDoS attack, the victim continues to mine valid blocks, but due to the restrictions imposed by the attack on the network, these blocks are rewritten by other nodes (nodes 2-4) that are not under attack before node 1 can transfer them to other nodes and receive the reward. As a result, node 1 loses the longest chain competition and any blocks it mined during the DoS attack become obsolete or invalid according to the longest chain rule.

Thus, it is established that DDoS attacks can lead to serious problems in the operation of the blockchain network, such as an increase in the number of outdated blocks and the loss of a node's ability to broadcast its blocks in a timely manner. The security and resilience of the blockchain to such attacks are important aspects for ensuring the reliability and integration of the network.



Source: author's development в ПКBlockchain Simulator [34]

Fig. 8. Dynamics of information transactions in the central server (node 1 - victim) during a DDoS attack on a decentralised .NET Blockchain network, block/s

Based on the results of modelling a DDoS attack on a decentralised .NET Blockchain network, we come to the following conclusions:

- in a decentralised network, information is distributed among many nodes. This means that even if one or more nodes are attacked, other nodes can continue to function. This reduces the overall impact of a DDoS attack on the network;
- decentralised networks often distribute processing among many nodes responsible for verifying and processing transactions. This makes it difficult to load a single node, which reduces the success of a DDoS attack;
- decentralised networks such as Ethereum can use smart contracts to automatically validate and process transactions. This helps reduce attack vulnerabilities and the impact of DDoS attacks on the network;
- most blockchain networks use cryptography to secure data and transactions. This can make it difficult for attackers to hack or modify data;
- in decentralised networks, not all nodes have the same status or importance. Some may be more important, while others may be less important. This creates asymmetry in the network, which can make it difficult for DDoS attacks to target all nodes simultaneously.

Thus, decentralised .NET Blockchain networks are more resistant to DDoS attacks due to the distributed nature and security measures used in such networks.

Based on the research and simulations, it can be concluded that decentralised .NET Blockchain networks demonstrate better performance and security compared to the typical centralised topology of information networks for medical service support. Decentralised networks are more resistant to various types of attacks, such as DDoS attacks, due to the distributed nature of the network and cryptographic security measures. Decentralised networks can provide faster data transfer speeds and reduced response times due to the distributed processing of information across many nodes. The loss of a single node in a decentralised network does not lead to a system failure as a whole, as other nodes can continue to operate. The use of cryptography in decentralised networks helps to protect data and transactions from unauthorised access and modification.

In general, decentralised .NET Blockchain networks are more reliable and productive solutions for healthcare information networks compared to centralised systems.

VI. DISCUSSION

The following theses are presented for discussion:

- .NET Blockchain networks have a high potential for preserving the integrity of medical data and stable operation of multi-component systems even during digital attacks;
- .NET Blockchain networks have optimal topological solutions that allow for greater productivity and stability of medical services built on the principles of blockchain decentralisation.

A number of authors confirm the expediency of using blockchain technology to protect networks from various types of criminal influence, in particular, to protect against DDoS attacks. Relevant research, analytical conclusions, and proposals are provided in the following publications [41]– [45]:

- the authors of the study [41] emphasise the importance of protecting against DDoS attacks and botnets in IoT networks using blockchain and SDN. The researchers focus on the development of a botnet prevention system for IoT that takes advantage of both Software Defined Networking (SDN)

and the distributed blockchain (DBC). Through simulations and analysis, the study demonstrates how the integration of blockchain and SDN can effectively detect and dismantle botnets, thus protecting devices from falling under the control of malicious actors;

- the authors of [42] explore the use of blockchain and SDN to protect against DDoS attacks in multiple network domains. The researchers create an architecture with a smart contract in a private blockchain, which allows for a distributed protection system for all hosts. The blockchain helps to implement shared protection, and SDN allows to activate security services and policies;
- the authors of [43] investigate the use of blockchain to protect an SDN network from DDoS attacks. The BSD-Guard system uses the blockchain to calculate suspicious flows and develop collective defence strategies. Experiments show the effectiveness of BSD-Guard in detecting and preventing DDoS attacks in the context of multiple controllers by identifying the attack path;
- researchers [44] propose a method for detecting DDoS attacks in a blockchain network based on a model of cross-multilayer convolutional neural networks. The method improves the detection accuracy and reduces false signals caused by the peculiarities of attacks and the complexity of analysis used by other methods. Experimental results demonstrate the success of the proposed method;
- the authors of the study [45] point out the importance of redesigning IoT network management with security and efficiency in mind, using the approach of Software-Defined Networking (SDN), blockchain, and neural networks to detect and prevent DDoS attacks in IoT systems.

The listed relevant publications ([41]-[45]), although confirming the theses of the current study on the benefits of using blockchain technologies to build secure networks, study the security aspect separately from the topological aspects of deploying such networks, which significantly affects the performance and, as a result, the resilience of the systems under study. Accordingly, the results of this study are more systematic and useful for the formation of information support networks for medical services.

There have also been published scientific works whose authors study topological solutions for the deployment and arrangement of blockchain networks, in particular, such publications include [46] - [50]:

- The authors of the study [46] found that the requirements for a blockchain-enabled network differ from traditional networks. A detailed study of these requirements is an important task. The work on understanding the network aspects of blockchains is relevant and has open research questions;
- researchers [47] developed and successfully implemented the BTCmap system to identify and map the topology of the Bitcoin network. This system was used to create a snapshot of the Bitcoin network topology and confirmed that it is connected. The results can be useful for further research and analysis of the Bitcoin network and other similar cryptocurrency networks;
- study [48] demonstrates the possibility of reducing the block generation interval without increasing the frequency of forks by improving the network topology of nodes and reducing the block propagation time. The presented method of selecting neighbouring nodes affects the block propagation time in the network and improves its efficiency by analysing it in a blockchain simulator. The study confirms that the proposed method indeed improves the speed of block propagation in the network;
- publication [49] presents the results of a study of the use of the DAG blockchain for mobile and ad hoc networks (MANETs), which is called a “blockchain”. The paper defines the characteristics of the blockchain framework, such as consensus protocol requirements for network partitioning resistance, blockchain protocol specifications to support the blockchain data structure, and a group management system that responds to network topology changes and provides relevant information about the network topology of the blockchain framework;
- paper [50] investigates the use of blockchain to improve network performance and data transmission reliability. An improved P2P topology for fast transmission and a trusted blockchain network is proposed. The simulation results showed the advantages of BlockP2P-EP compared to Bitcoin and Ethereum.

Thus, the cited relevant publications ([46]-[50]) also describe only one aspect of blockchain networks, namely, topology and network architecture. Although these authors confirm the conclusions of this study regarding the importance of decentralisation enabled by blockchain technology, they consider only certain aspects related to the details of network deployment and design. In this study, however, a correlation has been established between data integrity, cybersecurity, data auditing, efficiency, optimal performance, and stability of .NET Blockchain networks, which are the result of the decentralised approach of blockchain technology. The results obtained in the current study confirm the relevance of the .NET Blockchain framework for the

deployment of healthcare information support networks, as the modelled decentralised networks have demonstrated stability, security, high performance, and distributed access.

VII. CONCLUSION

The results of the study demonstrated that the use of .NET Blockchain technology in the context of information support for medical services can lead to a significant improvement in data integrity, cybersecurity, audit, and network performance. The distinctive feature of a decentralised .NET Blockchain network is its ability to ensure resilience and stability of operation even in demanding scenarios of information exchange (due to cyber-attacks), which makes it an attractive alternative for creating safe and reliable information support networks for medical services. Given the powerful potential of this technology, the .NET Blockchain framework can be used to create networks that meet the high standards of security, integrity, and performance required to provide medical services with a reliable and efficient information infrastructure.

The aspects considered, such as data transfer performance, DDoS resistance, the use of smart contracts, and the asymmetry of node importance, emphasise the importance of decentralisation and the use of .NET Blockchain to ensure reliable and secure information support for medical services. The results of the study demonstrate the relevance of the use of these technologies in the healthcare sector and the possibility of improving the quality of services and protecting patient data.

The results of this study can be used for the practical implementation of secure and stable information support networks for medical services using .NET Blockchain technology. They will allow developers, architects, and information systems engineers to implement decentralised solutions that provide high performance, cybersecurity, intrusion resistance, and ensure reliable data transmission.

VIII. Acknowledgements

An acknowledgment section may be presented after the conclusion if desired.

REFERENCES

[1] Wu, H., Dwivedi, A. D., & Srivastava, G. (2021). Security and privacy of patient information in medical systems based on blockchain technology. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, *17*(2s), 1-17.https://doi.org/10.1145/3408321

[2] Chukwu, E., & Garg, L. (2020). A systematic review of blockchain in healthcare: frameworks, prototypes, and implementations. *Ieee Access*, *8*, 21196-21214. https://doi.org/10.1109/ACCESS.2020.2969881

[3] *Blockchain in Healthcare Market Size & Share Analysis - Industry Research Report - Growth Trends*. (2023). Mordor Intelligence. https://www.mordorintelligence.com/industry-reports/blockchain-market-in-healthcare

[4] *Blockchain in Healthcare Market Insights, Trends*. (2023). Allied Market Research. https://www.alliedmarketresearch.com/blockchain-technology-in-the-healthcare-market-A10259

[5] *Blockchain In Healthcare Market Size, Report 2032*. (2022).Precedence Research. https://www.precedenceresearch.com/blockchain-in-healthcare-market

[6] *Blockchain Technology in Healthcare Market Report, 2030*. (2017).Grand View Research. https://www.grandviewresearch.com/industry-analysis/blockchain-technology-healthcare-market

[7] *Blockchain Technology in Healthcare Market Revenue Forecast | Latest Industry Updates | Markets and Markets*. (2018). Markets and Markets. https://www.marketsandmarkets.com/Market-Reports/blockchain-technology-healthcare-market-109977720.html

[8] *Blockchain in Healthcare Market Demand Forecast Report, 2030*. (2022). P&S Intelligence. https://www.psmarketresearch.com/market-analysis/blockchain-in-healthcare-market

[9] *Blockchain In Healthcare Market Size, Share, Opportunities, And Forecast*. (2021). Verified Market Research. https://www.verifiedmarketresearch.com/product/blockchain-in-healthcare-market/

[10] *Blockchain in Healthcare Market Size USD 20976.96 Million by 2030*. (2022). Vantage Market Research. https://www.vantagemarketresearch.com/industry-report/blockchain-in-healthcare-market-1223

[11] *Global Blockchain Technology in Healthcare Market* (2022 to 2030). (2022). Business Wire. https://www.businesswire.com/news/home/20220614005643/en/Global-Blockchain-Technology-In-Healthcare-Market-2022-to-2030---Size-Share-Trends-Analysis-Report---ResearchAndMarkets.com

[12] *Blockchain in Healthcare Market Size, Share Global Analysis Report, 2022 - 2030*. (2022). Polaris Market Research. https://www.polarismarketresearch.com/industry-analysis/blockchain-in-healthcare

[13] *5 blockchain healthcare use cases in digital health*. (2023). STL Advisory Limited. https://stlpartners.com/articles/digital-health/5-blockchain-healthcare-use-cases/
[14] *9 Applications of Blockchain in Healthcare*. (2022). Geekflare. https://geekflare.com/applications-of-blockchain-in-healthcare/
[15] *Top 9 Use Cases of Blockchain in Healthcare & Benefits You Should Know*. (2022). Softermii Inc. https://www.softermii.com/blog/blockchain-in-healthcare-practical-use-cases-benefits-you-should-know
[16] *6 Applications of Blockchain in the Healthcare Sector*. (2022). Analytics Steps Infomedia LLP. https://www.analyticssteps.com/blogs/6-applications-blockchain-healthcare-sector
[17] *Top 7 blockchain use cases in healthcare*. (2022). Itrex Group. https://itrexgroup.com/blog/blockchain-use-cases-in-healthcare-advantages-challenges/
[18] *9 promising blockchain use cases in the healthcare industry*. (2023). Cointele graph. https://cointelegraph.com/news/blockfi-appeals-to-cancel-bankruptcy-status-for-sbf-s-offshore-investment-vehicle
[19] *Blockchain Applications in Healthcare*. (2023). News-Medical.Net. https://www.news-medical.net/health/Blockchain-Applications-in-Healthcare.aspx
[20] *Benefits of Blockchain in Healthcare*. (2023). Geeks for Geeks. https://www.geeksforgeeks.org/benefits-of-blockchain-in-healthcare/
[21] *Blockchain For Healthcare: Use Cases And Applications*. (2019).101 Blockchains. https://101blockchains.com/blockchain-for-healthcare/
[22] *Blockchain Healthcare Use Cases for 2023*. (2022). Pixel Crayons. https://www.pixelcrayons.com/blog/blockchain-healthcare-use-cases/
[23] Jabbar, R., Fetais, N., Krichen, M., & Barkaoui, K. (2020, February). Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. In *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)* (pp. 310-317). IEEE.https://doi.org/10.1109/ICIoT48696.2020.9089570
[24] Dai, H., Young, H. P., Durant, T. J., Gong, G., Kang, M., Krumholz, H. M., ... & Jiang, L. (2018). TrialChain: A blockchain-based platform to validate data integrity in large, biomedical research studies. *arXiv preprint arXiv:1807.03662*. https://doi.org/10.48550/arXiv.1807.03662
[25] Barbaria, S., Mahjoubi, H., & Rahmouni, H. B. (2023). A novel blockchain-based architectural modal for healthcare data integrity: Covid19 screening laboratory use-case. *Procedia Computer Science*, *219*, 1436-1443. https://doi.org/10.1016/j.procs.2023.01.433
[26] Zhang, J., Yang, Y., Liu, X., & Ma, J. (2022). An efficient blockchain-based hierarchical data sharing for Healthcare Internet of Things. *IEEE Transactions on Industrial Informatics*, *18*(10), 7139-7150.https://doi.org/10.1109/TII.2022.3145851
[27] Zaabar, B., Cheikhrouhou, O., Jamil, F., Ammi, M., & Abid, M. (2021). Health Block: A secure blockchain-based healthcare data management system. *Computer Networks*, *200*, 108500. https://doi.org/10.1016/j.comnet.2021.108500
[28] Benil, T., & Jasper, J. J. C. N. (2020). Cloud based security on outsourcing using blockchain in E-health systems. *Computer Networks*, *178*, 107344.https://doi.org/10.1016/j.comnet.2020.107344
[29] Shen, B., Guo, J., & Yang, Y. (2019). MedChain: Efficient healthcare data sharing via blockchain. *Applied sciences*, *9*(6), 1207. https://doi.org/10.3390/app9061207
[30] Lee, A. R., Kim, M. G., & Kim, I. K. (2019, November). SHARE Chain: Healthcare data sharing framework using Blockchain-registry and FHIR. In *2019 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)* (pp. 1087-1090). IEEE.https://doi.org/10.1109/BIBM47256.2019.8983415
[31] Shae, Z., & Tsai, J. J. (2017, June). On the design of a blockchain platform for clinical trial and precision medicine. In *2017 IEEE 37th international conference on distributed computing systems (ICDCS)* (pp. 1972-1980). IEEE.https://doi.org/10.1109/ICDCS.2017.61
[32] Choudhury, O., Fairoza, N., Sylla, I., & Das, A. (2019). A blockchain framework for managing and monitoring data in multi-site clinical trials. *arXiv preprint arXiv:1902.03975*.https://doi.org/10.48550/arXiv.1902.03975
[33] *ParaLab*. (2023). Lobachevsky University. https://hpc-education.unn.ru/en/trainings/teachware/paralab
[34] *Blockchain Simulator*. (2023). Simewu. https://simewu.com/blockchain-simulator/index.html
[35] *The Latest DDos Attack Statistics 2023 You Shouldn't Ignore*. (2023). Gitnux. https://blog.gitnux.com/ddos-attack-statistics/#
[36] *20+ DDoS attack statistics and facts for 2018-2023*. (2023). Comparitech Limited. https://www.comparitech.com/blog/information-security/ddos-statistics-facts/

[37] *45 Global DDOS Attack Statistics 2023*. (2023). ASTRA IT, Inc.https://www.getastra.com/blog/security-audit/ddos-attack-statistics/

[38] *Radware Full Year 2022 Report: Malicious DDoS Attacks Rise 150%*. (2022). Radware.https://www.radware.com/newsevents/pressreleases/2023/radware-full-year-2022-report-malicious-ddos-attacks/

[39] *DDoS threat report for 2023 Q1*. (2023). Cloudflare, Inc. https://blog.cloudflare.com/ddos-threat-report-2023-q1/

[40] *DDoS Attack Timeline*. (2023). NETSCOUT. https://www.netscout.com/threatreport/ddos-threat-intelligence-report/#attack-timeline

[41] Shafi, Q., & Basit, A. (2019, January). DDoS botnet prevention using blockchain in software defined internet of things. In *2019 16th international Bhurban conference on applied sciences and technology (IBCAST)* (pp. 624-628). IEEE.https://doi.org/10.1109/IBCAST.2019.8667147

[42] Giri, N., Jaisinghani, R., Kriplani, R., Ramrakhyani, T., & Bhatia, V. (2019, December). Distributed denial of service (DDoS) mitigation in software defined network using blockchain. In *2019 third international conference on I-SMAC (IoT in social, mobile, analytics and cloud)(I-SMAC)* (pp. 673-678). IEEE.https://doi.org/10.1109/I-SMAC47947.2019.9032690

[43] Jiang, S., Yang, L., Gao, X., Zhou, Y., Feng, T., Song, Y., ... & Cheng, G. (2022). Bsd-guard: a collaborative blockchain-based approach for detection and mitigation of sdn-targeted ddos attacks. *Security and Communication Networks*, *2022*. https://doi.org/10.1155/2022/1608689

[44] Dai, Q. Y., Zhang, B., & Dong, S. Q. (2022). A DDoS-attack detection method oriented to the blockchain network layer. *Security and Communication Networks*, *2022*. https://doi.org/10.1155/2022/5692820

[45] Jmal, R., Ghabri, W., Guesmi, R., Alshammari, B. M., Alshammari, A. S., & Alsaif, H. (2023). Distributed Blockchain-SDN Secure IoT System Based on ANN to Mitigate DDoS Attacks. *Applied Sciences*, *13*(8), 4953. https://doi.org/10.3390/app13084953

[46] Dotan, M., Pignolet, Y. A., Schmid, S., Tochner, S., & Zohar, A. (2021). Survey on blockchain networking: Context, state-of-the-art, challenges. *ACM Computing Surveys (CSUR)*, *54*(5), 1-34.https://doi.org/10.1145/3453161

[47] Deshpande, V., Badis, H., & George, L. (2018, September). Btcmap: Mapping bitcoin peer-to-peer network topology. In *2018 IFIP/IEEE International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN)* (pp. 1-6). IEEE.https://doi.org/10.23919/PEMWN.2018.8548904

[48] Aoki, Y., & Shudo, K. (2019, July). Proximity neighbor selection in blockchain networks. In *2019 IEEE International Conference on Blockchain (Blockchain)* (pp. 52-58). IEEE.https://doi.org/10.1109/Blockchain.2019.00016

[49] Cordova, D., Laube, A., & Pujolle, G. (2020, October). Blockgraph: A blockchain for mobile ad hoc networks. In *2020 4th cyber security in networking conference (CSNet)* (pp. 1-8). IEEE.https://doi.org/10.1109/CSNet50428.2020.9265532

[50] Hao, W., Zeng, J., Dai, X., Xiao, J., Hua, Q. S., Chen, H., ... & Jin, H. (2020). Towards a trust-enhanced blockchain P2P topology for enabling fast and reliable broadcast. *IEEE Transactions on Network and Service Management*, *17*(2), 904-917.https://doi.org/10.1109/TNSM.2020.2980303