Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

Design of A Decentralized Medical Data Exchange System Based on the IOTA Tangle

Yaroslav Kliuchka
Postgraduate student, Department of Software Engineering and Management Information Technologies
National Technical University „Kharkiv PolytechnicInstitute”
Kharkiv, Ukraine

Nataliia Fonta
PhD, Associate Professor, Department of Software Engineering and Management Information Technologies
National Technical University „Kharkiv PolytechnicInstitute”
Kharkiv, Ukraine

Oleksander Shmatko
PhD, Associate Professor, Department of Software Engineering and Management Information Technologies
National Technical University „Kharkiv PolytechnicInstitute”
Kharkiv, Ukraine

***Abstract*—The exchange of patient medical records between healthcare providers is essential for quality care but faces challenges related to privacy, security, and centralized control. This article presents the development of a decentralized medical data exchange system using Distributed Ledger Technology based on the IOTA Tangle. The system architecture and core components for immutable storage and transmission of medical records are described. The system uses masking and encryption techniques to maintain patient privacy while allowing healthcare providers to access full records with patient consent. The IOTA Tangle enables fee-less transactions and data integrity verification via its Directed Acyclic Graph structure. System validation through simulation experiments demonstrates the ability to securely share medical data at scale with lower resource costs compared to traditional blockchain designs. The system proves the viability of a decentralized, self-sovereign approach for efficient and confidential medical data sharing using Distributed Ledger Technology. The secure data exchange platform can enable new models of care and research while maintaining patient privacy and healthcare ethics.**

***Keywords*—**electronic healthcare system, medical patient data, distributed ledger technology, IOTA Tangle, blockchain technology

I. INTRODUCTION

Now there is an increase in the use of distributed ledger technology (DLT) in various industries, including healthcare. and this is not surprising since the same blockchain is an immutable, transparent, and decentralised database [1]. The use of blockchain technology in healthcare systems will make it impossible to change medical data. Recently, all information was recorded on paper, which could easily be changed. There are already problems in modern medical systems related to privacy and security [2]. If security and privacy are low or nonexistent, people will be reluctant to share their sensitive information or refuse treatment [1]. As well as access control, data integrity, and reliability, these are the problems that can be solved by implementing DLT in healthcare [2]. We should not forget about health issues that include poor compatibility (or lack thereof) of medical systems, data fragmentation, and a lack of patient activity [3].

The use of DLT in healthcare can transform data storage and sharing, making processes safer and more efficient. Because the main characteristics of this technology are transparency, traceability, reliability, and decentralisation, Therefore, the introduction of DLT in various healthcare systems will avoid problems related to security, privacy, and compatibility [1]. Blockchain is already used in various healthcare systems. In [4], the main areas of blockchain application were presented, among which the main ones can be distinguished: telemedicine, diagnostics, data management and exchange, and supply chain monitoring. However, most of these projects are represented by prototypes or small projects with a small user base. In addition, the blockchain itself has not reached optimal maturity. The technology still has shortcomings that have yet to be addressed. The main ones are scalability, bandwidth, power consumption, and transaction fees. Against the background of all this, IOTA Tangle is a suitable replacement for the blockchain, as it allows you to eliminate all these shortcomings.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

I. LITERATURE REVIEW

The privacy and security of patients' medical records is an ongoing issue, and researchers are trying to develop a system that can help stop the compromise of patient data. A decentralised medical system using IOTA Tangle to protect patients' medical records and medical IoT devices is presented in [5]. As part of this work, four prototype applications were developed to demonstrate the proposed solution: a web recording application, a patient application, a doctor application, and an application for a remote IoT medical device (internet of things). The results show that the proposed framework can improve healthcare services by providing immutable, secure, scalable, reliable, self-managed, and traceable patient health records, giving patients complete control over their own medical records.

The combination of distributed ledger technology and the Internet of Things (IoT) has opened up new opportunities for innovation in medical data management. Security breaches, privacy breaches, and data fragmentation are just some of the issues that DLT can solve. [6] analyses 10 scientific papers published from 2018 to 2021 that suggest the use of IOTA Tangle to solve existing problems. The results show that IOTA Tangle is a good candidate for managing medical data and that it has been successfully implemented as a proof of concept. This forms the basis for further research on the suitability of the IOTA Tangle for managing medical data. And in [7], we analyse articles published from 2017 to 2023 that use blockchain technology to exchange medical data. The results show that the development of blockchain technology and its use for the exchange of medical data is growing. Most studies suggest a unique structure, architecture, or methodology for sharing medical data using blockchain technology. A systematic review of the literature to analyse existing blockchain-based approaches to improving privacy and security in electronic healthcare systems is proposed in [8]. 51 articles published between 2018 and December 2022 were analyzed. The paper discusses in detail the main ideas, the type of blockchain, evaluation metrics, and the tools used for each selected article.

In [9], the CoviReader architecture based on IOTA Tangle is presented, developed for the medical information management system to combat the outbreak of the COVID-19 pandemic. This system allows you to protect the privacy of citizens and their health data from unauthorised access. The proposed CoviReader architecture provides accessibility and, at the same time, restricts data manipulation.

A triple-encrypted authentication architecture that will help patients easily and securely share personal medical records with medical personnel is presented in [10]. The process of transferring records is protected by an encryption mechanism via CEDA, and the correctness of records is checked by the hash value and the blockchain, since information in the blockchain cannot be changed or deleted. The use of such triple protection allows you to achieve the highest level of confidentiality and security for medical records.

A scheme for a medical system based on blockchain technology for implementing the storage and exchange of medical information is proposed in [11]. This system is a multi-node service and collaborative management system that can prevent falsification of medical data and information leakage. It can be used to solve health data management problems.

In [12], it is proposed to use DLT to solve problems related to the security and confidentiality of medical data in developing health systems. In particular, it is proposed to use MAM (Masked Authenticated Messaging) for secure data exchange in the healthcare system. The authors proposed an IOTA Tangle-based model for secure and confidential storage and exchange of information.

To solve problems related to the security of medical data and patient privacy, the authors in [13] propose a new system based on blockchain technology. This system allows you to maintain the confidentiality of medical data by providing patients with mechanisms to control their personal information, which allows them to independently grant access rights to their medical data.

As can be seen from the literature review, in an era of data insecurity, health organisations are increasingly considering the possibilities of global implementation of distributed ledger technology. Blockchain is already being used in all areas of healthcare, from protecting patient data to managing the pharmaceutical supply chain. Blockchain allows you to securely exchange medical data, which was previously considered impossible. However, distributed ledger technology also does not stand still, and, in addition to the blockchain, new types of DLT began to appear. The second prime example of DLT is the IOTA Tangle. However, the use of the IOTA Tangle is not currently widespread. Although IOTA Tangle has a number of advantages over blockchain, which can raise the quality of medical care to a new level, Therefore, it is important to develop systems using IOTA Tangle in the healthcare sector to ensure secure data exchange.

II. PURPOSE AND OBJECTIVES OF THE STUDY

The aim of the study is to develop a medical system based on IOTA Tangle for the secure exchange of medical data between patients and healthcare professionals, institutions, and organisations in the healthcare system.

To achieve this goal, you need to solve the following tasks:

- review the traditional healthcare model and present a model based on IOTA Tangle, determine the basis of the essence of the new model, and describe their interaction;
- develop a model of a decentralised system for storing, processing, and managing medical data using IOTA Tangle technology and describe the main models for implementing the system.

III. PROBLEM DESCRIPTIONS AND PROPOSED MODEL

The traditional healthcare model is shown in Figure 1.a. All medical data is stored with the central authority (a medical institution). If the central organ is compromised intentionally

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

(manipulation) or unintentionally (hacking), it can cause significant damage to the medical system. The IOTA Tangle-based model eliminates central authority by distributing copies of records to all network participants. The IOTA Tangle-based model (Figure 1.b) is much more secure than the traditional model, and it does not require an intermediary.

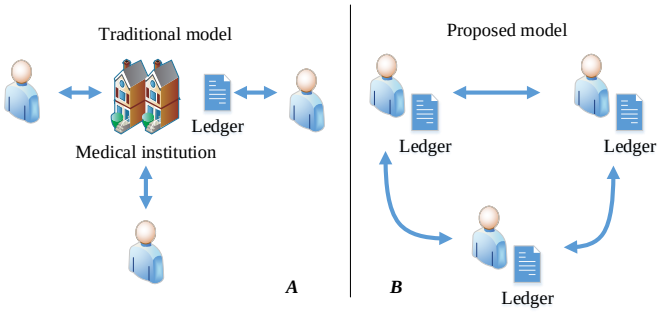

Fig. 1. Traditional Model and IOTA Tangle-Based Model

The proposed model is characterised by three main entities: client, iota node, and IOTA tangle (Figure 2).

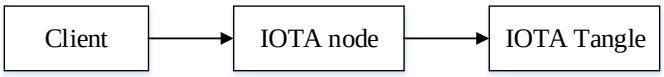

Fig. 2. Model Entities

Clients are users of a medical system that can send transactions (medical data) to nodes.

A node is a connected device that, together, forms an IOTA network and is responsible for following the underlying protocol.

The IOTA Tangle is a distributed ledger that stores immutable transactions.

The interaction of these entities is shown in Figure 3.

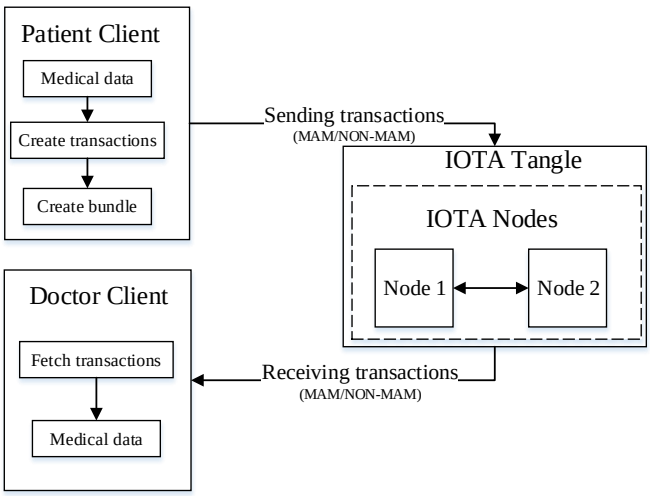

Fig. 3. Interaction of Entities

The patient client generates transactions with their medical data that they want to send to the doctor. Patient transactions are sent to the Tangle node, where they will later be transmitted to the Tangle network. After confirming the transaction, patients are sent to the doctor's node and then to the doctor's system.

The transaction lifecycle begins when a patient or doctor creates a request for consultation with a doctor or patient. To send a transaction to the IOTA network, it goes through the following steps:

1) The sender fills out the appropriate form, which can be a form with symptoms, prescriptions, and diagnoses. Separate transactions are created based on this data

2) In the next step, these individual transactions are grouped into an atomic unit of the IOTA network called a bundle. Transactions in a package are indexed individually and contain information about how many other transactions are in the package. Once completed, incoming transactions in the package must be signed to confirm ownership. To sign transactions, the system creates public and private keys. Keys are generated based on a unique access key called a seed. Seed is created in the appropriate field in the profile settings.

3) To send transactions to the network, you must confirm the previous two transactions. To do this, a request is made to the IOTA network node to select two unconfirmed transactions. The weighted random walk algorithm is used to select two unconfirmed transactions.

4) To join Tangle, each transaction in the package requires a nonce. Nonce is the result of PoW (Proof of Work). The POW confirmation calculation must be performed separately for each transaction, so the more transactions in the package, the longer it will take. The complexity of the calculation also depends on the MWM (minimum weight magnitude) set by the network. The POW calculation takes place locally on the user's device and may take some time.

5) The last step is to fix the packet for the network. Nodes will broadcast transactions on the network and store them in their local database.

Fig.4 Context diagram

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

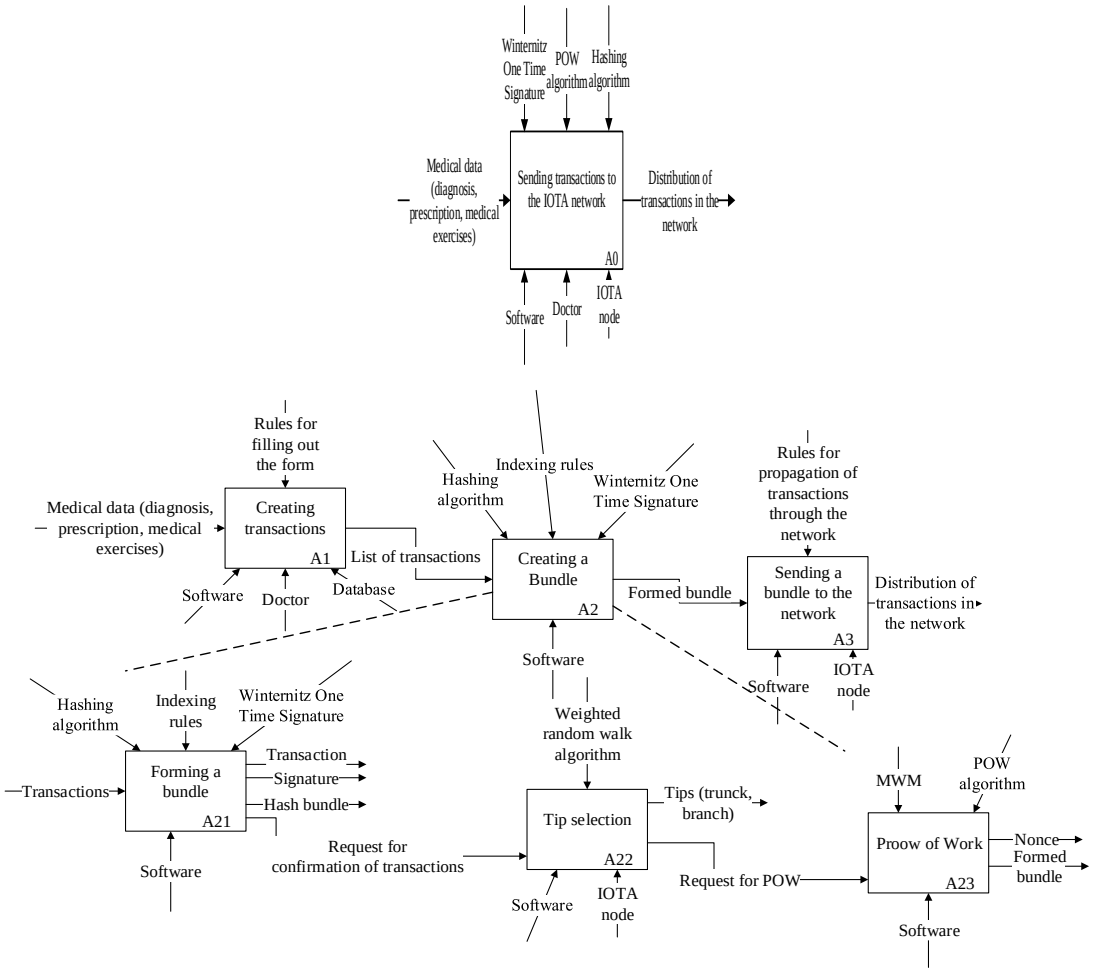

Fig. 4. Results of Context Diagram Decomposition

Data sent by the doctor from his system follows this series of actions. The main difference is that the doctor, after reviewing the patient's symptoms, fills out the diagnosis form. The doctor can also fill out other forms in which he can write out a prescription or prescribe medical exercises. Once transactions have been added to Tangle, they will be marked as unconfirmed. In the future, new transactions that will be added to Tangle will refer to sender transactions. The larger the reference to these transactions, the greater the total weight of these transactions. The higher the total weight of transactions, the higher the chance of their confirmation.

In points 3 and 4 of the transaction lifecycle, it was written that when sending transactions to the network, you need to find two transactions for confirmation and calculate the POW. Schematically, adding a new transaction to Tangle and selecting two unconfirmed transactions is shown in Figure 6.

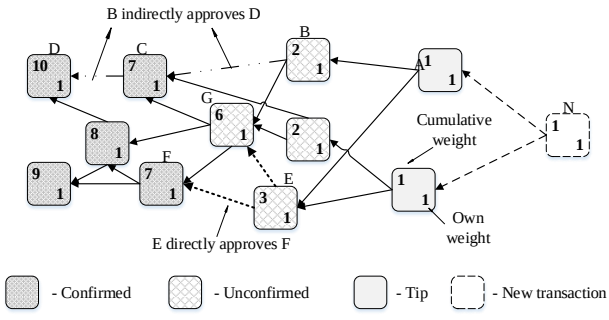

Fig. 5. Tangle

The IOTA Tangle consists of confirmed and unconfirmed transactions and tips. Each transaction can be represented as the vertex of a graph. Each time a new transaction is created, the node selects two other transactions using the WRW algorithm. The algorithm goes through the tangle and selects the vertices that have the highest total weight. Once a node is sure that the selected transactions are not conflicting, it solves a cryptographic puzzle called nonce search. After that, the transaction is added to the tangle and becomes a new vertex [1]. The process of finding new transactions for confirmation is shown in the activity chart (Figure 7).

The chart shows that the initial tx0 transaction is selected first, which will start searching for unconfirmed transactions.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

Then, for each transaction (Tx1 and Tx2—these transactions directly confirm the tx0 transaction), the probability of passing P is calculated. Next, select the branch of the transaction that has a higher probability of P. If the probabilities of both transactions are equal, either of these transactions is selected. If there are no more transactions in the branch, the last transaction will be a new confirmation transaction. If the branch still has transactions, then we return to calculating the probability of subsequent transactions.

Converting medical data to an array of bytes Based on this array, we calculate the hash using the BLAKE2b-256 hash function and convert it to trits. After that, we take an arbitrary nonce value and add it to the hash trits. The resulting value is hashed using the Kerl hash function. After that, we count the number of zeros in the hash. If the number 0 corresponds to MWM, the transaction is valid. If the number 0 corresponds to MWM, then the Nonce value increases by 1, and the process repeats.

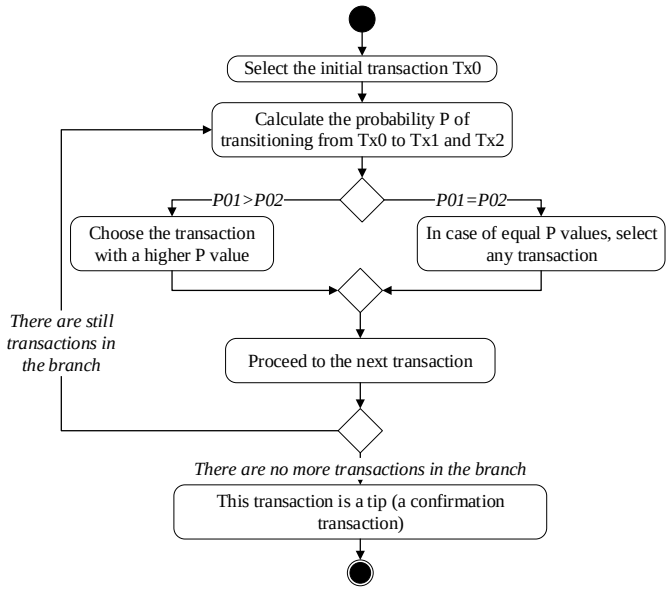

Fig. 6. Tips Selection Algorithm

Figure 8 shows the POW calculation process.

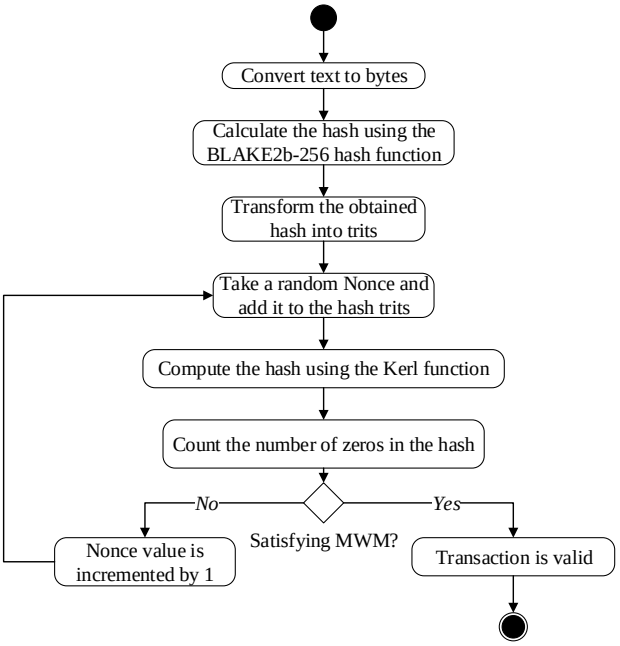

Fig. 7. POW calculation

However, before sending any data, the user (patient or doctor) must log in to the system. Therefore, when visiting the system for the first time, the doctor or patient fills out the form with the appropriate data (last name, first name, doctor/patient ID, etc.). To consult a doctor, the patient must enter the name of the specialty of the doctor they want to contact in the search bar. Or choose a doctor's specialty from the list that is presented on the same page. After selecting the appropriate doctor, the patient fills out the form with the symptoms that are bothering them. Based on this data, transactions will be generated and broadcast to the network.

The search for a doctor in the IDEF0 notation is shown in Figure 9.

Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

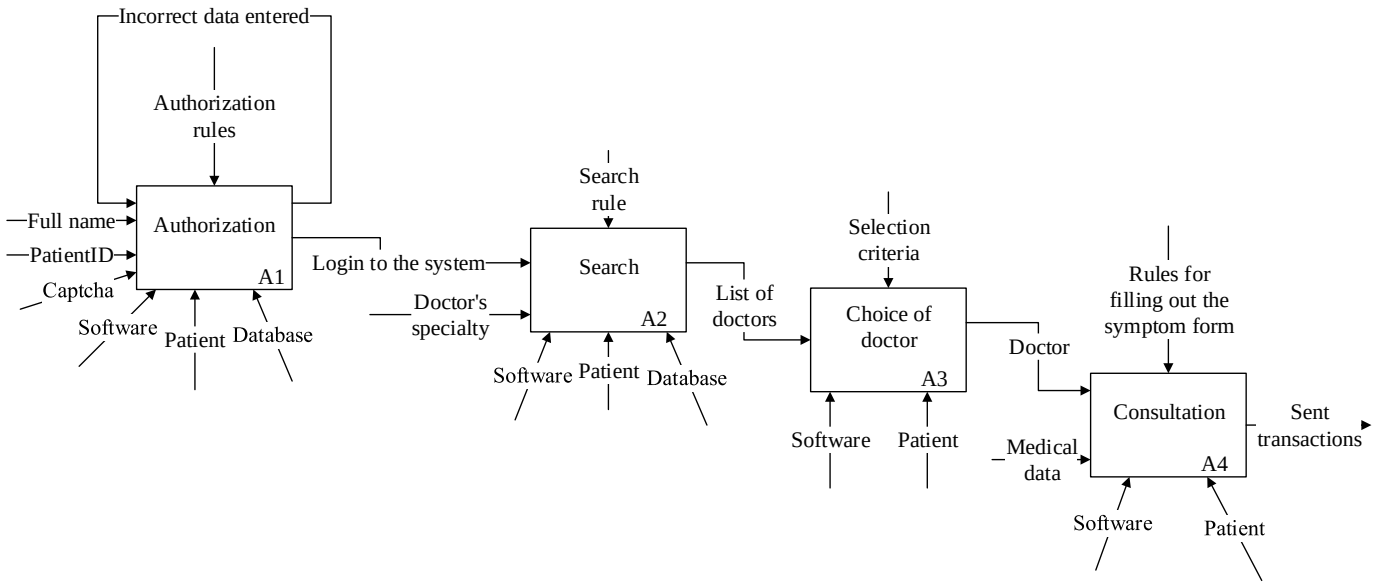

Fig. 8. Finding a doctor in IDEF0 notation

First of all, the patient needs to log into the system. To do this, the patient fills in the appropriate fields in the form. If the patient does not keep the data correctly, the system will indicate errors. After authorization, the patient searches for a doctor. In the search box, enter the doctor's specialty. The system will display a list of doctors that you can contact for a consultation. After selecting a doctor, the patient indicates the symptoms that are bothering them. Then, based on this data, transactions are generated, which are then sent to the IOTA network.

A general model of a decentralised system for storing, processing, and managing medical data using IOTA Tangle technology is shown in Figure 9.

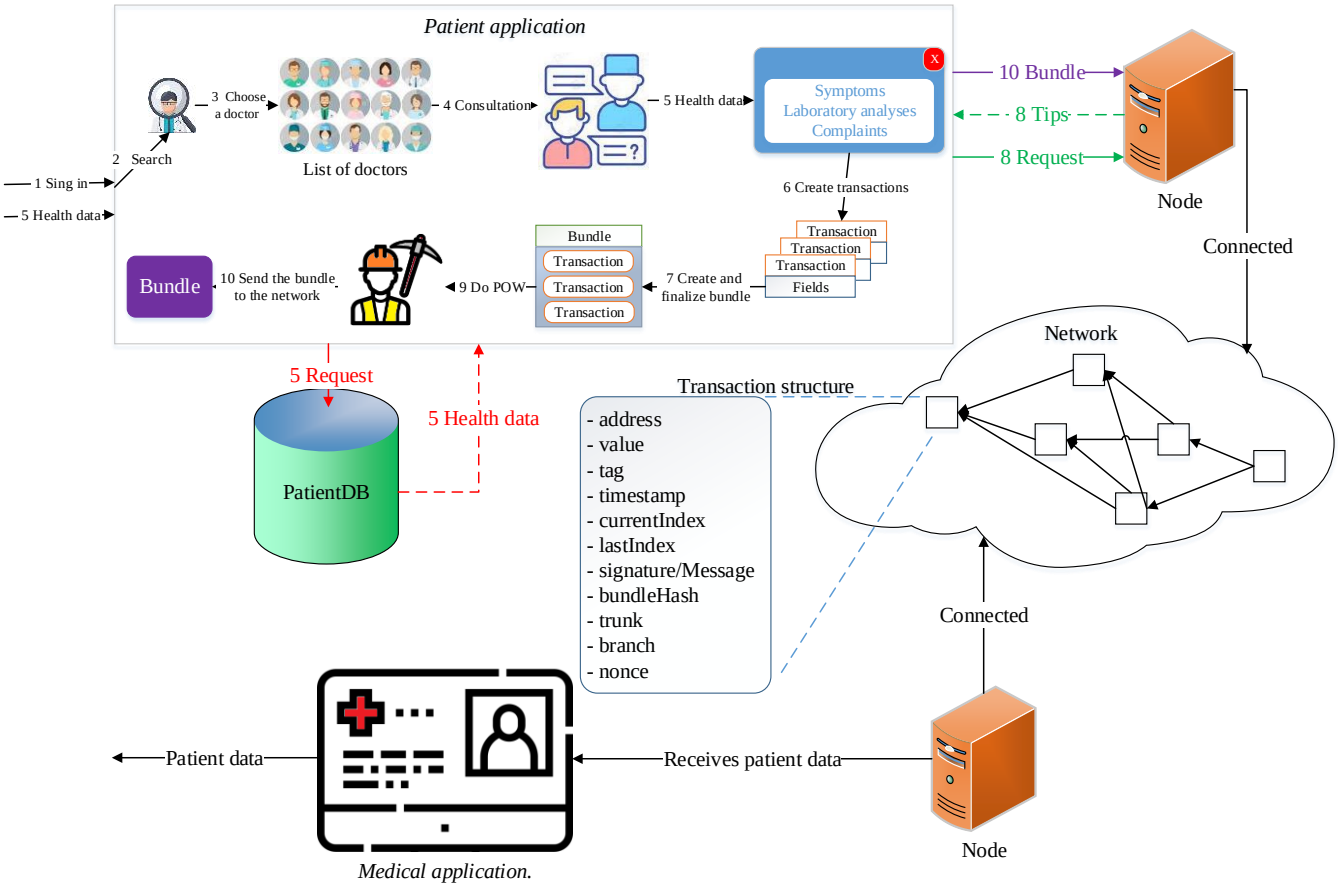

Fig. – 9 Model of a decentralised system for storing, processing, and managing medical data using IOTA Tangle technology

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

To receive medical care, the patient must log in to the medical system. By entering identity data, the patient can search for a doctor by selecting (specifying in the search bar) a specialty. The system will provide a list of doctors who can provide medical care. After reviewing the services of each of the doctors, the patient can choose a suitable specialist. To send symptoms that are bothering the patient, you must fill out the appropriate form. Transactions are generated based on this data. Then these transactions go through the corresponding stages, which were presented above.

IV. RESEARCH RESULTS

From the traditional healthcare model, we can conclude that it is outdated and requires the introduction of new technologies and solutions. Since the patient only plays a passive role in this model, consultations take place infrequently, and healthcare professionals use isolated systems, which causes data fragmentation. Table 1 shows a comparison of the traditional model and the proposed one.

TABLE I. COMPARISON OF THE TRADITIONAL MODEL AND THE PROPOSED

Models / ***Criteria***	***Traditional model***	***Proposed model***
Patient role	Passive	Active
Consultations with a doctor	Episodic	Continuous
Characteristics of the quality of medical data	Fragmented, isolated	Distributed, shared, and constantly updated
Data availability	Episodic	Constant
Data immutability	Data can be rewritten, forged	Immutable (geographical distribution of equivalent copies)
Data storage method	Centralized	Decentralized
Data security	Existing systems are vulnerable to many types of attacks	More stable systems, there is no single point of failure that affects the stability of the system, and public key cryptography is used

Patient data is stored centrally, i.e., in systems where data is stored in a central database and only doctors have access to it. And in most cases, all data is stored on a paper medical card, which will be stored in the office of the family doctor. All this creates a number of difficulties associated with accessing and exchanging information. Therefore, a solution was proposed to use IOTA Tangle, which will allow the secure exchange of medical data with guarantees of its integrity. And most importantly, not only doctors but also patients will have access to this data. The patient will always have a complete medical history, which will avoid data fragmentation. The patient's role in such a system becomes active, and he can always conduct continuous consultations with the doctor. Tangle's low resource requirements are ideal for IoT devices that are primarily used in healthcare. Tangle technology also overcomes two disadvantages of blockchain: scalability and transaction costs. Therefore, this article develops an IOTA Tangle-based system for data exchange between patients and healthcare providers.

V. CONCLUSIONS

In conclusion, this work demonstrates the feasibility of leveraging Distributed Ledger Technology, specifically the IOTA Tangle, to create a decentralized platform for secure and private exchange of medical records between healthcare providers.

The system architecture presented allows patients to maintain ownership over their medical history while seamlessly sharing it with authorized parties to enable coordinated care. Encryption and access controls ensure data privacy is preserved throughout. The asynchronous transaction model and lightweight consensus of IOTA Tangle are well suited for decentralized medical applications.

There remain challenges around patient consent management, key management, and ease of adoption that form avenues for future work. But overall, the developed system provides a foundational platform for patient-centered medical data exchange that prioritizes security, privacy, and accessibility.

As healthcare becomes more collaborative and data-driven, decentralized solutions will be key to balance innovation with ethics. This work demonstrates the value of Distributed Ledger Technology in securely unlocking medical data to improve health outcomes.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

REFERENCES

[1] H. Taherdoost, "Privacy and Security of Blockchain in Healthcare: Applications, Challenges, and Future Perspectives", MDPI, 2023.

[2] R. Saranya, A. Murugan, "A systematic review of enabling blockchain in healthcare system: Analysis, current status, challenges and future direction", Materials Today: Proceedings, vol. 80, pp. 3010-3015, 2021.

[3] V. Mahor, S. Bijrothiya, "E-Healthcare Systems Based on Blockchain Technology with Privacy", Robotic Process Automation, pp.355-370, 2023.

[4] Y. Kliuchka, O. Shmatko, S. Yevseiev, S. Milevskyi, "Peculiarities of blockchain technology introduction in the field of healthcare: current situation and prospects", Information processing systems, vol. 1, (164), pp. 33-44, 2021.

[5] S. Akbulut, F. H. Semantha, S. Azam, I. C. A. Pilares, M. Jonkman, K. C. Yeo, B. Shanmugam, "Designing a private and secure personal health records access management system: A solution based on IOTA distributed ledger technology", Sensors, vol. 23, (11), p. 5174, 2023.

[6] E.S. Rydningen, E. Asberg, L. Jaccheri, J. Li, "Advantages and opportunities of the IOTA Tangle for Health Data Management: A Systematic Mapping Study", Proceedings of the 5th International Workshop on Emerging Trends in Software Engineering for Blockchain. pp. 9–16, 2022.

[7] H. Taherdoost, "The Role of Blockchain in Medical Data Sharing", Cryptography, vol. 7, (3), p.36, 2023.

[8] K. Kiania, S. M. Jameii, A. M. Rahmani, "Blockchain-based privacy and security preserving in electronic health: A systematic review", Multimedia Tools and Applications, pp 28493–28519, 2023.

[9] M. Alhavan, A. Azimi, J. M. Corchado, "A CoviReader Architecture Based on IOTA Tangle for Outbreak Control in Smart Cities during COVID-19 Pandemic", Medical Journal of the Islamic Republic of Iran, 2022.

[10] Y. L. Lee, H.A. Lee, C. Y. Hsu, H. H. Kung, H. W. Chiu, "SEMRES-A triple security protected blockchain based medical record exchange structure", Computer Methods and Programs in Biomedicine, vol. 215, p.106595, 2022.

[11] J. Qu, "Blockchain in medical informatics", Journal of Industrial Information Integration, vol. 25, 2022.

[12] S. Abdullah, J. Arshad, M. M. Khan, M. Alazab, K. Salah, "PRISED tangle: A privacy-aware framework for smart healthcare data sharing using IOTA tangle", Complex & Intelligent Systems, vol. 9, (3), pp.3023-3041, 2023.

[13] H. Saidi, N. Labraoui, A. A. A. Ari, L. A. Maglaras, J. H. M. Emati, "DSMAC: Privacy-aware Decentralized Self-Management of data Access Control based on blockchain for health data", IEEE Access 2022, vol. 10, pp. 101011–101028, 2022.

