Design and Implementation of Blockchain in a Website-Based Electronic Medical Record System Using the Prototype Model

Umi Chotijah[*1], Harunur Rosyid[2], Deni Sutaji[3], Danang Haedar Guswanrinandi[4], Muhammad Rizaldi Zidan Nabil[5], Muhammad Asad Muhibbin Akbar[6]

[1-2,4-6]Department of Informatics, Faculty of Engineering, Universitas Muhammadiyah Gresik, Indonesia

[3]Institute of Informatics, Computer Science, Gazi University, Turkey

E-mail: umi.chotijah@umg.ac.id[1], harun@umg.ac.id[2], deni.sutaji@gazi.edu.tr[3]

Abstract. The security and integrity of medical record data is a crucial issue in the era of healthcare service digitalization. Traditional systems still face risks of manipulation, information leaks, and issues with interoperability between healthcare institutions. Blockchain technology has emerged as a promising solution to address this issue thanks to its features of decentralization, openness, and difficulty in modification. One consensus method that can be applied is Proof of Work (PoW), which has proven to maintain the authenticity of transactions on a distributed network. This research aims to design and evaluate a blockchain-based medical record application using the PoW consensus algorithm to ensure the security, transparency, and reliability of medical data storage. The approach used is experimental, involving the development of a blockchain-based application prototype. The PoW algorithm is applied to ensure the validity of medical record data transactions. The evaluation was conducted by measuring the security aspect (resistance to data changes), performance (time to verify transactions), and scalability (number of transactions that can be handled). The results of the experiment show that implementing PoW in a medical record system can maintain data integrity with a high level of resistance to unauthorized changes. The average time for transaction verification is 2.4 seconds per block, with the ability to handle up to 150 transactions per minute. Although the performance of PoW requires significant computational resources, the level of security it offers suggests potential for implementation in larger healthcare systems. The application of blockchain with the PoW algorithm to medical records has proven to improve the security and transparency of medical information. This research successfully met the established objectives, although computational efficiency issues still need to be addressed. Further research is suggested to explore other consensus algorithms such as Proof of Stake (PoS) or Practical Byzantine Fault Tolerance (PBFT) to improve performance without sacrificing security aspects.

Keywords: Blockchain, Electronic Health Records (EHR), Proof of Work (PoW), Smart Contract, Healthcare Information System

1. Introduction

The development of information and communication technology in the last two decades has had a significant impact on various fields, including the healthcare sector. One important innovation is the digitalization of medical records, which allows patient data to be stored, accessed, and managed

electronically. Electronic Health Records (EHRs) serve as a vital information hub regarding patients' health conditions, medical history, medical procedures, laboratory results, and treatment records [1].

The implementation of EHR is expected to improve the efficiency of healthcare services, minimize medical errors, and facilitate data sharing between healthcare facilities. However, the digitalization of medical records also presents significant challenges, particularly concerning security, privacy, and data integrity. Medical data is sensitive information that is highly vulnerable to leaks and misuse. Studies show that cyberattacks on the healthcare sector have increased significantly, with serious consequences for patient trust and the reputation of healthcare institutions [2]. Furthermore, compatibility between various EHR systems is still a common issue. Since many clinics and hospitals have unintegrated systems, it is challenging to securely and effectively transmit data [3].

Blockchain has surfaced as a possible remedy for these issues. Satoshi Nakamoto initially presented this concept in relation to the virtual currency Bitcoin in 2008. Since then, blockchain has developed into a system that is utilized in many industries, including medical. Blockchain technology is transparent, decentralized, and capable of preserving data integrity through consensus processes. Every transaction is documented in interconnected blocks, and modifications to the data require network consensus. Because of this, unilateral manipulation or alteration of blockchain is extremely challenging [4].

Blockchain technology can be used as a safe way to distribute and store data in the context of medical records. MedRec, a blockchain-based system that gives individuals control over who can access their medical data, was presented by Azaria et al. (2016). This strategy places a strong emphasis on openness and trust while granting patients complete discretion over who can access their personal data. Blockchain's auditability, which allows for unambiguous tracking of all accesses and data changes without the risk of losing the digital trail, is another benefit.

However, choosing a consensus method is one of the technical difficulties associated with integrating blockchain technology into medical record systems. The consensus algorithm acts as a safeguard to guarantee that every node in the network agrees on the legitimacy of transactions. Proof of Work (PoW) is one of the most widely used consensus algorithms. Before a block can be added to the chain, PoW requires network nodes, often known as miners, to solve a challenging cryptographic challenge [5]. Because it necessitates substantial processing power, this technique offers a high degree of security, making it challenging for some parties to execute data manipulation assaults.

PoW is known to have drawbacks, though, including significant energy consumption and comparatively lengthy transaction verification times. This problem becomes significant in the healthcare industry since medical record systems need to be effective and have access to real-time data [1]. Nevertheless, initial research suggests that PoW remains viable for the initial implementation of blockchain in medical records, particularly for testing the security and data integrity resilience before transitioning to more efficient alternative consensus algorithms. [6].

The goal of this study was to develop and assess a blockchain-based PoW consensus application for medical records. The system's performance, security, and integrity in handling medical record data were the main topics of the study. It is anticipated that this research would significantly advance knowledge about blockchain deployment in the healthcare industry by creating an application prototype. Furthermore, this discovery can be used as a starting point for future investigations into more energy-efficient and secure consensus algorithms like Proof of Stake (PoS) or Practical Byzantine Fault Tolerance (PBFT).

In particular, this study offers a number of significant insights. Initially, a medical record application architecture is shown that combines blockchain technology with the PoW algorithm to create a transparent and impenetrable data recording system. Secondly, offering the system performance evaluation data for practitioners and policymakers to take into account when implementing blockchain technology in the healthcare industry. Third, offering suggestions for future lines of inquiry into the creation of blockchain-based medical record systems that are more effective, safe, and scalable.

In particular, this study offers a number of significant insights. Initially, a medical record application architecture is shown that combines blockchain technology with the PoW algorithm to create a transparent

and impenetrable data recording system. Secondly, offering the system performance evaluation data for practitioners and policymakers to take into account when implementing blockchain technology in the healthcare industry. Third, offering suggestions for future lines of inquiry into the creation of blockchain-based medical record systems that are more effective, safe, and scalable.

2. Literature Review

2.1. Previous Research

In order to uncover parallels and studies and to support the theory of the research to be done, this study makes use of references from earlier studies:

Table 1. Previous Research.

	Research Theme	Reasearch Methodology	Result
1	Optimizing Proof-of-Work for Secure Health Data Blockchain Using Compute Unified Device Architecture [7].	*Proof-of-Work* (*PoW*)	In order to improve throughput while lowering power consumption, this study addresses gaps in the investigation of energy-efficient consensus processes, such as GPU-accelerated proof-of-stake. For long-term blockchain uses in the medical field, this is crucial.
2	Development and Research of the Methodology for Improving the Proof-of-Work Blockchain Technology by Implementing Dynamic Clustering of Network Nodes [8].	*Proof-of-Work* (*PoW*)	This study suggests a technique for enhancing proof-of-work blockchain technology using dynamic node clustering, which enhances network performance by lowering energy consumption, speeding up transactions, and cutting down on transaction times. The outcomes show notable increases in effectiveness and real-world uses for the suggested strategy.
3	Lightweight Proof of Game (LPoG): A Proof of Work (PoW)' s Extended Lightweight Consensus Algorithm [9].	*Proof-of-Work* (*PoW*)	The creation of a simulation-optimization technique to enhance data transmission quality in an Industry 4.0 healthcare system is covered in this study. It highlights the significance of interoperability and suggests a patient-centered strategy that makes use of blockchain technology to improve data security and management in medical procedures.

There is a known research gap because the majority of studies published on Google Scholar between 2019 and 2025 mainly address the use of the PoW method in creating blockchain applications for electronic medical records, with an emphasis on security, energy-efficient consensus, and boosting throughput while consuming less power. However, there isn't much talk on how to create and implement desktop or web-based information system applications, or what models or techniques are applied when creating blockchain applications for electronic medical records [7]. However, most research has not been extensively evaluated

in actual medical settings and is still in the prototype stage. Issues with user acceptance, regulations, and technology continue to be major roadblocks [10].

By integrating a web-based PoW consensus with a prototype model to construct a blockchain-based medical record application, this project attempts to close this gap. The system's performance will be evaluated in terms of security, transaction time, throughput, and resource consumption. As a result, the research findings can significantly aid in the creation of an EHR system that is safer, more transparent, and more dependable.

2.2. Blockchain

Blockchain is a distributed ledger technology that uses cryptographic techniques to store data in linked blocks. Blockchain's benefits include its immutability, transparency, and decentralisation, which make it a viable option for managing medical data [5].

In the healthcare field, blockchain has been proposed as a solution for various needs, including:

1. Patient data interoperability – enables the secure transfer of data between healthcare facilities [11].
2. Audit and history tracking – every transaction can be traced back without the risk of manipulation.
3. Patient access control, which allows patients complete control over who can view their health information [12].
4. Security and privacy: Only authorized parties can access data thanks to public-private key cryptography.

Although technical issues like scalability, regulation, and computing costs continue to be barriers, recent studies demonstrate that integrating blockchain technology into EHR can boost consumer confidence and stop data breaches [13].

2.3. Elektronic Health Records (EHR)

The foundation of contemporary healthcare information systems is electronic medical records, or EHRs. The goal of electronic health records (EHRs) is to replace manual paper-based medical records with digital systems that medical staff can rapidly and accurately access [14]. By supporting big data-driven health analytics, expediting clinical decision-making, and easing the interchange of patient data, this system raises the standard of healthcare services. Data security, confidentiality, and interoperability across various hospital systems present difficulties, though [15].

Weak authentication and encryption systems on traditional EHR platforms are frequently the cause of data breaches, information manipulation, and unauthorized access, according to certain research [2]. In order to ensure the long-term dependability, integrity, and security of medical record data, a new technological method is required.

2.4 Proof of Work (PoW) as an Algorithm for Consensus

In the Bitcoin network, PoW was the initial consensus algorithm [5]. In order to validate transactions and add new blocks to the chain, nodes in the network must solve challenging cryptographic puzzles. PoW's high level of security is a benefit because network attacks demand a lot of processing power. Because of this, PoW is highly successful at preventing simple manipulation of medical data integrity. Its primary disadvantages, however, are its high energy usage and transaction speed restrictions, which frequently cast doubt on its suitability for widespread deployment [1].

PoW can be employed in the context of EHRs to guarantee that each medical record submitted to the blockchain is unchangeable and the product of valid validation. Long-term, it is advised to look for more energy-efficient algorithmic alternatives like Proof of Stake or Practical Byzantine Fault Tolerance, but some preliminary study has shown the promise of PoW for medical applications [16].

3. Methodology

This study employs an experimental methodology by creating a prototype model for a web-based blockchain application for electronic medical records. Needs analysis, system architecture design, Proof of Work (PoW) consensus algorithm implementation, system testing and assessment, and results analysis are the five key steps of the research process, which is carried out methodically.

3.1 Research Design

The research design explicitly aligns with the study objectives, which focuses on evaluating security, performance, scalability of a blockchain-based EHR system and on using blockchain technology to address practical issues with handling medical record data, the study methodology employed is applied research (Figure 1). The purpose of the system prototype is to test the viability of applying the PoW algorithm in the healthcare industry as a proof of concept. The system development research methodology model [17], which stresses the iterative cycle between design, implementation, and assessment, is referred to in the design of this study.Each phase of the prototype model directly corresponds to these objectives: system design addresses security architecture, implementation evaluates PoW transaction validation, and testing measures latency, throughput, and resistance to data manipulation.

3.2 Analysis of Needs

The basic issues with the current electronic medical record system were identified in order to conduct a needs analysis. These issues are as follows: (a) security: medical data is susceptible to alteration or unauthorized access; (b) privacy: patients do not have complete control over who can access their data; and (c) interoperability: it is difficult to exchange data between various hospital systems. The usage of blockchain as a data distribution and storage platform, with PoW serving as the primary consensus mechanism to preserve transaction integrity, is the suggested remedy based on this identification.

3.3 Blockchain Architecture Design

The blockchain architecture proposed in this study adopts a layered architecture model to ensure scalability, security, and modularity. The architecture consists of four main layers: (1) User Layer, (2) Application Layer, (3) Blockchain Layer, and (4) Storage Layer.

The User Layer represents system actors, including doctors, patients, and administrators, who interact with the system through a web-based interface. The Application Layer handles authentication, access requests, and transaction initiation. This layer communicates with smart contracts deployed on the blockchain network.

The Blockchain Layer is implemented using a private Ethereum network with a Proof of Work (PoW) consensus mechanism. Smart contracts are responsible for validating access permissions, recording medical record transactions, and ensuring immutability. Each transaction is cryptographically hashed and linked to previous blocks, preventing unauthorized data modification.

The Storage Layer utilizes the InterPlanetary File System (IPFS) to store large medical files off-chain. Only the hash of each medical record is stored on the blockchain, ensuring data integrity while reducing blockchain storage overhead. The Zhang et al. research is cited in the system architecture model, which has been adjusted for the Indonesian medical record setting [4].

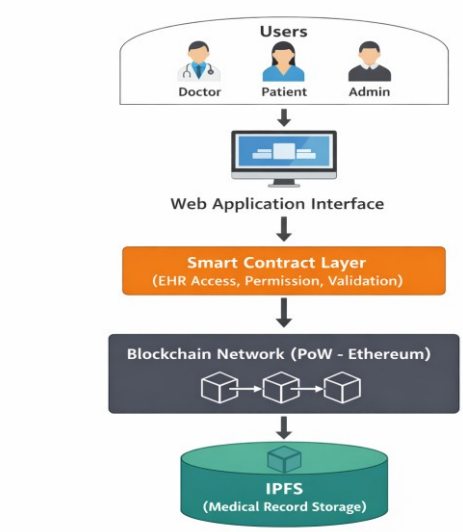

Figure 1. Blockchain-based Electronic Health Record (EHR) System

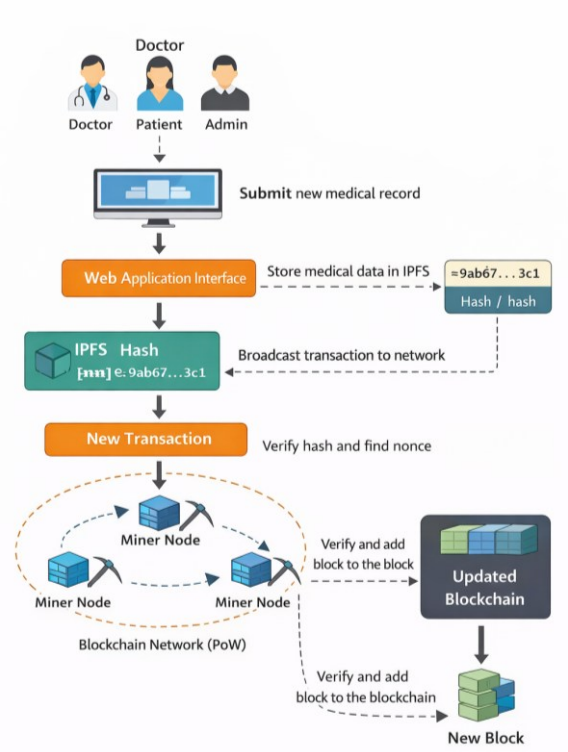

Figure 2. Transaction flow of medical data validation

Figure 2 illustrates the transaction flow of medical record management using the Proof of Work consensus mechanism. When a doctor submits a new medical record, the system generates a transaction containing the hash of the medical data stored in IPFS. The transaction is broadcast to the blockchain network, where miner nodes compete to solve a cryptographic puzzle.

Once a valid nonce is found, the block is verified and added to the blockchain. This process ensures that medical records cannot be altered without recalculating all subsequent blocks, which would require control over the majority of network computational power.

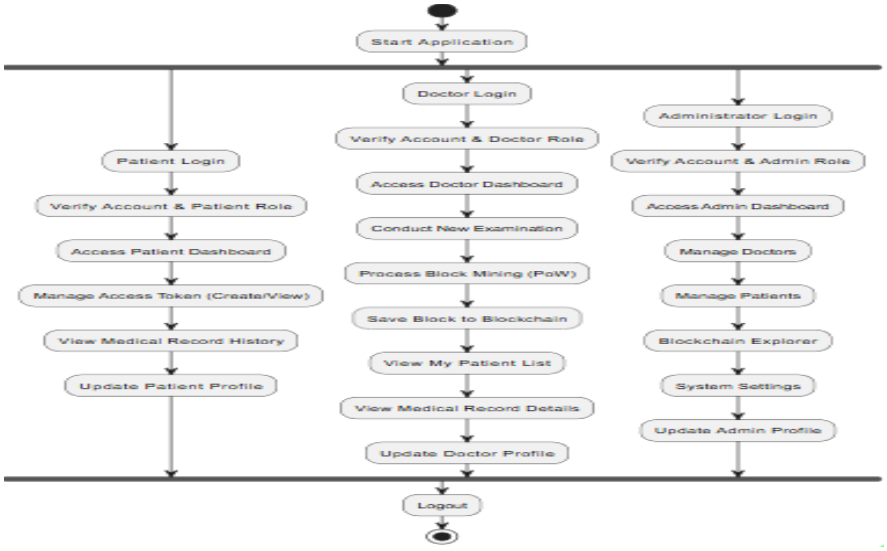

Figure 3. HIPO Diagram of Blockchain-Based Electronic Health Record (EHR) System

Figure 3 illustrates the Hierarchy Input–Process–Output (HIPO) diagram of the proposed blockchain-based Electronic Health Record (EHR) system. The diagram describes the functional structure of the system by categorizing system activities based on user roles, processes, and outputs. The system supports three main user roles: Patient, Doctor, and Administrator. Each user begins by accessing the system through a secure login process, followed by account verification to ensure role-based authorization.

Patients are provided access to the patient dashboard, where they can manage access tokens, view their medical record history, and update personal profile information. Access tokens are used to control and authorize data access in the blockchain network, ensuring privacy and transparency.

Doctors access the system through the doctor dashboard after successful verification. The main processes include conducting new medical examinations, generating medical record data, and initiating the Proof of Work (PoW) mining process. Once validated, medical records are stored as new blocks in the blockchain. Doctors can also view assigned patient lists, access detailed medical records, and update their professional profiles.

Administrators are responsible for system-level management tasks. Through the administrator dashboard, they can manage doctor and patient accounts, monitor blockchain transactions using the blockchain explorer, configure system settings, and update administrative profiles.

The HIPO diagram demonstrates how user interactions are systematically processed and recorded through blockchain mechanisms, ensuring data integrity, role-based access control, and secure medical record management within the EHR system.

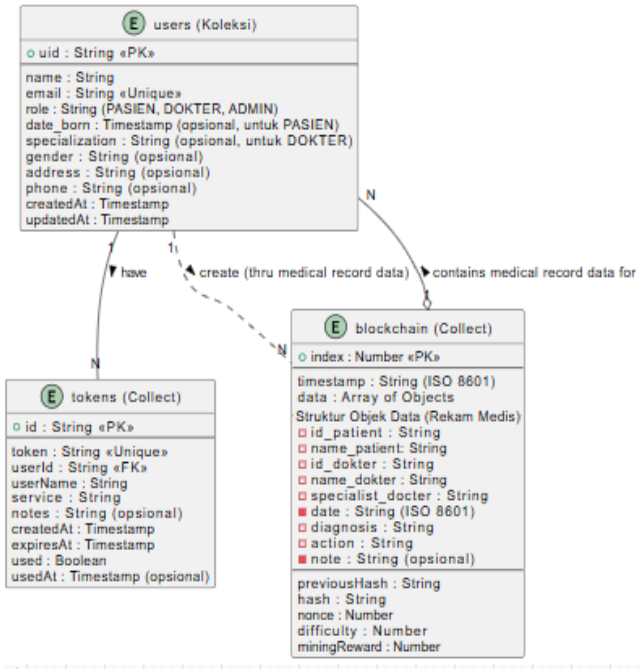

Figure 4. Entity Relationship Diagram (ERD) of Blockchain- based Electronic Health Record (EHR) System

Figure 4 presents the Entity Relationship Diagram (ERD) of the proposed blockchain-based Electronic Health Record (EHR) system. The ERD illustrates the logical structure of the system database and describes the relationships between core entities involved in managing medical records using blockchain technology.

The Users entity represents all system actors, including patients, doctors, and administrators. Each user is uniquely identified by a user ID and is associated with role-based attributes such as name, email, role type, specialization (for doctors), and personal profile information. Timestamp attributes are included to support auditability and data traceability.

The Tokens entity is used to manage access control within the blockchain-based system. Each token is uniquely generated and linked to a specific user. Tokens define access permissions and expiration status, enabling patients to securely authorize doctors to access their medical records. This mechanism supports privacy preservation and transparent access management.

The Blockchain entity represents medical record transactions stored in the blockchain network. Each blockchain record contains encrypted medical data, including patient identity references, doctor identity, diagnosis, action, and timestamp. Additionally, blockchain-specific attributes such as previous hash, current hash, nonce, mining reward, and difficulty number are included to ensure immutability and Proof of Work (PoW) validation.

The relationships between entities demonstrate that users can create and access medical record data through authorized tokens, while each medical record transaction is permanently stored as a blockchain block. This ERD highlights how traditional relational data structures are integrated with blockchain principles to ensure data integrity, security, and traceability in electronic health record management.

3.4 Implementation of The System

The Ethereum private network, which offers smart contracts that may be used to control data access permissions, was utilized to construct the prototype. The Ethash protocol, a PoW variation on Ethereum, is used to implement the PoW algorithm [18]. Programming languages: Python for application integration, Solidity for smart contracts. Database: Blockchain stores hashes as data integrity markers, whereas IPFS

(InterPlanetary File System) is utilized to store big medical files. A server PC with an Intel i7 processor, 16 GB of RAM, and an NVIDIA GTX GPU to facilitate mining is the test setting.

3.5 Assessment and Testing

Three primary aspects were assessed through testing: (1) Data security is evaluated by mimicking attacks, including trying to change outdated blocks. The system's ability to withstand attacks was used to evaluate its effectiveness; (2) System Performance: assessed using metrics such as transaction verification time (latency) and transactions per minute throughput; (3) Scalability: evaluated by simulating a range of transaction volumes, from 50 to 500 transactions, to gauge the system's capacity to manage growing workloads. With modifications made to the medical record transaction characteristics, the evaluation method makes reference to the study conducted by Xia et al. [6].

3.6 Tools and Methods of Analysis

Among the tools and methods employed are: (1) software tools: Metamask as a transaction testing interface, Remix IDE for smart contract implementation, and Ganache for local blockchain simulation; (2) data analysis tools: blockchain transaction logs were examined using Python libraries (web3.py) to extract information on transaction count and verification time; and (3) comparative analysis: evaluation outcomes were contrasted with security and performance guidelines suggested in the literature [18].

3.7 Validity of Reasearch

The following actions were performed in order to preserve the validity of the study findings: (1) Reliability: every experiment was conducted a minimum of three times, and the final data was derived from the average results; (2) Internal validation: the attack scenario was created using the blockchain security threat simulation model [19]; (3) External validation: the prototype was tested in a simulated environment, but the architectural design was modified to fit the actual circumstances of hospital medical record implementation.

3.8 Etichs in Reasearch

There are no direct patient interactions and no privacy concern because this study makes use of synthetic medical record data, or "dummy data." Nonetheless, the system design continues to take into account the confidentiality, access authorization, and audit transparency requirements of medical ethics [10].

With this approach, it is intended that the research findings will offer a thorough analysis of the advantages and disadvantages of using blockchain technology and the PoW algorithm in medical records, as well as act as a basis for future studies with more effective consensus.

3.9 Technical Parameters of PoW Implementation

The Proof of Work implementation uses a difficulty level adjusted to maintain an average block generation time of approximately 2–3 seconds. The hash function applied is SHA-256, ensuring collision resistance and cryptographic security. Each block contains a block header, previous hash, timestamp, nonce, and Merkle root of transactions. This configuration follows standard blockchain security practices while being adapted for healthcare transaction characteristics.

4. Results and Discussion

4.1 Implementing a System Prototype

Using an Ethereum private network and the Proof of Work (PoW) consensus method, a blockchain-based medical record application prototype was successfully constructed. The user application (front-end), smart contract, and blockchain layer make up the prototype's three primary parts. Physicians and patients can more easily obtain medical data thanks to the user application's web-based interface. When a patient gives permission for a certain doctor to read their medical records, for instance, smart contracts are used to control access permissions.

Every transaction involving the addition, modification, or access of medical data is captured in blocks at the blockchain layer. While the blockchain holds the file hashes to guarantee data integrity, IPFS houses large medical records files, such as radiology or lab reports.

4.2 Findings from Security Testing

A threat simulation scenario that includes trying to alter previously stored blocks in the blockchain was used for security testing. The findings demonstrate that any effort to modify one block leads in a hash mismatch in every block that follows. Consequently, the transaction was denied by the network. This demonstrates that PoW offers strong protection against illegal data alteration.

A simulation of a double-spending attack was also carried out, in which the attacker tried to incorporate two distinct transactions into a single block. Consequently, only the first transaction that is correctly validated is approved by the PoW algorithm, which rejects double spending. As a result, it has been demonstrated that the system strictly upholds the consistency of medical data.

4.3 Performance Testing Results

Transaction verification latency and transactions per minute throughput were the two metrics used to gauge system performance. (1) Latency: 2.4 seconds were spent on average each block for transaction verification. Though slower than alternative consensus algorithms like PoS or PBFT, this figure is nevertheless quite realistic for a PoW-based prototype; (2) Throughput: the average capacity exceeds 150 transactions per minute. Throughput drops to 120 transactions per minute when the number of transactions rises to 500 per minute, while latency rises to 3.7 seconds. This finding suggests that PoW can manage medium-sized medical record transactions, but scalability issues are still a major problem.

4.4 Scalability Evaluation

There were five, ten, and twenty nodes in the network when the simulation was run. The average consensus time was 2.1 seconds in the 5-node setup and 3.2 seconds in the 20-node setup. This suggests that because validation becomes more sophisticated as the number of nodes in the network increases, the consensus process takes longer. However, as control over most nodes is necessary to alter transactions, adding more nodes also makes the system more resistant to attacks. Performance and system security must therefore be traded off.

4.5 User Feedback

As part of the limited trial, the prototype was tested by 5 lecturers and students who played the roles of simulated doctors and patients. The questionnaire results show that 80% of respondents found the system easy to use, while 20% stated that improvements were needed in the interface design. All respondents rated the system as providing better transparency compared to conventional medical data storage.

4.6 Analysis of the Findings

From a scientific perspective, the findings confirm that PoW-based blockchain provides a strong immutability guarantee suitable for sensitive medical data. However, the trade-off between security and computational efficiency remains a critical challenge. This reinforces existing blockchain theories that emphasize the security–performance trade-off in distributed ledger systems. Overall, the study's findings show that: (1) the prototype was successfully constructed with the primary features operating as intended; (2) the PoW algorithm was successful in preserving the security and integrity of medical data; (3) system performance was fairly good on a medium scale but declined on a large scale; and (4) limited testing demonstrated positive user acceptance.

In contrast to conventional medical record systems, the study's findings demonstrate that integrating blockchain technology with proof-of-work (PoW) can offer more robust security and data integrity guarantees for medical records. Data cannot be altered without the knowledge of the entire network thanks to the hashing and validation method provided by PoW. This is consistent with research by Azaria et al.

(2016), which demonstrated that blockchain technology can offer transparent access control for the administration of medical data.

Nevertheless, the results of performance tests verify that PoW has computational efficiency restrictions. Although an average latency of 2.4 seconds per transaction is still tolerable, PoW is obviously slower than alternative algorithms, such as PBFT, which only need milliseconds [20].

4.6 Evaluation in Relation to Other Studies

Although scalability is still a significant obstacle, the study by Shahnaz et al. (2019) indicates that blockchain can be used to create safe EHRs. The results of this investigation are in line with prior studies, which show that transaction throughput falls as demand grows. In the meantime, Radanović & Likić (2018) stressed how crucial it is to strike a balance between energy efficiency and security. According to the study's findings, PoW offers excellent security but at the expense of speed and resource usage. This prototype offers an extra empirical assessment of PoW consensus performance on medical data in comparison to MedRec [18], This study concentrates on technical performance and security, whereas MedRec is primarily concerned with a permission management paradigm.

4.9 Practical Implications

Practically speaking, adding PoW-based blockchain to medical records can benefit patients in three ways: (1) security and integrity (hard to tamper with, increasing patient trust); (2) auditability (all access is permanently recorded, making tracking easier); and (3) transparency (patients can manage access to their data). However, throughput constraints and energy usage must be taken into account if implemented nationally. Therefore, rather than being a long-term solution, PoW is better suited for initial testing (pilot projects) or limited application in particular healthcare organizations.

4.10 Limitations of the Study

Some limitations of this study include: (1) Limited testing environment: the prototype was tested on a private blockchain network, not in real-world hospital conditions with thousands of transactions per second; (2) Focus on PoW: this study has not yet explored alternative, more efficient algorithms.

4.11 Recommendations for Further Research

There are a number of possible directions for further study: Examining faster and more energy-efficient alternative consensus algorithms like Proof of Stake (PoS) or Practical Byzantine Fault Tolerance (PBFT); integrating with medical interoperability standards like HL7 FHIR to help healthcare institutions adopt the system; conducting extensive testing using simulations of thousands of nodes to evaluate performance in the real world; and creating hybrid models, like fusing blockchain with off-chain storage technology to lessen network load.

4.12 Theoretical and Practical Contributions

*T*his study's contributions fall into two categories: (2) Practical: creating a prototype that developers and healthcare organizations can use as a guide to comprehend the potential and constraints of blockchain technology in EHRs; (1) Theoretical: offering empirical proof that PoW is successful in preserving the integrity of medical data and contributing to the body of literature on blockchain implementation in healthcare.

5. Conclusion

A blockchain-based medical record application prototype using the Proof of Work (PoW) consensus mechanism has been successfully conceived and implemented by this research. The test findings demonstrate that the system can effectively avoid any attempts at modification or double attacks by maintaining the confidentiality and integrity of medical data through hashing and block validation procedures. With a medium-scale capability of up to 150 transactions per minute, the average transaction verification time is 2.4 seconds, which is still more than sufficient for limited deployment.

Practically speaking, this study demonstrates that blockchain technology can offer superior access control, auditability, and transparency when compared to conventional medical record systems. However, PoW's energy consumption and scalability restrictions are issues that must be resolved prior to widespread adoption, such as in national healthcare systems.

This study makes a theoretical and practical contribution. Theoretically, this study adds to the body of knowledge regarding blockchain's possible use in healthcare. From a practical standpoint, the created prototype can be used as a starting point for the creation of a more integrated and safe contemporary medical record system. It is advised that future studies investigate more effective consensus methods like Proof of Stake or Practical Byzantine Fault Tolerance and test the system with a bigger user base and in actual hospital settings.

6. References

[1] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, "Blockchain technology in healthcare: A systematic review," *Healthc.*, vol. 7, no. 2, 2019, doi: 10.3390/healthcare7020056.

[2] C. S. Kruse, M. Soma, D. Pulluri, N. T. Nemali, and M. Brooks, "The effectiveness of telemedicine in the management of chronic heart disease – a systematic review," *JRSM Open*, vol. 8, no. 3, pp. 1–7, 2017, doi: 10.1177/2054270416681747.

[3] U. Zaman, Imran, F. Mehmood, N. Iqbal, J. Kim, and M. Ibrahim, "Towards Secure and Intelligent Internet of Health Things: A Survey of Enabling Technologies and Applications," *Electron.*, vol. 11, no. 12, pp. 1–43, 2022, doi: 10.3390/electronics11121893.

[4] X. Zhang, Y. Jian, X. Li, L. Ma, G. Karanis, and P. Karanis, "The first report of Cryptosporidium spp. in Microtus fuscus (Qinghai vole) and Ochotona curzoniae (wild plateau pika) in the Qinghai-Tibetan Plateau area, China," *Parasitol. Res.*, vol. 117, no. 5, pp. 1401–1407, 2018, doi: 10.1007/s00436-018-5827-5.

[5] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," . bitcoin.org. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[6] et al. Xia, C., "Role of T Lymphocytes in Type 2 Diabetes and Diabetes Associated Inflammation," *J. Diabetes Res.*, 2017, doi: https://doi.org/10.1155/2017/6494795.

[7] S. Mehammed, "Optimizing Proof-of-Work for Secure Health Data Blockchain Using Compute Unified Device Architecture," vol. 1, pp. 1–10.

[8] D. Soloviova, "Development and Research of the Methodology for Improving the Proof-of-Work Blockchain Technology by Implementing Dynamic Clustering of Network Nodes," 2025, doi: 10.1049/blc2.70006.

[9] A. Kumar, D. K. Sharma, A. Nayyar, and S. Singh, "Lightweight Proof of Game (LPoG): A Proof of Work (PoW)' s Extended Lightweight Consensus Algorithm".

[10] A. Roehrs, C. A. Da Costa, R. Da Rosa Righi, and K. S. F. De Oliveira, "Personal health records: A systematic literature review," *J. Med. Internet Res.*, vol. 19, no. 1, 2017, doi: 10.2196/jmir.5876.

[11] A. Azaria, A., Ekblaw, A., Vieira, T. and Lippman, "Medrec: Using Blockchain for Medical Data Access and Permission Management," in *2016 2nd International Conference on Open and Big Data (OBD)*, 2016, pp. 25–30.

[12] S. Angraal, H. M. Krumholz, and W. L. Schulz, "Blockchain technology: Applications in health care," *Circ. Cardiovasc. Qual. Outcomes*, vol. 10, no. 9, pp. 1–3, 2017, doi: 10.1161/CIRCOUTCOMES.117.003800.

[13] T. T. Kuo, H. E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *J. Am. Med. Informatics Assoc.*, vol. 24, no. 6, pp. 1211–1220, 2017, doi: 10.1093/jamia/ocx068.

[14] N. Menachemi and T. H. Collum, "Benefits and drawbacks of electronic health record systems," *Risk Manag. Healthc. Policy*, vol. 4, no. May 2011, pp. 47–55, 2011, doi: 10.2147/RMHP.S12985.

[15] D. Bates, M. Mächler, B. M. Bolker, and S. C. Walker, "Fitting linear mixed-effects models using lme4," *J. Stat. Softw.*, vol. 67, no. 1, 2015, doi: 10.18637/jss.v067.i01.

[16] A. A. Yaqoob, M. N. M. Ibrahim, and C. Guerrero-Barajas, "Modern trend of anodes in microbial fuel cells (MFCs): An overview," *Environ. Technol. Innov.*, vol. 23, p. 101579, 2021, doi: https://doi.org/10.1016/j.eti.2021.101579.

[17] and W. K. J. Vijay Vaishnavi, Vijay K. Vaishnavi, "No Title," in *Design Science Research Methods and Patterns Innovating Information and Communication Technology (Second edition.)*, CRC Press, 2015. [Online]. Available: https://doi.org/10.1201/b18448

[18] A. Ekblaw and A. Azaria, "Viral Communications MedRec: Medical Data Management on the Blockchain License: Creative Commons Attribution 4.0 International License (CC-BY 4.0)," *assets.pubpub.orgA Ekblaw, A Azaria, T Vieira, A LippmanViral Commun. 2016•assets.pubpub.org*, 2016, [Online]. Available: https://assets.pubpub.org/77ffonfi/fac98e84-5f2c-4828-a1ba-e2141e747ee6.pdf

[19] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A Survey on Security and Privacy Issues of Bitcoin," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018, doi: 10.1109/COMST.2018.2842460.

[20] F. D. Wihartiko, S. Nurdiati, A. Buono, and E. Santosa, "Blockchain dan Kecerdasan Buatan dalam Pertanian : Studi Literatur," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 8, no. 1, p. 177, 2021, doi: 10.25126/jtiik.0814059.