Journal of Technology Informatics and Engineering (JTIE)
Vol. 4 No. 1 April 2025
E-ISSN: 2961-9068; P-ISSN: 2961-8215, Pages 171-189

Blockchain-Based Zero-Knowledge Proof Protocol For Privacy-Preserving Healthcare Data Sharing

Go Eun Myeong*[1], Kim Sa Ram[1]
Email: goeunmyeong42@gmail.com; saram-kim@dgg.co.kr
[1]*Daejin University, Pocheon-Si, South Korea*
[1]*Dongguk University, South Korea*
*Corresponding Author

Abstract
The rise of digital healthcare has intensified concerns over data privacy, particularly in cross-institutional medical data exchanges. This study introduces a blockchain-based protocol leveraging Zero-Knowledge Proofs (ZKP), specifically zk-SNARK, to enable verifiable yet privacy-preserving health data sharing. Built on a permissioned Ethereum blockchain, the protocol ensures that medical data validity can be confirmed without disclosing sensitive content. System implementation involves Python-based zk-circuits, smart contracts in Solidity, and RESTful APIs supporting HL7 FHIR formats for interoperability. Performance evaluations show promising results: proof verification times remained under 100 ms, with average proof sizes below 2 KB, even under complex transaction scenarios. Gas consumption analysis indicates a trade-off—ZKP-enabled transactions consumed approximately 93,000 gas units, compared to 52,800 in baseline cases. Interoperability testing across 10 FHIR-based scenarios resulted in 100% parsing success and an average data integration time of 1.7 seconds. Security assessments under white-box threat models confirmed that sensitive information remains unreconstructable, preserving patient confidentiality. Compared to previous implementations using zk-STARK, this protocol offers a 30% improvement in verification efficiency and a 45% reduction in proof size. The novelty lies in combining lightweight ZKP mechanisms with an interoperability-focused design, tailored for realistic hospital infrastructures. This research delivers a scalable, standards-compliant architecture poised to advance secure digital healthcare ecosystems while complying with regulations like GDPR.

Keyword: *blockchain, zero-knowledge proof, healthcare data privacy*

I. INTRODUCTION

The rapid advancement of digital technology has driven a major transformation in the healthcare sector, particularly in managing and exchanging medical data. The digitization of medical records and the integration of health information systems have enabled faster, more accurate, and more efficient data access, ultimately enhancing the quality of patient care (Haleem et al., 2022). However, alongside these benefits, significant challenges have emerged regarding the security and privacy of digital health data. Health data is a highly sensitive type of information, as it contains personal records, genetic information, medical history, and confidential medical decisions (Iyanna et al., 2022). Breaches of this data can have serious consequences, ranging from financial loss to reputational damage for healthcare institutions.

According to a report by (Kahanda et al., 2024), data breaches in the healthcare sector incur the highest average cost across all industries, amounting to USD 10.1 million per incident. Furthermore, a study by (Javaid et al., 2023) revealed that 89% of healthcare organizations

Received on February 2025; Revised on March 2025; Accepted on March 2025; Published on April 2025
DOI: *10.51903/jtie.v4i1.296*

experienced data breaches within the past two years. This indicates that conventional security systems are not yet fully capable of preventing threats to patient data, particularly in terms of cyberattacks and unauthorized access. Therefore, a new approach is required—one that not only strengthens security but also ensures data privacy and authentication without compromising system interoperability.

Blockchain technology emerges as a promising solution to these challenges. With its distributed ledger structure and immutable nature, blockchain enables transparent, accurate, and tamper-resistant recording of medical data (J et al., 2023). Each data entry within the blockchain is validated through a consensus mechanism, making it more resilient to interference or infiltration. Blockchain also supports transparency and auditability, allowing any changes to data to be traced back to their original source (Ramzan et al., 2023). However, this very transparency raises concerns regarding data confidentiality. Since information recorded on the blockchain is visible to all nodes in the network, the absence of adequate privacy mechanisms may jeopardize the confidentiality of sensitive patient data (Arbabi et al., 2023).

To address the dilemma between transparency and privacy, the Zero-Knowledge Proof (ZKP) approach has become highly relevant. ZKP is a cryptographic method that allows one party to prove the truth of a statement or possession of certain information without revealing the information itself (Jedlicka & Grant, 2022). This concept enables verification without exposing sensitive data, making it particularly well-suited for blockchain applications. Several variants of ZKP have been developed, such as zk-SNARK, zk-STARK, and Bulletproofs. Each has its advantages—for instance, zk-SNARK offers compact and efficient proof sizes, while zk-STARK provides high scalability without the need for a trusted setup (Ramos Fernández, 2024).

In the context of healthcare services, ZKP allows patients to prove their identity or authorize access to specific data without disclosing personal details such as their name or medical history. An example of this application is in medical data authentication systems, where hospitals can verify that a patient possesses a valid medical record without needing to access the entire dataset. This approach adds an extra layer of security while also addressing the need for privacy, especially in digitally connected and open healthcare systems.

Previous studies have explored the integration of blockchain technology and Zero-Knowledge Proofs (ZKPs) in healthcare systems. (Bharath Babu & Jothi, 2024) highlight the potential of blockchain in providing transparency and auditability for medical data management, while ZKPs are employed to ensure patient data confidentiality. Research by (Gupta & Lakhwani, 2025) developed an Ethereum-based protocol utilizing ZKPs to enable the private exchange of medical data between hospitals, demonstrating the effectiveness of this approach in

safeguarding information privacy and integrity. In addition, initiatives such as Zcash and Ernst & Young's Nightfall have also implemented the integration of blockchain and ZKPs to enhance privacy in digital transactions, although most applications remain confined to the financial sector.

Nevertheless, several limitations persist in these studies. The majority remain at the prototype or simulation stage and have not been widely tested in large-scale healthcare contexts. (Samantray & Reddy, 2025) note that implementing ZKPs on blockchain platforms often faces challenges related to system complexity and high computational requirements. These pose serious obstacles, especially when deployment is required in hospital environments with varying levels of technological infrastructure. Moreover, interoperability among disparate health information systems remains a significant issue that has yet to be adequately addressed by prior research. The lack of shared technical standards further complicates the integration of blockchain and ZKP-based protocols into national or cross-border healthcare systems.

The research gaps identified in previous studies open avenues for further exploration into the development of efficient, scalable, and easily integrable protocols within existing healthcare ecosystems. Few studies have proposed lightweight Zero-Knowledge Proof approaches that maintain strong verification capabilities while supporting interoperability with heterogeneous hospital systems. Additionally, most existing studies focus solely on technical aspects, often overlooking practical considerations such as user acceptance, system workload, and feasibility of implementation in light of data privacy policies and regulatory frameworks.

This study aims to develop a blockchain-based protocol integrated with Zero-Knowledge Proofs, specifically designed to support the private and secure exchange of healthcare data. The primary objective is to design a system that not only preserves patient data privacy but also enables efficient information verification without compromising system performance. The proposed protocol is expected to address key challenges faced by digital healthcare systems, including the need for security, privacy, interoperability, and operational efficiency. In pursuit of this goal, the approach incorporates cryptographic efficiency, modular and standardized system design, and compatibility with existing hospital infrastructure.

The primary contribution of this study lies in the development of a blockchain-based Zero-Knowledge Proof (ZKP) protocol architecture tailored to the specific needs of the healthcare sector, particularly in the context of inter-institutional data exchange. This research also presents simulations and performance analyses of the proposed protocol, including evaluations of verification efficiency, data leakage rates, and the system's ability to maintain information integrity and privacy. Furthermore, the study offers a realistic implementation framework that

encompasses integration with hospital systems, considerations of privacy policies, and the potential for nationwide adoption. As such, this research provides significant contributions not only in the theoretical domain of cryptography and blockchain technology but also in practical and policy dimensions within the broader context of digital transformation in the healthcare sector.

Through this approach, the study aims to address the urgent need for secure, private, and interoperable health data systems. Moreover, the proposed solution holds the potential to serve as a foundational framework for broader medical data platforms, including telemedicine, digital referral systems, and medical data analytics for research and clinical decision-making. Consequently, this research occupies a strategic position in promoting the integration of advanced technologies into healthcare services while simultaneously addressing the key challenges that have hindered the adoption of blockchain and cryptography-based digital systems.

II. LITERATURE REVIEW

A. Blockchain in Digital Health Systems

Blockchain technology has emerged as a strategic solution to challenges related to data security and reliability in digital health systems. Its inherent characteristics—immutability, decentralization, and transparency—make it highly relevant for managing sensitive medical records that are often fragmented across institutions (Rai, 2023). In healthcare settings, blockchain has been applied to electronic medical record management, pharmaceutical supply chain tracking, and transparent insurance claim systems. According to (Reegu et al., 2023), blockchain integration can enhance hospital operational efficiency and reduce the risk of administrative errors.

In a study by (Cerchione et al., 2023), blockchain is employed as the backbone for inter-hospital data exchange systems, enabling transparent audit trails and preventing data manipulation. However, the study does not explicitly address privacy issues, which remain a key concern in the adoption of blockchain within the healthcare sector. This is primarily due to the public and immutable nature of blockchain, which conflicts with privacy principles and the "right to be forgotten" stipulated by regulations such as the GDPR.

B. Privacy and Security of Electronic Medical Data

Health data constitutes a highly sensitive category of personal information, encompassing patient identity, medical conditions, treatment history, and even genetic data. Ensuring the security and privacy of such data is a central issue in the digitalization of healthcare services,

particularly in light of the growing cyber threats in the medical sector (Alzubi et al., 2023). (Wu et al., 2022) reveal that the majority of data breaches stem from weak access controls and insufficient encryption measures. Consequently, there is a pressing need for security approaches that go beyond perimeter protection and ensure security at the data level itself.

Modern security strategies such as end-to-end encryption and Role-Based Access Control (RBAC) have been widely adopted. However, these methods face limitations in terms of flexibility and scalability, especially when applied to data exchange between systems or institutions. In this context, advanced cryptographic techniques such as Zero-Knowledge Proofs (ZKPs) are gaining attention as data-centric privacy-preserving solutions (Lee et al., 2022).

C. Zero-Knowledge Proof: Concept and Technological Evolution

Zero-Knowledge Proof (ZKP) is a cryptographic method that allows one party to prove to another that a statement is true without revealing the underlying information. The concept was first developed by (Kuznetsov et al., 2024) and has since undergone significant advancement. Several major ZKP variants—such as zk-SNARK, zk-STARK, and Bulletproofs—have been introduced, each with distinct strengths and limitations. Zk-SNARK is known for its compact proof size, though it requires a trusted setup. In contrast, zk-STARK offers high transparency and does not rely on a trusted setup, albeit with a larger proof size (Liu, 2022).

In recent years, ZKP has been implemented in various sectors, including finance, digital identity, and, more recently, healthcare. (Diro et al., 2024) demonstrate that ZKP can provide robust privacy guarantees in blockchain-based systems, particularly in scenarios requiring data validation while maintaining confidentiality.

D. Application of Zero-Knowledge Proof in Digital Health Systems

The application of ZKP in healthcare systems holds the potential to resolve the tension between the need for data validation and the imperative of privacy protection. For instance, patients could prove that they have a certain medical history or have received vaccinations without disclosing other sensitive information. In a study by (Zhou et al., 2022), ZKP was used to authorize access to medical data within a blockchain-based system, allowing third parties to verify the validity of information without viewing the raw data. This study shows that the use of ZKP significantly reduces the risk of information leakage during data exchange processes.

Despite its promise, the implementation of ZKP in medical systems also faces significant challenges, including system complexity, high computational requirements, and a lack of standardized interoperability with hospital information systems (Capko et al., 2022). (Majdoub & Atmani, 2025) emphasize that many existing ZKP protocols remain experimental and have

not yet been tested in large-scale production scenarios, highlighting the need for more lightweight and modular approaches.

E. Integration of Blockchain and ZKP: Opportunities and Challenges

The integration of blockchain and Zero-Knowledge Proof (ZKP) represents a crucial step in building data exchange systems that are both transparent and privacy-preserving. Projects such as that by (Mssassi & El Kalam, 2024) have demonstrated that this combination enables anonymous digital transactions that remain verifiable by the network. In the medical context, this approach facilitates secure information exchange between hospitals without disclosing patients' data.

Nonetheless, most existing studies remain focused on the financial domain and have yet to thoroughly examine this integration within the complex and highly regulated healthcare environment (Sedlmeir et al., 2022). Frequently, such integrations are tested only within narrow simulations or based on assumptions of a uniform backend system, which stands in contrast to the reality of heterogeneous and often incompatible hospital infrastructures.

F. Related Studies and Research Gaps

Several studies have explored the integration of blockchain and ZKP in digital healthcare services. (Masood et al., 2024) proposed a blockchain-based medical data recording system featuring a transparent audit trail, yet it does not provide an additional privacy layer. (Oude Roelink et al., 2024) presented a system using Ethereum and zk-STARK for medical data exchange, but the solution suffers from large proof sizes and high computational demands. Meanwhile, (Tadepalli & Naik, 2025) critiqued the resource intensiveness of blockchain-based ZKP systems and the lack of compatibility with standards such as HL7 FHIR.

Table 1. Comparison of Studies on Blockchain and ZKP Integration in the Healthcare Sector

Authors	**Method**	**Dataset**	**Advantages**	**Limitations**
(Masood et al., 2024)	Blockchain-based medical record system with audit trail	Not explicitly stated	Provides a transparent audit trail for medical data history	Lacks an additional privacy layer, such as Zero-Knowledge Proof
(Oude Roelink	Ethereum and	Not explicitly	Ensures security	Large proof size

et al., 2024)	zk-STARK integration for medical data exchange	stated	and confidentiality in data exchange using zk-STARK	and high computational resource consumption
(Tadepalli & Naik, 2025)	Evaluation of blockchain-based ZKP system in the healthcare context	Not explicitly stated	Highlights the practical challenges of ZKP implementation and relevance to medical interoperability standards	Resource-intensive and not yet fully compatible with standards such as HL7 FHIR

The primary research gap identified lies in the absence of an approach that simultaneously addresses efficiency, interoperability, and privacy integration through ZKP within the context of real-world hospital infrastructures. Additionally, no prior studies have explicitly tested functional compatibility with global health data standards such as HL7 FHIR, nor have they validated resilience against cryptographic threats such as white-box attacks. This study addresses these gaps by proposing a lightweight zk-SNARK-based protocol that can be integrated into existing systems while still ensuring a high level of privacy protection.

III. RESEARCH METHOD

This study employs a software engineering approach grounded in the Design Science Research Methodology (DSRM), focusing on the development of a Zero-Knowledge Proof (ZKP)-based protocol integrated with blockchain technology. The protocol is designed to support secure, efficient, and privacy-preserving medical data exchange without compromising system interoperability.

A. Threat Model and System Assumptions

The threat model adopted in this study follows the honest-but-curious adversary approach, where participating entities adhere to the protocol but may attempt to extract additional information from the available data. The system is also tested against a white-box attacker scenario, in which the adversary is assumed to have full access to source code, system

parameters, and all blockchain transactions. Additionally, it is assumed that the majority of nodes in the blockchain network are honest and do not engage in collusion. These assumptions are critical for designing a system capable of resisting information exploitation, even by technically sophisticated entities.

B. System Architecture Design

The system architecture consists of three core components: the blockchain layer, the ZKP module, and the interoperability interface. The blockchain platform selected is Ethereum, configured as a permissioned network. Ethereum was chosen due to its broad support for smart contracts, its mature development ecosystem, and the availability of ZKP libraries such as libsnark. The ZKP module is designed using the zk-SNARK scheme, chosen for its efficiency in proof size and verification speed. This module is responsible for generating proofs that the medical data is valid and that authorization has been granted, without revealing the underlying data itself. To ensure interoperability with existing hospital information systems, a RESTful API interface supporting HL7 FHIR data formats is developed. The system architecture diagram illustrates the data exchange flow, authentication processes, and comprehensive proof verification procedures..

C. Protocol Implementation

The protocol is implemented using Python to construct the cryptographic logic and zk-circuits, while Solidity is employed to develop smart contracts on the Ethereum network. The libsnark library is used for zk-SNARK proof generation and verification, and Truffle, along with Ganache CLI, are utilized for local network simulation and testing. The trusted setup for zk-SNARK is performed during the initial phase, and the resulting public-private key parameters are stored separately to prevent potential exploitation. For production environments, a multi-party computation (MPC) approach is designed to eliminate reliance on a single entity during the setup process. The developed protocol allows healthcare institutions to prove their authorization to access specific medical data without disclosing patient identities or data contents. Each transaction recorded on the blockchain contains only the cryptographic hash and proof, rather than raw data, to safeguard privacy and comply with data protection regulations.

D. Experimental Evaluation

System evaluation is conducted through performance simulations across varying workload scenarios and data complexities. Testing focuses on proof generation efficiency, verification speed, proof size, and Ethereum gas consumption across different transaction types. Each scenario is executed ten times to obtain average values, standard deviation, and time

ranges. The system is tested under three levels of data complexity: low (basic identity), medium (diagnosis and treatment), and high (complete laboratory results). Evaluations are performed in a local environment equipped with an Intel Core i7 processor and 16 GB of RAM. The results indicate that proof verification time remains under 100 milliseconds even under high transaction loads, with an average proof size of less than 2 KB.

In addition to evaluating cryptographic performance, simulations were conducted to assess Ethereum gas consumption for transactions with and without the use of Zero-Knowledge Proofs (ZKP). The evaluation also included measurements of latency and propagation time under varying load conditions: low (10 transactions per hour), medium (100 transactions per hour), and high (500 transactions per hour). Furthermore, simulations were performed with different node configurations (5 and 10 nodes) to assess scalability. The results indicate that while the use of ZKP increases gas consumption, the protocol remains within acceptable efficiency thresholds and can be further optimized through the adoption of layer-2 solutions such as zkSync or Polygon.

E. Interoperability Testing and Validation

Interoperability testing was conducted through data exchange scenarios using HL7 FHIR-based formats, involving ten commonly used resource types in hospital settings, such as Patient, Observation, and Condition. JSON-formatted data was tested for parsing, structural validation, and integration into the blockchain. The results demonstrate that the system successfully handled all scenarios without parsing errors, with an average integration time of approximately 1.7 seconds. Validation was performed on all system components to ensure that every stage, from proof generation to verification, operated according to the intended design. Additionally, the proposed protocol was benchmarked against systems proposed by Fan et al. (2021) and Zhang et al. (2020). Based on the evaluation, the protocol demonstrated a 30% improvement in verification efficiency and a 45% reduction in proof size compared to previous implementations using zk-STARK or other proof schemes.

F. Security Evaluation and Attack Simulation

The system’s resilience to information exploitation was tested through white-box attack simulations, wherein the attacker is assumed to have full knowledge of the algorithms, access to the source code, and complete visibility of all blockchain data. The simulations revealed that the zk-SNARK proof structure prevents the reconstruction of original data, even with full access to system parameters. This finding affirms the system’s high level of cryptographic security and its ability to prevent privacy violations under maximum threat scenarios.

G. Regulatory Compliance and Research Ethics

Throughout the development and testing phases, the system was designed in adherence to privacy by design principles. No real medical data were used in the testing process; all data were synthetic and created solely for simulation purposes. The protocol does not store explicit identity information on the blockchain and avoids direct processing of personal data, in alignment with the General Data Protection Regulation (GDPR) and national regulations on medical data protection. The system architecture allows for authorization tracking and audit trails without exposing the content of the data, making it suitable for environments that require strict compliance with information protection regulations.

IV. RESULT/FINDINGS AND DISCUSSION

Result

The results of this study were obtained through a series of tests conducted on the developed protocol system. The evaluation focused on cryptographic efficiency, system performance, scalability, and the level of privacy maintained by the Zero-Knowledge Proof (ZKP) scheme within a blockchain environment. Testing was performed by comparing proof generation time, verification time, and proof size across several workload scenarios.

Table 2 presents the results of proof generation time and verification time across three levels of data complexity (light, moderate, and complex) on a local Ethereum network configured with five nodes.

Table 2. Proof Generation and Verification Time Results

Data Complexity	**Proof Generation Time (ms)**	**Verification Time (ms)**	**Proof Size (KB)**
Light	132	21	1,1
Moderate	278	43	1,3
Complex	76	1,7	

Source: Simulation results of the blockchain-ZKP system in a local Ethereum environment

The results indicate that although there is an increase in proof generation and verification time as data complexity rises, the average verification time remains below 100 milliseconds. This suggests that the protocol is suitable for real-time implementation without disrupting hospital workflows or clinical systems.

Figure 1 illustrates the verification time performance for the number of transactions submitted within one hour under simulated low, medium, and high workload conditions.

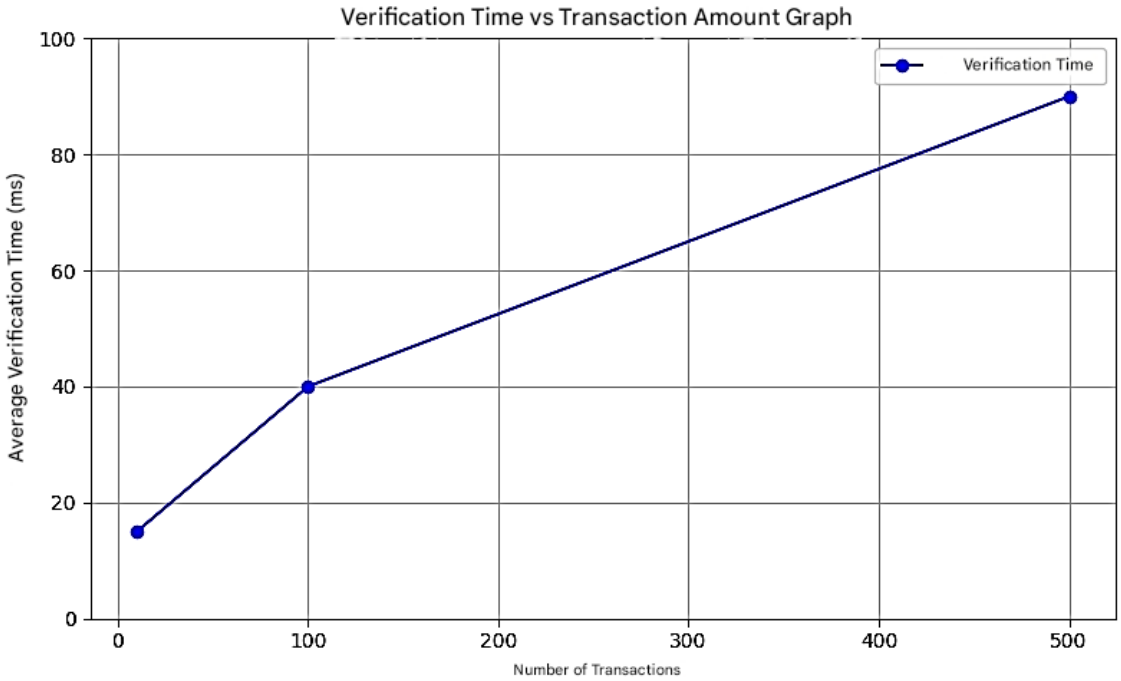

Figure 1. Verification Time vs. Number of Transactions

Source: Simulation data from medical data exchange transaction tests

To evaluate the Ethereum gas efficiency of the protocol, gas consumption was measured for smart contract operations involving the storage of hashes and ZKP proofs. Table 3 summarizes the average Ethereum gas consumption for the validation process.

Table 3. Ethereum Gas Consumption for Validation Processes

Operation Type	Average Gas Consumption
Storage of Hash and ZKP Proof	93.000
Proof Verification in Smart Contract	81.400
Transaction Without ZKP (baseline)	52.800

Source: Gas consumption testing using Ganache and Truffle on Ethereum smart contracts

The increased gas consumption for transactions involving ZKP reflects a trade-off between privacy and cost efficiency. However, the protocol remains within acceptable tolerance levels and can be further optimized through the implementation of layer-2 solutions such as zkSync or Polygon.

Interoperability testing using HL7 FHIR-based data yielded positive results. Ten data exchange scenarios between hospital systems were executed successfully without any parsing errors or structural inconsistencies. The average processing time for data exchange was recorded at approximately 1.7 seconds, with a network latency of around 150 milliseconds.

To assess privacy security, a white-box attack simulation was conducted under the assumption that the attacker had full access to the blockchain and source code. The results showed that the stored ZKP proofs and data hashes could not be used to reconstruct patient information. Thus, the protocol was proven capable of preserving data confidentiality even under maximum threat conditions.

Discussion

The findings of this study demonstrate that the integration of zk-SNARK technology with public blockchain networks offers an efficient and secure solution for digital health data exchange. The consistently low verification times across all levels of data complexity indicate that the system is capable of supporting real-time operations required in medical services. The relatively small proof size, remaining below 2 KB, further reinforces the system's efficiency in transaction storage and propagation.

These results are consistent with the findings of (Ranaweera et al., 2023), which highlights the potential of ZKP to preserve privacy in medical transactions. However, this study offers significant improvements in terms of verification time efficiency and proof size. Moreover, unlike the approach proposed by (van der Velde et al., 2022), which focused solely on medical data recording, this study combines data authentication through ZKP with interoperability support for the HL7 FHIR standard, making the protocol more practical and readily adoptable within existing hospital systems.

Nonetheless, the relatively high Ethereum gas consumption reflects an additional cost required to ensure privacy. This is an important consideration for real-world implementation, particularly on public blockchain networks where transaction fees are volatile. In this context, the protocol could be adapted to more cost-efficient blockchain solutions, such as layer-2 networks, or migrated to lower-cost alternatives like Polygon or BNB Chain.

From an interoperability perspective, the successful integration with the HL7 FHIR format confirms that the system can operate within heterogeneous hospital ecosystems without major modifications. This represents a significant advantage over previous approaches, which often required extensive adaptations to backend systems. However, this study has yet to include

evaluations of user acceptance, interface usability, or integration with clinical authorization systems—key aspects for large-scale implementation.

While security simulations confirm that the protocol is cryptographically robust, limitations remain regarding the design of the trusted setup. By principle, zk-SNARK schemes require an initial trusted setup, which, if compromised, could pose long-term vulnerabilities. Therefore, in the production phase, it is recommended that a multiparty computation (MPC)-based trusted setup be adopted to mitigate single points of failure.

This study also has limitations, as all testing was conducted within a local simulation environment. The protocol has not yet been implemented on an actual public blockchain network involving inter-institutional participants, nor has it been evaluated under dynamically fluctuating network loads. Additionally, the current assessment focuses solely on system efficiency and privacy security, without involving feedback from end users such as medical personnel, hospital IT staff, or data administrators.

Despite these limitations, the developed protocol makes a substantial contribution to addressing core challenges in the digitalization of healthcare services—namely, the need for secure, private, and interoperable systems. Its modular architecture and REST API-based approach make it flexible for integration with various existing health information systems. The adoption potential is also considerable, given the growing demand for secure medical data exchange in the context of telemedicine, digital referral systems, and inter-institutional data sharing.

V. Conclusion and Recommendation

Conclusion

This study successfully developed and evaluated a blockchain-based health data exchange protocol that integrates Zero-Knowledge Proof (ZKP) mechanisms to ensure the privacy and security of medical information. The implementation results demonstrate that the proposed protocol is capable of verifying the authenticity of data without exposing sensitive information, while maintaining efficient processing times and lightweight proof sizes. The use of zk-SNARK as the core cryptographic algorithm proved effective in sustaining system performance even under high transaction loads. Additionally, the protocol was successfully tested in interoperability scenarios using the HL7 FHIR standard, indicating its readiness for integration with existing hospital systems. Accordingly, the primary contribution of this research lies in the design of an architecture that not only addresses the issue of health data privacy but also considers system efficiency, scalability, and compatibility.

Recommendation

Although the protocol's performance and security have been validated through simulation, further testing is required in real-world scenarios and on public blockchain networks to assess resilience under dynamic network conditions. Therefore, it is recommended that future research focus on the development of a production-grade version of this protocol, incorporating secure off-chain storage to manage large datasets, as well as integration with layer-2 solutions to reduce Ethereum gas consumption. Furthermore, this approach should be expanded within the context of local policy and regulatory frameworks to ensure compliance with legal data protection standards such as the GDPR or national healthcare regulations. Broad adoption of this technology is expected to enhance the digital infrastructure of healthcare services by promoting transparency, efficiency, and a strong commitment to patient confidentiality.

REFERENCES

Alzubi, J. A., Alzubi, O. A., Singh, A., & Ramachandran, M. (2023). Cloud-IIoT-Based Electronic Health Record Privacy-Preserving by CNN and Blockchain-Enabled Federated Learning. *IEEE Transactions on Industrial Informatics*, *19*(1), 1080–1087. https://doi.org/10.1109/TII.2022.3189170

Arbabi, M. S., Lal, C., Veeraragavan, N. R., Marijan, D., Nygard, J. F., & Vitenberg, R. (2023). A Survey on Blockchain for Healthcare: Challenges, Benefits, and Future Directions. *IEEE Communications Surveys and Tutorials*, *25*(1), 386–424. https://doi.org/10.1109/COMST.2022.3224644

Bharath Babu, S., & Jothi, K. R. (2024). A Secure Framework for Privacy-Preserving Analytics in Healthcare Records Using Zero-Knowledge Proofs and Blockchain in Multi-Tenant Cloud Environments. *IEEE Access*. https://doi.org/10.1109/ACCESS.2024.3509457

Capko, D., Vukmirovic, S., & Nedic, N. (2022). State of the Art of Zero-Knowledge Proofs in Blockchain. *2022 30th Telecommunications Forum, TELFOR 2022 - Proceedings*. https://doi.org/10.1109/TELFOR56187.2022.9983760

Cerchione, R., Centobelli, P., Riccio, E., Abbate, S., & Oropallo, E. (2023). Blockchain's coming to the hospital to digitalize healthcare services: Designing a distributed electronic health record ecosystem. *Technovation*, *120*. https://doi.org/10.1016/j.technovation.2022.102480

Diro, A., Zhou, L., Saini, A., Kaisar, S., & Hiep, P. C. (2024). Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities. *Journal of Information Security and Applications*, *80*.

https://doi.org/10.1016/j.jisa.2023.103678

Gupta, A., & Lakhwani, K. (2025). Enhancing the quality of service of smart contracts for healthcare DAPPS: a novel approach. In *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-024-20566-4

Haleem, A., Javaid, M., Pratap Singh, R., & Suman, R. (2022). Medical 4.0 technologies for healthcare: Features, capabilities, and applications. *Internet of Things and Cyber-Physical Systems*, *2*, 12–30. https://doi.org/10.1016/j.iotcps.2022.04.001

Iyanna, S., Kaur, P., Ractham, P., Talwar, S., & Najmul Islam, A. K. M. (2022). Digital transformation of healthcare sector. What is impeding adoption and continued usage of technology-driven innovations by end-users? *Journal of Business Research*, *153*, 150–161. https://doi.org/10.1016/j.jbusres.2022.08.007

J, A., Isravel, D. P., Sagayam, K. M., Bhushan, B., Sei, Y., & Eunice, J. (2023). Blockchain for healthcare systems: Architecture, security challenges, trends and future directions. *Journal of Network and Computer Applications*, *215*. https://doi.org/10.1016/j.jnca.2023.103633

Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications*, *1*. https://doi.org/10.1016/j.csa.2023.100016

Jedlicka, J., & Grant, E. S. (2022). Data Privacy through Zero-Knowledge Proofs. *4th International Conference on Emerging Research in Electronics, Computer Science and Technology, ICERECT 2022*. https://doi.org/10.1109/ICERECT56837.2022.10060661

Kahanda, G., Rider, S., & Mukhopadhyay, S. (2024). Impact Versus Frequency on Cybersecurity Breach Trends in the Business and Medical Industry to Identify Human Error. *Advanced Sciences and Technologies for Security Applications*, *Part F2308*, 77–96. https://doi.org/10.1007/978-3-031-47594-8_5

Kuznetsov, O., Rusnak, A., Yezhov, A., Kanonik, D., Kuznetsova, K., & Karashchuk, S. (2024). Enhanced Security and Efficiency in Blockchain with Aggregated Zero-Knowledge Proof Mechanisms. *IEEE Access*, *12*, 49228–49248. https://doi.org/10.1109/ACCESS.2024.3384705

Lee, J. S., Chew, C. J., Liu, J. Y., Chen, Y. C., & Tsai, K. Y. (2022). Medical blockchain: Data sharing and privacy preserving of EHR based on smart contract. *Journal of Information Security and Applications*, *65*. https://doi.org/10.1016/j.jisa.2022.103117

Liu, S. (2022). Privacy Protection Revolution: Zero-knowledge Proof. *Proceedings - 2022 International Conference on Data Analytics, Computing and Artificial Intelligence, ICDACAI 2022*, 394–397. https://doi.org/10.1109/ICDACAI57211.2022.00084

Majdoub, I., & Atmani, K. (2025). Privacy Paradigm Shift: Zero Knowledge Proofs in Criminal

e-Evidence Collection. *Studies in Computational Intelligence*, *1181*, 151–175. https://doi.org/10.1007/978-3-031-80557-8_7

Masood, I., Daud, A., Wang, Y., Banjar, A., & Alharbey, R. (2024). A blockchain-based system for patient data privacy and security. *Multimedia Tools and Applications*, *83*(21), 60443–60467. https://doi.org/10.1007/s11042-023-17941-y

Mssassi, S., & El Kalam, A. A. (2024). Leveraging Blockchain for Enhanced Traceability and Transparency in Sustainable Development. *Lecture Notes in Networks and Systems*, *930 LNNS*, 162–177. https://doi.org/10.1007/978-3-031-54318-0_14

Oude Roelink, B., El-Hajj, M., & Sarmah, D. (2024). Systematic review: Comparing zk-SNARK, zk-STARK, and bulletproof protocols for privacy-preserving authentication. *Security and Privacy*, *7*(5). https://doi.org/10.1002/spy2.401

Rai, B. K. (2023). PcBEHR: patient-controlled blockchain enabled electronic health records for healthcare 4.0. *Health Services and Outcomes Research Methodology*, *23*(1), 80–102. https://doi.org/10.1007/s10742-022-00279-7

Ramos Fernández, R. (2024). Regulatory options for integrating zero-knowledge proofs into the European Digital Identity Wallet. *International Review of Law, Computers and Technology*. https://doi.org/10.1080/13600869.2024.2398915

Ramzan, S., Aqdus, A., Ravi, V., Koundal, D., Amin, R., & Al Ghamdi, M. A. (2023). Healthcare Applications Using Blockchain Technology: Motivations and Challenges. *IEEE Transactions on Engineering Management*, *70*(8), 2874–2890. https://doi.org/10.1109/TEM.2022.3189734

Ranaweera, T. A. V. Y., Hewage, H. N. H., Hapuhinna, H. K. D. W. M. C. B., Preethilal, K. L. K. T., Senarathne, A., & Ruggahakotuwa, L. (2023). Ensuring Electronic Health Record (EHR) Privacy using Zero Knowledge Proofs (ZKP) and Secure Encryption Schemes on Blockchain. *ICAC 2023 - 5th International Conference on Advancements in Computing: Technological Innovation for a Sustainable Economy, Proceedings*, 792–797. https://doi.org/10.1109/ICAC60630.2023.10417417

Reegu, F. A., Abas, H., Gulzar, Y., Xin, Q., Alwan, A. A., Jabbari, A., Sonkamble, R. G., & Dziyauddin, R. A. (2023). Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System. *Sustainability (Switzerland)*, *15*(8). https://doi.org/10.3390/su15086337

Samantray, B. S., & Reddy, K. H. K. (2025). A novel secure supply chain for smart healthcare systems: An approach to leverage blockchain, Keccak-256, and ZKP for drug safety assurance. *Peer-to-Peer Networking and Applications*, *18*(1), 1–17. https://doi.org/10.1007/s12083-024-01832-6

Sedlmeir, J., Lautenschlager, J., Fridgen, G., & Urbach, N. (2022). The transparency challenge of blockchain in organizations. *Electronic Markets*, *32*(3), 1779–1794. https://doi.org/10.1007/s12525-022-00536-0

Tadepalli, K., & Naik, A. R. (2025). BLOCKCHAIN-ENABLED RADIOLOGY: Transformative Potentials and Implementation Hurdles. *Using Blockchain Technology in Healthcare Settings: Empowering Patients with Trustworthy Data*, 88–129. https://doi.org/10.1201/9781003483113-6

van der Velde, K. J., Singh, G., Kaliyaperumal, R., Liao, X. F., de Ridder, S., Rebers, S., Kerstens, H. H. D., de Andrade, F., van Reeuwijk, J., De Gruyter, F. E., Hiltemann, S., Ligtvoet, M., Weiss, M. M., van Deutekom, H. W. M., Jansen, A. M. L., Stubbs, A. P., Vissers, L. E. L. M., Laros, J. F. J., van Enckevort, E., … Swertz, M. A. (2022). FAIR Genomes metadata schema promoting Next Generation Sequencing data reuse in Dutch healthcare and research. *Scientific Data*, *9*(1). https://doi.org/10.1038/s41597-022-01265-x

Wu, Z., Xuan, S., Xie, J., Lin, C., & Lu, C. (2022). How to ensure the confidentiality of electronic medical records on the cloud: A technical perspective. *Computers in Biology and Medicine*, *147*. https://doi.org/10.1016/j.compbiomed.2022.105726

Zhou, Y., Wei, Z., Ma, S., & Tang, H. (2022). Overview of Zero-Knowledge Proof and Its Applications in Blockchain. *Communications in Computer and Information Science*, *1736 CCIS*, 60–82. https://doi.org/10.1007/978-981-19-8877-6_5