Enhancing Privacy and Security in Blockchain-based Health Insurance Management System using Zero-Knowledge Proof

Damilare E. Bakare
MosaiQ Labs, London, United Kingdom

Adekemi O. Amoo
Department of Computer Science & Engineering,
Obafemi Awolowo University, Ile-Ife, Nigeria

Mary T. Onifade
Department of Computer Science & Engineering,
Obafemi Awolowo University, Ile-Ife, Nigeria

ABSTRACT

The health insurance sector has been facing many challenges recently, such as fraudulent activities in insurance claims, data breaches, and high transaction costs, particularly with existing systems built on the Ethereum network, which negatively affect its efficiency and effectiveness. These challenges undermine the trust and financials of insurance providers while compromising the privacy of the patient's health records. To address this issue, this study proposes a conceptual framework that uses zero-knowledge proof within the blockchain system and is deployed on the Polygon Network for its low transaction fees and higher throughput.

The proposed model allows the verification of an insurance claim without revealing sensitive patient health records, ensuring privacy while preventing fraudulent activities. In this conceptual design, the hospital can issue verifiable proof of treatment, appointment, and bill that shows the validity of the insurance claim without revealing the underlying health record to the insurer.

This study, therefore, contributes to supporting research in decentralized applications for healthcare insurance by presenting a conceptual model and comprehensively analyzing the feasibility, rather than a full-scale implementation. It also emphasizes the need to preserve privacy in sensitive domains and the potential benefits of blockchain and ZKP integration.

In conclusion, the research's findings show that, in theory, integrating ZKP with blockchain technology can enhance healthcare insurance processes in terms of reliability, efficiency, privacy, and security. However, further research and practical development are required to realize and evaluate a fully operational system.

Keywords

Zero-Knowledge Proof (ZKP), Blockchain, Healthcare Data Security, Secure Healthcare Systems, Decentralized Applications (dApps), Fraud Prevention, Polygon Network, zk-SNARKs, Health Insurance, Privacy Preservation.

1. INTRODUCTION

Health insurance, according to [15], is a form of insurance that covers or pays the medical and surgical expenses of the insured. It covers the expenses incurred from illness or injury of an insured individual, either by reimbursement or directly to the care provider.

Despite this role, the health insurance industry has, in recent times, been affected by a number of challenges that negatively affect its efficiency and effectiveness.

However, despite its critical role in providing financial protection against healthcare expenses, the health insurance sector faces persistent challenges that hinder efficiency and trustworthiness. For instance, [3] noted that fraudulent claims have been on the rise in health insurance; this is one of the major problems facing the insurance industry. They further explained that these fraudulent claims or activities can lead to financial losses and result in the rejection of genuine claims for policyholders. The scale of the problem is substantial: the Society of Actuaries Research Institute estimates global annual losses from health insurance fraud at nearly US$308 billion, underscoring the need for more robust verification mechanisms[8].

The emergence of blockchain technologies, therefore, provides a great solution to these issues due to their ability to ensure immutability, enhance security, and provide a tamper-proof environment that has driven growth in different industries. The health sector, by far, benefited from adopting blockchain in various areas such as electronic health records (EHR), pharmaceutical and supply chains, insurance and claims, and many more. [33] also emphasized how blockchain technologies can empower innovations to decentralize and digitalize the healthcare system, specifically in health insurance.

These characteristics of blockchain allow the issuer to create a tamper-proof environment that is accessible only to authorized parties, which will help reduce the risk of fraudulent activities.

However, despite the benefits of integrating blockchain technology, privacy concerns remain, especially where sensitive information, such as patient health records, is shared. This is where Zero-Knowledge Proof (ZKP) comes into play as a crucial technology to enhance privacy to maintain data integrity.

Zero-knowledge proof allows an individual to prove the validity of a statement without revealing any underlying information. The application of this concept in the healthcare insurance system, particularly in verifying claims, will ensure that sensitive information like patient health records remains protected, hence addressing a major concern for privacy and improving trustworthiness. [30] further demonstrate that integrating blockchain with ZK-Rollup technology can significantly enhance data management in electronic medical record systems, improving scalability and processing efficiency.

Moreover, the integration of ZKP will also contribute to the prevention of fraudulent activities by ensuring that only verified and genuine claims are processed, which will drastically reduce the possibility of fraudulent claims in the system. This will further streamline the workflow by speeding up the process for insurers and patients. This is in line with larger industrial trends toward digital transformation, which emphasizes the need for robust, privacy-preserving systems in sensitive domains.

2. LITERATURE REVIEW

[34] develop a blockchain-based framework for health insurance that combines smart contracts, advanced validation mechanisms, and a quadratic voting (QV) approach to enable personalized insurance plan selection and dynamic pricing. The model operates across eight stages, from application submission to smart contract deployment, and incorporates machine-learning-based KYC verification and fraud detection. It addresses key issues such as inefficiency, opaque decision-making, limited customization, and fraud risk in traditional health insurance systems. However, while the framework proposes integration of modern technologies, it lacks a concrete discussion about how it would safeguard patient privacy for sensitive health records specifically.

[29] defined health insurance as an assurance that provides financial help to its holder during an emergency. He further explained that it serves as a contract between the holder and the issuer, covering the holder's medical expenses that might occur due to illness, injury, or accident. Currently, the health insurance sector has faced different issues affecting the efficiency and effectiveness of service delivery, most especially those of the insurance issuer or company. Some of these issues are related to data privacy, security, and, most significantly, fraudulent activities.

[40] testified that the key challenges facing the domain are related to issues with data transparency, traceability, data immutability, audit, data provenance, data access control, trust, user privacy, and security. Also, [20] explained that fraud has been a critical issue in the health insurance sector for the past few years, as it incurs high losses for stakeholders (individuals, private firms, and governments). [3] also stressed the issue of fraud in the aspect of fraudulent claims, which is also significant for the insurance industry, as it can lead to substantial financial losses. These challenges have a significant impact, which can result in the denial of genuine claims. This can produce a ripple effect outwards, nudging everything from costs and resources, thereby affecting the system's efficiency and effectiveness.

[9] highlighted some of the common forms of fraudulent activities, including undertaking unnecessary surgeries or treatments by the healthcare provider to generate higher insurance payments, falsifying tests for patients to justify unnecessary medical actions, billing insurance providers for services that were not rendered, or padding claims with charges for procedures that did not take place, misrepresenting non-covered treatments, billing a patient for more than their co-pay or deductible amount. He further indicated that over USD 308.6 billion is lost annually in the United States, and fraudulent health insurance claims account for over 50% of the loss.

In addition to the issue of fraud, patient health data privacy is a main concern, as it is important to ensure that only authorized individuals or organizations have access to it and are kept away from bad actors. [39] explained that during the process of insurance claiming in a typical traditional health insurance system, sensitive information about the patient is shared between the healthcare provider, the patient, and the insurance issuer to validate the claim; this often results in sensitive data leakage. Hence, there is a need for an innovative solution that ensures security and data privacy and reduces or eliminates fraudulent activities in health insurance.

Blockchain, in recent years, has gained a lot of popularity due to its peculiar features or characteristics. These characteristics include decentralization (cannot be controlled by a single entity), integrity (data stored is correct and reliable), immutability (the ability for the data to remain unchanged and unaltered), anonymity (operating under an anonymous identity), transparency (all events and transactions are visible to everyone), audibility, e.t.c.

Because of the unique characteristics of a blockchain, it has had different areas of application across different sectors, including finance and health. Its capability to provide secure, transparent, and decentralized solutions has made it a valuable technology in this application area, enabling solutions like secure financial transactions, improved data management in healthcare, and the potential for enhanced privacy and trust in other sectors. In healthcare, blockchain offers a secure, decentralized, and transparent way to manage data and addresses many challenges, such as patient health data security, interoperability, and privacy. [40] made it known in their literature that blockchain is an emerging and disruptive decentralized technology that has the ability to revolutionize and reshape the way data in the healthcare industry is being handled, thereby helping us solve most of the challenges (Privacy, security, etc.) facing the industry.

Leveraging these capabilities, the technology can help address some of the challenges facing the traditional health insurance system discussed earlier.

[21] worked on an agent-free insurance system using blockchain for healthcare 4.0. They proposed an Ethereum-based framework called ChainSure, using TOPSIS to help users select a need-based insurance policy and also to preserve the privacy of the electronic health records of their users. The proposed system removes the dependency on a central authority and automates the process of choosing the best insurance, thereby reducing the bottleneck of administrative work and cost. However, the study failed to address the process of claiming insurance and the risk and fraudulent activities that are associated with it.

[31] developed a blockchain-based health insurance system to tackle the issue of fraud. They introduced the use of a distributed network to prevent fraudulent insurance claims by ensuring data integrity and transparency among the stakeholders. They proposed a framework that leverages the Ethereum smart contract, a frontend framework (React.js and Redux), a backend framework (Flask), and databases like MongoDB and Neo4j. The process involves validating insurance claims through HIPAA guidelines, storing validated claims in a blockchain network, and using a graph database (Neo4j) to detect potential fraud scenarios. However, the paper does not address the privacy concern related to sensitive patient health records as a result of data integration from different stakeholders, particularly in terms of who has access and how the patient's consent is managed. Also, the transaction fee is high because the framework is Ethereum-based.

[3] developed a decentralized application using blockchain technology to manage health insurance and prevent fraud in the healthcare sector. The system aims to enhance transparency, security, and efficiency in handling insurance claims. It uses Ethereum-based smart contracts to automate the processes involved in health insurance claims, including policy application, verification, claim submission, and approval. The implementation involves several steps to ensure that only verified entities can participate, and smart contracts manage interactions between customers, insurance companies, and hospitals. However, the transaction fee is high as it is

Ethereum-based.

With the use of zero-knowledge proof, the insurance company can verify claims efficiently and securely while preserving the privacy of the patient's medical data. Zero-knowledge Proofs are a different type of cryptographic protocol through which one party (the prover) can prove to another party (the verifier) that a statement is correct or true without necessarily revealing any underlying information about the statement. This concept is increasingly being explored in different domains, particularly to enhance or tackle the issue of privacy and security in blockchain-based systems.

[41] worked on developing a novel blockchain-based framework for handling medical insurance claims, which integrates zero-knowledge proofs to ensure the privacy and authenticity of patient data during the insurance claim process. The framework operates in two main phases: insurance purchasing and claiming, each using cryptographic techniques like non-interactive zero-knowledge proofs and homomorphic encryption algorithms. This system addresses several challenges, including low efficiency, complex service, unreliable data, and data leakage. However, there is no discussion on how this new system could be integrated with the existing healthcare IT infrastructure and insurance systems.

[32] developed an innovative approach to healthcare insurance by building a Zcash algorithm's Zk-SNARKs to enhance data privacy and security. They utilized Zero-knowledge Proof, specifically ZK-SNARKs, to verify transactions without revealing sensitive patient data, which further streamlines the insurance processes and improves data sharing among healthcare providers and insurers. However, the paper failed to explain how this framework could be integrated with the existing healthcare infrastructure, and the approach was Ethereum network-based, which implies a high transaction fee.

In conclusion, using zero-knowledge proofs in healthcare insurance not only promises increased privacy and security but also has the potential to speed claim verification processes and prevent fraudulent activity. ZKPs can help health insurance processes, specifically, the claim verification process, become more trustworthy, efficient, and patient-centered by allowing for proof without revealing patients' sensitive health records. This is consistent with larger industrial trends toward digital transformation, emphasizing the necessity for robust, privacy-preserving systems in sensitive domains. More research and development are needed to maximize the integration of these technologies into current systems and overcome obstacles such as high transaction costs and technical complexity. This ensures that the potential benefits of blockchain and ZKPs are fully realized, resulting in significant improvements in healthcare data administration and insurance claim processing.

3. PROPOSED FRAMEWORK

To define a more efficient and effective framework, a comprehensive review of previous works in blockchain-based healthcare insurance systems and Zero-Knowledge Proof applications was conducted to identify both functional and non-functional requirements. These requirements informed the design of the proposed conceptual model, ensuring it addresses the critical challenges of fraudulent claims, data privacy breaches, and high transaction costs while remaining feasible for practical implementation within existing healthcare and insurance infrastructures. [3] highlighted the key requirements for the blockchain-based health insurance management system. These are:

1) The system is managed by a smart contract deployed on the Ethereum network, which oversees all entities involved in the process and restricts participation.
2) Hospitals can submit registration requests, and the insurance companies on board are responsible for verifying the requests.
3) Before verifying the hospital registration request, at least three associated insurance companies must endorse it.
4) Insurance companies can add multiple insurance policies, with details including premium amounts, policy sum insured, and distinct policy IDs.
5) Each policy belongs to a particular insurance company.
6) Patients can register and submit new insurance policy applications using the policy ID.
7) The policy's insurance company verifies the customer's application, and the policy's sum is remitted to the contract, which retains the amount.
8) To reduce fraudulent actions, the insurance provider contributes 30% of the total actual premium amount to the contract.
9) The customer pays a premium amount to the contract, which is then forwarded to the insurance company.
10) The hospital is responsible for creating medical bills to the contract, along with a bill ID.
11) The insurance company from which the patient has purchased the policy must be connected to the hospital that is creating the bill details.
12) The patient can create a claim application with the claim ID for the insurance company.
13) Before a claim can be approved, the claim must be from a user who has an active policy, and the bill ID must be from the hospital affiliated with them.
14) The insurance company disburses the claim amount if all the requirements are met.

Banate et al. noted that after conducting various tests, they discovered that the optimal premium payment percentage is 30%.

In addition to these established requirements, the proposed framework in this study incorporates the following enhancements to address privacy and cost limitations identified in previous systems:

1) The contract will be built on the Polygon network, thereby reducing the transaction gas fee on the network.
2) The hospitals can issue a verification ID for the patients to verify that the medical emergency was handled.
3) The insurance company can verify the insurance claim submitted by the patient or customer through the verification ID issued by the hospital based on the parameters around the bill submitted by the customer.
4) Given the parameters, the verification contract can confirm the insurance company's verification request without revealing the patient's medical record.

3.1 Framework Components

Table 1: Framework Components

Component	**Description**
Patient	Receives treatment, obtains verification ID from the hospital, and submits a claim with proof.
Hospital	Issues zk-SNARK proofs, verifying treatment validity without disclosing health records.
Insurance Issuer	Verifies claim validity using the verifier without accessing the underlying medical data.
Polygon Network	Hosts smart contracts, offering low transaction fees and high scalability.
Zero-Knowledge Proof Module (Zokrates)	Generates proofs of treatment validity and verifies claims without revealing underlying data.
Frontend	Provides a user interface for patients to submit claims and retrieve proofs securely.
AuthProvider/ Signer (Metamask, Magic Link)	Facilitates user authentication and digital signing of transactions.
File Storage	Stores verification IDs and proofs in a decentralised, tamper-proof manner.
Provider (Alchemy, Metamask)	Connects frontend to blockchain smart contracts using JSON RPC calls.
The Graph	Indexes blockchain transactions for retrieval by the frontend, enabling efficient blockchain queries.

3.2 Architectural Diagram

The system's architecture was designed with modularity in mind, ensuring clear separation of concerns between data storage, verification, and interaction layers.

Figure 1 shows the proposed architectural diagram of the Health insurance management system, comprising different components that interact.

These components are:

1) The Frontend Component: The component the user interacts with to perform specific system actions. It depicts the application's user interface.
2) Auth Provider / Signer: This component provides the authentication method or layer to the application. It helps verify the user's identity on the blockchain and ensures a secure connection between the user and the blockchain network. Metamask and Magic Link are popular wallets and gateways in this context.
3) IPFS (Interplanetary File System): IPFS is a tool for decentralized storage. It allows us to store files across multiple nodes in the network, thereby ensuring data availability and redundancy. In context, this component is used to securely store the user's verification ID as proof to hide the ID from others on the chain.
4) The Graph: This protocol indexes and queries blockchain data or transactions. This component allows the front end to retrieve users' transactions or interactions indexed on the blockchain.
5) Zokrates (zkSNARKS): Zokrates is a toolbox for zkSNARKS, a form of zero-knowledge cryptography. This component handles the claim verification process using the verification ID issued to the user.
6) Provider: This component ensures a secure connection with the Polygon network and helps handle requests and queries from the front end in the form of JSON-RPC. Alchemy is a popular tool in this regard.
7) Smart Contract: This component handles the blockchain's business logic and transaction validation. The smart contract component is written in Solidity and deployed on the Polygon network.

3.3 Process Flow

Figure 2 outlines the process flow for the healthcare insurance claim framework, which incorporates a verification component using zero-knowledge proof, specifically Zokrates. The diagram illustrates the interaction and workflow between the key entities: patients, healthcare providers, insurance issuers, and the Zokrates verification system.

The process starts with the healthcare provider documenting the patient's health information, generating the bill, and issuing a verification ID after providing a medical service to the patient. The patient can then apply for an insurance claim to the insurance issuer using the verification ID received from the healthcare provider after paying for the medical service just received. The insurance issuers then use the verification ID to request claim validation from the Zokrate verification system. This system uses

the zero-knowledge proof concept to verify the claim without disclosing sensitive health information. Upon successful verification, the insurance issuer's contract approves the claim and disburses payment to the patient based on the subscribed insurance policy to cover the medical expenses.

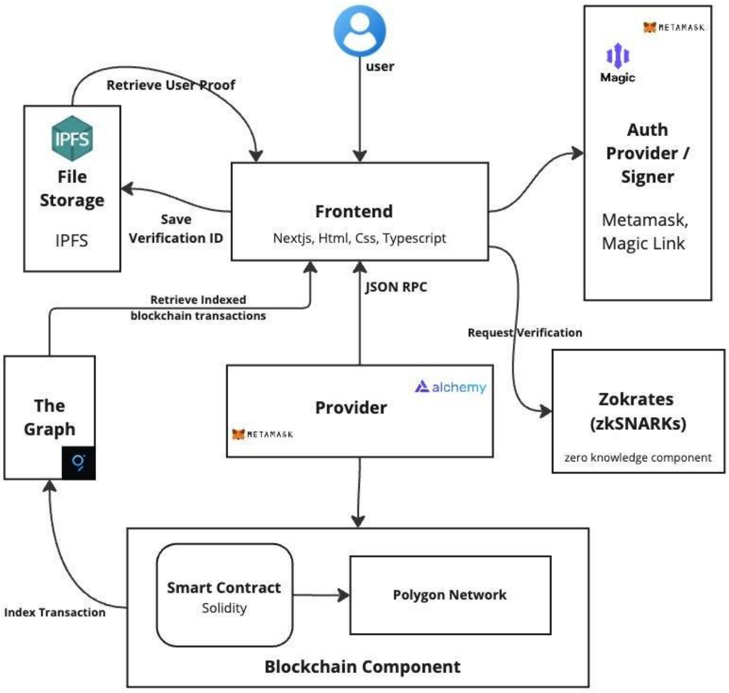

Fig 1: Health Insurance System Architectural Diagram

The proposed framework thus ensures:

1) Preservation of patient privacy by verifying claims without disclosing health data.
2) Fraud prevention, by requiring cryptographic proof-based validation for claims.
3) Cost-effectiveness and scalability are enabled by deploying smart contracts on the Polygon Network with significantly reduced transaction fees compared to Ethereum-based implementations.

4. FEASIBILITY AND RESULT ANALYSIS

4.1 Architectural Feasibility Analysis

The architecture integrates seven major components(as outlined in the architectural model): frontend DApp, authentication provider, IPFS storage, The Graph, Zokrates (zk-SNARK engine), Polygon provider, and smart contracts.

4.1.1 Feasibility Justification

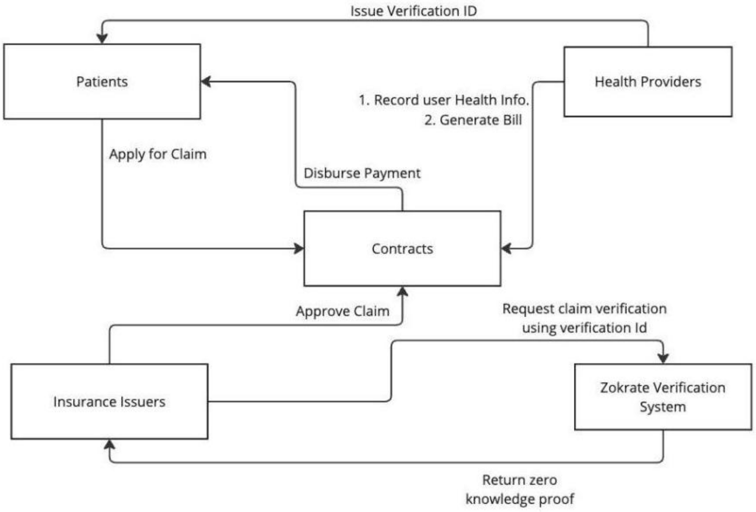

Fig 2: Claim Verification Process Flow Diagram

- Low operational cost: The use of the Polygon network makes the model economically feasible compared to Ethereum-based systems used in prior literature. Polygon's high throughput and minimal gas fees make it suitable for large-scale healthcare operations.

- Modular interoperability: Each subsystem has distinct responsibilities, e.g., ZKPs handle privacy verification, IPFS stores documents securely, and smart contracts enforce business logic. This enables maintainability and scalability.
- Decentralized trust model: Distributed endorsements for hospitals, blockchain immutability, and verifiable on-chain interactions ensure trust without relying on centralized authorities.

4.2 Workflow and Process Analysis

4.2.1 Claim Verification Workflow

The claim verification process introduces a multi-layer validation mechanism involving hospitals, patients, insurers, and the ZKP module. This workflow ensures:

- Authenticity: A hospital-issued verification ID anchors each claim securely.
- Consistency: Only treatments tied to real hospital-insurer relationships can be verified.
- Privacy preservation: ZKPs validate correctness without revealing sensitive medical data.
- Fraud reduction: Claims that fail identity, policy, or treatment constraints cannot pass verification

4.2.2 Claim Verification Workflow

The endorsement process requires endorsement from at least three insurers before a hospital becomes active on the platform.

This significance introduces decentralized validation, reduces the entry of fraudulent hospitals, and establishes early-stage data integrity before claims are ever made.

4.3 Security and Privacy Analysis

The proposed blockchain-based health insurance model integrates multiple layers of security and privacy mechanisms to address fraud, unauthorized access, data integrity challenges, and exposure of personal health information (PHI).

4.3.1 Security

- Immutable event logs: All critical operations, such as policy creation, hospital endorsement, verification ID issuance, claim submission, and claim validation, are recorded as immutable blockchain events, which prevent tampering or retrospective fraud.
- ZKP Proof-Based Fraud Prevention: (ZKPs) provide a foundational security layer by enabling mathematical verification of claim correctness without exposing confidential data

4.4 Result Analysis

This section evaluates the conceptual framework through comparative analysis, feasibility assessments, and projected advantages over existing systems. While no experimental implementation is presented at this stage; however, a theoretical analysis of expected results based on the integrated technologies provides insight into the expected system behaviour and anticipated outcomes.

4.4.1 Comparative Analysis of Expenses

Table 2: Comparative Analysis of Expenses

Administrative Expense	**Expenses in the traditional system, as presented by Banate et al. (2023)**	**How the existing system by Banate et al. (2023) can reduce expenses**	**How the proposed framework can reduce expenses**
Provider Credentialing	4% of expenses	The system automates and streamlines the credentialing process for healthcare providers.	Automates and streamlines the healthcare providers' credentialing process, patients, and insurance issuance.
Fraud Prevention	3% of expenses	The system prevents fraud by providing a secure, transparent, and tamper-proof record of all transactions.	Help prevent fraud by automating the process of insurance claiming using the zero-knowledge concept in claim verification and offering a more secure, transparent, and tamper-proof record of

			transactions.
Data Management	10% of expenses	The system ensures the accuracy and security of customer data and reduces costs.	Ensure the accuracy, security, and privacy of customer data while reducing costs.

4.4.2 Comparative Evaluation with Existing Models

This analysis shows that the proposed model conceptually improves privacy, efficiency, and fraud resistance.

Table 3: Comparative Evaluation with Existing Models

Criteria	**Existing Ethereum Model**	**Centralized Systems**	**Proposed Framework**
Transaction Fee	High	None	Very Low
Privacy	Weak (PHI Exposed)	Weak	Strong (ZKP-based)
Fraud Prevention	Partial	Weak	Strong (workflow+ZKP)
Interoperability	Limited	Limited	High (modular design)
Scalability	Low	Moderate	High (polygon + indexing)

4.4.3 Conceptual Workflow Efficiency

Table 4: Comparative Evaluation with Existing Models

Aspect	**Traditional Time**	**Expected Improvement**
Claim Validation	Slow	Faster (automated logic)
Data Verification	Manual	Automated via ZKP
Fraud Detection	Weak	Strong due to multi-step validation
Stakeholder Coordination	Fragmented	Streamlined

5. CONCLUSION AND FUTURE WORK

5.1 Conclusion

This research proposes a conceptual framework for a blockchain-based healthcare insurance management system that significantly improves the way healthcare insurance processes, particularly claim verification, can be managed. By integrating Zero-Knowledge Proof (zk-SNARK) technology, the framework addresses critical challenges of privacy preservation, security improvement, and fraud reduction inherent in traditional and existing blockchain-based insurance systems.

The proposed model incorporates the roles of three key stakeholders, patients, hospitals, and insurance issuers, each performing distinct but interrelated functions securely coordinated and automated through smart contracts. The inclusion of Zero-Knowledge Proofs enables insurance claims to be verified without disclosing sensitive patient health data, thereby ensuring confidentiality while maintaining trust and compliance with data protection standards.

Furthermore, deploying the framework on the Polygon Network, a layer-2 scaling solution, ensures enhanced performance with faster transaction times, significantly lower gas fees, and reduced network congestion, overcoming a major limitation of Ethereum-based implementations.

In summary, the proposed blockchain-based healthcare insurance management framework effectively combines decentralized technologies and privacy-preserving cryptographic protocols to overcome limitations in existing systems. It offers a robust, scalable, and secure solution that meets the demands of modern healthcare insurance management by ensuring improved performance, cost efficiency, and enhanced data privacy and security.

Although this research focuses on conceptual design and feasibility analysis, the findings support the potential adoption of such a system for transforming health insurance claim processes.

5.2 Future Work

To build upon this conceptual research, future studies and developments should focus on:

1) Detailed Model Design: Develop a comprehensive technical model design, specifying algorithms, database schemas, smart contract logic, and integration workflows to transition from the conceptual framework to an implementable system architecture.

2) Framework Implementation and Testing: Develop and deploy a proof-of-concept implementation of the proposed framework on the Polygon Network.

3) Conduct performance evaluations assessing transaction speed, gas costs, and zk-SNARK proof generation times.

6. REFERENCES

[1] Alnuaimi, A., Alshehhi, A., Salah, K., Jayaraman, R., Omar, I.A., and Battah, A. (2022) *Blockchain-Based Processing of Health Insurance Claims for Prescription Drugs*. IEEE Access, 14 November.

[2] Available at: https://doi.org/10.1109/ACCESS.2022.3219837 [Accessed 18 June. 2024]

[3] Amponsah, A.A., Adekoya, A.F., and Weyori, B.A. (2022). Improving the Financial Security of National Health Insurance using Cloud-Based Blockchain Technology Application. *International Journal of Information Management Data Insights,* 2, 100081.

[4] Available at:

[5] https://www.elsevier.com/locate/jjimei [Accessed 18 June 2024].

[6] Banate, H., Jagtap, Y., Choudhary, D., and Dhage, S. (2023.) *Decentralized Application for Health Insurance Management using Blockchain*, IEEE.

[7] Bakharev, N. (2023). *Unit Testing: Definition, Examples, and Critical Best Practices. AppSec Testing.* Published: 26 July 2023. Updated: 6 September 2024. Available at: https://brightsec.com/blog/unit-testing/

[8] [Accessed:10 September 2024].

[9] Brown, W., Yen, P.-Y., Rojas, M., and Schnall, R. (2013). Assessment of the Health IT Usability Evaluation Model (Health-ITUEM) for evaluating mobile health (mHealth) technology, *Journal of Biomedical Informatics*, 46(6), 1080-1087. doi: 10.1016/j.jbi.2013.08.001.

[10] Chainlink (2024). *What Is a Zero-Knowledge Proof?*, *Chainlink*. Available at:

[11] https://chain.link/education/zero-knowledge-proof-zkp. [Accessed: 8 August 2024].

[12] Chen, H.S., Jarrell, J.T., Carpenter, K.A., Cohen, D.S., and Huang, X. (2019) *Blockchain in Healthcare: A Patient-Centered Mode*l. *Biomed J Sci Tech Res*, 20(3), 15017–15022. Available at:

[13] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6764776/. [Accessed: 7 August 2024].

[14] Chi, P.-W., Lu, Y.-H., and Guan, A. (2023). *A privacy-preserving zero-knowledge proof for blockchain*. *IEEE Access*, 11, 2056. Available at:

[15] https://ieeexplore.ieee.org/abstract/document/10210292 [Accessed: 8 August 2024].

[16] Chung, E. (2024). *Health Insurance Fraud and Its Impact on You*. *Pacific Prime*. Available at:

[17] https://www.pacificprime.com/blog/healthcare-system-fraud-impacts.html [Accessed: 1 August 2024].

[18] Committee on the Consequences of Uninsurance, Board on Health Care Services, Institute of Medicine (2001) *Coverage Matters: Insurance and Health Care. Washington, D.C.: National Academy Press*. Available at:

[19] http://www.nap.edu/catalog/10188.html [Accessed: 31 July 2024]

[20] De Santis, A. and Persiano, G. (1992) *Zero-knowledge proofs of knowledge without interaction*. In *Proceedings of the 33rd Annual Symposium on Foundations of Computer Science*. IEEE Computer Society, 427-436.

[21] Donmez, A. and Karaivanov, A. (2021). *Transaction fee economics in the Ethereum blockchain*. *Economic Inquiry*. [online] Available at: https://doi.org/10.1111/ecin.13025 [Accessed: 19 September 2024].

[22] Gad, A.G., Mosa, D.T., Abualigah, L., and Abohany, A.A. (2022.) Emerging Trends in Blockchain Technology and Applications: A Review and Outlook. *Journal of King Saud University - Computer and Information Sciences*,

34(9), 6719-6742. Available at:

[23] https://www.sciencedirect.com/science/article/pii/S1319157822000891. [Accessed: 2 August 2024].

[24] Goldwasser, S., Micali, S., and Rackoff, C. (1989). The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1), 186-208.

[25] HDFC Life (2024) *Health Insurance- Meaning and Definition.* Available at:

[26] https://www.hdfclife.com/insurance-knowledge-centre/about-life-insurance/health-insurance-meaning-and-types [Accessed: 15 June 2024]

[27] Hölbl, M., Kompara, M., Kamišalić, A., and Nemec Zlatolas, L. (2018). *A Systematic Review of the Use of Blockchain in Healthcare*. Symmetry, 10(10), 470. Available at: https://doi.org/10.3390/sym10100470 [Accessed: 7 August 2024].

[28] Hypersign (2023). *Zero Knowledge Proof: Types, Advantages, Use Cases*. *Hypersign*. Available at: https://www.hypersign.id/blogs/tpost/oyeti7uia1-zero-knowledge-proof-types-advantages-us [Accessed: 9 August 2024].

[29] Hossain, M.I. (2024). Software Development Life Cycle (SDLC) Methodologies for Information Systems Project Management. *International Journal for Multidisciplinary Research (IJFMR)* [online]. Available at:

[30] https://www.ijfmr.com/papers/2023/5/6223.pdf. [Accessed 18 August 2024]

[31] Investopedia Team (2024). *What Are Smart Contracts on the Blockchain, and How Do They Work?* [online] Investopedia. Available at:

[32] https://www.investopedia.com/terms/s/smart-contracts.asp [Accessed: 29 August 2024].

[33] Kapadiya, K., Patel, U., Gupta, J., Alshehri, M.D., Tanwar, S., Sharma, G., Bokoro, P.N., et al. (2022) *Blockchain and AI-Empowered Healthcare Insurance Fraud Detection: an Analysis, Architecture, and Future Prospects*, IEEE Access, 10. Available at:

[34] https://ieeexplore.ieee.org/abstract/document/9843995 [Accessed: 31 July 2024].

[35] Karmakar, A., Ghosh, P., Banerjee, P.S., and De, D. (2023). *ChainSure: Agent-free insurance system using blockchain for healthcare 4.0. Intelligent Systems with Applications*, 17, 200177. Available at:

[36] https://www.sciencedirect.com/science/article/pii/S2667305323000029 [Accessed 18 June. 2024]

[37] Krichen, M., Ammi, M., Mihoub, A., and Almutiq, M. (2022) *Blockchain for Modern Applications: A Survey*. Sensors, 22(14), 5274. Available at:

[38] https://doi.org/10.3390/s22145274. [Accessed: 1 August 2024].

[39] Krysiak, A. (2023) *SDLC Guide: How to Conduct Software Design Phase*. Strato Flow. Available at: https://stratoflow.com/sdlc-design-phase/ [Accessed: 22 August 2024].

[40] Kotarkar, A., Padamadan, S., Warekar, Z., and More, J. (2022). *Leveraging the Power of Blockchain in the Health Insurance Industry*. Proceedings of the 2022 2nd International Conference on Intelligent Technologies, [online] IEEE. Available at:

[41] https://ieeexplore.ieee.org/abstract/document/9848345. [Accessed: 7 August 2024].

[42] K-CRIO (2011): *An ontology for organizations involved in product design*. Scientific Figure on ResearchGate. Available at:https://www.researchgate.net/figure/Software-development-process-Waterfall-Model_fig5_216702344 [accessed 19 Aug 2024]

[43] Lee, A.R., Kim, M.G., and Kim, I.K. (2019) *SHAREChain: Healthcare data sharing framework using Blockchain-registry and FHIR*. 2019 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), San Diego, CA, USA, 18-21 November 2019. IEEE. Available at:

[44] https://doi.org/10.1109/BIBM47256.2019.8983415. [Accessed: 7 August 2024]

[45] Lindrea, B. (2023). *Ethereum, Bitcoin users reignite scalability debate as gas fees surge*. Cointelegraph. [online] November 2023.Available at:

[46] https://cointelegraph.com/news/ethereum-bitcoin-gas-fee-surge-reignite-scalability-debate [Accessed: 19 September 2024].

[47] Lteif, G. (2024). *Software Development Life Cycle (SDLC) Demystified: A Thorough Beginner's Handbook in Software Engineering*. SoftwareDominos. Available at:

[48] https://softwaredominos.com/home/software-design-development-articles/understanding-the-sdlc-in-software-engineering-a-comprehensive-guide/. [Accessed 18 August 2024].

[49] Maheshwari, R. (2023). *What is Health Insurance: Meaning, Benefits & Types*. [online] Forbes. Available at: https://www.forbes.com/advisor/in/health-insurance/what-is-health-insurance/ [Accessed: 31 July 2024].

[50] Ma, S. and Zhang, X., 2024. *Integrating blockchain and ZK-ROLLUP for an efficient healthcare data privacy protection system via IPFS.* Scientific Reports, 14(1), p.11746. Available at:

[51] https://doi.org/10.1038/s41598-024-62292-9 [Accessed 21 Oct. 2025].

[52] Saldamli, G., Reddy, V., Bojja, K.S., Gururaja, M.K., Doddaveerappa, Y., and Tawalbeh, L. (2022).*Health Care Insurance Fraud Detection Using Blockchain*. Proceedings of the 2022 2nd International Conference on Software-Defined Systems, [online] IEEE. Available at: https://ieeexplore.ieee.org/abstract/document/9143900 [Accessed 7 August 2024].

[53] Samanta, M., Bisht, C., & Singh, P. (2024). *Application of Ethereum Smart Contract in healthcare and health insurance using Zk-SNARKs in Zcash.* In Proceedings of the IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation. 2024.

[54] Shouri, S. & Ramezani, R. (2025) 'A blockchain-based health insurance model enhanced with quadratic voting', Health Informatics Journal, published online 2 May. doi:

10.1177/14604582251339422.

[55] Singh, D., Monga, S., Tanwar, S., Hong, W.C., Sharma, R., and He, Y.L. (2023.) *Adoption of Blockchain Technology in Healthcare: Challenges, Solutions, and Comparisons*. Appl. Sci., 13(4), 2380. Available at:

[56] https://doi.org/10.3390/app13042380 [Accessed 23 July 2024].

[57] S. Chiaradonna, P. Jevtić, and D. Boscovic, *Zero-Knowledge Proofs: Emerging Opportunities for the Insurance Industry*, Society of Actuaries Research Institute, Oct. 2023.

[58] Taya, S. and Gupta, S. (2011).Comparative Analysis of Software Development Life Cycle Models. IJCT, 2(4), 1-4. Available at: http://ijcst.com/vol24/3/sanjana.pdf. [Accessed 18 August 2024]

[59] Tripathi, G., Ahad, M.A., and Casalino, G. (2023). A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges. *Decision Analytics Journal*, 9, 100344. Available at: https://doi.org/10.1016/j.dajour.2023.100344 [Accessed: 1 August 2024].

[60] Unchained (2024). What are Zero-Knowledge Proofs? ConsensusMagazine, 11 January. Updated 8 March 2024. Available at:

[61] https://www.coindesk.com/consensus-magazine/2024/01/11/what-ae-zero-knowledge-proofs/ [Accessed: 9 August 2024].

[62] X. He, S. Alqahtani, and R. Gamble. *Toward Privacy-Assured Health Insurance Claims*. 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 2018, 1634-1641

[63] Yaqoob, I., Salah, K., Jayaraman, R., and Al-Hammadi, Y. (2021) *Blockchain for healthcare data management: opportunities, challenges, and future recommendations*. Neural Computing and Applications, 34, 11475–11490. Available at:

[64] https://link.springer.com/article/10.1007/s00521-020-05519-w. [Accessed: 31 July 2024].

[65] Zheng, H., You, L., and Hu, G. (2022). *Novel insurance claim blockchain scheme based on zero-knowledge proof technology*. Computer Communications, 195, 207-216. Available at: https://doi.org/10.1016/j.comcom.2022.08.007. [Accessed: 13 August 2024].