Blockchain-Based Fraud Detection System for Healthcare Insurance Claims

Hopewell Bongani Ncube[1], Belinda Mutunhu Ndlovu[1], Sibusisiwe Dube[1] and Kudakwashe Maguraushe[2]

[1]Department of Informatics and Analytics, National University of Science and Technology, Bulawayo, Zimbabwe

[2]Mangosuthu University of Technology, Durban, South Africa

ncubehopewellb@gmail.com
belinda.ndlovu@nust.ac.zw
sibusisiwe.dube@nust.ac.zw
kuda.maguraushe@mut.ac.za

Abstract: Healthcare fraud is a huge concern that affects not only the financial viability of insurance companies but also the well-being of patients who may receive compromised care due to fraudulent acts. Addressing this issue demands novel solutions that can detect and prevent fraudulent conduct in healthcare insurance claims. The project intends to establish an automated fraud detection system using blockchain technology, which has advantages such as security, transparency, and data immutability. By leveraging blockchain's decentralized ledger, the system creates a tamper-proof platform for processing healthcare insurance claims, preventing fraudulent alterations and enhancing trust in the integrity of the claims process. Ethereum's blockchain platform and smart contracts play a critical role in ensuring the secure recording of transactions while preventing retroactive alterations. Moreover, an on-chain database is employed to manage relevant claim data, thereby safeguarding its integrity and ensuring accessibility. The decentralized nature of blockchain technology brings additional advantages by eliminating the need for intermediaries, thereby reducing administrative costs and streamlining the claim processing workflow. The adoption of methodologies such as Personal Extreme Programming (PXP) and Design Science Research Methodology (DSRM) fortifies the project's framework. PXP facilitates continuous improvement through incremental and iterative development, while DSRM ensures a structured approach to problem-solving, yielding reliable results. Through rigorous testing and validation, the automated fraud detection system enhances the efficiency and accuracy of fraud identification in healthcare insurance claims. By combining blockchain technology with methodological frameworks, this project offers a promising solution to combat healthcare fraud, safeguarding insurance systems' integrity and ensuring quality care for patients. Future iterations will focus on expanding the system's capabilities and refining its algorithms to counter the evolving fraudulent tactics prevalent in the healthcare industry.

Keywords: Healthcare fraud, Insurance claims, Blockchain, Automated detection system, Ethereum, Smart contracts

1. Introduction

Healthcare fraud is a pervasive issue that affects the financial stability of insurance companies and the quality of patient care. These fraudulent activities not only result in financial losses but also compromise patient safety, leading to potential harm due to unnecessary or falsified medical procedures (Ismail & Zeadally, 2019). Current fraud detection mechanisms primarily rely on manual audits and rule-based systems, which are often inadequate in identifying sophisticated fraudulent schemes. Traditional methods are plagued by issues such as data quality, scalability, and the ability to adapt to new types of fraud (Amponsah et al., 2022). The integration of advanced technologies like machine learning (ML) and artificial intelligence (AI) has shown promise in enhancing fraud detection capabilities. However, these approaches still face significant challenges, including data privacy concerns, the interpretability of complex models, and the high computational resources required (Kapadiya et al., 2022; Kaafarani et al., 2023). Blockchain technology offers a novel approach to addressing these issues. With its decentralized and immutable nature, blockchain provides a secure, transparent, and tamper-proof platform for processing healthcare insurance claims (Ncube et al., 2022). By leveraging Ethereum's blockchain platform and smart contracts, the proposed system aims to fulfill the following objectives: 1. create a tamper-proof ledger for all claims 2. validate claims in real-time 3. verify the authenticity of claims using blockchain 4. identify fraudulent claims in real-time.

2. Literature Review

This literature review explores the current landscape of healthcare insurance fraud and the potential of blockchain technology in mitigating fraudulent activities. Kapri and Venkatesh (2023) define healthcare insurance as a means of providing financial protection against medical expenses, emphasizing its significance in ensuring the well-being of subscribers. However, fraudulent activities, such as filing false claims, pose a threat to the integrity of insurance systems, as highlighted by Ismail and Zeadally (2019).

2.1 Blockchain Technology in Healthcare

The blockchain network is based on a peer-to-peer network where each participant maintains a replica of the shared ledger, which can only be appended to but not edited ensuring the authenticity and integrity of data (Ncube et al., 2022). Scholars leverage two types of blockchain platforms, Ethereum and Hyperledger, in healthcare insurance fraud detection, which are gaining traction. Kapri & Venkatesh (2023) advocated for Ethereum's scalability and security features in managing insurance processes, highlighting its compliance with healthcare standards and ability to handle thousands of transactions per second while securing user data through its permissioned network.

Ethereum is particularly noted for its ability to address existing system challenges, such as verifying insurance records using EDI (Electronic Data Interchange) Validators and adhering to HIPAA (Health Insurance Portability and Accountability Act) standards (Saldamli, 2020). Mackey et al. (2020) further highlighted Ethereum's support for democratic autonomous organizations, smart contract execution environments, and tokens via the ERC-20 standard, crucial for enhancing data security and ensuring tamper-proof transaction auditing in healthcare fraud detection.

In contrast, Hyperledger is also prominent in healthcare insurance fraud detection. Kaafarani et al. (2023) provide a decision-making framework for selecting blockchain platforms, emphasizing mandatory features like support for smart contracts, a permissioned blockchain, and decentralized networks. They highlight Hyperledger's capabilities in supporting enterprise-grade applications with features such as private networks, data privacy technologies, and multi-language support like Java and Golang.

In summary, the integration of blockchain technology in healthcare insurance aims to enhance data security, compliance, and efficiency in fraud detection processes. Both Ethereum and Hyperledger offer distinct advantages that cater to the specific needs and challenges of the healthcare industry. Ethereum's scalability, robust security features, and support for decentralized applications position it as a strong choice for enhancing fraud detection mechanisms in healthcare insurance compared to Hyperledger's emphasis on enterprise-grade applications and data privacy technologies (Elda Hiererra et al., 2022; Kapri & Venkatesh, 2023).

Flagging Fraudulent Claims in Blockchain

Fraudulent claims are effectively flagged and mitigated through the inherent features of blockchain technology, as discussed by Saldamli (2020). The immutability of blockchain data ensures that once a claim is recorded on the blockchain, it cannot be altered or tampered with. This means that if a healthcare professional submits a bogus claim, it is permanently recorded, making it impossible for the supplier to modify or erase the claim later (Kapadiya et al.,2022).

Furthermore, the use of smart contracts, ledger broadcasting, and network consensus enhances fraud detection and risk reduction (Elda Hiererra et al., 2022). Smart contracts, for instance, can be programmed to automatically verify the authenticity of claims based on predefined criteria, flagging suspicious transactions for further review. Additionally, the consensus mechanism employed in blockchain networks ensures reliability and trust among unknown peers, further strengthening fraud detection efforts.

Predefined rules play a crucial role in flagging fraudulent claims on the blockchain. These rules are typically encoded into smart contracts, which are self-executing contracts with predefined conditions and outcomes. By establishing predefined rules within smart contracts, insurance companies can automate the validation and verification process for claims submission. By leveraging predefined rules within smart contracts, insurance companies can streamline the claims processing workflow, reduce the risk of fraudulent activities, and ensure compliance with regulatory standards. This automation not only improves efficiency but also enhances transparency and trust in the insurance ecosystem (Elda Hiererra et al., 2022; Saldamli 2020).

2.2 Related Works

Artificial Intelligence (AI), Machine Learning (ML), and Data Analytics (DA) have been extensively studied for their roles in healthcare insurance fraud detection (Amponsah et al., 2022a; Kaafarani et al., 2023; Gohil et al., 2022). Kapadiya et al. (2022) emphasized the use of AI in detecting fraud through behavioral profiling and various learning techniques. AI models are praised for their accuracy and efficiency in identifying fraudulent activities. However, they are heavily dependent on high-quality data and are challenged by imbalanced datasets where fraudulent instances are significantly fewer than non-fraudulent ones. Moreover, the integration of AI systems with existing technologies requires specialized knowledge, and ensuring real-time data access remains difficult. Amponsah et al. (2022) discussed ML techniques such as decision trees, support vector machines, and logistic

regression. ML models automate fraud detection effectively and can handle large datasets, enhancing detection capabilities. However, they face significant concerns regarding data quality, scalability, and their reliance on pre-established fraud scenarios, which limits their ability to detect new types of fraud. Additionally, security and privacy issues arise due to the sensitive nature of the data being processed.

Scholars also highlighted the role of advanced data analytics in processing large healthcare datasets to identify anomalies indicative of fraud. DA's strength lies in its ability to manage the volume, variety, velocity, and variability of big data, which are crucial for effective fraud detection. The analytics approach offers comprehensive insights into fraudulent behavior patterns, enhancing detection accuracy. However, managing such complex data presents significant challenges, and the limited evaluation of improvement strategies due to small dataset sizes hampers the effectiveness of these analytics methods. Despite these constraints, integrating ML with DA can provide a more robust understanding of fraud patterns and improve the accuracy of detection systems. Together, AI, ML, and DA offer a multifaceted approach to enhancing fraud detection, each contributing unique strengths while facing specific challenges related to data quality, scalability, and integration (Amponsah et al., 2022a; Kaafarani et al., 2023; Gohil et al., 2022; Herland, 2019).

Blockchain technology, a peer-to-peer network, ensures secure transactions by maintaining a shared ledger with immutability and an append-only nature. This technology preserves data integrity by preventing alterations and simplifying tracking, thereby enhancing transparency and trust. Ncube et al. (2022), Mackey et al. (2020), Kapri & Venkatesh (2023), Saldamli (2020), and Elda Hiererra et al. (2022) advocate for blockchain technology due to its decentralized structure, which eliminates single points of failure and makes it resilient to attacks. Predefined rules in smart contracts can automate validation and verification processes, flag fraudulent claims, reduce fraud risks, and ensure regulatory compliance. These features significantly enhance the efficiency and robustness of fraud detection systems.

In conclusion, while AI, ML, and Data Analytics each offer significant advancements in healthcare insurance fraud detection, they also face substantial challenges related to data quality, scalability, and integration. Blockchain technology addresses many of these issues by ensuring data integrity, security, and transparency through its decentralized nature and the use of smart contracts. Adopting blockchain in the healthcare insurance industry can develop more robust, efficient, and trustworthy fraud detection systems, ultimately enhancing the overall integrity and reliability of the insurance ecosystem.

2.3 Research Gaps

This study identified a critical research gap in healthcare insurance fraud detection. Current technologies, including machine learning (ML), artificial intelligence (AI), and data analytics (DA), rely on high-quality data, but face significant issues related to data quality, ambiguity, and scalability, impacting their ability to detect fraud accurately (Ali, 2019). Amponsah et al. (2022) highlighted that traditional methods, such as manual audits and rule-based systems, are inadequate for detecting sophisticated and complex fraud schemes, necessitating more advanced approaches.

The existing literature (Ncube et al., 2022; Mackey et al., 2020; Kapri & Venkatesh, 2023; Saldamli, 2020; Elda Hiererra et al., 2022) underscores the potential of blockchain technology, but its application in healthcare insurance fraud detection remains underexplored. Developing a comprehensive fraud detection system that incorporates blockchain technology could address the limitations of current methods, offering a more secure, efficient, and trustworthy solution. Further research is essential to fully leverage blockchain's capabilities and create more robust and reliable fraud detection mechanisms.

Blockchain technology offers a promising solution to these challenges by enhancing transparency, accountability, traceability, security, and immutability (Ali, 2019). Its decentralized, tamper-proof ledger ensures data integrity and automates validation processes, reducing human error and ensuring regulatory compliance (Kapri & Venkatesh, 2023). Integrating blockchain can significantly increase the efficiency and effectiveness of fraud detection systems in healthcare insurance.

3. Research Methodology

The methodologies employed Design science as the research methodology and Personal Extreme Programming as the software development approach to create a complete blockchain-based fraud detection system. The software development methodology utilized is known as Personal Extreme Programming (PXP). PXP improves software quality and empowers independent developers by integrating modified XP with Personal Software Process (PSP) methodologies (Iyawa, 2020). PXP prioritizes high-importance skills in each iteration to ensure

customer satisfaction and continuing progress. We divided requirements into functional and non-functional categories using the PXP technique, focusing on claims submission, authentication, verification, analysis, and reporting. Periodic reviews ensure alignment with user demands. Key functional and nonfunctional requirements include**:** The research uses Visual Studio Code as the primary IDE, the Ethereum blockchain platform for smart contract creation, and React for front-end development. For UI prototype, smart contract creation, and local testing, tools such as Hardahat, Remix, and Figma are utilized, in that sequence

4. System Activity Diagram

Activity diagrams are intended to show the activities that make up a system process and the flow of control from one activity to another (Sommerville, 2011). They show how different workflows in the system are constructed, how they start, and the possible decision paths that can be taken from start to finish. Activity diagrams are comprised of activities, states, and transitions between them. Figure 1 below shows the activity diagram for the system

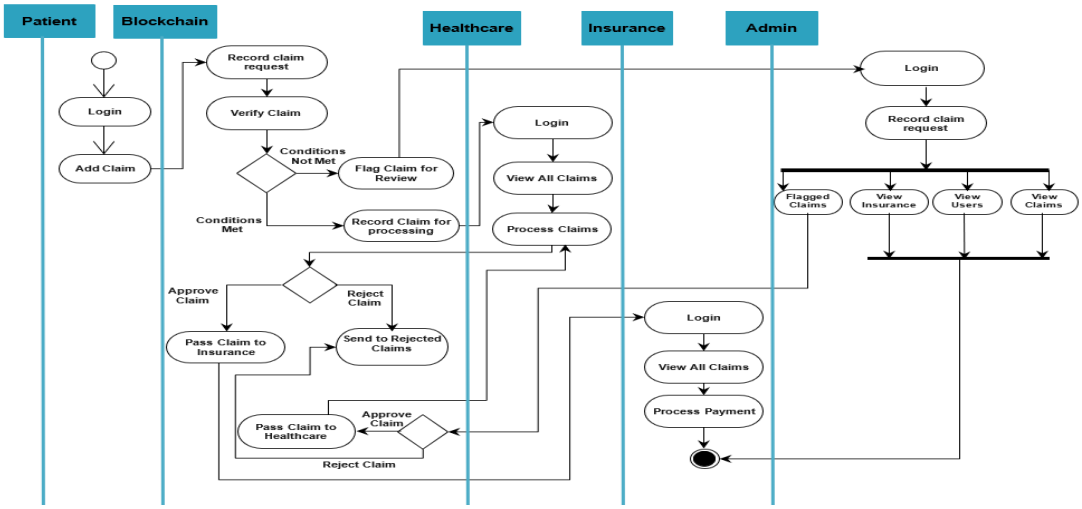

Figure 1: Activity Diagram

The process of initiating a claim begins with a patient submitting a claim request through a web browser, providing details about the medical service received and the cost. This information is then encrypted and sent to a blockchain network for verification and processing. The blockchain verifies the patient's eligibility and the healthcare provider's legitimacy, as well as checks the claim details against per-defined rules encoded in smart contracts. If the verification is successful, the claim is approved, updating the status on the blockchain and potentially initiating a payout to the provider. If the claim does not meet the verification criteria, it may be flagged as potential fraud and passed for further review or rejected. There is also a scenario that allows Admin to view all claims, adding, and listing insurance providers and users.

5. Results and Discussions

The blockchain-based fraud detection system in healthcare insurance demonstrated efficient capabilities through seamless integration of the fronted user interface, backed, and Ethereum blockchain. This system offers transparency, security, and real-time data access, enhancing fraud prevention and detection processes. The results highlight the potential of blockchain based solutions to revolutionize fraud detection in healthcare insurance, providing a reliable platform for mitigating fraudulent activities and ensuring insurance claim integrity. The system consists of interfaces through which patients, healthcare providers, administrators, and insurance professionals interact. These interfaces play a crucial role in facilitating communication, data exchange, and fraud detection within the healthcare insurance ecosystem.

Login

The login screen prompts the user to enter their credentials and gives feedback if the credentials are incorrect. Figure 2 shown below is the visual view of a user logging on to the system.

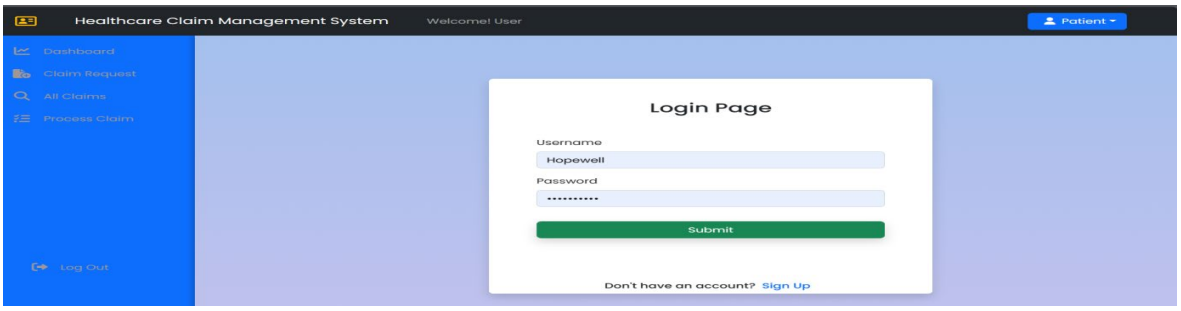

Figure 2: Login Screen

Admin Screen

Administrators utilize an interface to manage user-related tasks, including adding new users such as healthcare providers, patients, and insurance representatives. This interface collects essential personal details and assigns user roles accordingly. Administrators can also add insurance providers to the system. Furthermore, they review and approve user role requests to ensure appropriate role assignments based on user responsibilities. Additionally, administrators have access to tools within the interface to review flagged fraudulent claims, facilitating the investigation and necessary actions such as rejection or further inquiry this is shown in Figure 3.

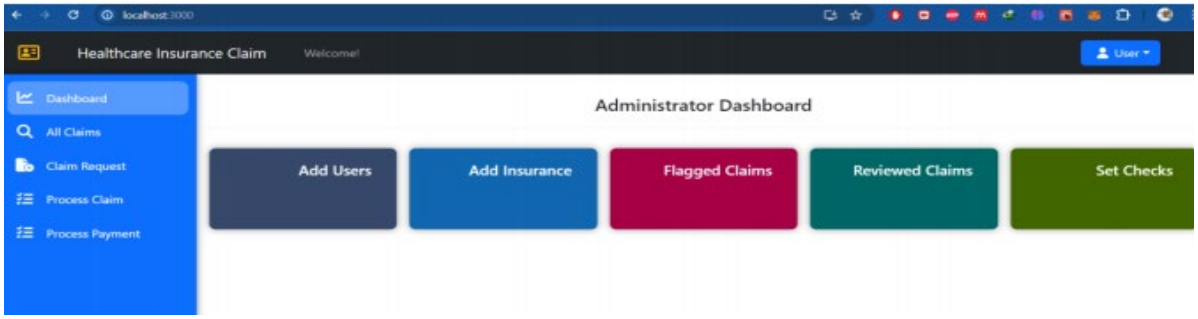

Figure 3: Admin Screen

User Registration Screen

Figure 4 simulates the registration process for a new user in the system by inputting new user information, including name, email, and password, into the registration form. The expected outcome is that upon successful registration, the system creates a new user account and provides confirmation to the user, ensuring a seamless and efficient registration process for new users.

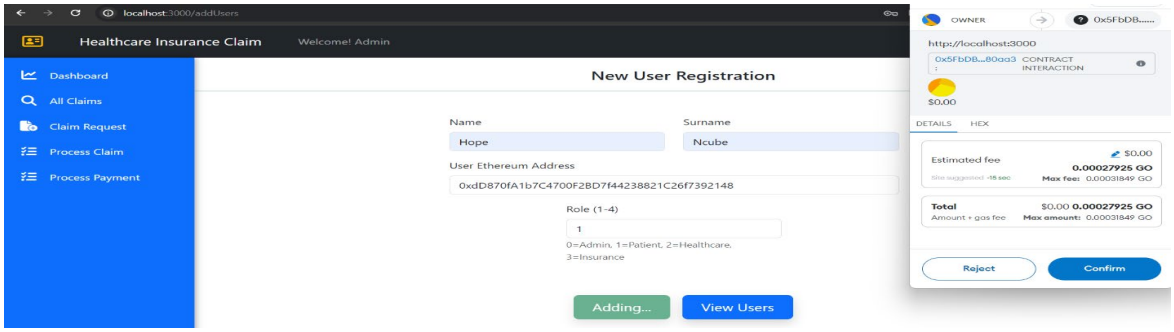

Figure 4: User Registration Screen

Patient Screen

Figure 5 simulates a Patient initiating a claim request for healthcare services received, providing details such as the patient details, healthcare provider information, and treatment received. They can track the status of their submitted claims, including updates on claim processing, approval, or rejection, ensuring transparency and keeping them informed about reimbursement progress.

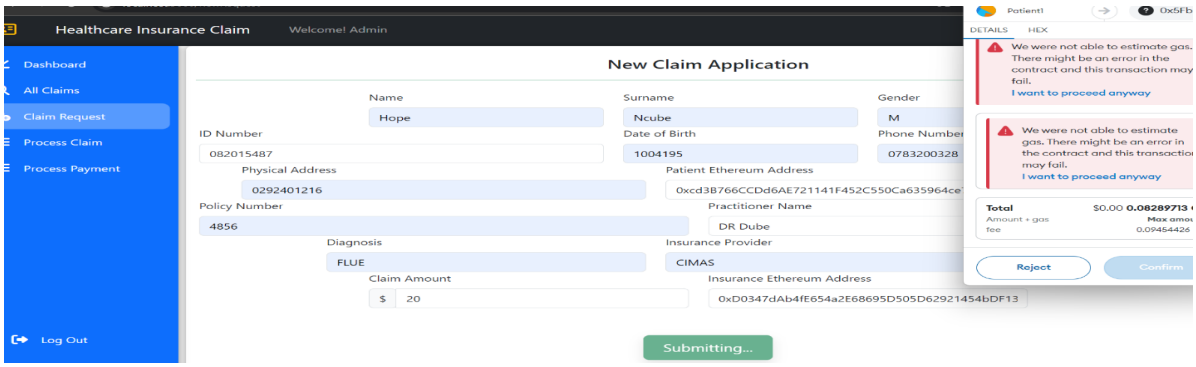

Figure 5: Patient Screen

Healthcare Screen

Healthcare providers review, assess validity, and process claim applications submitted by patients. They access a dashboard displaying all submitted claims, including pending, approved, and rejected claims, enabling them to track claim statuses and take necessary actions accordingly. Figure 6 shows the page for the process of viewing all claims

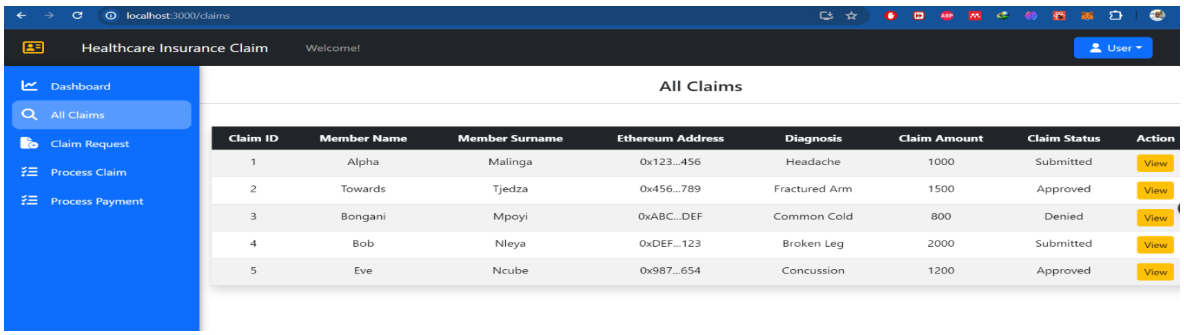

Figure 6: Healthcare Screen

When viewing a single claim, the user interacts with the Claims component, which displays a table of all claims. Each entry has a "View" button. Clicking this button redirects the user to a dedicated page via a dynamic route with the claim's unique ID. The component then fetches and displays the full details of the selected claim in a receipt-like format. This allows users to easily access detailed information about specific claims from the list view. The full Individual claim application made by a user is shown in Figure 7 below.

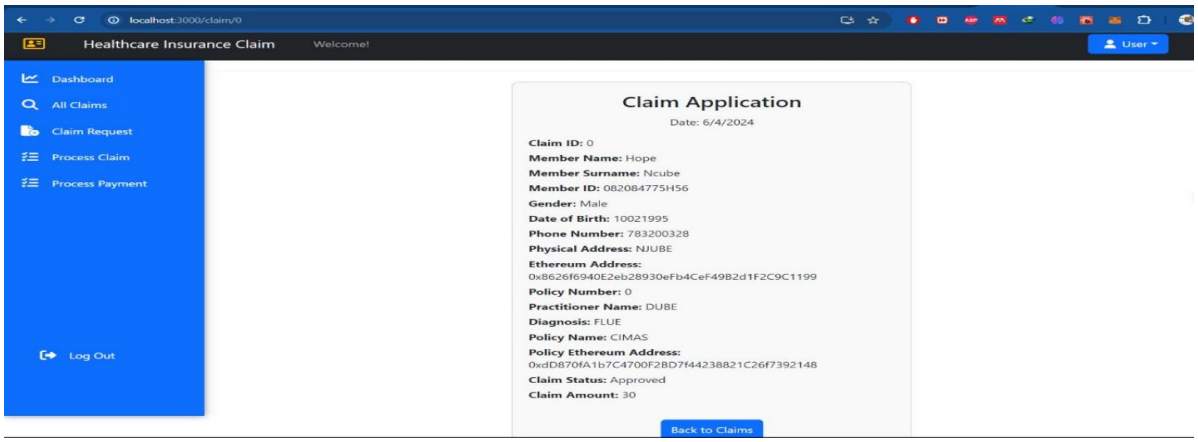

Figure 7: Viewing Full Individual Claim

In the Process Claim interface, the user sees the full details of the claim and is provided with buttons to either approve or deny the claim, along with fields to input any necessary notes or reasons for the decision. This interface is designed to streamline the decision-making process, ensuring that all relevant information is easily accessible, and actions can be taken efficiently. Figure 8 shows the process claim screen

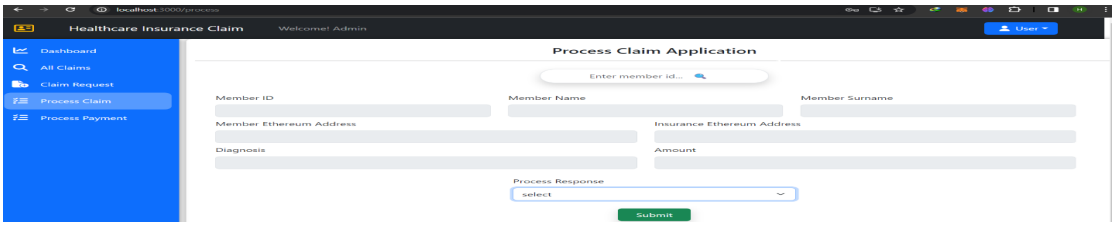

Figure 8: Processing Individual Claim

When a claim with suspicious or irregular details that may indicate fraudulent activity the system detects and flags the claim for further investigation by administrators or designated authorities and displays it alongside other flagged claims this is shown in Figure 9 below

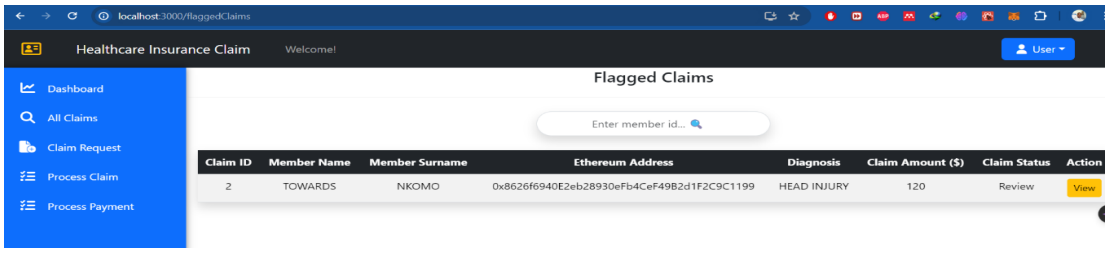

Figure 9: Flagged Claims

Figure 10 below simulated viewing a flagged claim with suspicious or irregular details that may indicate fraudulent activity. The system generates a report of the claim and displays a reason why it was flagged for further investigation by administrators or designated authorities.

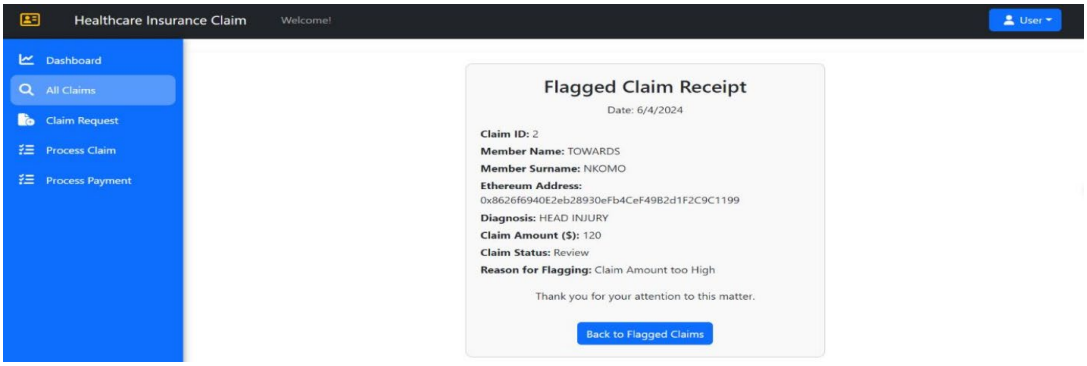

Figure 10: View Flagged Claim Report

Blockchain Claim Application Snippet

Figure 11 simulates the addClaim function which is pivotal in the smart contract, managing the addition of new claims. It requires various parameters detailing the patient, practitioner, diagnosis, insurance policy, and claim amount. These parameters undergo rigorous checks to ensure the validity of the claims.

```
function addClaim(    ⛽ undefined gas
    User memory patient,
    string memory _practitionerName,
    string memory _diagnosis,
    string memory _policyName,
    address _policyEthAddress,
    uint256 _amount
) public onlyPatient {
    require(insuranceProvider[_policyEthAddress], "Insurance provider not registered");

    // Check if the amount exceeds the max claim amount
    require(_amount <= maxClaimAmount, "Claim amount exceeds the maximum allowed amount");

    // Check the number of claims the patient has made this month
    require(patientClaimCount[patient.ethAddress] < maxClaimsPerMonth, "Patient has exceeded the maximum number of c

    Practitioner memory practitioner = Practitioner(_practitionerName, _diagnosis);
    patient.policyNumber = allPatients[_policyEthAddress].policyNumber; // Assign policy number to patient

    // Create a new claim
    Claim memory newClaim = Claim(patient, practitioner, _policyName, _policyEthAddress, ClaimStatus.Submitted, _amo
```

Figure 11: Blockchain Claim Application Snippet

6. Proposed Improvements

Future improvements for the blockchain based fraud detection system could involve seamless integration with Electronic Health Records (EHR) and the development of a mobile application. By integrating with EHR systems, the fraud detection system can access comprehensive patient data, enabling more accurate fraud detection and

prevention. Additionally, the development of a mobile app can enhance user accessibility and convenience, allowing stakeholders to monitor and interact with the system on the go. Future enhancements may also include advanced machine learning algorithms for predictive fraud detection, real-time monitoring features, and enhanced security measures to safeguard sensitive healthcare data. Furthermore, continuous updates and refinements based on user feedback and emerging technologies can ensure the system remains at the forefront of fraud detection in healthcare insurance.

7. Conclusion

In conclusion, the automated fraud detection system utilizing blockchain technology offers a proactive solution for combating healthcare fraud in insurance claims. By harnessing blockchain's security and transparency, the system enhances the accuracy of fraud detection in healthcare insurance claims. Integration with Ethereum's blockchain platform and smart contracts ensures transaction integrity and reduces the risk of alterations. The decentralized nature of blockchain streamlines claims processing by eliminating intermediaries and reducing administrative costs. The strategy strives to protect the interests of patients in healthcare insurance, while also reducing financial losses through extensive testing and validation. Subsequent editions will focus on improving functionality and optimizing algorithms to combat evolving deceitful methods in the healthcare sector.

References

Ali, D. (2019). Blockchain for Insurance and Claims Fraud Detection.

Amponsah, A. A., Adekoya, A. F., & Weyori, B. A. (2022). A novel fraud detection and prevention method for healthcare claim processing using machine learning and blockchain technology. Decision Analytics Journal, 4. https://doi.org/10.1016/j.dajour.2022.100122

Baimyrzaeva, M. (n.d.). Institute of Public Policy and Administration Beginners' Guide for Applied Research Process: What Is It, and Why and How to Do It?

Carstensen, A. K., & Bernhard, J. (2019). Design science research–a powerful tool for improving methods in engineering education research. European Journal of Engineering Education, 44(1–2), 85–102. https://doi.org/10.1080/03043797.2018.1498459

Dias, J. S. (n.d.). Analysis of Design Science Research Methodology and Entrepreneurship Connections Summary of dissertation for the degree of Master in Information Systems and Computer Engineering.

Dzhurov, Y., Krasteva, I., & Ilieva, S. (2009). Personal Extreme ProgrammingAn Agile Process for Autonomous Developers

Herland, M. A. (2019). BIG DATA ANALYTICS AND ENGINEERING FOR MEDICARE FRAUD DETECTION.

Ismail, L., & Zeadally, S. (2019). Healthcare Insurance Frauds: Taxonomy and Blockchain-based Detection Framework (Block-HI).

Iyawa, G. E. (2020). Personal Extreme Programming: Exploring Developers' Adoption Completed Research. http://shura.shu.ac.uk/27536/

Kaafarani, R., Ismail, L., & Zahwe, O. (2023). An Adaptive Decision-Making Approach for Better Selection of Block-chain Platform for Health Insurance Frauds Detection with Smart Contracts: Development and Performance Evaluation. Procedia Computer Science, 220, 470–477. https://doi.org/10.1016/j.procs.2023.03.060

Kapadiya, K., Patel, U., Gupta, R., Alshehri, M. D., Tanwar, S., Sharma, G., & Bokoro, P. N. (2022). Block-chain and AI-Empowered Healthcare Insurance Fraud Detection: An Analysis, Architecture, and Future Prospects. IEEE Access, 10, 79606–79627. https://doi.org/10.1109/ACCESS.2022.3194569

Kapri, P., & Venkatesh, B. (2023). Usage of Block-chain Technology for Tamper-Proof Audit and Managing Insurance Process. https://doi.org/10.13140/RG.2.2.12389.17122

Mackey, T. K., Miyachi, K., Fung, D., Qian, S., & Short, J. (2020). Combating health care fraud and abuse: Conceptualization and prototyping study of a block-chain antifraud framework. Journal of Medical Internet Research, 22(9). https://doi.org/10.2196/18623

Mudassar, S., & Khan, A. (2023). RAD Model Used in Software Development Reference: Software Requirements Engineering Second Step: Data Modeling.

Ncube, N., Mutunhu, B., & Sibanda, K. (2022). Land Registry Using a Distributed Ledger. *IST-Africa Conference (IST-Africa)*, Ireland, https://ieeexplore.ieee.org/document/9845584,pp.1-7, doi:10.23919/ISTAfrica56635.2022.9845584

Paresh Gohil, Dr. Sheshang Degadwala, & Dhairya Vyas. (2022). Fraud Detection in Medical Insurance Claim System using Machine Learning : A Review. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 417–427. https://doi.org/10.32628/cseit228664

Saldamli, G. (2020). 2020 Seventh International Conference on Software Defined Systems (SDS) : Paris, France. April 20-23, 2020.

vom Brocke, J., Hevner, A., & Maedche, A. (2020). Introduction to Design Science Research (pp. 1–13). https://doi.org/10.1007/978-3-030-46781-4_1