Clamora – Blockchain-Based Health Insurance Claim Management System

[1] *Rakesh B*,[1] *Rajesh Kumar A*, [1*] Rajashree S,[2]Santhanakrishnan R, [1]Jemshia Miriam ,[3]Srinivasan R

[1] *Sathyabama Institute of Science and Technology, Chennai, India;*
[2]*Amity University,Bangalore,India*
[3]*Galgotias University, Greater Noida,India*
Email: Writetorakeshb@gmail.com, Rajeshcreation75@gmail.com
** Correspondence: rajashree.cse@sathyabama.ac.in.*
sanskrish@gmail.com
jemshia.cse@sathyabama.ac.in

Abstract:Manual claims approval cycles are typically involved in the processing of health insurance claims, as well as delayed approvals, data tampering and poor visibility for both patient, hospital and insurer during the claims cycle. Clamora is a decentralized application utilizing blockchain technology and InterPlanetary File System (IPFS) to automate and secure each step of the claim process from submission through payment. Centralized database vulnerabilities have been eliminated by replacing them with an immutable distributed ledger, which also eliminates the opportunity for unauthorized alteration or duplicate claim submissions. Hospitals upload documents that are then encrypted and stored on IPFS, however only their content hash is recorded on the blockchain to ensure the content of the documents remains private but can be verified at any time. Rule based validations are executed through smart contracts written in solidity, and automatically update the status of the claim in real-time, thereby removing all need for manual processing. Patient authentication occurs via MetaMask wallet to eliminate risk associated with user/password-based systems. Testing has shown to improve transparency, minimize fraudulent activity, reduce the amount of time required to process a claim and simplify auditing processes. Clamora represents a scalable and private model that can be utilized to transform many aspects of the way insurance operates within a variety of healthcare ecosystems.

Keywords -- Blockchain, decentralized application, IPFS, smart contract, insurance claims.

I. INTRODUCTION

Claims processing is often one of the most labor-intensive aspects of health insurance; this process has many inefficiencies due to the use of several middlemen, time consuming verification of patient records by hand, and central repositories that can be easily compromised through hacking, unauthorized access or manipulation of data. This combination of inefficiency creates extended claims cycle times, conflicts between parties involved in claims processing, and also a lack of responsibility in the claims decision-making process. Ultimately, these inefficiencies cause patients to wait for their payments to be processed, create administrative burdens for hospitals and cause insurance companies to expend additional resources on detecting fraudulent activity and audits.
There currently isn't a comprehensive, integrated digital system that will provide transparent, authentic and traceable medical records. In today's health care environment, multiple versions of the same document are usually being distributed, which causes discrepancies when trying to verify information. Fraudulent claims (inflated bills, fake prescriptions, duplicate claims) continue to grow and cost the health insurer's large sums of money, and cause a loss of confidence in the entire health care delivery network. And because health care data is in silos at individual institutions, it makes collaboration between hospitals and insurance companies extremely difficult, and also complicates the process of verifying information across entities.

Traditional systems are being used to support emerging technologies; however, they are built using centralized servers that have potential for unauthorized changes made to the system as a whole or to individual data records (thus, lack of assurance). Existing data infrastructure is also vulnerable to tampering, enabling alteration of documents post-claim submission, and therefore leaves no reliable audit trail. As such, there is an opportunity to develop a robust and tamper-resistant method that preserves the authenticity of documents, while providing unimpeachable evidence of claim related actions. Additionally, examining documents manually results in a high degree of subjectivity regarding decision making, an excessive administrative burden, and prolonged timeframes for processing claims, each of which has negative impacts on both the patient experience and the operational efficiency of the insurer.

The use of Blockchain as a means to address the above long-standing challenges is largely attributed to it's decentralized, immutable, and cryptographically assured attributes. rather than relying on trusted third parties to

R. Vasanth Kumar Mehta et al. (eds.), *Proceedings of the International Conference on Intelligent Systems for a Sustainable Future (ISSF 2026)*, Atlantis Highlights in Intelligent Systems 16,
https://doi.org/10.2991/978-94-6239-693-7_14

verify transactions (as is common with many forms of digital identity), blockchain provides an opportunity to distribute the trust required in such verification mathematically through the creation of an immutable, distributed ledger which records all transactions. Additionally, smart contracts provide the ability to automate workflows such as checking eligibility, validating information, and approving claims in a transparent and autonomous manner. Furthermore, decentralized storage methods, utilizing distributed file systems like IPFS, ensure that private medical documents are stored off-chain, yet the hash of those files remain on-chain to allow for verifiable proof of existence; this hybrid method of storage reduces redundancy and allows for scalable solutions without burdening blockchain memory.

Clamora was created to build a decentralized method for the healthcare industry to efficiently process insurance claims, and provide real time interaction with all the parties involved in the processing of the claim that is both verifiable and secure. The decentralized method will allow hospitals to authenticate via blockchain wallet as opposed to password, which will help to minimize impersonation fraud. Once a hospital has authenticated it will be able to securely submit medical records and discharge summaries to IPFS (Interplanetary File System) to ensure that once submitted there can be no alteration made to the data. The smart contract within the platform will enforce claim processing rules to prevent duplicate claims, unauthorized claims, or post-submission changes to previously submitted claims. Each transaction entered into the blockchain will create a recordable audit trail, providing significantly improved transparency and trust.

Clamora's distributed methodology automates and fraud-proof's the traditional approval process to create a decentralized and efficient fraud-proof system for making and verifying claims for insurance companies. With respect to latency, it is reduced as there are no longer any manual verifications that can create bottlenecks in the process of making claims for insurance. With respect to traceability, Clamora provides the ability to follow events in the claim processing and settlement process through its use of immutable event logs. Additionally, Clamora uses cryptographic hashing and decentralized identity to ensure the integrity of the data involved in the claim processing and settlement process. Therefore, with respect to addressing the shortcomings of current claim processing systems; providing scalability; and ensuring reliability in the context of real-world healthcare environments, Clamora offers a highly scalable, reliable method for making and settling claims on behalf of insurance companies.

II. LITERATURE SURVEY

Due to the blockchain's decentralization as well as its immutability features, blockchain technology has attracted significant attention in the health care field. Studies conducted previously have shown that distributed ledgers can preserve the integrity of the health care information it is storing, through the prevention of unauthorized modifications and the ability to track each modification to allow for auditing purposes[1]. In addition, the literature states that centralized databases provide a higher risk of data breach, identify theft, and the possibility of manipulating or altering patient records. These issues create the need for greater trust when relying upon centralized systems to manage claim processing and increases the risk of fraudulent claims being submitted. As a result, blockchain technology will enable the creation of an immutable ledger to store all actions associated with the health care data allowing for secure and transparent management of this highly sensitive data.

The scalability problems of keeping complete medical records on the blockchain lead to the use of off-chain, distributed, decentralized storages (IPFS) for medical documents[2]. Research shows that having only a file's hash on the blockchain, while the file itself is stored in a decentralized storage system preserves confidentiality, and significantly reduces the processing load of the blockchain. The "hybrid" approach has been suggested as a viable way to overcome the blockchain storage limitation problem while still enabling users to verify that they linked the submitted files with the stored metadata. Most research studies are focused on the secure archiving of electronic health information rather than developing automated or rule-based claim verification processes[3].

The fraud prevention continues to be an ongoing theme in the literature[4]. The researchers have indicated that current centralized verification systems are not sufficient for detecting duplicate claims submissions, exaggerated medical bills, and forged treatment records. The use of blockchain technology provides a digital paper trail for all aspects of a claim's life cycle, from submission through to claim settlement[5]. While many of the previous research studies focused on conceptual models and/or higher level security frameworks, this study will implement

an end-to-end business workflow that will include the necessary components such as, authentication, document verification, data storage, and claim settlement.

Research also emphasizes the necessity of authenticating stakeholders (and preventing unauthorized claims or alterations) through various methods including role-based access models using blockchain identity frameworks[6]. Wallet-based cryptography based authentication is used as a method of eliminating the use of insecure password-based authentication methods. Prior research has shown the potential for decentralized identity management but there are limited numbers of implementations where authentication is integrated directly into the interaction between hospitals, insurance companies and patients. Additionally, many previous implementations have not provided real time synchronized claim status updates.

There is also an identified gap in the real world use of blockchain as most blockchain applications have only been proposed as methods to provide auditing and decentralized data storage capabilities[7]. Most existing solutions have only demonstrated proof of concept, or are limited to providing isolated services. Most do not address the entire claim lifecycle, nor are there any that provide contract based automation to enforce business logic on their own, which leaves room for systems that can provide fraud resistant, auditable, and privacy aware claim processing[8].

Blockchain technology and IPFS collectively provide an encouraging framework to facilitate the safe and efficient processing of claims from insurance companies[9]. A number of voids exist currently however with regard to unifying the following areas into one system architecture: authentication; decentralized storage of documents; automatic execution of smart contract logic; and real-time tracing. Clamora addresses the current voids by incorporating the elements of wallet-based authentication, tracking claim status via immutable hash values, using IPFS to create hash values for documents, and executing the logic of smart contracts automatically to develop a completely decentralized, fraud resistant solution specific to the needs of insurance companies[10].

III. PROPOSED METHODOLOGY

The proposed clamora system is based on a system to automate the claims process for insurance utilizing a transparent, immutable, and accessible at all times decentralized architecture. it has five (5) main elements: user authentication; submitting documents; decentralized storage; smart contract processing; and tracking claim status. each component of the workflow was designed so as to remove any possibility of manual interaction or unauthorized alteration of data. this method will follow a linear sequence of actions taken by stakeholders in order to create a permanent and non-reversible record of every transaction made with respect to the blockchain.

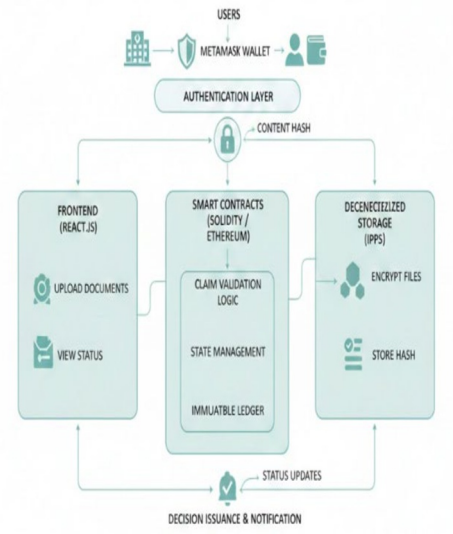
Authentication is the first step in this process; Hospitals, Patients, Insurance Providers etc., use blockchain wallet based identities instead of using traditional usernames and passwords to access the system. As a result, decentralized identity authentication eliminates the risks associated with impersonation and password breaches. Following authentication, the hospital will add medical documentation, discharge summaries and billing information to the system. The medical documentation, discharge summaries and billing information will be uploaded to an off-chain secure environment via the Interplanetary File System (IPFS). IPFS produces a unique, cryptographic hash for each document that is stored within its environment. Those hashes will then reference those documents through the blockchain, which will maintain the security and privacy of the information while allowing for scalability in terms of data storage.

Following the submission of the document(s), the system will invoke smart contracts to automatically authenticate the submitted documents. The smart contracts are deployed on the Ethereum blockchain and include all the necessary commercial rules for validating each claim. These rules include whether a claimant meets the requirements to be eligible, if the document(s) submitted have been verified as true, and if there has been an attempt to submit another identical claim; they also confirm the authenticity of each document submitted. In addition, since the submitted claim(s) are issued with a unique identifier which is tied to the corresponding IPFS hash, it prevents resubmission or tampering with the submitted documents. Due to the fact that the authentication process is contained in the smart contract itself, no party has the ability to alter or circumvent the predetermined rules contained within the smart contract, therefore creating deterministic and non-bias based claim evaluations.

After verifying the claim data, the smart contract will update the claim's status from "pending" to "approved" or "rejected" according to the rules that were configured prior to creating the smart contract. In addition, since all transitions (status updates) are immutable and logged in the blockchain, there can be no dispute about how claims have been resolved. As an additional benefit of this decentralized process, all parties involved have real time access to information in the system, which enables the insurer to immediately view all new claim submissions and

the patient to continuously track their claim status, both without the need to rely on third party intermediaries. Additionally, since all events in the claim life cycle are recorded as a block chain event, it becomes easy and fast to retrieve and audit the history of claims.

The proposed methodology, through decentralized authentication, hybrid storage, smart contract automation and permanent status monitoring, presents a comprehensive solution to current centralized claim management systems. Clamora eliminates manual bottlenecks that exist as barriers to verification; it reduces fraud by eliminating unauthorized access to the data; and it increases operational efficiency by automating adherence to policies. By providing a scalable architecture via on-chain tracking, while maintaining patient's privacy with off-chain storage, Clamora is well-suited for use in real world health care environments where reliability and security are paramount.



IV. Results and Discussion

Testing of Clamora demonstrated that it is practical to implement an entire claims processing life-cycle through a decentralized (secure), tamper-proof environment, utilizing automation. Hospitals tested uploading actual claim files (prescriptions, invoices, discharge summaries) into the system, which were stored in a secure manner using IPFS; the hash for each file was recorded to the blockchain. Therefore, the data can be verified while maintaining patient confidentiality (no raw medical information was ever written to the blockchain). The time to upload and hash files was found to be acceptable, having very low latency, and no observed degradation in blockchain execution speed.

The Smart Contract was used to execute each transaction within the decision-making workflow process. A Deterministic Validations Process was automatically invoked from all claim submissions. The validations were automatic, which allowed for determination of whether documents were complete, unique and authentic. Once validated, the Smart Contract would cross check submitted claims against existing IPFS Hashes on the Blockchain. As a result, there was no way a fraudulent or previously processed claim could be resubmitted. All validation results were displayed in real-time on the Frontend so that patients and insurance companies could see in real-time the status of claims without any need for third party assistance. Due to the automated nature of Smart Contract Decision Making, this greatly minimized delays associated with the Manual Evaluation Process.

A hybrid storage model showed substantial scalability benefits. Since Clamora retained full documents off-chain but stored only the IPFS hash of the document on-chain, it significantly decreased the amount of blockchain memory used per transaction. Thus, Clamora allowed for a low cost of deployment and high-speed execution while providing verification of document integrity. IPFS retrieval time remained consistent as it enabled rapid access to files that were referenced without requiring centralized data repositories. Overall, this demonstrates that

decentralized storage can be effectively implemented within a real-world process for processing large medical files and highly sensitive patient information for healthcare claims.

In terms of security, the system was able to show high levels of resistance against unauthorized access, as well as tampering. The immutable nature of the blockchain records created an environment where claims cannot be altered from submission through the end of their record, while the use of IPFS ensured that all documentation uploaded to the network would remain un-alterable after creation. Additionally, wallet based authentication removed two of the biggest security risks that come from user account compromise (passwords), and identity spoofing. Each time a user interacts with the system, it creates a permanent record of that interaction in the form of an event log, creating a permanent audit trail that is unchangeable. This gives the system an ability to maintain a level of traceability that no traditional system can provide, giving organizations in this industry significant advantages when dealing with regulatory compliance, as well as the need for forensic investigations into cases of suspected fraud.

The total results show that Clamora presents an entirely new level of transparency, lower levels of latency, and higher degrees of operational performance compared to central processing systems for claims. In contrast to the subjective nature of a centralized system where claims are evaluated by a person; the Clamora claims were processed based upon pre-defined rules. Therefore, the claims processing system produced a fairer and more predictable result. Additionally, eliminating intermediaries decreased administrative burdens for users, and the real time status interface provided users with a better experience. Although the demonstration took place on test networks, the Clamora architecture is completely scalable and may also be implemented on Layer-2 blockchain platforms to decrease the cost of transactions in large volume insurance environments.

Smart contract integration, use of decentralized identity (Decentralized Identity), and use of Filecoin-based IPFS file verification were found to create an innovative method for solving the problems of insurance claim processing. This method transforms traditional medical claim workflow to fully automated, completely transparent, and fraud-proof digital pipeline. Results demonstrate that Clamora aligns itself with the expected specifications for the next generation of health care systems that are interoperable, therefore has potential for greater adoption as part of public and private insurance infrastructure.

V CONCLUSION AND FUTURE WORK

Clamora has demonstrated it is feasible to perform decentralized, tamper-proof and transparent claims processing for health insurance using blockchain and IPFS technologies. The method shows that it is possible to avoid the common delay in claim payments due to reliance on centralized server systems and/or third parties and the need for manual claims verification. In this way, by implementing wallet-based authentication, smart contracts and a decentralized file storage system, the entire claim lifecycle can be traced, immutable and verifiable. As such, the results show that Clamora provides a viable method for reducing administrative burden in relation to claims processing; improving the accuracy and reliability of decision making regarding approvals or denials; and reducing fraudulent claims through the implementation of automated validation mechanisms.

A hybrid storage solution was created with Clamora to ensure that the confidential medical information is securely stored in IPFS (InterPlanetary File System) and that its integrity is being verified through cryptographic hash verification stored on chain, but the two are separate which will allow for scalability and confidentiality and auditing capabilities. Deterministic smart contract rules for claim eligibility and approvals have been built into the system which creates a fair, and un-biased environment for claimants by limiting human error. Also real time updates of claim status will be available at all times for all parties involved so everyone can see where the process stands.

By employing the principles of blockchain technology in the design of its solution, Clamora has effectively addressed the primary issues of delays, lack of transparency and/or accountability, risk of alteration/data tampering, and variability in claims decision-making that exist within the typical workflow of health insurance claims processing. As well, Clamora's use of an immutable audit log allows for the regulatory compliance required to support claims processing and provides a reliable source of evidence when disputes arise. Likewise, Clamora's implementation of decentralized identity verification eliminates the security risks inherent in password based systems and protects against impersonation attacks. As such, Clamora offers a viable and scalable replacement to current, centralized methods of claims processing and maintaining the integrity of documents in environments requiring safe, secure and accurate claims processing and document integrity.
Further research in the area of future development may include incorporating advanced fraud analytic techniques into Clamora. Machine learning algorithms will be able to identify anomalies in the way claims are submitted that

would not have been identified using a rules based validation system alone. By adding predictive behavioral models to machine learning algorithms it is possible to further enhance the ability to identify fraudulent behavior as soon as possible. Combining Clamora with government or nation wide medical databases would also add an additional layer of interoperability and facilitate inter-institutional verification of medical information thereby allowing the use of this system to be extended to a wider audience of hospitals, insurance companies, and regulatory agencies.

A further area of potential scalability improvement is through deploying Clamora on Layer-2 blockchain networks (e.g., Polygon, Arbitrum and Optimism). Layer-2 networks provide lower cost per transaction and improved throughput compared with Layer-1 networks; this makes Layer-2 networks an ideal platform for facilitating high volume real time claim processing. Future developments in Clamora may also include using tokens to settle claims, automating low-value micro-claims or allowing for decentralized pooling of claims across different health care schemes. Further development in each of these areas could allow Clamora to evolve from a successful decentralized platform, into a fully intelligent, fully interoperable, and industry-grade insurance ecosystem.

References

[1] F. Ahmed, M. Khan, and S. Hussain, "A Privacy-Aware Smart Contract Model for Health Insurance Claims," *Journal of Biomedical Informatics*, vol. 138, pp. 104256, 2023.

[2] A. Bose, S. Tripathi, and N. Verma, "HealthChain: Blockchain-Based Audit Trails for Medical Records," *Health and Technology*, vol. 13, no. 2, pp. 145–158, 2023.

[3] P. Singh and J. Thomas, "Decentralized Medical Record System using IPFS and Blockchain," *Journal of Systems and Software*, vol. 196, pp. 111267, 2023.

[4] Y. Liu, X. Wang, and T. Zhang, "Blockchain-Enabled Secure Sharing of Health Data," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 432–440, 2023.

[5] R. Pati and A. Sen, "Smart Health Insurance Claim Processing using Ethereum," in *Proc. IEEE Int. Conf. on Blockchain and Data Science*, 2024, pp. 102–108.

[6] M. Ramezani, M. Hossain, and M. Tavakkoli, "Smart contract-based health insurance automation," *Computers in Biology and Medicine*, vol. 154, pp. 106273, 2023.

[7] K. Sharma and R. Kapoor, "DApp for Real-Time Insurance Payouts Using Solidity," *Lecture Notes in Computer Science*, vol. 14120, pp. 312–324, 2022.

[8] L. Zhao, W. Huang, and D. Lin, "Secure Medical Data Storage and Retrieval using Blockchain and IPFS," *Future Generation Computer Systems*, vol. 147, pp. 693–704, 2024.

[9] Z. Zhang, B. Liu, and F. Chen, "Role-Based Access Control for eHealth Systems using Smart Contracts," *IEEE Access*, vol. 11, pp. 30401–30412, 2023.

[10] R. Gupta and A. Mehta, "Decentralized Insurance Claim Settlement using Blockchain and Smart Contracts," *IJCA*, vol. 183, no. 17, pp. 24–29, 2022.