Impact Factor (SJIF): 6.126 E-ISSN: 2583-1615

International Journal of Research in Academic World

Received: 12/March/2025 IJRAW: 2025; 4(4):158-162 Accepted: 18/April/2025

Blockchain Enabled Health Care Management and Transparency System

[1]B Ramadasu, [2]P Adhitya Ram and [*3]R Manocharith

[1]Assistant Professor, Department of CSE, CBIT, Osmania University, Hyderabad, Telangana, India.

[2, *3]Department of CSE, CBIT, Osmania University, Hyderabad, Telangana, India.

Abstract

It is problematic at its core because it lacks transparency and leads to inefficient use, susceptibility to fraud, and inefficient application. A leading problem is inefficiency due to manual processes, lack of tracking systems, and unauthorized access to sensitive information. We thus propose an effort to device a blockchain-based framework specifically customized for efficient health-care fund management. This system utilizes core blockchain features like immutability, consensus mechanisms, and encrypts the use of healthcare funds in a manner that is secure and transparent. Through decentralization, records of the fund allocation and the accounting through smart contracts, it reduces human intervention, thus accelerating processing and prevention of misappropriation. Access and tampering with it can only be done by the authorized because citizen requests are verified against predefined eligibility rules. The blockchain will maintain records of all transactional funds allocation in such a way that it is immutable and unchangeable regarding any form of tampering. The same permissioned blockchain facilitates secure interaction between government organisations and healthcare companies; off-chain storage results in better efficiency because most of the data management is done off-chain, which is less critical. This focused approach will give confidence to the stakeholders and present an efficient cost-effective method the same system offering safe funds for health care tracking. The proposed system is a model for leveraging the latest technologies to overcome administrative challenges in public health care systems.

Keywords: Blockchain, Smart contracts, Ganache etc.

1. Introduction

One age-old problem with which traditional centralized systems seem to cope is inefficiencies in governance funding of healthcare. There is a propensity to bureaucratic delays, and the fund disbursal process does not have proper mechanisms of control or auditing. Thus, it is an issue of fraudulence, misallocation, and delays in administration. This project will thus focus on overcoming these challenges using blockchain technology, which represents a decentralized, transparent, and immutable ledger system. Blockchain increases the accountability through secure data handling and discouraging unauthorized access. We make use of a permissioned blockchain platform-a combination of cryptographic security and smart contracts-to automate the allocation of funds and keep track of transactions and all those transactions will be immutable. Our system is health-care-specific, enabling citizens, health-care institutions, as well as government agencies, to transparently control their funds. To make our system scalable and performance-friendly, off-chain storage for non-critical data would be integrated into our system. This proposed solution, therefore, increases trust and reduces fraud; with its increasing efficiency in the dispersal of funds, it serves as a model for application of blockchain technology in a public healthcare system.

2. Preliminaries

i). **Blockchain Technology:** It is a decentralized, immutable ledger that would ensure record-keeping happened in a secure manner and transparently. In the sense of being agreed upon by nodes that validate transactions, it is an accepted system and considered so on account of some consensus mechanism of validation that might be a Proof of Work (PoW) or Practical Byzantine Fault Tolerance (PBFT). Interestingly, it will be a permissioned blockchain used in the system proposed here: permission only to authorized users or, alternatively, privacy besides scalability.

ii). **Smart Contracts:** The smart contracts are self-executing programs that are stored within a blockchain to automatically enforce rules. It would then avoid human intervention associated with verification for eligibility of people and disbursal of funds-all which have been needed to follow the government policies.

iii). **Cryptographic Techniques:** It utilizes cryptographic algorithms in order to make data integrity and security assured.

SHA-256 Hashes secret data. Thus, the chain will retain an immutable and integral record.

***Corresponding Author:** R Manocharith

Such data would include user documents and personal information. AES-256 is given with usage of encrypting the data off the chain. Data is safe so well considering data privacy.

iv). **Permissioned Blockchain Framework:** The solution applies a permissioned blockchain. Its features include modularity, support for private transactions; therefore it has been chosen for this solution, hence it provides a secure role-based environment set up to work with the sensitive health care fund data.

v). **Off-chain data management:** The mechanism would actually cache all of the big, noncritical data-most notably the user information or scans of documents-off-chain in a secure database and maintain its integrity on-chain through content-addressable hashes.

3. Literature Survey

i). **Blockchain for Transparent Healthcare Fund Allocation (2022):** This paper discusses how blockchain can be applied towards the purpose of illuminating the healthcare fund allocation process. It demonstrates a system wherein smart contracts allow one to verify-and consequently disburse-funds in order to allow only the appropriate recipients to access those funds. In this instance, it displays how blockchain, based on the Ethereum platform-can be used with its characteristics of immutability and automation to deny unauthorized access and administrative inefficiency. There was more transparency and fewer fraud levels; the system had numerous disadvantages and involved big computational costs and integration problems with the old system of health care.

ii). **Decentralized Ledger System for the Disbursal of Grants to Hospitals (2021):** This paper gives a decentralized ledger system that is secure yet transparent to the hospital regarding grants using the multi-signature protocols in combination with ECDSA. This way, without approvals from multiple authorized individuals that must be allowed to be in control of the funds, dispersals of the fund cannot happen. This also reduces fraud while increasing accountability since only valid recipients are allowed to receive their money. There has been a time lag in funding distribution in the study, contrary to the one using multi-signature processes and coordination costs amongst stakeholders.

iii). **Blockchain-based Hospital Fund Management System (2021):** This study uses blockchain-based security in allocating and tracking money within a hospital; this study made use of the Ethereum blockchain, applied Merkle Tree hashing to preserve integrity in transactions, thus ensuring management of hospital funds through the management of immutable records of every single transaction performed as a form of safe storage for the distribution of the hospital's funds. Although these were advantages, the research pointed out high transaction fees on the Ethereum network and mostly public availability of data about funds as significant drawbacks.

iv). **Consortium Blockchain for Transparent Hospital Subsidy Management (2022):** This paper presents a consortium blockchain framework for governance, aiming to increase the level of transparency and accountability in hospital subsidies. The system supports a multi-layered mechanism to access fund-related data by accredited participants only. Using a consortium blockchain, the paper aims to overcome the problems of fraud avoidance and building trust among the stakeholders. The study identifies some major critical negative aspects like high setup and operating costs and that it is not so easy to achieve seamless interoperability with the legacy health care systems.

v). **Biometric-Based Blockchain for Healthcare Fund Distribution (2023):** This present research work derives the possibilities of merging biometric verifications with blockchain technology for a better secured health fund distribution. Here, the work of this research makes biometric data that involves fingerprints and iris scans to be hashed and recorded in the blockchain, which therefore prevents the tampering of identity checking by making it accurate without fraud in distributing funds to the intending people. Although the paper significantly enhances the precision in accuracy and data security, it raises privacy concerns regarding employment of biometric data and compliance challenges about regulatory standards concerning data preservation.

4. Proposed System

The Blockchain-Enabled Healthcare Fund Management System is a secure, transparent, and efficient platform designed to address challenges in managing government healthcare funds. It leverages blockchain's core properties—immutability, decentralization, and cryptographic security—to ensure transparency in fund allocation while protecting sensitive data. Unlike traditional centralized systems, our solution eliminates vulnerabilities such as unauthorized access, delays, and fraud through automated workflows and immutable records. This system uses a permissioned blockchain where, based on access, only health officials and administrators can access the data and manage it securely. Smart contracts are at the core: automation of important processes such as eligibility verification as well as fund disbursement on due and applicable rules shall ensure fairness and compliance with government policies. To optimize performance, the system follows a hybrid storage model: storing critical transaction detail on-chains while non-critical data is allowed off-chains with strong encryption. This system makes great improvements to the efficiency of healthcare fund management by combining the transparency, security, and use of automation.

A) System Architecture

The proposed system is developed to eliminate inefficiencies, lack of transparency, and fraud in healthcare fund management. It makes use of blockchain technology combined with off-chain storage for the best performance, security, and scale.

i). OnChain (Blockchain) Data Management

- **Core Transaction Data:** All records about fund disbursals, changes in application status, and approval logs are maintained on-chain to facilitate traceability and transparency.
- **Smart Contracts:** The policy decisions can be automatically made towards fund allocation and eligibility criteria, thereby achieving government policy compliance.
- **Hash Storage:** Incomes proofs, bills, etc., are hashed into the blockchain so that one can verify integrity without revealing the actual documents.

- **Mechanism of Consensus:** PBFT is utilised to achieve fast, energy-efficient consensus in the permissioned network.

ii). Off-Chain (Database) Data Management

- **User Information:** Off-chain storage of profile information such as names, contact information and metadata of applications lowers the overhead of blockchain
- **Document Storage:** Scanned copies of the documents of the beneficiaries and very detailed descriptions of the scheme are saved in a database off-chain with proper security.
- **Scheme Metadata:** Details about all schemes, budgetary allocations, and eligibility conditions are stored, updated dynamically, and reflected.
- **Encryption:** All the off-chain data will be encrypted with AES-256 algorithms so that it does not get monitored and hacked.

iii). Blockchain Implementation with Frontend

- **User Interfaces:** Citizens, health officers, and administrators will access the system through simple, user-friendly web and mobile interfaces that abstract the blockchain.
- **API Gateway:** Using APIs to connect the frontend properly with the blockchain network and the off-chain database in order to make retrieval and updates smooth.
- **Role-Based Access Control:** Through smart contracts, it determines the limitations of user roles-for example, citizens, healthcare officials, admin

B) Security and Data Privacy Features

i). Biometric Verification for Identity Management

- Biometric details such as fingerprints or face recognition are hashed and stored on-chain for identity validation in an application and distribution process.
- Biometric data is integrated with blockchain-based digital signatures to ensure security through multi-factor authentication.

ii). Chain-Based Data Integrity and Encryption

- Data integrity on-chain uses SHA-256 hashing to guard against tampering or unauthorized changes.
- All off-chain data, including the user's documents, would use AES-256 for encryption and a hash of that would be stored on-chain, thus making the records off-chain and on-chain consistent.

iii). Controlling Access through Smart Contracts

- Tokenized permissions assigned for accessing and modification of data would be implemented using smart contracts
- Only authorized members of the Healthcare Services Department can approve applications and ensure only verified users get access to their application and fund status.

C) Fund Allocation and Workflow Automation

i). Smart Contract-Based Allocation

- **Eligibility Criteria Verification:** The Smart contracts validate applications against pre-defined conditions such as income, hospital bills.
- **Conditional Expenditure:** Expenditure occurs only after all the contract conditions are met; for example, approval from healthcare officials or validated documents.
- **Audit Logs:** Every single expenditure on the blockchain would be recorded immutably; thus traceable

ii). Automated Notifications and Reporting

- Change of Status to the application triggers automatic notifications to citizens.
- The Healthcare Services Department receives detailed reports on the utilization of funds, pending applications, and even approval rates generated from blockchain records.

5. System Architecture

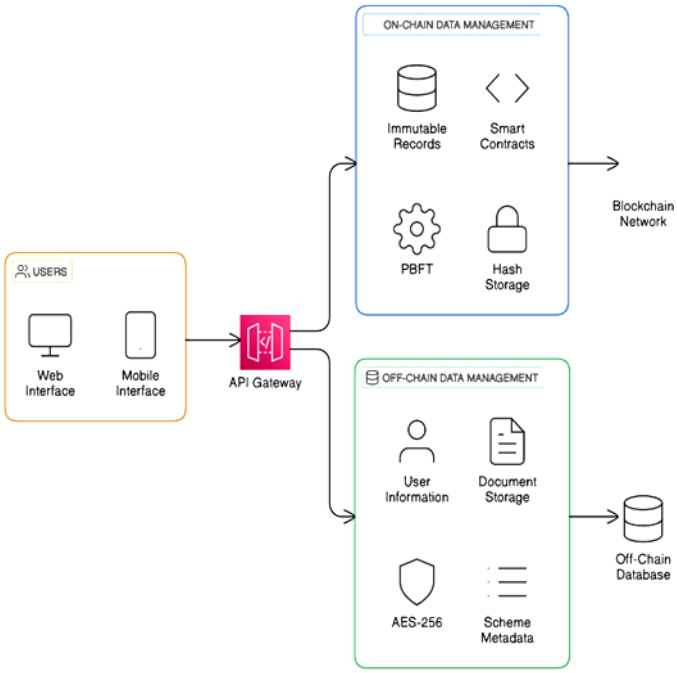

Fig 1: System Architecture

The above figure depicts the architecture of the Blockchain-Enabled Healthcare Fund Management System, which encapsulates the integration of blockchain technology into both off-chain storage and user interfaces. The architecture is a build-up of some of its key modules such as the User Module, the Healthcare Services Department Module, and the Admin Module-all of which interact with a permissioned blockchain for safe, transparent transactions. Non-material information such as fund allocation and the status of an application are immutable on the blockchain, while non-critical information like user details and documents are safely stored in an off-chain database. The Smart Contracts Module automates verification and disbursal of funds together with the imposition of necessary eligibility rules without requiring any manual intervention. Role-based access controls implement sensitive actions in the blockchain only to authorized users such as healthcare officials and administrators. The API layer allows connectivity between the blockchain and database, fronted by natural interfaces of the user's convenience. This architectural construction creates a scalable efficient, and secure system for managing healthcare fund management.

6. Data Flow

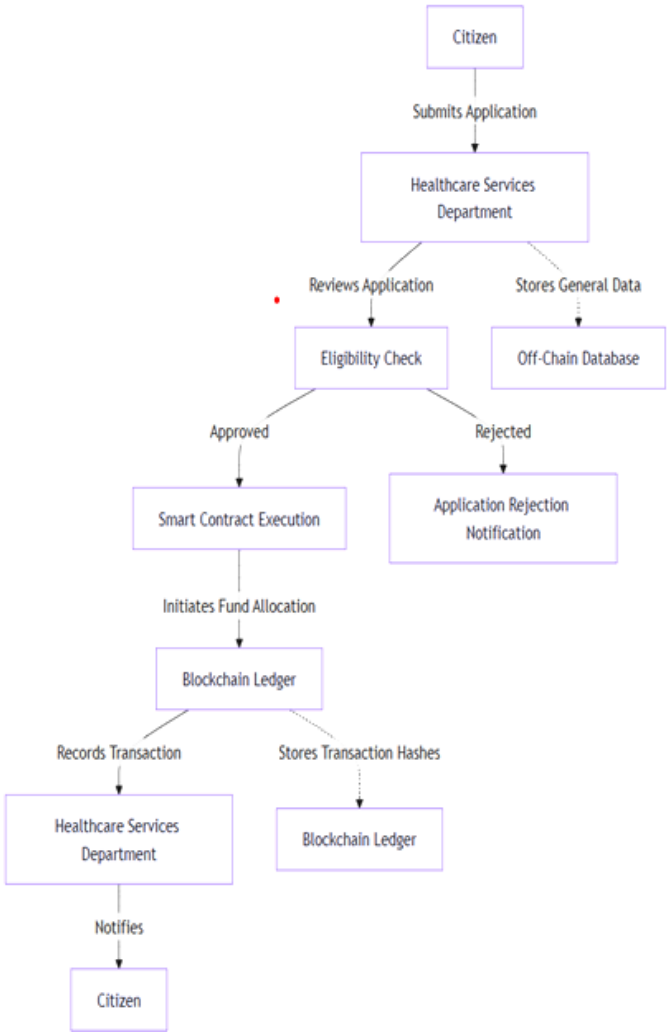

Fig 2: Data Flow

The data flow diagram makes explicit the step-by-step process by which data flows in the system-from a citizen's application-submission that takes place up to disbursement and notification. It captures how different components of the system interact with each other, elaborating on how on-chain and off-chain elements coexist.

i). **User (Citizen):** The application complete with all personal details and supporting documents is submitted to the user module whereby off-chain databases store the application data while the blockchain was applied for recording hashes of documents for integrity.

ii). **Healthcare Services Department:** Where officials concerned in the department access off-chain database for review, application data and documents are authenticated for ascertaining the applicant's eligibility, and he or she approves or rejects it. In this way, his decision would be logged on the blockchain for transparency.

iii). **Smart Contracts:** This simple smart contract only provisionally allocates the funds if the application is approved and first of all, checks all applicable conditions of eligibility defined beforehand, prior to sending money to the applicant's account.

iv). **Blockchain Ledger:** The blockchain does store all application status updates, fund disbursement and approval logs. Thus, it gives a tamper-proof audit trail.

v). **Notification System:** During runtime, status is forwarded to the user that his or her fund is like pending or approved, rejected or disbursed.

vi). **Off-Chain Data:** The method that optimizes blockchain without sacrificing its accessibilities is by storing generic application metadata, scheme information, and noncritical user data in off-chain storages.

7. Hardware and Software Particulars

i). ***Software Requirements:***

- **Frameworks/Libraries:** React
- **Languages:** HTML, CSS, JavaScript
- Django Framework
- **Language:** Python
- Platforms: Ethereum
- **Language:** Solidity
- **Database:** MongoDB
- **Cryptographic Libraries:** OpenSSL

ii). **Hardware Requirements**

- **Developing Machines:** Minimum: Intel Core i3 equivalent dual-core processor, 4 GB RAM, and 128 GB SSD.
  - **Recommended:** Intel Core i5 or equivalent (quad-core, 8 GB RAM, 256 GB SSD).

- **Server Requirements**
  - **Minimum:** Dual-core (Intel or AMD equivalent), 4GB RAM, 256GB SSD, Minimum 1 Gbps Ethernet Quad-core CPU processor based on Intel or AMD, 8 GB RAM, 512 GB SSD.

- **Blockchain Nodes**
  - Intel or AMD equivalent dual-core processor, 4 GB RAM, 256 GB SSD, Ethernet port with at least 1 Gbps.

8. Future Scope

i). **Diversification of Funds to Other Markets:** The system can expand quite easily to include funds for other government services, including education, agriculture, and disaster relief among others.

ii). **IoT Devices:** The hospital system can be interfaced to IoT devices, which allow in real-time the carrying out of data verification with speed and accuracy.

iii). **Advanced Analytics and AI:** AI-based analytics will be integrated to enable anticipation in usage of funds and fraud patterns.

iv). **Cross-Border Collaborative Healthcare:** As if it's not obvious, the system can easily be tailored for application in international healthcare collaborations thus ensuring secure and transparent cross-border transfers of funds.

v). **Citizens Feeding and Involvement:** The system can easily be modified for application in the international healthcare collaborations, ensuring secure and transparent cross-border transfers of funds.

vi). **Citizens Feeding and Involvement:** The interface can be designed to feed citizens who report problems or propose enhancements to create trust in the system and continually enhance it. Utilize ZK-SNARKs for Privacy Improvement Zero-Knowledge Proofs: With zero-knowledge proofs, also referred to as ZK-SNARKs, data could be proven valid without proving that the sensitive data exist.

Conclusion

This system offers great care in regard to the management of the identified critical health fund management issues, such as

inefficiency, lack of transparency, and vulnerability to fraud. It is optimum balance between performance, scalability, and security by using blockchain immutability and automation with off-chain data storage. The solution integrates smart contracts that will enable the automated release in fund allocations as per the set rules, minimizing mistakes likely to occur through manual intervention. Role-based access control and biometric authentication ensure maximum security for authorization of access or modification by only authorized people. Encryption techniques-AES-256 for off-chain data encryption, SHA-256 for on-chain hashing-of sensitive information aimed at confidentiality without losing traceability and trust among stakeholders through this system: it is already capable of solving issues concerning the distributions of allocations of fund support in health merits; it is also one of the bases for constructing government systems which are transparent, efficient, and citizen-oriented.

References

1. Elklit J and Reynolds A. A framework for the systematic study of election quality. Democratization. 2005; 12(2):147-162.
2. Gawade R, Kale A, Mane V & Koli S. Government Fund Allocation and Tracking System Using Blockchain. *International Journal of Multidisciplinary Innovative Research*, 2022, 2(2).
3. Vadher M, Pandey P, Sawant R & Lopes F. "State government fund allocation and transaction system using blockchain technology" *Journal of Emerging Technologies and Innovative Research* 8.6, 2021.
4. Katore R & Choubey S. Government Scheme and Funds Tracker Using Blockchain. *International Journal of Engineering Research & Technology*, 2021, 10(5).
5. Ansari H, Patodia V & Mirza S. Government fund's allocation and tracking system using blockchain technology. *International Journal of Advanced Research in Computer and Communication Engineering*, 2022, 11(3).
6. Jambulkar N & Ratnaparkhi A. Government Fund Distribution and Tracking System Using Blockchain Technology. *Journal of Emerging Technologies and Innovative Research*. 2020; 7(9):1379–1387.
7. Chen Y & Wang Y. A Blockchain-Based Secure Framework for Transparent Health Fund Allocation. IEEE Access. 2021; 9:134571-134583.
8. Mohite A & Acharya A. Blockchain for government fund tracking using Hyperledger. 2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS), 2018, 231-234.
9. Zhang W & Xue Y. Blockchain and Smart Contracts for Government Fund Management. *International Journal of Information Security and Privacy*. 2020; 14(4):48-62.
10. Lee M and Liu F. Blockchain Applications in Public Sector and Government Administration: A Review. *Journal of Public Administration and Governance*. 2021; 11(4):74-92. S.
11. Gupta A & Kumar R. Efficient Health Care Data Management with Blockchain Technology. *Journal of Health Informatics in Developing Countries*. 2022; 16(2):45-58.
12. Peng G, Zhang A & Lin X. Patient-Centric Fine-Grained Access Control for Electronic Medical Record Sharing with Security via Dual-Blockchain. IEEE Transactions on Network Science and Engineering. 2023; 10(6):908-3919.
13. Yu X. Consortium Blockchain for Secure and Efficient EMR Sharing During the COVID-19 Pandemic. IEEE Access. 2022; 8:120945-120954.
14. Amofa K & Boateng A. Smart Contracts for Secure Medical Data Sharing in Healthcare Systems. *Journal of Medical Systems*. 2022; 46(3):120-130.
15. Zhuang Z & Wu F. Patient-Centric Healthcare Data Sharing with Privacy Preservation Using Blockchain Technology. IEEE Transactions on Information Forensics and Security. 2022; 17:3212-3225.
16. Feng L & Wang M. Collaborative authentication protocol for EMR sharing between cloud and users. IEEE Access. 2020; 8:50356-50366.
17. Tan J & Chen L. Fine-Grained Access Control of EMRs with Blockchain-Based Encryption Schemes. ACM Transactions on Privacy and Security. 2021; 24(2):1-23.
18. Liu T & Sun G. Attribute-Based Encryption for Fine-Grained Access Control in EMR Systems on Blockchain. *Journal of Information Security and Applications*. 2022; 64:102999.
19. Sun Y and Zhao H. Efficient EMR Access Control Scheme Using Blockchain and Attribute-Based Encryption. IEEE Access. 2022; 10:23914-23926.
20. Xu Z & Liu J. A Dual-Blockchain Framework for Efficient EMR Sharing with Privacy Protection. Future Generation Computer Systems. 2021; 117:345-356.