Blockchain Technology

Mini Project Report

Title: Medical Records Management System using Blockchain

Group Members: Rushi Bedmutha (BE-A-45)

Sharvay Chandgude (BE-A-46)

Gaurav Aher (BE-A-47)

Abstract

This project focuses on developing a decentralized medical records management system using blockchain technology. The system allows patients to control their medical records, share them securely with healthcare providers, and ensure data integrity and privacy. The application is built using Solidity smart contracts on the Ethereum blockchain, with IPFS as off-chain storage for large files. This report discusses the theoretical background, implementation details, and security features of the system, along with practical applications and future potential improvements.

Introduction

In healthcare, managing patient records efficiently and securely is crucial. Traditional centralized systems are prone to data breaches, lack transparency, and often limit patient control over their data. Blockchain technology, with its decentralized nature, immutability, and transparency, provides an innovative solution for secure medical record management. This project explores the development of a decentralized medical records management application, where patients have complete control over access to their medical information, ensuring privacy and integrity.

System Overview

- **Smart Contracts:** The application uses Solidity to develop smart contracts that manage patient records, including creation, sharing, and access control.

- **Blockchain Platform:** Ethereum is used as the blockchain platform for storing transaction records and access permissions, while IPFS is used for off-chain storage of larger medical files like X-rays and MRIs.

- **Privacy and Security:** Patients have control over who can access their records, and every interaction is recorded on the blockchain to ensure immutability and transparency.

Key Features:

- Decentralized and patient-centric system.

- Data integrity and immutability.

- Secure sharing of medical records.

- Auditable access logs.

Implementation Details

Blockchain Layer (Smart Contracts)

The medical records are managed through a smart contract system where patients, doctors, and healthcare providers interact. The core functionalities are:

- **Registering Patients and Doctors**: The contract administrator (or a trusted entity) registers patients and doctors on the system.

- **Record Management**: Patients can upload new medical records, which are stored off-chain (on IPFS), with the reference (IPFS hash) stored on the blockchain.

- **Permission Management**: Patients control who can access their records by authorizing specific doctors or healthcare providers.

- **Immutable Ledger**: Every interaction (view, update) is logged on the blockchain, providing an auditable record of access.

Off-Chain Storage (IPFS)

Due to the large size of medical files (e.g., MRIs), they are stored off-chain using IPFS. The blockchain stores the hash of the file, ensuring that the data can be verified for integrity without being stored on-chain.

Test Cases and Experimental Setup

Test Case 1: Adding a Medical Record

- Patient: Registers a new medical record (e.g., blood test report) by uploading it to IPFS.

- Blockchain: The IPFS hash is stored on the blockchain.

- Outcome: The record is securely stored off-chain, and the patient can authorize doctors to access it.

Test Case 2: Access Control

- Doctor: Requests access to a patient's medical record.

- Patient: Authorizes the doctor to view the record.

- Outcome: The doctor can view the record, and the access event is logged on the blockchain.

Results and Observations

- **Security:** The use of blockchain ensures that medical records cannot be tampered with, and unauthorized access is prevented through smart contracts.
- **Performance:** While the off-chain storage ensures scalability for large medical files, the interaction with the blockchain introduces some latency, which needs to be optimized for real-time applications.
- **Usability:** Patients can easily manage their records and grant access through a user-friendly web interface integrated with MetaMask for secure blockchain transactions.

Detailed Analysis

1. **Efficiency:**

   The system ensures data integrity and security by utilizing blockchain's immutability. Off-chain storage (e.g., IPFS) is used for large medical files, reducing blockchain bloat. While blockchain ensures high security, transaction speed and costs can be bottlenecks, especially in public networks like Ethereum. Future scalability can be improved by exploring Layer 2 solutions.

2. **Scalability:**

   The use of off-chain storage helps with scalability by storing only the file hashes on the blockchain. However, the system may face limitations with high transaction volumes. Implementing Layer 2 scaling techniques or permissioned blockchains can enhance performance and handle more users efficiently.

3. **Practical Applications:**

   This system is ideal for hospitals, clinics, and telemedicine platforms, offering secure, patient-controlled medical record

management. It aligns with healthcare regulations like HIPAA and GDPR and could be a valuable tool for personal health record (PHR) systems.

Conclusion

The blockchain-based medical records management system offers a secure, decentralized solution that empowers patients with full control over their medical information. This project demonstrates the potential of blockchain technology in healthcare, providing a tamper-proof and transparent system for managing sensitive health data. Future work could focus on integrating the system with existing healthcare platforms and improving the scalability of the system for larger user bases.