Securing Hospital Management Systems: Towards Decentralization and Enhanced Security with Smart Contracts

MSc Research Project

Cybersecurity

Rony Paul

Student ID: X22233717

School of Computing

National College of Ireland

Supervisor: Mark Monaghan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Rony Paul		
Student ID:	x22233717		
Programme:	MSc in Cybersecurity	**Year:**	2023-2024
Module:	Research Project		
Supervisor:	Mark Monaghan		
Submission Due Date:	12/08/2024		
Project Title:	Securing Hospital Management Systems: Towards Decentralization and Enhanced Security with Smart Contracts		
Word Count:	6040	**Page Count:**	22

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Rony Paul
Date: 12/08/2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Securing Hospital Management Systems: Towards Decentralization and Enhanced Security with Smart Contracts

Rony Paul

X2233717

Abstract

This study explores the potential for increasing security and efficiency in hospital management systems (HMS) by integrating blockchain technology and smart contracts. Data breaches and illegal access have traditionally of a centralized HMS can jeopardize patient data and overall system security. This research aims to explore solutions to these problems through the automation features of smart contracts and the decentralized nature of blockchain. A comprehensive literature review was conducted from 2016 to 2024 to identify current weaknesses and existing strategies. Additionally, an electronic health record system was developed using Python, Web3, Flask, Ganache, and MetaMask. Solidity was used to make smart contracts. Decentralized testing significantly increased both safety and performance. Systematic reviews were enabled by Knowledge Discovery (KDD) models in databases so that results driven by robust, data-driven convincing of the concept of HMS can benefit from blockchain technology and smart contracts to provide secure and efficient healthcare services. Additional research and commercialization efforts are recommended to address scalability, performance management, and compliance issues.

1 Introduction

1.1 Introduction

Health management systems are sophisticated administrative systems that are used to control virtually all aspects of a hospital including patient records and staff scheduling to optimize the functionality of the facility. However, there are very crucial concerns that arise with the accuracy and safety of the data that is stored in these systems. It is essential to note that the use of conventional focused HMS puts the established patient information and patients' money and confidence in medical care suppliers at risk with the enhanced risk of exposure to data theft, illegitimate access, and system failures (Saini *et al.*, 2020). In search of answers to these questions, more and more people are beginning to consider the use of decentralized technologies such as blockchain and smart contracts for the enhancement of HMS's security and reliability. Due to the above characteristics of decentralization, non-erasure, simplicity, and no central authority, blockchain innovation is considerably more alluring when contrasted and unified frameworks which are inherently vulnerable (Chang *et al.*, 2020). Blockchain innovation deals with informal communication by making it almost impossible for unauthorized alterations to take place as the information is shared over P2P connections, which eliminates the 'weakest' link.

Smart contracts are self-executing business agreements written in code which adds value to the use of Blockchain in healthcare. Less human error and secure and simple exchanges are two of the benefits of using them to fully automate clinical and regulatory procedures such as patient attestation, billing, and prescription distribution. For the examination of how HMS can profit from the use of blockchain innovation and savvy agreements, this segment researches their application (Chang *et al.*, 2020). This examination will expect to achieve a boundless understanding of how this advancement can alter emergency clinic organizations to perceive existing obstructions, innovative stresses, and real solutions. The final goal is to argue that frameworks of medical services are superior as well as more trustworthy, adopting decentralized action and that delicate clinical data is additionally better secured.

1.2 Background

When it comes to administrative functions, clinical management, and patient records, the healthcare industry has always valued centralized HMS implemented for their operations. Even though doctors and healthcare provider industries have significantly benefited from this technology, major factors are threats of data leakage and system compromise. This has negative effects such as infringement of the patient's right to anonymity, and money loss, productivity reduction due to interruption, among others (Tanwar *et al.*, 2020). New developments in blockchain technology provide an opportunity to overcome these challenges. In blockchain structure, data is scattered on multiple nodes which makes it hard for unauthorized data to be manipulated or hacked most of the time which will minimize the case of a single failure, and the openness and the immutability of this technology can enhance HMS security.

Smart contracts relations of blockchain implemented by HMS. These personalization contracts can help many current healthcare systems to run more efficiently than they are now, as well as to become safer for all the patients who seek help from medical providers. Presently, the applications of blockchain and smart contracts in improving the healthcare system are still under the process of research and development of pilot studies (Chang *et al.*, 2020). Some of the areas that have recorded positive outcomes after the implementation include the security of data, the practical functionality, and improvements in stakeholders' confidence in the system. This examination intends to create this corpus of data for an extensive appraisal of the progressive capability of decentralization and shrewd contacts in HMS. Technological aspects, existing and emerging threats allied with legal frameworks, and real-life situations highlighting how such technologies can make systems safer and more efficient are looked at in this study.

1.3 Research Aim and Objectives

1.3.1 Aim

This study aims to plan and construct a decentralized, auditable, and secure electronic health record (EHR) framework utilizing blockchain innovation.

1.3.2 Objectives

- To create a secure and scalable blockchain framework that facilitates the efficient storage and retrieval of Electronic Health Records (EHRs).
- To develop and deploy smart contracts that automate and secure interactions between healthcare providers and patients within the EHR system.
- To ensure patient data confidentiality, integrity, and availability by leveraging blockchain's inherent security features and encryption techniques.
- To seamlessly integrate the blockchain-based EHR system with existing healthcare IT systems and standards for interoperability and data exchange.
- To assess the effectiveness, efficiency, and user satisfaction of the blockchain-based EHR system through comprehensive testing and user feedback.

1.4 Research Questions

How can healthcare systems best deal with issues like data breaches, patient information confidentiality, and privacy concerns while maximizing the use of decentralization, smart contracts, and blockchain technology to improve security, privacy, and interoperability?

1.4.1 Hypothesis

H0: Patients' personal information will be far more protected with a blockchain-based EHR system than with an older more insecure one.

H1: Smart contracts, when integrated with the blockchain-based EHR system will improve the reliability and precision of healthcare data management and provider-patient interactions.

1.5 Research Rationale

There is an urgent need to improve the safety and effectiveness of HMS, which is why this study is being conducted. Cyberattacks and data breaches in healthcare are all common in modern times, threatening patients’ trust in healthcare professionals and exposing their privacy due to its traditional design. HMS is vulnerable to this threat and Blockchain technology provides a strong answer to these security issues due to its decentralized, immutable, and transparent nature (Arunkumar and Kousalya, 2020). Blockchain makes it extremely difficult, if not impossible, for unauthorized parties to manipulate by dispersing data across the network, thus eliminating potential points of failure, smart contracts are made will integrate can protect and automate more healthcare services, reducing the margin for human error, and assuring the accuracy of the claim.

To keep patients' certainty and assurance consistent with administrative standards, information security in medical services is a critical theme that this study handles. By investigating how blockchain technology and smart contracts can decentralize and secure HMS, this project aims to contribute to the development of more dependable healthcare systems. A definitive objective of this exploration is to show that emergency clinics might build their administration tasks' productivity and reliability while at the same time expanding the security of their patient's information by utilizing this state-of-the-art innovation.

1.6 Research Significance

Improving the security, efficiency, and reliability of the hospital management system (HMS) are the main focus areas of this study, which is also noteworthy if for other reasons a cyberattack the increasing number and severity of attacks on healthcare organizations immediately require strong security measures to protect sensitive patient data. Such weaknesses affect traditional centralized HMSs and pose significant risks to patient privacy and organizational integrity. This study examines the integration of smart contracts and blockchain technology to address these important security challenges. Using blockchain’s decentralized and immutable record-keeping, data breaches and unauthorized access can be significantly reduced (Arunkumar and Kousalya, 2020). This means that patient data remains secure and reliable. The use of smart contracts enables the automation and simplicity of many business and clinical operations, improving efficiency and reducing human error.

By proving the feasibility and practical benefits of implementing blockchain-based solutions in HMS, the results of this study can influence healthcare policy and practice. Healthcare professionals, legislators, and tech developers all greatly benefit from the findings of this study, which can lead to safe and effective solutions. Besides, this study adds to what is already known about blockchain that can applied to healthcare, which should further the development of the future. Healthcare systems around the world can benefit from this research, which emphasizes improving trust and confidence in the transformative potential of this technology.

1.7 Literature Gap

The examination is absent on the genuine use and evaluation of EHR frameworks based on the blockchain, and this study intends to rectify that. Although the theoretical foundations and potential benefits of blockchain technology have received a lot of attention, little to no research has examined the practical operation of these systems. By demonstrating how blockchain-based electronic health record systems function, are secure and are effective, the present study seeks to close the knowledge gap between theory and practice. It will likewise underline the importance of smart contracts in improving healthcare data management.

2 Related Work

2.1 Introduction

The financial sector, food industry, energy sector, Internet of Things, health care, and supply chain management among others are some of the many domains that are finding applicability of this technology as a reliable platform for safe sharing of data. The existing literature on blockchain technology and its fields of application and the present investigation in health care (Khatoon, 2020). Further, this study puts forward several more possibilities for healthcare ecosystem applications that incorporate the concept of blockchain technology for the better handling of data. Surgical operations and actual clinical trials are among the different medical processes that have been created and conducted using the Ethereum blockchain network. The processing and retrieval of a huge volume of medical information is also encompassed in this study. In terms of the smart contract system’s workflow for healthcare management within the scope of this article, the feasibility study formulated in this paper also provides an approximate calculation of the costs associated with the system (Khatoon, 2020). The study focuses on enhancing the quality of the healthcare services being delivered and containing the costs for all the entities involved in the health system.

The concept of Blockchain has numerous scientific fields such as applications based on Blockchain are anticipated to increase at a high rate in the coming years. The exercise of smart contracts, which are concise scripts containing a series of coded instructions, by Blockchain to affect contract performances also raises the number of contract enforcement while eliminating intermediaries (Sharma *et al.*, 2020). This article presents the concept of Blockchain and smart contracts for use in the Internet of Medical Things in the context of the e-healthcare domain. This research investigates the future possibility of IoMT in e-healthcare in the aspect of decentralization and smart contracts, proposes a new architectural facet for IoMT, and introduces the advantages, limitations, and future trends of implementing it (Sharma *et al.*, 2020). However, compared to more traditional designs, the suggested one reveals superior results in terms of the routine benchmarks of networking such as average end-to-end latency, average packet delivery ratio, and average energy efficiency.

2.2 Smart contracts based on blockchain

Cryptocurrencies and blockchain technology have brought Szabo's smart contracts which are computerized protocols that execute and manage digital contracts without the need for an overseeing authority in the recent past. Smart contracts are currently implemented into Ethereum and Hyperledger, which are the mainstream blockchain-based development platforms and smart contracts are proven to have wide use in the digital economy and intelligent industries including financial services, management, health care, and the Internet of Things (Wang *et al.*, 2019). Smart contracts are still under evolution and the issues of security and privacy are still matters that require extensive research. One example is the "The DAO Attack" where in June 2016, over $50 million Ether was transferred to an opponent. As a result, we provide a comprehensive and structured meta-analysis of blockchain smart contracts in this research to motivate future research in this expanding field. We elucidated the advanced working models and channels of blockchain smart contracts and provided a distinct six-tier smart contract analysis framework. Second, there are technological, legal, and research issues brought out in the paper (Wang *et al.*, 2019). Third, these are the following applications that have been recounted commonly. Last but not least, the trends of smart contract development were also discussed. Consequently, the findings of this study shall inform future research.

Reputation systems help users to understand how credible or reliable persons, who offer services or goods on the Internet are. Researchers have attempted to use reputation systems in the past using blockchain. IT terms known as ‘smart contracts’ are mostly designed to manage, perform, or verify the contracting parties’ dialogues or fulfillment (Almasoud *et al.*, 2020). However, based on the systematic literature assessment of this paper, there is no proposed architecture for social reputation systems that is based on blockchain, which permits the flexibility of a smart contract. In other words, there is a need to find out where the research is sparse as part of the systematic literature analysis of 30 papers and collecting data from them. This responds to one of the existing gaps in the literature as the FarMed framework allows for the construction of reliable blockchain-based reputation value exchange between medical providers while also containing the implementation of reputation systems with Ethereum smart contracts (Almasoud *et al.*, 2020). Before moving on to the next projects in this dissertation, it is crucial to summarize the recommended framework.

While most people think of Blockchain Technologies (BT) when they hear about cryptocurrencies, the technology is slowly making its way to other industries that can benefit from decentralized, reliable, and immutable models. Smart contracts are gaining popularity with many applications of blockchain technology. These are computer programs that, when executed on a blockchain, consist of a set of blocks that describe the rules that two or more parties agree to interact with each other. Computer rules facilitate and validate contractual agreements by customers and service providers on misinterpretation of approved policies. Some current uses of blockchain technology, as well as smart contracts -a vulnerable and will be at issue. The paper discusses the potential legal implications of this technology.

2.3 Smart contract-based EHR system

The efficiency and convenience of Internet of Things (IoT) technologies and remote healthcare systems are being further investigated in this study. As the number of IoT devices in healthcare grows exponentially, patient privacy and security become a concern. The authors provide blockchain-based smart contracts for patient and medical device management to store personal device-generated data. In short, the authors developed a remote healthcare system including hospitals, doctors, and patients using an Ethereum-based blockchain (Pham *et al.*, 2018). Sensors monitor patients' health and automatically update the blockchain. Their study also provides a controlled approach to securely and less dependently on patient health data for medical devices. Before publishing sensor data in the blockchain, we filter it. The authors state that they can reduce blockchain size and save money for more efficient services. Abnormal sensor data will be instantly uploaded to the blockchain and trigger emergency calls to doctors and hospitals for timely treatment (Pham *et al.*, 2018). The study tested the smart contract in Ethereum's TESTRPC test environment and used it in real machines.

Data security during transmission and encryption is an emerging issue with the proliferation of IoT devices and other remote diagnostics. The study recommends the use of smart contracts built on blockchain and enables safe testing and use of medical sensors, as well as handling Protected Health Information (PHI) generated by these devices. The study developed a system that uses a private blockchain built on top of the Ethereum protocol. The sensors talk to a smart device, which in turn invokes smart contracts and records every transaction on the blockchain. By implementing secure records and alerting communication for patients and physicians, this smart contract system will enable medical engagement and real-time patient monitoring (Griggs *et al.*, 2018). Automating alerts to all stakeholders mitigates many of the security concerns associated with remote patient care in a HIPAA-compliant manner.

2.4 Challenges and Advantages of Smart Contract-based EHR System

2.4.1 Challenges

One of the biggest problems with cloud computing and record sharing among stakeholders is that unauthorized users can access sensitive information in electronic health records (Kumar *et al.*, 2018). The main objective of this study is to develop a referral method using sophisticated smart contracts to facilitate the efficient exchange of medical information among different stakeholders in the healthcare system. Only authorized physicians within the health information network can access this referral system, and it is built on a patient-centered concept (Kumar *et al.*, 2018). To safely and efficiently exchange big data in the healthcare industry, Hyperledger Fabric, an opensource blockchain that uses Hyperledger Composer to run CouchDB, and Interplanetary File System, a decentralized data repository, are used to design the system.

Blockchain development has adapted to the changing technology. Blockchain is widely used in finance, but vertical industries like healthcare are evolving and changing in the future. In this article, we presented a Blockchain-based healthcare system smart contract architecture. We ensure that the implementation of public ledger principles and technologies will transform the strategy and vision of Blockchain-based health systems. Health information, test data, physician opinions, and standardized health data can be shared across services. Blockchain allows these pieces to be combined into a distributed ledger based on events. Complex practice and manual intervention can be eliminated. Blockchain-based applications can be completely open and secure with an identity manager (Amir Latif *et al.*, 2020). Based on the expected results, the proposed Blockchain-based system will be helpful in healthcare. To evaluate the maturity level of the proposed system, the authors map it to an Ethereum-based application and test it in a clinical environment.

2.4.2 Advantages

Today, healthcare organizations and people produce data every day. Protecting and sharing such volumes of data is important but difficult, expensive, and time-consuming. This barrier prevents healthcare organizations from communicating with each other, leaving patient medical records scattered across multiple databases (da Fonseca Ribeiro and Vasconcelos, 2020). One of the emerging answers to these issues is blockchain technology. Cryptographic encryption makes records stored in a distributed database immutable, transparent, and generally usable. Several blockchain-based apps are currently being developed in an attempt to address the issue of coordination between different healthcare providers. The main objective of this study is to analyze the developments in smart contracts and blockchain technology from a healthcare service perspective (da Fonseca Ribeiro and Vasconcelos, 2020).

Blockchain has been a fascinating topic of study for years, and many fields have taken advantage of its benefits. The healthcare industry benefits immensely from blockchain technology due to security, privacy, confidentiality, and decentralization. However, there are issues with the security, integrity, and maintenance of EHR systems (Shahnaz *et al.*, 2019). In this article, the authors explain how blockchain technology can transform EHR systems and address these concerns. The study provides an approach to the application of blockchain technology in healthcare HR. The approach first uses blockchain technology for EHRs and then secures electronic records by establishing granular access controls for users. This approach also solves the scalability problem of blockchain technology in storing records off-chain (Shahnaz *et al.*, 2019). This architecture provides EHRs with a scalable, secure, and comprehensive blockchain solution.

3 Research Methodology

3.1 Introduction

The study is being done using a mixed approach in which both qualitative and quantitative methods are being used. Using a qualitative approach all the literature sources and internet articles related to the topic are analyzed and the methods that are being applied by the previous authors who have worked on a similar topic in previous years. To keep this study relevant the papers selected are from 2016-2024 and all the papers previous to 2016 are being discarded from this study. Using a quantitative approach, an EHR application is being developed using the tools Python, Web3, Flask, Ganache, and Metamask, and the smart contract is written using the Solidity framework.

3.2 Data Collection and Analysis

Both qualitative and quantitative methods are combined in this research which is known as mixed methods research. Hospital management system (HMS) security through decentralization and smart contracts is a topic of extensive literature and online study. To ensure relevance and up-to-date insights, documents and statistics from 2016 to 2024 are required to be thoroughly reviewed to identify methodology and analyze findings from the past. The quantitative method involved building an EHR app with Solidity-written smart contracts and Python, Web3, Flask, Ganache, and Metamask. This application can be used to simulate HMS systems for decentralization. Controlled experiments and simulations are used to collect data on application performance, security, and performance. As part of the evaluation, we compare the application to more traditional systems and see how it can improve security and speed up product development. Speed of transactions, data security, and attack resistance are some of the metrics tracked. Now, we’ll combine the findings from the two approaches to give you a more complete picture of how smart contracts and blockchain can impact HMS.

3.3 KDD Framework

To methodically extricate important insights from the information created through the examination, this study applies the Knowledge Discovery in Databases (KDD) paradigm.

Selection: The identified and gathered relevant data sources include experimental data from the developed EHR application and literature from 2016 to 2024.

Preprocessing: Information is cleaned and changed over to guarantee consistency and get rid of any duplicate or unnecessary data.

Transformation: Encoding of reasonable information designs for research incorporates sorting out writing results and encoding EHR application execution markers.

Data Mining: To find patterns and connections in the data, analysts use tools like statistical analysis and performance reviews.

Interpretation/Evaluation: In order to comprehend how blockchain and brilliant agreements affect EHR productivity and security, the study examines the data.

This study presents a philosophy for evaluating the possible advantages of decentralization and brilliant agreements in improving the Electronic Health Record (EHR) framework. The review uses the Information Disclosure in Data sets (KDD) structure to assemble both quantitative and subjective information efficiently. The EHR system's safety and operational efficiency will rise as a result of the straightforward and evidence-based insights gleaned from this data.

4 Design Specification

Our electronic health record (EHR) system is built on blockchain to ensure privacy, efficiency, and security of data management. To further support these goals, smart contracts are included in the architecture.

Technology Stack:

- **Backend Framework:** Flask (Python) for the web application backend.
- **Blockchain Platform:** Ganache for local Ethereum blockchain simulation.
- **Smart Contracts:** Solidity for writing the contracts.

- **Database:** SQLite for storing patient data locally.
- **Front-end:** HTML, CSS, and JavaScript for creating the user interface.

Development Environment:

- **Python Version:** 3.11.5
- **Flask Version:** 2.2.2
- **Web3.py Version:** 6.20.0
- **Truffle Suite:** Truffle v5.11.5 for compiling and deploying smart contracts.
- **Ganache Version:** 7.9.1 for simulating a local blockchain network.
- **Node.js Version:** 20.15.1

Smart Contract Design:

Contract Address: Deployed on Ganache local blockchain.

Functions:

- **registerDoctor():** Registers a new doctor.
- **addPatient(name, disease, medication):** Adds a new patient’s medical record.
- **updateMedicalHistory(patient_id, disease, medication):** Updates a patient's medical history.
- **getPatient(patient_id):** Retrieves patient details.

Database Design:

SQLite Database: Used for storing patient information.

Tables:

- **Patient:** Stores patient ID, name, disease, medication, and doctor's address.

Front-End Design:

- **HTML Templates:** Used Flask’s render_template to serve HTML pages.
- **CSS Styling:** Applied custom styles to ensure a user-friendly interface.

- **Forms:** Used HTML forms to capture user input for registering doctors and patients, and updating medical records.

API Endpoints:

User Registration:

- **/register_doctor:** HTML form for doctor registration.
- **/register_patient:** HTML form for patient registration.

Dashboards:

- **/doctor_dashboard:** Allows doctors to add and update patient records.
- **/patient_dashboard:** Allows patients to view their medical history.

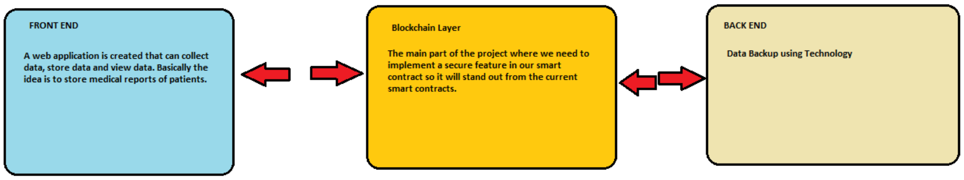
Smart Contract Interaction:

- **/add_doctor:** Endpoint for adding a doctor via a POST request.
- **/add_patient:** Endpoint for adding a patient via a POST request.
- **/update_medical_history:** Endpoint for updating a patient’s medical history via a POST request.
- **/get_patient:** Endpoint for retrieving patient details via a GET request.

Security Measures:

- **Private Keys:** Ensured secure handling and storage of private keys.
- **Data Integrity:** Used blockchain immutability to prevent unauthorized data modifications.
- **Access Control:** Implemented basic form validation and secure transmission protocols.

Using the benefits of blockchain innovation, this design detail ensures an electronic health record system that is protected, effective, and simple to utilize.



FRONT END

A web application is created that can collect data, store data and view data. Basically the idea is to store medical reports of patients.

Blockchain Layer

The main part of the project where we need to implement a secure feature in our smart contract so it will stand out from the current smart contracts.

BACK END

Data Backup using Technology

Figure 1: Concept of our EHR system

5 Implementation/Solution Development

To guarantee a secure, efficient, and user-friendly application, the implementation of a blockchain-based EHR system must go through several well-designed steps. First, virtual was formed environment-based "env" to manage Python dependencies. The following packages were installed using pip: SQLAlchemy, Web3.py, Flask-Migrate, and Flask. The project started by creating Solidity smart contracts which included patient registration, physician registration, medical history updates, and data retrieval with contract address in Flask Ganache using Truffle Suite to do so these contracts were implemented in a local blockchain simulator. Created Flask application, configured SQLite as a local database for patient records, and used SQLAlchemy as an Object-Relational Mapper (ORM) in all backend development. Database migration was handled through Flask-Migrate. Doctor and patient registries, dashboard access, and the ability to edit medical records are just a few of the API endpoints designed to facilitate communication between databases and smart contracts uniform and visually appealing we used an HTML template generated by the Flask render_template function and we include input forms and special CSS styles.

Web3.py, which was designed to run on the local Ganache blockchain, gained integration with smart contracts. Activities such as signing and adding to the blockchain using private keys were used to process transactions. It also has robust error handling for troubleshooting. To confirm the speed of the system, we ran several functional tests to ensure that all features worked as expected. Blockchain validation was done to make sure that the local Ganache blockchain transactions were real and could not be changed. The application was finally launched following extensive local machine testing and validation. User manuals, design specifications, and design instructions were all included in the complete documentation. The program will run smoothly and be much simpler to develop and maintain in the future as a result of this. The interest for improved information security and protection in medical services frameworks has been met with the advancement of a blockchain-based electronic health record framework that is secure, proficient, and simple to utilize.

6 Evaluation

Like conventional EHR frameworks, our application gives decentralized, carefully designed information capacity and smooth correspondence of information between medical services suppliers while safely dealing with the electronic health record (EHR) through blockchain innovation and smart contract for uprightness, protection, and access by which they get an assurance. As per the review, our blockchain-based EHR programming is creative and fruitful in overseeing delicate clinical data safely and proficiently. The information is secure, searchable, and unavailable to change by this software as it combines blockchain technology with easy online transactions. Anyone involved in patient care can feel safe to enroll in the system, access their medical records, and communicate with it. Since blockchain technology is decentralized, it removes the need for a central authority, which improves patient privacy and reduces the potential for data breaches. This proves our null hypothesis H0: Patients' personal information will be far more protected with a blockchain-based EHR system than with an older more insecure one.

6.1 Security features present in our system

- **Ownership and Role-Based Access Control:** The owner of the contract is associated with the address used to execute the contract. Only registered physicians whose addresses are entered in a physician map can register patients and make changes to their medical history. Functions such as addPatient and update use requirement statements. By design, MedicalHistory restricts access to these features to only authorized physicians or doctors.
- **Data Integrity:** To make sure the data is organized and easy to handle, we employ mappings like patients, physicians, and addressToPatientId. To aid in the proper identification and management of patient information, a unique identifier is issued to each patient.

- **Event Logging:** Every time a patient is added or their medical history is changed, events like PatientAdded and MedicalHistoryUpdated are emitted. This keeps a record of significant events, which might be helpful for monitoring and auditing modifications.
- **Security Best Practices:** Only authorised users can execute specific operations since msg.sender is used to authenticate who is calling the function. The latest version of Solidity, 0.5.16, which the contract is written in, has many security enhancements over previous versions.

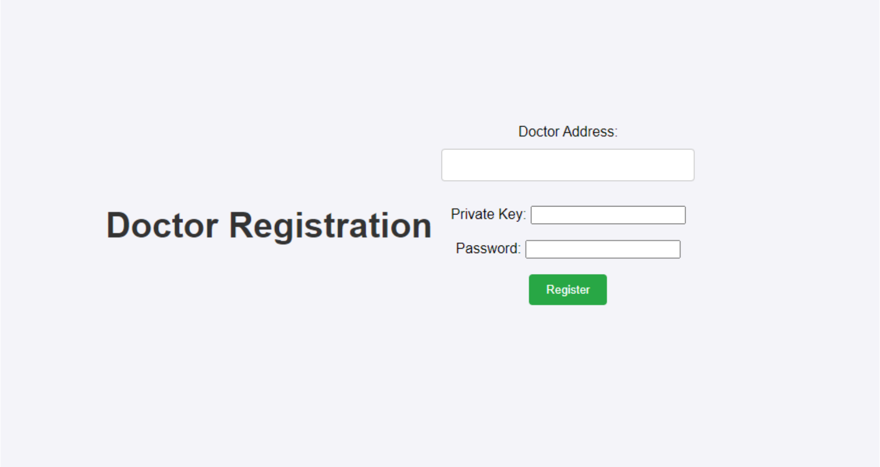


Figure 2: Doctor Registration Portal

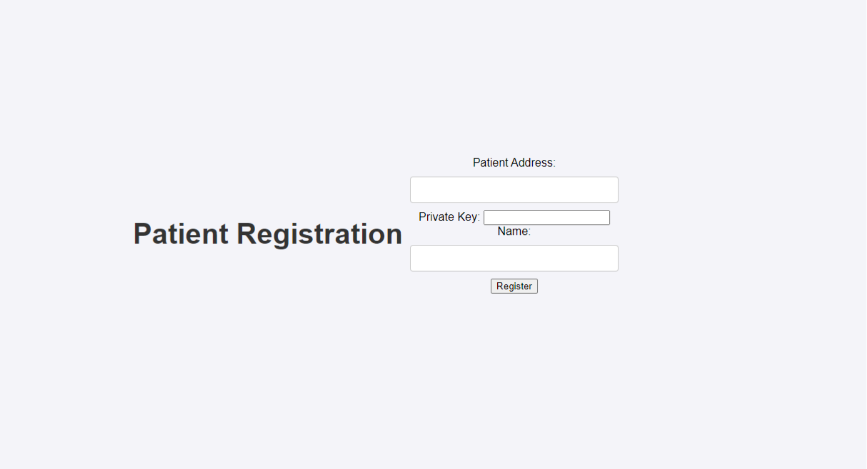
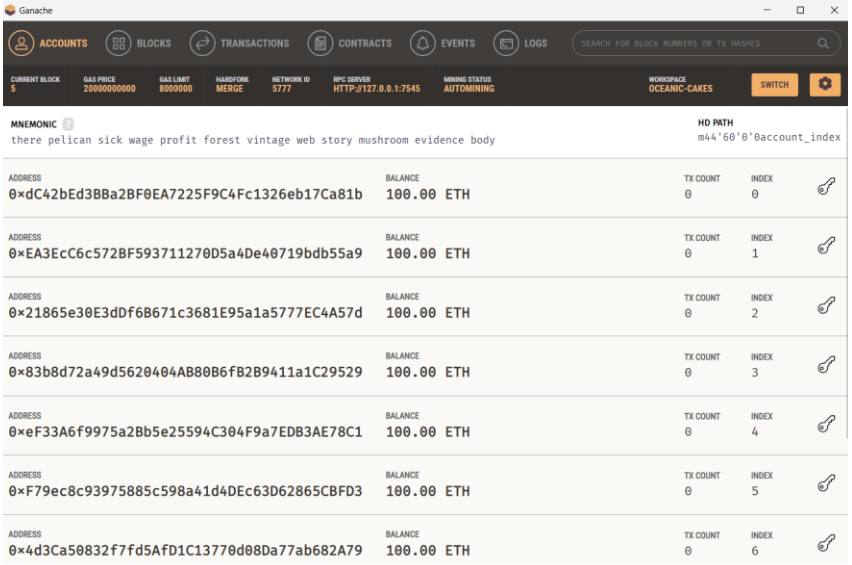


Figure 3: Patient Registration Portal

The above images clearly show that for doctor and patient registration we need to have the public key to put in and then the private then only that Doctor or patient can login to their respective portals to check information.



CURRENT BLOCK 5 | GAS PRICE 20000000000 | GAS LIMIT 8000000 | HARDFORK MERGE | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING | WORKSPACE OCEANIC-CAKES

MNEMONIC
there pelican sick wage profit forest vintage web story mushroom evidence body

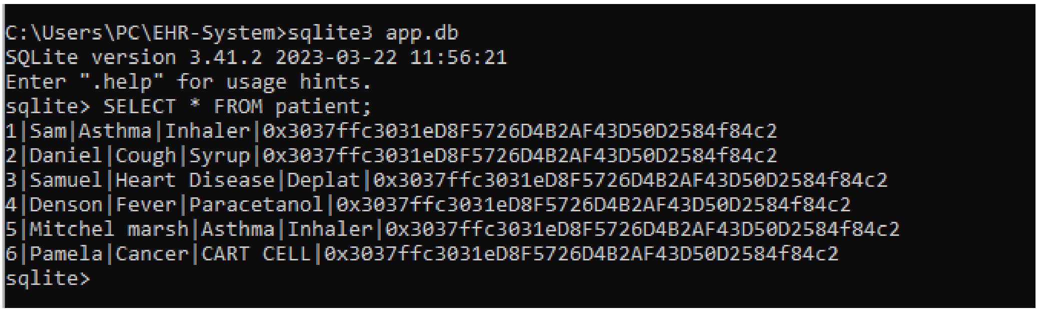
HD PATH
m44'60'0'0account_index

ADDRESS	BALANCE	TX COUNT	INDEX
0×dC42bEd3BBa2BF0EA7225F9C4Fc1326eb17Ca81b	100.00 ETH	0	0
0×EA3EcC6c572BF593711270D5a4De40719bdb55a9	100.00 ETH	0	1
0×21865e30E3dDf6B671c3681E95a1a5777EC4A57d	100.00 ETH	0	2
0×83b8d72a49d5620404AB80B6fB2B9411a1C29529	100.00 ETH	0	3
0×eF33A6f9975a2Bb5e25594C304F9a7EDB3AE78C1	100.00 ETH	0	4
0×F79ec8c93975885c598a41d4DEc63D62865CBFD3	100.00 ETH	0	5
0×4d3Ca50832f7fd5AfD1C13770d08Da77ab682A79	100.00 ETH	0	6

Figure 4: Ganache

The SQLite3 database is used by the program to store local data, increasing blockchain possibilities. Lightweight and efficient SQLite3 is a serverless database engine that stores and retrieves data quickly. It guarantees that authorized individuals have simple access to the app to edit patient records. Quick creation and organization of utilizations because of SQLite3's usability and similarity with the Flask web system.

The SQLite3 database efficiently stores and retrieves patient information, including names, diseases, medications, and doctor addresses, as demonstrated by the provided SQL query results. This element guarantees that the blockchain and nearby information base parts complete one another, and give a strong option in contrast to EHR execution. By coordinating blockchain innovation into social data sets, the framework exhibits a critical development in medical care IT by giving a productive and secure EHR framework.



```
C:\Users\PC\EHR-System>sqlite3 app.db
SQLite version 3.41.2 2023-03-22 11:56:21
Enter ".help" for usage hints.
sqlite> SELECT * FROM patient;
1|Sam|Asthma|Inhaler|0x3037ffc3031eD8F5726D4B2AF43D50D2584f84c2
2|Daniel|Cough|Syrup|0x3037ffc3031eD8F5726D4B2AF43D50D2584f84c2
3|Samuel|Heart Disease|Deplat|0x3037ffc3031eD8F5726D4B2AF43D50D2584f84c2
4|Denson|Fever|Paracetanol|0x3037ffc3031eD8F5726D4B2AF43D50D2584f84c2
5|Mitchel marsh|Asthma|Inhaler|0x3037ffc3031eD8F5726D4B2AF43D50D2584f84c2
6|Pamela|Cancer|CART CELL|0x3037ffc3031eD8F5726D4B2AF43D50D2584f84c2
sqlite>
```

Figure 5: Database of our EHR System

7 Conclusion and Discussion

7.1 Conclusion

By developing an electronic health record (EHR) application that incorporates smart contracts and blockchain technology, this study focuses on the security and efficiency of hospital management systems (HMS). This examination shows the capacity of this innovation to resolve gives usually seen in customary unified HMS utilizing a mix of subjective and quantitative examination. Moreover, it features the groundbreaking capability of this innovation in the area. An exhaustive cognizance of the current examples and challenges in achieving HMS was achieved by looking at subjective writing from 2016 to 2024. The rising perceivability of information breaks, unapproved access, and framework shortcomings represent a threat to patient protection and hierarchical integrity.

For our intelligent contracts and the Electronic Health Record (EHR) application, we used Python, Web3, Flask, Ganache, MetaMask, and Solidity for numerical operations. Data integrity, transaction speed, and resistance to unauthorized access are common considerations when comparing this decentralized application's performance to that of more conventional systems. The discoveries showed that the use of blockchain innovation in the development of HMS brought about a significant improvement in security by guaranteeing information straightforwardness and unchanging nature. By automating several operations, smart contracts have improved operational efficiency and reduced the likelihood of human error. Using the databases-based Knowledge Discovery (KDD) method, the data were analyzed systematically. This worked with huge disclosures. The review gave undeniable evidence of the upsides of decentralization in the field of HMS using blockchain innovation and shrewd agreements. A methodical approach was used to achieve this, which resulted in resilient and data-focused outcomes.

7.2 Discussion

Ensuing examinations concerning hospital management systems (HMS) (HMS) using blockchain innovation and smart contracts ought to focus on settling versatility and interoperability concerns. Researchers are looking into mixed hybrid blockchain topologies that include both public and private chains to improve scalability and adaptability. To make it easier to trade healthcare management systems made possible by blockchain technology, standard rules and procedures must be established. As a result, healthcare facilities may be more likely to accept it. By cultivating coordinated efforts between medical care specialists and innovation organizations, possible and promptly accessible arrangements might be contrived. Pilot projects and contextual analyses displaying viable execution will essentially add to building trust and featuring the commonsense benefits of this innovation. To be monetarily practical, arrangements should likewise stick to health information security necessities, like HIPAA. Adopting a multidisciplinary approach that involves collaborating among health experts, regulators, and technology developers is necessary to advance research and commercialization in this field.

References

Almasoud, A.S., Hussain, F.K. and Hussain, O.K., 2020. Smart contracts for blockchain-based reputation systems: A systematic literature review. *Journal of Network and Computer Applications*, *170*, p.102814.

Amir Latif, R.M., Hussain, K., Jhanjhi, N.Z., Nayyar, A. and Rizwan, O., 2020. A remix IDE: smart contract-based framework for the healthcare sector by using Blockchain technology. *Multimedia tools and applications*, pp.1-24.

Arunkumar, B. and Kousalya, G., 2020. Blockchain-based decentralized and secure lightweight e-health system for electronic health records. In *Intelligent Systems, Technologies and Applications: Proceedings of Fifth ISTA 2019, India* (pp. 273-289). Springer Singapore.

Chang, S.E., Chen, Y., Lu, M. and Luo, H.L., 2020. Development and evaluation of a smart contract–Enabled blockchain system for home care service innovation: Mixed methods study. *JMIR medical informatics*, *8*(7), p.e15472.

Chang, S.E., Chen, Y., Lu, M. and Luo, H.L., 2020. Development and evaluation of a smart contract–Enabled blockchain system for home care service innovation: Mixed methods study. *JMIR medical informatics*, *8*(7), p.e15472.

da Fonseca Ribeiro, M.I. and Vasconcelos, A., 2020, May. MedBlock: Using Blockchain in Health Healthcare Application based on Blockchain and Smart Contracts. In *ICEIS (1)* (pp. 156-164).

Griggs, K.N., Ossipova, O., Kohlios, C.P., Baccarini, A.N., Howson, E.A. and Hayajneh, T., 2018. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *Journal of medical systems*, *42*, pp.1-7.

Khatoon, A., 2020. A blockchain-based smart contract system for healthcare management. *Electronics*, *9*(1), p.94.

Kumar, T., Ramani, V., Ahmad, I., Braeken, A., Harjula, E. and Ylianttila, M., 2018, September. Blockchain utilization in healthcare: Key requirements and challenges. In *2018 IEEE 20th International conference on e-health networking, applications and services (Healthcom)* (pp. 1-7). IEEE.

Mezquita, Y., Valdeolmillos, D., González-Briones, A., Prieto, J. and Corchado, J.M., 2019. Legal aspects and emerging risks in the use of smart contracts based on blockchain. In *Knowledge Management in Organizations: 14th International Conference, KMO 2019, Zamora, Spain, July 15–18, 2019, Proceedings 14* (pp. 525-535). Springer International Publishing.

Pham, H.L., Tran, T.H. and Nakashima, Y., 2018, December. A secure remote healthcare system for hospital using blockchain smart contract. In *2018 IEEE globecom workshops (GC Wkshps)* (pp. 1-6). IEEE.

Saini, A., Zhu, Q., Singh, N., Xiang, Y., Gao, L. and Zhang, Y., 2020. A smart-contract-based access control framework for cloud smart healthcare system. *IEEE Internet of Things Journal*, *8*(7), pp.5914-5925.

Shahnaz, A., Qamar, U. and Khalid, A., 2019. Using blockchain for electronic health records. *IEEE access*, *7*, pp.147782-147795.

Sharma, A., Sarishma, Tomar, R., Chilamkurti, N. and Kim, B.G., 2020. Blockchain based smart contracts for internet of medical things in e-healthcare. *Electronics*, *9*(10), p.1609.

Tanwar, S., Parekh, K. and Evans, R., 2020. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications*, *50*, p.102407.

Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X. and Wang, F.Y., 2019. Blockchain-enabled smart contracts: architecture, applications, and future trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *49*(11), pp.2266-2277.