SRM University AP

Department of Computer Science And Engineering

Software Engineering Project Report on

"Patient Database Management Using Blockchain"

Kotharu Bhoomika

AP21110011616

CSE-W

Table of contents

Abstract

The Blockchain-Based Patient Data Management System, developed with HTML, CSS, and PHP for frontend and backend operations, leverages Ganache and Truffle for blockchain integration. This innovative system aims to address critical vulnerabilities in traditional medical record-keeping methods, enhancing security and efficiency in processing medical bills and insurance claims.

The system facilitates seamless interaction among the Hospital Department, Medical Department, and Insurance Company while ensuring the integrity and confidentiality of patient data. Through the utilization of blockchain technology, patient records and financial information are securely stored on a tamper-resistant ledger, mitigating the risks of data manipulation and unauthorized access.

It involves three main entities: the Hospital Department, Medical Department, and Insurance Company. It starts with the Hospital Department, responsible for adding patients and generating unique IDs. Once a patient ID is created, the Medical Department can add associated medical bills. Simultaneously, the Insurance Company can search for patients using their ID and retrieve all bills uploaded by the Medical Department.

Utilizing HTML and CSS for frontend design provides a user-friendly interface for hospitals, medical departments, insurance companies, and patients to manage and access medical records and bills efficiently. Meanwhile, PHP serves as the backend framework, enabling dynamic data processing and interaction with the blockchain.

Ganache and Truffle are utilized to integrate blockchain capabilities into the system, offering transparency and accountability in data management. This integration ensures that patient data remains secure and immutable throughout its lifecycle, preventing fraud and enhancing trust between stakeholders.

Overall, the Blockchain-Based Patient Data Management System represents a significant advancement in healthcare record management, offering a secure, transparent, and efficient platform for managing medical records, bills, and insurance claims. Its adoption holds the potential to revolutionize healthcare delivery by streamlining processes, reducing fraud, and improving overall patient care.

Introduction

In today's digital age, the management of patient records and healthcare data has become increasingly crucial for ensuring efficient and secure healthcare services. Traditional systems for managing patient databases often face challenges related to data security, privacy, and interoperability. In response to these challenges, innovative technologies such as blockchain are being explored as potential solutions to revolutionize the healthcare industry.

Blockchain technology, initially popularized by cryptocurrencies like Bitcoin, is a distributed ledger system that offers a decentralized and immutable record of transactions. Its key features, including transparency, security, and decentralization, make it a promising candidate for various applications beyond finance, including healthcare.

This report focuses on the development of a Patient Database Management System using blockchain technology. The system aims to address the shortcomings of traditional patient database management systems by leveraging the security and transparency offered by blockchain. By integrating blockchain into the healthcare ecosystem, we can enhance data integrity, streamline processes, and improve patient outcomes.

Before delving deeper into the project, it's essential to understand some basic concepts and terminologies related to blockchain and healthcare data management:

Blockchain: A decentralized, distributed ledger technology that records transactions across multiple nodes in a secure and transparent manner. Each transaction is cryptographically linked to the previous one, forming a chain of blocks.

Smart Contracts: Self-executing contracts with predefined rules and conditions encoded on the blockchain. Smart contracts automate and enforce the terms of agreements, eliminating the need for intermediaries.

Decentralization: The distribution of control and authority across multiple nodes or participants in a network. Decentralization enhances security, resilience, and transparency by removing single points of failure.

Patient Database Management: The process of collecting, storing, and managing patient-related information, including medical records, treatment history, and billing data.

Interoperability: The ability of different healthcare systems and applications to exchange and interpret data seamlessly. Interoperability is essential for ensuring the continuity of care and improving healthcare delivery.

ABI (Application Binary Interface): ABI is a standard interface for interaction between smart contracts and other parts of the system. It defines how functions are called and data is transferred in and out of the contract.

Contract Address: A contract address is a unique identifier assigned to each deployed smart contract on the blockchain. It is used to interact with the contract and execute its functions.

Migrations: Migrations are scripts used to deploy smart contracts onto the blockchain. They manage the deployment sequence and ensure that contracts are deployed in a coordinated manner.

Our project aims to develop a comprehensive Patient Database Management System that leverages blockchain technology to address key challenges in healthcare data management. By integrating blockchain into the system architecture, we aim to achieve the following objectives:

Enhance Data Security: By storing patient records on a decentralized blockchain network, we mitigate the risk of data breaches and unauthorized access.

Ensure Data Integrity: The immutability of blockchain ensures that patient records are tamper-proof, maintaining the integrity of the data throughout its lifecycle.

Facilitate Interoperability: Blockchain technology facilitates seamless data exchange and interoperability between different healthcare stakeholders, improving collaboration and patient care.

Empower Patients: Through secure access to their medical records via blockchain-based authentication mechanisms, patients have greater control over their healthcare data.

By incorporating blockchain technology and utilizing a combination of frontend technologies like HTML, CSS, and JavaScript, along with backend technologies like PHP, and blockchain tools like Web3, Truffle, and Ganache, the system ensures secure, efficient, and transparent management of patient data across the healthcare ecosystem.

This project aims to demonstrate the potential of blockchain technology in addressing the challenges of patient database management while improving the overall quality of healthcare services. Through the implementation of a blockchain-based patient database management system, we strive to contribute to the advancement of healthcare technology and enhance patient care outcomes.

Existing System/Literature review

In the domain of patient database management, traditional systems predominantly rely on centralized databases managed by healthcare institutions or third-party service providers. While these systems have been the backbone of healthcare data management for decades, they often encounter challenges related to data security, privacy, and interoperability. In this section, we examine some existing systems in the healthcare industry and discuss their advantages, limitations, and areas for improvement.

Existing Systems:

Electronic Health Records (EHR) Systems:

EHR systems have revolutionized the way healthcare institutions manage patient health information, transitioning from paper-based records to digital formats. The widespread adoption of EHR systems has brought several advantages to healthcare delivery:

Streamlined Workflow: EHR systems streamline administrative and clinical processes, reducing paperwork and improving efficiency. Healthcare providers can easily access and update patient records, leading to smoother workflow management.

Improved Data Accuracy: By digitizing patient health information, EHR systems minimize errors associated with manual record-keeping. Automated data entry, validation checks, and real-time updates enhance data accuracy, ensuring that healthcare providers have access to reliable information when making treatment decisions.

Facilitated Communication: EHR systems facilitate communication and collaboration among healthcare providers by enabling the sharing of patient records across different departments and specialties. This seamless exchange of information promotes coordinated care delivery and improves patient outcomes.

Despite these advantages, EHR systems encounter several limitations that warrant attention:

Data Security Vulnerabilities: EHR systems are susceptible to data breaches, hacking attempts, and unauthorized access, posing significant risks to patient privacy and confidentiality. Weaknesses in security protocols, inadequate encryption methods, and human error contribute to data security vulnerabilities, highlighting the need for robust cybersecurity measures.

Interoperability Issues: Interoperability challenges persist within the healthcare industry, hindering the seamless exchange of patient data between different EHR systems and healthcare organizations. Incompatibility between systems, proprietary data formats, and lack of standardized protocols impede data sharing efforts, impacting care coordination and continuity.

User Interface Complexities: The user interface design of EHR systems varies widely, leading to inconsistencies in usability and navigation. Complex interfaces, cluttered screens, and unintuitive workflows can overwhelm users and hinder their ability to efficiently navigate the system, resulting in reduced productivity and user satisfaction.

Health Information Exchange (HIE) Networks:

HIE networks play a crucial role in facilitating the exchange of patient health information across disparate healthcare entities, including hospitals, clinics, and laboratories. These networks offer several advantages for healthcare delivery:

Enhanced Care Coordination: HIE networks promote care coordination by providing healthcare providers with access to comprehensive patient information from multiple sources. Timely access to medical records, test results, and treatment plans enables providers to deliver more coordinated and personalized care to patients.

Reduction in Redundancy: By enabling the sharing of patient health information, HIE networks reduce duplication of tests, procedures, and administrative tasks. This not only saves time and resources but also minimizes the risk of unnecessary interventions and improves healthcare efficiency.

Improved Patient Outcomes: Timely access to medical records and clinical data through HIE networks facilitates informed decision-making and enhances patient outcomes. Healthcare providers can make more accurate diagnoses, develop tailored treatment plans, and monitor patient progress more effectively, leading to better health outcomes for patients.

However, HIE networks face several limitations that pose challenges to their effectiveness:

Challenges with Data Standardization: HIE networks encounter difficulties in standardizing data formats, terminology, and coding systems across different healthcare organizations. Inconsistencies in data representation and semantics impede data exchange and interoperability, limiting the utility of HIE networks for care coordination.

Consent Management Complexity: Managing patient consent for data sharing presents challenges for HIE networks, particularly concerning patient privacy and confidentiality. Ensuring compliance with regulatory requirements, obtaining informed consent, and respecting patient preferences are essential but complex processes that require careful attention and coordination.

Governance and Oversight: The governance structure and oversight mechanisms of HIE networks vary widely, leading to inconsistencies in policies, procedures, and data management practices. Establishing clear governance frameworks, accountability mechanisms, and data stewardship guidelines is crucial for ensuring the integrity, security, and trustworthiness of HIE networks.

Additionally, privacy concerns arise due to the sharing of sensitive patient information across multiple organizations, raising questions about data ownership, confidentiality, and patient rights.

In conclusion, while EHR systems and HIE networks offer significant benefits for healthcare delivery, they also face challenges related to data security, interoperability, consent management, and governance. Addressing these limitations requires collaborative efforts from healthcare stakeholders, policymakers, and technology providers to ensure the effective and responsible use of health information exchange technologies in improving patient care and outcomes.

Areas for Improvement:

Blockchain Integration: Introducing blockchain technology into patient database management systems can address security and interoperability concerns by providing a decentralized and tamper-proof platform for storing and sharing patient data.

Enhanced Privacy Controls: Implementing privacy-enhancing technologies, such as zero-knowledge proofs and differential privacy, can empower patients to control access to their health information and ensure data confidentiality.

Standardization and Interoperability: Developing standardized data formats, protocols, and interfaces can facilitate seamless data exchange and interoperability between different healthcare systems and organizations.

Patient-Centric Design: Designing systems with a focus on patient empowerment and engagement can improve user experience, foster trust, and promote better health outcomes.

In summary, while existing patient database management systems have made significant advancements in digitizing healthcare information, they still face challenges related to data security, privacy, and interoperability. By leveraging emerging technologies like blockchain and adopting patient-centric design principles, we can overcome these challenges and pave the way for a more secure, interoperable, and patient-centric healthcare ecosystem.

System Requirements

Software Requirements:

1. Operating System: Compatible with Windows, macOS, or Linux.

2. Integrated Development Environment (IDE): Visual Studio Code

3. Node.js: Required for running JavaScript applications and installing npm packages.

4. Truffle Suite: Truffle provides a development framework for smart contracts.

5.Ganache: Ganache is a personal blockchain for development, providing a local blockchain for testing and development purposes.

6. Web3.js: Web3.js is a JavaScript library that allows interaction with nodes

Frontend Development:

HTML, CSS, JavaScript: Use HTML for markup, CSS for styling, and JavaScript for frontend logic and interaction with smart contracts.

Backend Development:

PHP: Use PHP for server-side scripting and backend logic, handling user authentication, database operations, and interaction with the blockchain.

MySQL: Choose a relational database management system (RDBMS) for storing user data, transaction records, and other relevant information.

Hardware Requirements:

Processor: Intel Core i5 or equivalent AMD processor (or higher).

RAM: 8 GB of RAM (or higher) for smooth development experience.

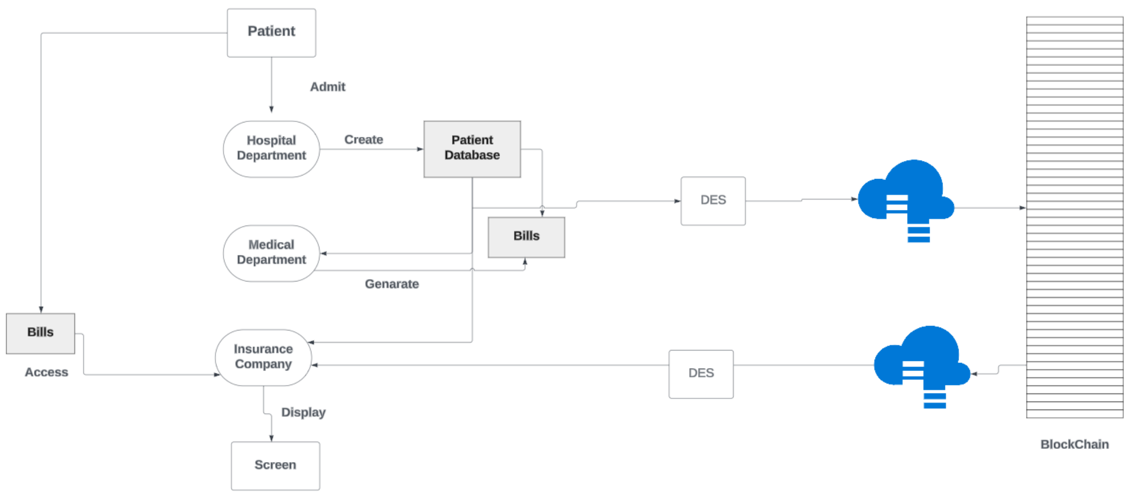
Storage: Adequate storage of available disk space for storing project files, dependencies, and blockchain data.

Web Server:

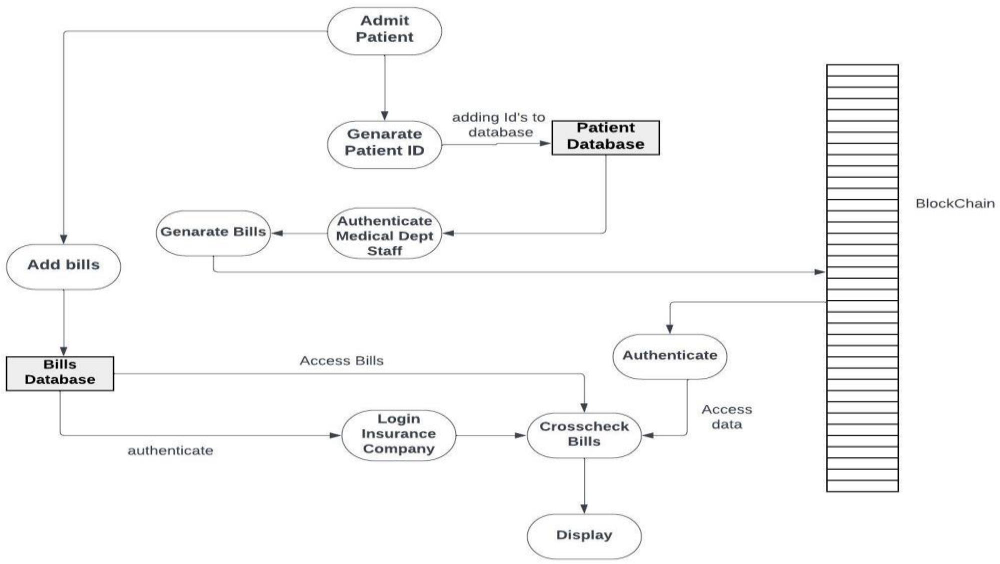
Apache or Nginx: Install and configure a web server to host the backend PHP application. Ensure that the server meets the minimum requirements for running PHP scripts and serving web content.

Proposed System

Basic Diagram:



More detailed:



Authentication process:

The authentication process begins with a user interface implemented using HTML forms, where users are prompted to input their username and password. When the form is submitted, the entered credentials are transmitted to a server-side script written in PHP. This PHP script, operating in conjunction with XAMPP's MySQL database management system, retrieves the username and associated password hash from the database. Upon retrieval, the script verifies the existence of the entered username and compares its associated hashed password with the password submitted by the user, ensuring security by hashing both values for comparison. If the hashed passwords match, authentication is successful, granting the user access to the application's secure features. Conversely, if there is a mismatch or the username does not exist, the user is promptly informed of an authentication failure. Upon successful authentication, users are seamlessly redirected to the application's dashboard, signifying a successful login.

Registration:

During registration, users provide necessary details such as username, email, and password via an HTML form. Upon submission, the entered information is sent to a PHP script for processing. Utilizing XAMPP's MySQL database, the script securely stores the user's data, including their hashed password, in the appropriate database tables. Error handling mechanisms are implemented to address potential issues like underage or invalid inputs, ensuring data integrity. Upon successful registration, users receive confirmation and are directed to the login page to access the application's features.

Home Page Display:

The system initiates by presenting a user-friendly home page interface to users. Users are given the option to select their designated role from a predefined list, including patient, hospital department, medical department, or insurance company.

User Role Selection:

Upon selecting a role, users are directed to a login/signup page tailored to their chosen role.This ensures that each user is provided with access to functionalities specific to their role within the healthcare ecosystem.

Patient Role:

Patients have the ability to log in or sign up to access their personal accounts within the system. Upon successful login, patients can view and manage their medical records, including adding bills, updating personal information, and accessing treatment history.

Hospital Department Role:

Hospital departments are required to log in or sign up to access their dedicated accounts.Once authenticated, hospital departments can create patient IDs, record patient data, and manage medical records within the hospital's database.

Medical Department Role:

Medical departments also undergo the authentication process to access their designated accounts. After successful login, medical departments can add bills and medical expenses to patient records, ensuring accurate billing and accounting practices.

Blockchain Integration:

The system integrates blockchain technology to enhance the security and transparency of patient data management.All bills and patient database entries are securely added to the blockchain, ensuring immutability and integrity of the records.Blockchain integration provides a tamper-proof audit trail, facilitating accountability and trust among healthcare stakeholders.

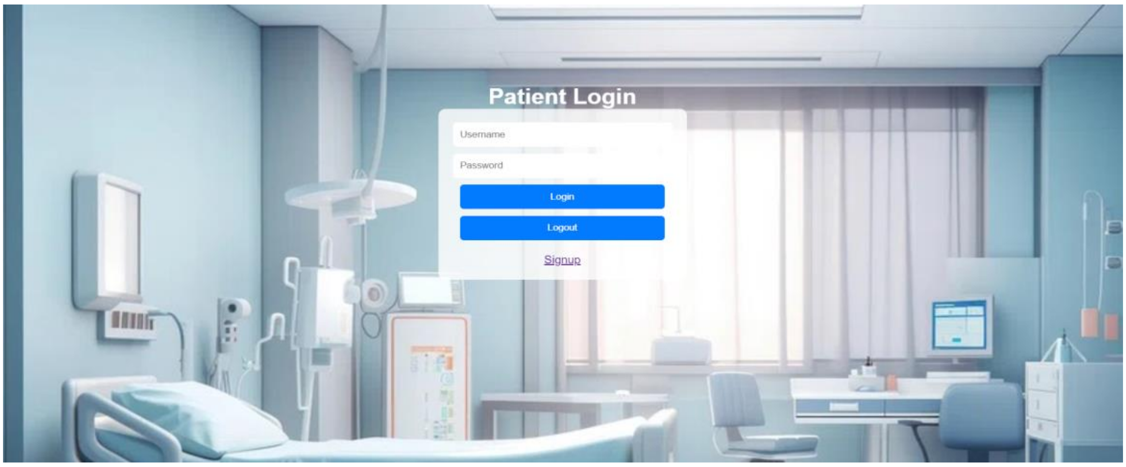
Insurance Company Role:

Insurance companies log in or sign up to access their dedicated accounts within the system.Upon authentication, insurance companies can cross-check bills and medical expenses with patient IDs to verify claims and ensure accuracy.Results of the verification process are displayed to insurance company personnel, enabling informed decision-making regarding claim approvals.

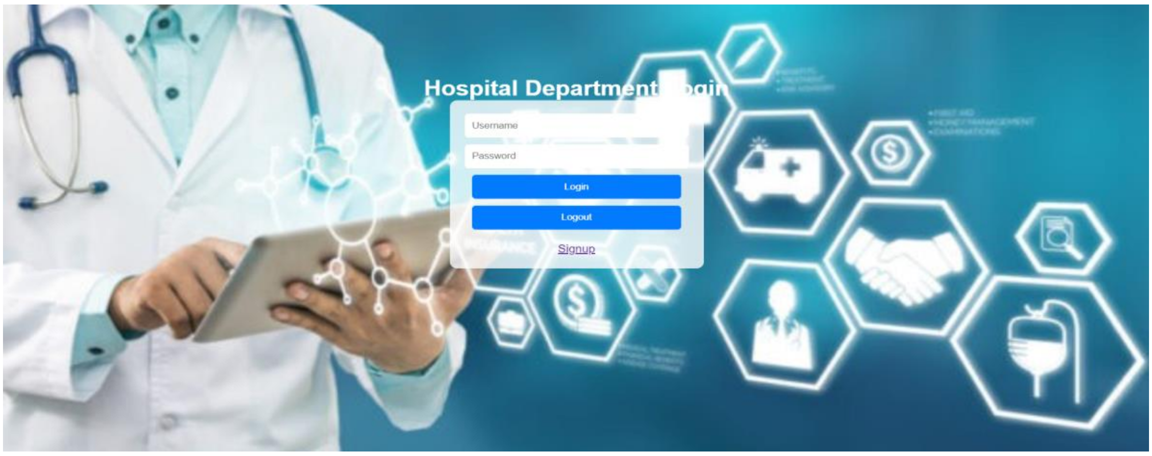
Result /Performance Evaluation

Index page:

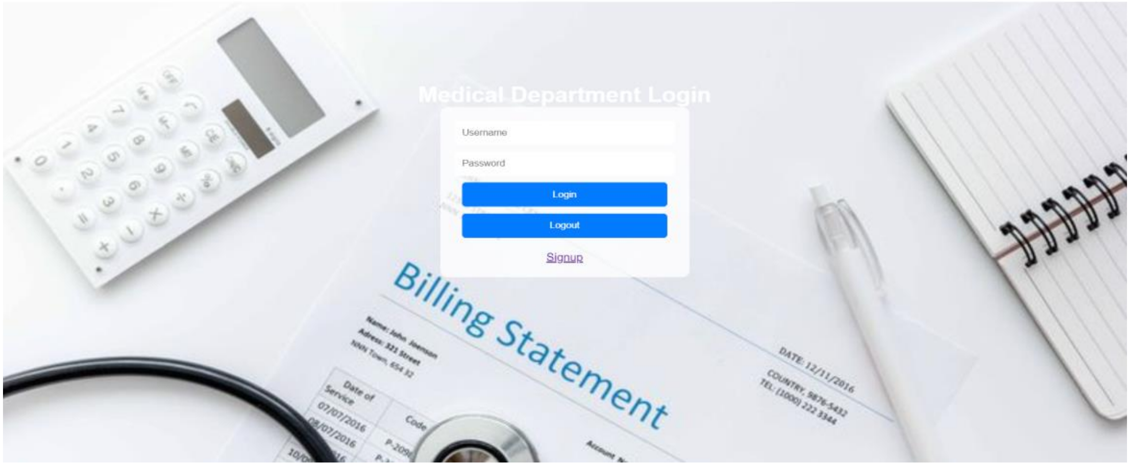
Patient Login page:



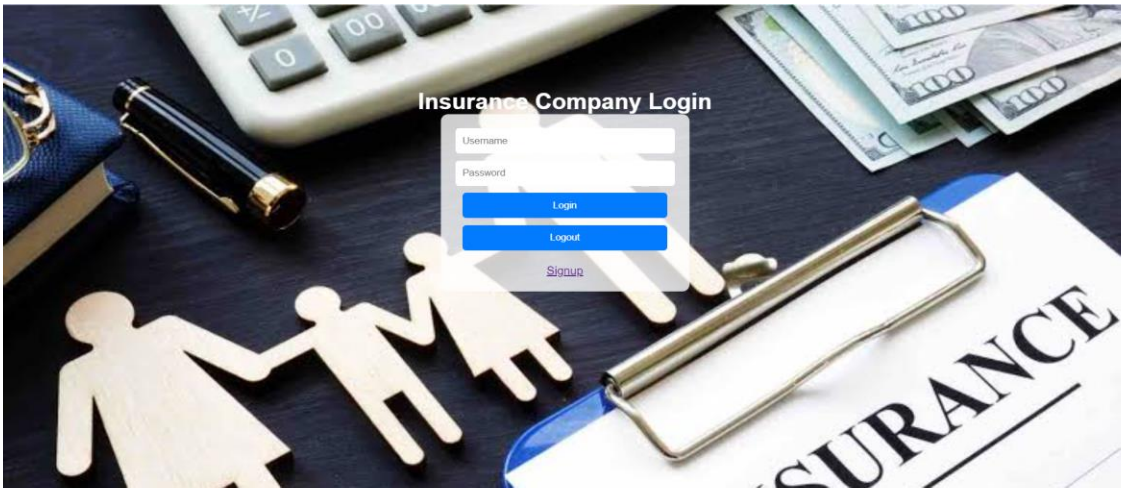
Hospital Login page:



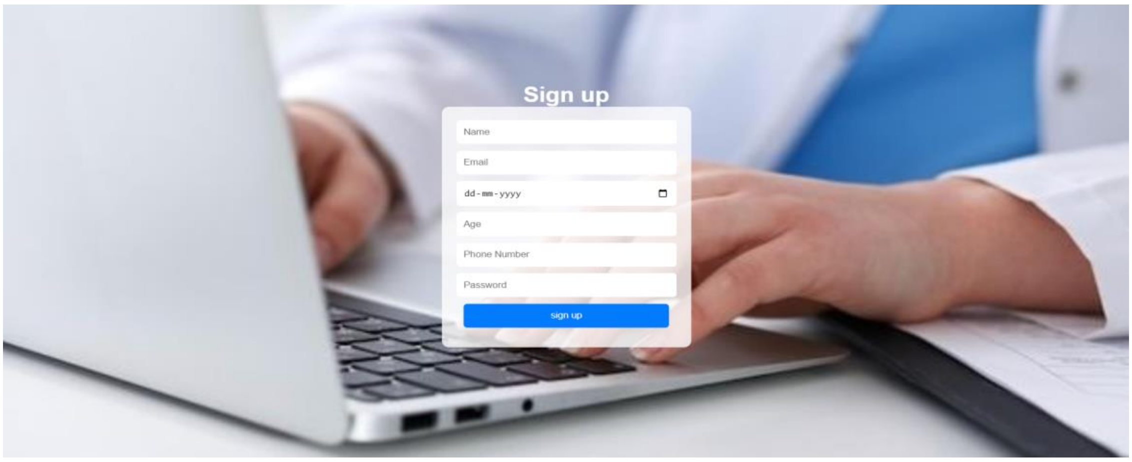
Medical Department Login page:



Insurance Login page:

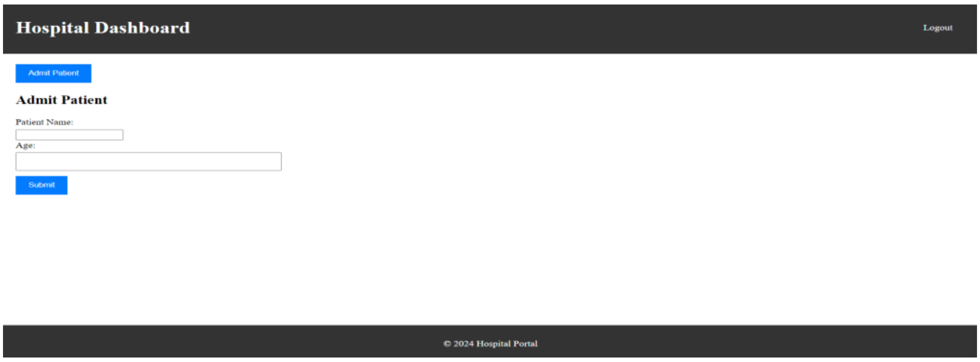


Registration page:



Patient page:

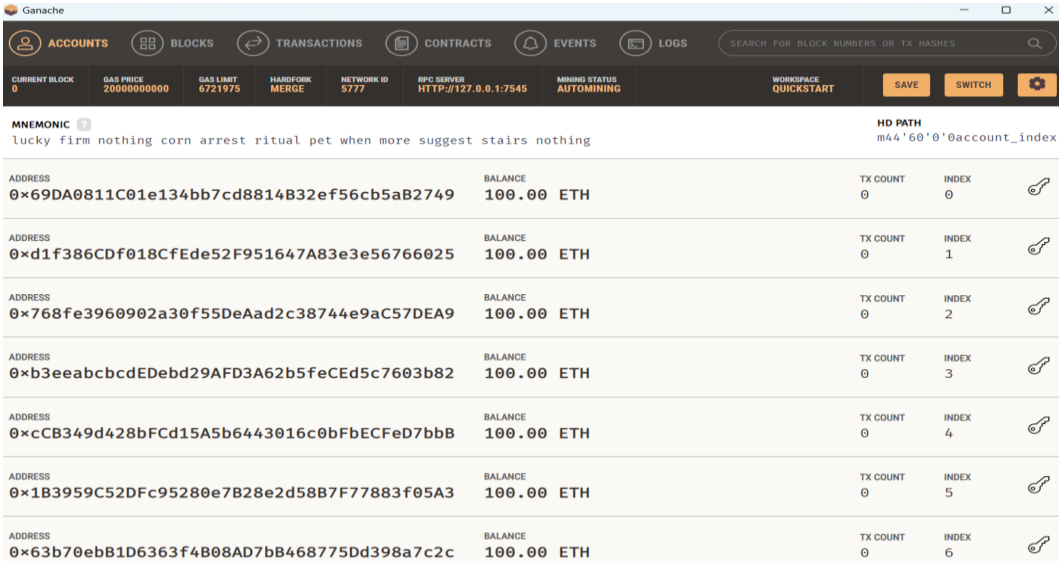
Hospital page:



Medical page:

Insurance page:

Initial account details:

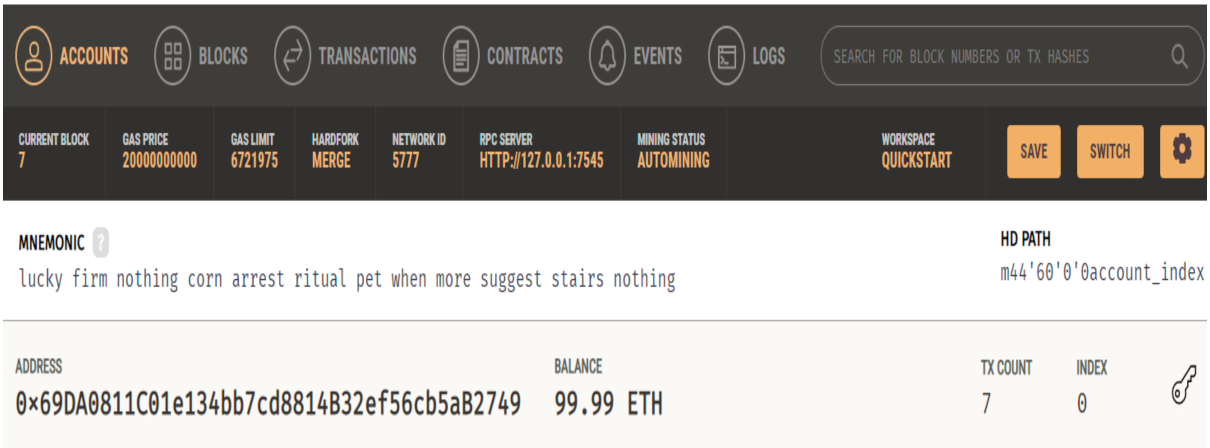


Deployed contracts:

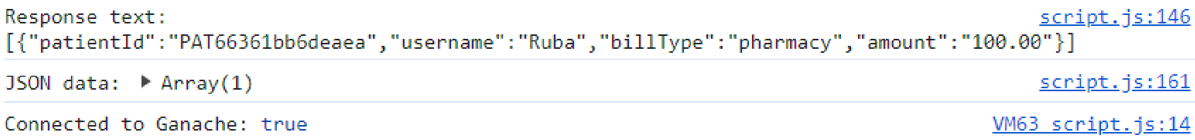
```
Starting migrations...
======================
> Network name:    'development'
> Network id:      5777
> Block gas limit: 6721975 (0x6691b7)


1_initial_migration.js
======================

   Replacing 'Migrations'
   ----------------------
   > transaction hash:    0x3a6a34a7adbb2b37c70c6f4707ecff4e5b19d35c59e188c4f4e1983f086f7492
   > Blocks: 0            Seconds: 0
   > contract address:    0xF4F2110Faf38091413fDA09070Ec6d7fFDd7D889
   > block number:        1
   > block timestamp:     1714873583
   > account:             0x69DA0811C01e134bb7cd8814B32ef56cb5aB2749
   > balance:             99.999347804875
   > gas used:            193243 (0x2f2db)
   > gas price:           3.375 gwei
   > value sent:          0 ETH
   > total cost:          0.000652195125 ETH

   > Saving migration to chain.
   > Saving artifacts
   -------------------------------------
   > Total cost:      0.000652195125 ETH


2_deploy_contracts.js
=====================

   Replacing 'Patient'
   -------------------
   > transaction hash:    0x8f584af82b31939bf33b09c5d8eb65f507144ac53ecfb679a17a6e3b62c946bd
   > Blocks: 0            Seconds: 0
   > contract address:    0x01db8FD4956f992667FC03D561EFA6F594dA1E79
   > block number:        3
   > block timestamp:     1714873583
   > account:             0x69DA0811C01e134bb7cd8814B32ef56cb5aB2749
```

```
   Replacing 'Insurance'
   ---------------------
   > transaction hash:    0x1dd146ad80cee1748263af291787aaa79666940c8bcba2767e1f600b0d731e86
   > Blocks: 0            Seconds: 0
   > contract address:    0xb513F17BBDd53E5a8C9D4A4134057482CC4CBfa1
   > block number:        6
   > block timestamp:     1714873583
   > account:             0x69DA0811C01e134bb7cd8814B32ef56cb5aB2749
   > balance:             99.992228607674723908
   > gas used:            715609 (0xaeb59)
   > gas price:           2.98399686 gwei
   > value sent:          0 ETH
   > total cost:          0.00213537500898774 ETH

   > Saving migration to chain.
   > Saving artifacts
   -------------------------------------
   > Total cost:     0.006969546415353222 ETH

Summary
=======
> Total deployments:   5
> Final cost:          0.007621741540353222 ETH
```

Account details after deployment:



Connected to Ganache:



Final Output:

Conclusion

In conclusion, the development of the Patient Database Management System using blockchain technology represents a significant step forward in revolutionizing healthcare data management. Throughout the course of this project, we have successfully implemented a system that addresses key challenges faced by traditional patient database systems, including data security, transparency, and interoperability.

By leveraging blockchain technology, we have ensured the integrity and immutability of patient data, thereby enhancing trust and accountability within the healthcare ecosystem. The integration of blockchain also facilitates secure and transparent transactions, allowing for seamless exchange of patient information among different stakeholders, including patients, hospital departments, medical departments, and insurance companies.

The role-based access control system ensures that each user is provided with access to functionalities specific to their role, thereby enhancing efficiency and confidentiality in managing patient information. Patients can conveniently access and manage their medical records, while healthcare providers can securely add and update patient data in compliance with privacy regulations.

Looking ahead, there are some avenues for future work and improvement. Firstly, we aim to further enhance the scalability and performance of the system to accommodate larger volumes of patient data and increased user traffic. Additionally, ongoing research and development efforts will focus on exploring advanced blockchain solutions, such as decentralized identity management and zero-knowledge proofs, to enhance privacy and security in patient data management.

References

1. https://doi.org/10.1109/JSYST.2020.2963840
2. https://healthcareweekly.com/blockchain-in-healthcare-guide/.
3. https://dragonchain.com/blog/top-blockchain-benefits/.
4. https://mlsdev.com/blog/blockchain-and-healthcare-use-cases-today-and-in-the-future.