الجمهوريــة الجزائريــة الديمقراطيــة الشعبيــة

People's Democratic Republic of Algeria

وزارة الـتعلـيـم الـعـالي و البـحـث الـعلـمــي

Ministry of Higher Education and Scientific Research

MUSTAPHA Stambouli University
Mascara

جامعة مصطفى اسطمبولي
معسكر

Faculty of Exact Sciences

Computer Science Department

Master’s THESIS

Speciality : Information System and Web Technology.

Titled

Implementation of Medical Records with Blockchain

Presented by: Mr Benyakhou El Hadj Larbi

On: 06/21/2024 at the Exact Science Faculty

Before the jury:

President	**Houari Amina**	**Dr**	**Mascara University**
Examiner	**Boudia Chérifa**	**Dr**	**Mascara University**
Co-Supervisor	**Mesmoudi Amin**	**Dr**	**Poitiers University**
Supervisor	**Khelil Abdellah**	**Dr**	**Mascara University**

Academic Year : 2023 - 2024

Abstract

One of the most critical aspects of information systems is the method of data storage, especially when it involves sharing and collecting data from various individuals and entities. Trust in their information is paramount. Typically, central databases are used to address this issue, requiring all partners to trust the organization that maintains the database as the central authority managing the data.

However, when it comes to storing medical health records, centralizing information introduces the risk of patient data manipulation. Blockchain technology, which has been in use for several years, offers a solution by enabling the sharing of information without relying on a central database, ensuring trust in both the data and the participants.

This project aims to create a private blockchain to implement Blockchain Smart Contracts for storing sensitive patient data, specifically Electronic Health Records (EHRs), in a medical application. This approach guarantees the immutability and integrity of these records.

key-words : Blockchain, Trust,Private Blockchain , Electronic Medical Record, access control,Smart contract, IPFS.

Acknowledgments

First and foremost, I would like to express my deepest gratitude to my supervisors, abdallah Khelil and amin mesmoudi, for their unwavering support, guidance, and valuable insights throughout the course of this research. Their expertise and encouragement have been instrumental in the completion of this thesis.

I would also like to extend my sincere thanks to the faculty and staff of the Department of Computer Science at the University of Mustapha Stambouli for providing an inspiring academic environment and for their assistance during my studies.

A heartfelt thanks to my colleagues and friends for their camaraderie and for the stimulating discussions, collaboration, and support that have enriched my research experience.

I am deeply grateful to my parents, my mom and dad, for their unconditional love, patience, and encouragement, which have been a constant source of strength and motivation throughout my academic journey.

Finally, I would like to acknowledge all the individuals and organizations who contributed to this research, directly or indirectly, for their invaluable contributions.

Thank you all for making this achievement possible.

Contents

List of Figures

General Introduction

In recent years, the healthcare industry has witnessed a surge in the adoption of digital technologies aimed at enhancing patient care, streamlining administrative processes, and ensuring the security and integrity of medical data. One such disruptive technology that has garnered significant attention is blockchain. Originally devised as the underlying technology for cryptocurrencies like Bitcoin, blockchain has since evolved into a versatile tool with applications across various sectors, including healthcare.

The management of medical records poses numerous challenges, ranging from issues of interoperability and data security to concerns regarding patient privacy and unauthorized access. Traditional systems for storing and accessing medical records are often siloed, fragmented, and susceptible to data breaches and cyberattacks. In this context, blockchain technology offers a promising solution by providing a decentralized and immutable ledger for recording and sharing sensitive medical information securely and transparently.

This thesis explores the implementation of blockchain technology in the context of medical record management. Specifically, it investigates the design, development, and deployment of a blockchain-based system for securely storing, accessing, and managing electronic health records (EHRs). By leveraging the inherent properties of blockchain, such as decentralization, transparency, and cryptographic security, this research aims to address the limitations of existing medical record systems and pave the way for a more efficient, interoperable, and patient-centric healthcare ecosystem.

Overall, this thesis contributes to the growing body of research on blockchain technology and its potential to revolutionize the way medical records are managed, accessed, and shared. By demonstrating the feasibility and efficacy of blockchain-based solutions in healthcare, this research seeks to pave the way for widespread adoption and integration of blockchain technology in the medical industry, ultimately leading to improved patient outcomes and healthcare delivery.

Chapter 1

Blockchain technology

1.1 Introduction

In the contemporary digital area, blockchain technology has emerged as a revolutionary paradigm, fundamentally transforming the way transactions and data are managed across diverse industries. Originating as the foundational technology supporting cryptocurrencies, blockchain has transcended its initial application to become a decentralized, transparent, and secure ledger system. This technology introduces a novel approach to data management, offering unparalleled levels of trust and integrity. As we delve into the intricacies of blockchain, it becomes evident that its decentralized architecture and cryptographic security not only redefine the concept of trust but also present opportunities for innovation that extend well beyond its initial applications.

1.2 Definition of Blockchain

Blockchain is an innovative technology that forms the basis of crypto-currency Bitcoin [2] created by Satoshi Nakamoto (pseudonym) who proposed a contribution on Bitcoin in 2008 and was released in 2009. However, the original paper did not discuss the Blockchain [3]. Therefore, it is possible that Blockchain is an unintentionally invented technology with a potential to be applied in numerous fields. The purpose of Blockchain is to ensure that transactions of value within a network of untrusted entities go through a trusted intermediary [3]. The emergence of Blockchain is contributing to a paradigm shift in computer science. The aim of this section is to explain the concept of Blockchain illustrated in Figure 1.1 , its beginnings, its development and its relevance for the proposed solution. A Blockchain represents a database structured as a one-dimensional hash chain of blocks whose origins are in a genesis block. The distribution and the maintenance of a Blockchain are done by a set of participants of a peer-to-peer network that do not trust each other. Thus, there must be a consensus mechanism among the participants, so that they all can agree about the state of the database. The introduction of a data structure to fingerprint the data would enhance a Blockchain storage efficacy. In particular, digital signatures should be used to ensure that the adequate identity issues the changes to data. Essentially, a Blockchain is defined as ”a one-dimensional hash chain”. It is argued that a Blockchain is a linked list implemented with hash pointers [4]. Nevertheless, some scholars, such as Abeyratne and Monfared [5], argue that a Blockchain is a database distributed in a peer-to-peer network. Nevertheless, the distributed property is not a requirement for a Blockchain, but rather a neat application of the Blockchain database. The Blockchain is powerful due to this property and, accordingly, it is often known as a distributed database. A decentralized distribution means that the participants do not need to trust each other in order to manage a Blockchain [6]. However, a distributed database requires a consensus mechanism so that the same version is ensured on all sites. The database depends on a chain structure. Accordingly, long chains consume the considerable memory. A hash pointer stored in one block points to the previous block. Hence, it is not possible to modify data in the previous block without invalidating the pointer in the next block. It means that the Blockchain is invalidated by removing unnecessary data. The Merkle tree [3] can resolve this challenge, as the participants would be able to keep only a valid copy of the data relevant to them by fingerprinting the transactions by using a data structure. The use of data structure for fingerprinting the data is not necessary for a Blockchain. However, it is a great tool to increase the storage efficiency for the Blockchain participants and accordingly, the overall usefulness of the Blockchain. Using digital signatures in a Blockchain ensures the origin of issued database transactions. In this way, data can be linked to the owner. Yet, this tool is not a requirement for the Blockchain. For a transaction to be valid, it must be consistent. It means the adequate identity corresponding must issue transactions to the altered data, which can be achieved by using digital signatures. Concerning the monetary system, it indicate spending only one's own money.

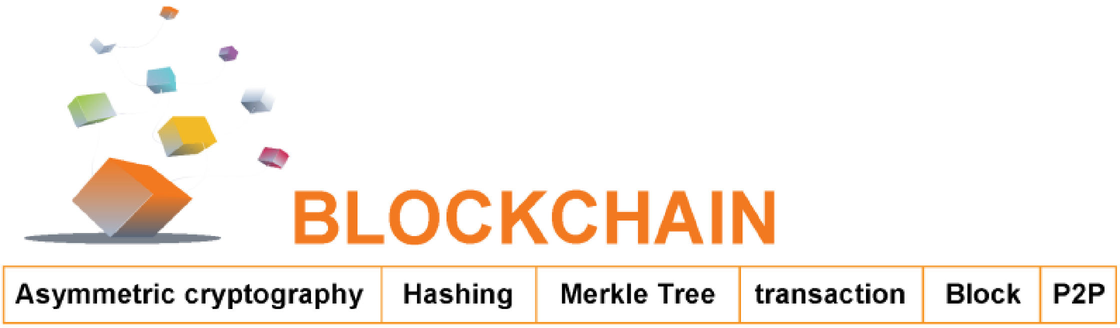


Figure 1.1: Key concepts of Blockchain

1.3 How blockchain works

You might be familiar with spreadsheets or databases. A blockchain is somewhat similar because it is a database where information is entered and stored. But the key difference between a traditional database or spreadsheet and a blockchain is how the data is structured and accessed. A blockchain consists of programs called scripts that conduct the tasks you usually would in a database: Entering and accessing information and saving and storing it somewhere. A blockchain is distributed, which means multiple copies are saved on many machines, and they must all match for it to be valid. The blockchain collects transaction information and enters it into a block, like a cell in a spreadsheet containing information. Once it is full, the information is run through an encryption algorithm, which creates a hexadecimal number called the hash. The hash is then entered into the following block header and encrypted with the other information in the block. This creates a series of blocks that are chained together. [2]

1.3.1 Transaction Process

Transactions follow a specific process, depending on the blockchain they are taking place on. For example, on Bitcoin's blockchain, if you initiate a transaction using your cryptocurrency wallet—the application that provides an interface for the blockchain—it starts a sequence of events.

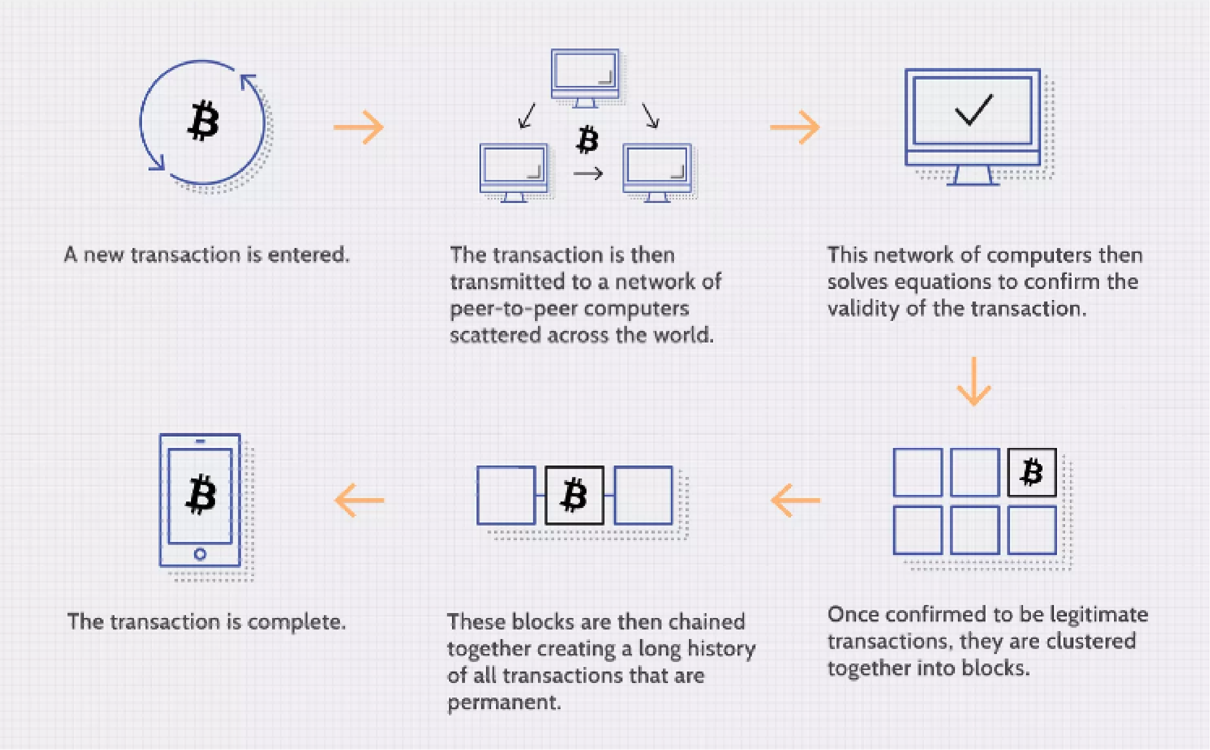

A new transaction is entered.
The transaction is then transmitted to a network of peer-to-peer computers scattered across the world.
This network of computers then solves equations to confirm the validity of the transaction.
Once confirmed to be legitimate transactions, they are clustered together into blocks.
These blocks are then chained together creating a long history of all transactions that are permanent.
The transaction is complete.

Figure 1.2: Transaction Process

In Bitcoin, your transaction is sent to a memory pool, where it is stored and queued until a miner or validator picks it up. Once it is entered into a block and the block fills up with transactions, it is closed and encrypted using an encryption algorithm. Then, the mining begins. The entire network works simultaneously, trying to "solve" the hash. Each one generates a random hash except for the "nonce," short for number used once. Every miner starts with a nonce of zero, which is appended to their randomly-generated hash. If that number isn't equal to or less than the target hash, a value of one is added to the nonce, and a new block hash is generated. This continues until a miner generates a valid hash, winning the race and receiving the reward. Once a block is closed, a transaction is complete. However, the block is not considered to be confirmed until five other blocks have been validated. Confirmation takes the network about one hour to complete because it averages just under 10 minutes per block (the first block with your transaction and five following blocks multiplied by 10 equals about 60 minutes). Not all blockchains follow this process. For instance, the Ethereum network randomly chooses one validator from all users with ether staked to validate blocks, which are then confirmed by the network. This is much faster and less energy intensive than Bitcoin's process.[7]

1.4 Consensus mechanisms

1.4.1 Proof of Work

To prove the credibility of data in blocks PoW mechanism uses the method to solve the puzzle. When a node wants to create a block it must resolve a puzzle. Upon resolving the puzzle successfully a new block is created and broadcasted to other nodes to achieve the consensus [8].

- Probability of mining a block directly depends on the work done by miner.

- Consumes more energy than other Mechanism like POS .
- can cause a 51% attack if overall computational power is achived.

The contents of a block may vary in different chains.

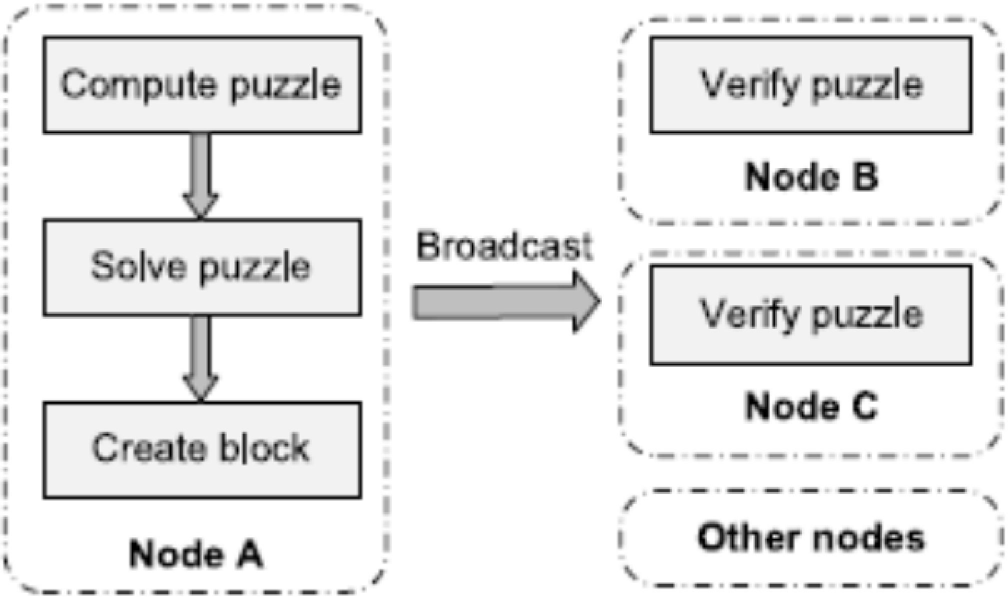


Figure 1.3: PoW Consensus Mechanism

1.4.2 Proof of Stake

Proof of work was the first cryptocurrency consensus mechanism, An alternative, proof of stack, came out in 2012 with the launch Peer coin. It chooses transaction validators based on how many coins they've staked or locked up, to the network. Because proof of stake doesn't require nearly as much computing power as proof of work, it's more scalable. It can process transactions more quickly for lower fees and with less energy usage, making Proof-of-stake . cryptocurrencies more environmentally friendly, It's also much easier to start staking crypto than mining since there's no expensive hardware required. However, proof of work is more proven from a security perspective.[9]

1.4.3 Proof of Authority

Proof of Authority (PoA) is designed to optimize the PoS mechanism and be used, ideally, in permissioned networks. Instead of choosing block miners on the basis of their stakes in cryptocurrency tokens, PoA selects a small group of authorities as transaction validators by their identity or reputation staked in the network To contend for validators, users go through a formal notarization process in which they provide documentation to prove their real identities and link them with their on-chain identities to establish their digital reputation. Existing validators can vote to add additional users into the authority group. A PoA-based system also rewards authorities for certifying and ordering transactions to incentivize honest behavior in providing service and moderating the network. PoA Network and Ethereum's test net Kovan are examples of public networks that use PoA consensus. [10]

1.5 Types of blockchain

1.5.1 Public blockchain

A public, or permission-less, blockchain network is one where anyone can participate without restrictions. Most types of cryptocurrencies run on a public blockchain that is governed by rules or consensus algorithms.

1.5.2 Permissioned or private blockchain

A private, or permissioned, blockchain allows organizations to set controls on who can access blockchain data. Only users who are granted permissions can access specific sets of data. Oracle Blockchain Platform is a permissioned blockchain.

1.5.3 Federated or consortium blockchain

A blockchain network where the consensus process (mining process) is closely controlled by a preselected set of nodes or by a preselected number of stakeholders.[11]

1.6 Blockchain today

1.6.1 Cryptocurrencies

Cryptocurrencies are digital or virtual currencies that utilize cryptographic techniques for security and operate on decentralized networks based on blockchain technology. They facilitate secure and transparent peer-to-peer transactions, eliminating the need for intermediaries such as banks.[12]

1.6.2 Bitcoin

Bitcoin (BTC), introduced by the pseudonymous Satoshi Nakamoto in 2009, is the pioneering cryptocurrency. Operating on a decentralized, peer-to-peer network, Bitcoin utilizes a public ledger called the blockchain. It serves not only as a medium of exchange but also as a store of value and a digital alternative to traditional currencies.[12][13]

1.6.3 Smart Contracts

Smart contracts are self-executing contracts with terms encoded directly into code. They automatically execute and enforce predefined conditions. Ethereum, a blockchain platform, is a prominent example that introduced the concept of smart contracts. It allows developers to create decentralized applications (DApps) using smart contracts.[14][15]

1.7 The advantages and disadvantages of blockchain

1.7.1 Advantages of Blockchain

- Decentralization: Eliminates the need for a central authority, promoting a trustless environment.[16]
- Immutability and Security: Transactions are cryptographically secured and stored in blocks, making them resistant to tampering.[13]
- Transparency: All participants in a blockchain network have access to the same data, ensuring transparency.[17]
- Efficiency and Cost Reduction: Streamlines processes by reducing the need for intermediaries, leading to cost savings.[15]
- Smart Contracts: Self-executing contracts automate and enforce agreements, enhancing efficiency.[14]
- Global Accessibility: Enables cross-border transactions without the need for traditional banking infrastructure.[18]

1.7.2 Disadvantages of Blockchain

- Scalability: Challenges in scaling blockchain networks to handle a high volume of transactions.[19]
- Energy Consumption: Proof-of-work consensus mechanisms, as used in Bitcoin, can be energy-intensive.[20]
- Regulatory Uncertainty: Ongoing regulatory developments and uncertainty in various jurisdictions.[21]
- Lack of Standardization: Lack of standardization across different blockchain implementations can hinder interoperability.[22]
- Privacy Concerns: Challenges in balancing transparency with the need for privacy in certain applications.[23]

- Adoption Barriers: Resistance to change, education gaps, and the complexity of integrating blockchain into existing systems.[17]

1.8 Conclusion

In conclusion, the significance of blockchain technology for various sectors is profound and far-reaching. Its decentralized nature, coupled with the ability to create transparent, tamper-resistant, and efficient systems, positions blockchain as a cornerstone for the future of digital interactions. Beyond its roots in cryptocurrency, blockchain holds the potential to revolutionize industries such as finance, supply chain, healthcare, and more. Embracing blockchain in research and practical applications promises a landscape where trust is inherent, security is paramount, and processes are streamlined. As we navigate the complexities of the digital age, blockchain stands as a transformative force, shaping a future characterized by resilience, transparency, and decentralized innovation.

Chapter 2

Healthcare Blockchain applications

2.1 Introduction

Blockchain technology has emerged as a transformative force in healthcare, offering solutions to longstanding challenges in data management and patient care. Its decentralized nature promises enhanced security, transparency, and efficiency across various healthcare processes. This thesis explores the impact of blockchain on healthcare, analyzing its potential to revolutionize electronic health records (EHRs), supply chain management, patient empowerment, and clinical research. By examining real-world use cases and addressing key considerations, this study aims to offer insights into the practical integration of blockchain in healthcare, driving towards a future of patient-centric, secure, and efficient healthcare delivery.

2.2 Blockchain applications in medicine

In the last time blockchain technology is known in the field of economics and cryptocurrencies, but today its utility is expanding in several other areas, including the biomedical field. The potential of blockchain technology can be witnessed in the fields of medicine, genomics, telemedicine, tele-monitoring, e-health, neuroscience, and personalized healthcare applications, by its mechanism of stabilizing and securing the data set with which users can interact through different types of transactions (as depicted in the model, shown in Figure)[24]

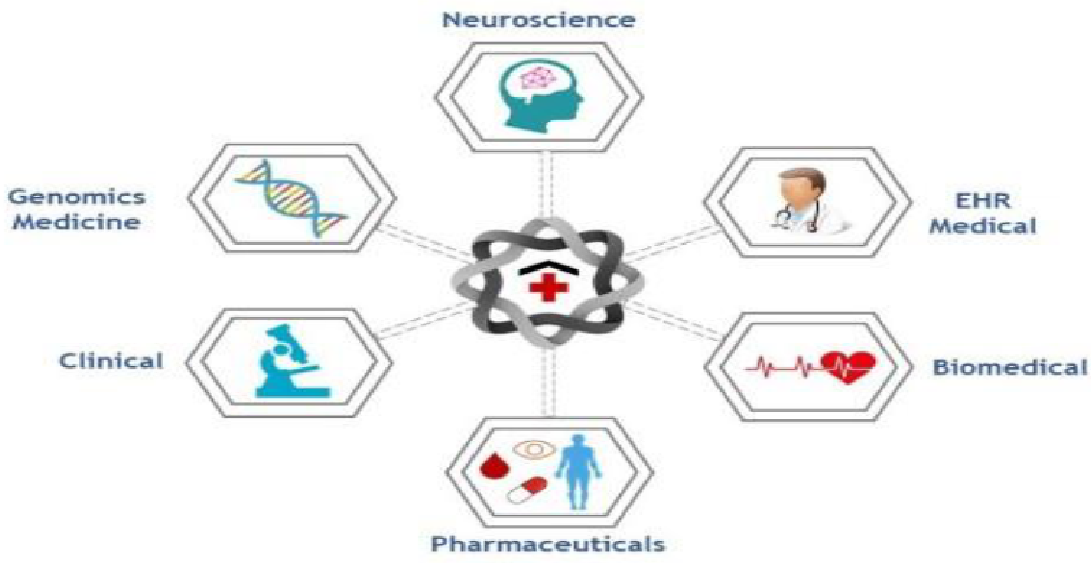


Figure 2.1: Blockchain healthcare applications

2.2.1 Medical Data Management

Blockchain ensures the secure storage and management of medical data by utilizing cryptographic techniques and decentralized consensus mechanisms. Patient records, test results, treatment histories, and other healthcare information can be stored in an immutable ledger, providing a transparent and tamper-resistant system. Blockchain facilitates data sharing among healthcare providers while maintaining patient privacy and consent through smart contracts and permissioned access.[25]

2.2.2 Optimization of Clinical Trials

Blockchain technology can streamline clinical trial processes by ensuring transparency, integrity, and security of trial data. Smart contracts on blockchain platforms can automate tasks such as patient recruitment, consent management, and data monitoring, reducing administrative overhead and improving efficiency. Decentralized trial data storage enhances accessibility for researchers while maintaining data privacy and compliance with regulatory standards.[26]

2.2.3 Pharmaceutical Industry and the Fight Against Counterfeiting

Blockchain enables the creation of transparent and traceable supply chains in the pharmaceutical industry, allowing stakeholders to track the journey of drugs from manufacturing to distribution. Each transaction recorded on the blockchain provides a permanent and auditable record of a drug's provenance, reducing the risk of counterfeit products entering the market. Smart contracts can automate verification processes, ensuring that only genuine products are allowed to proceed along the supply chain.[27]

2.2.4 Blockchain in Medical Fraud

Blockchain technology can mitigate medical fraud by providing transparent and immutable records of healthcare transactions, making it difficult for bad actors to manipulate or falsify data. Smart contracts can enforce rules and permissions, ensuring that only authorized parties can access and modify sensitive information. Immutable audit trails enable quick detection and investigation of fraudulent activities, enhancing accountability and trust in the healthcare system.[28]

2.2.5 Electronic Medical Healthcare Records (EHR)

Blockchain-based EHR systems provide patients with greater control over their health data, allowing them to grant or revoke access to healthcare providers as needed. Interoperability between different healthcare systems is improved through standardized data formats and secure data exchange protocols on blockchain networks. Data integrity and security are enhanced through cryptographic hashing and distributed consensus mechanisms, reducing the risk of data breaches and unauthorized access.[29]

2.3 Cloud-computing bolockchain in healthcare data storage

2.3.1 Security and Privacy

Blockchain provides a decentralized and immutable ledger, ensuring that healthcare data stored on the cloud remains secure and tamper-proof. By encrypting data and storing it on a distributed network of nodes, blockchain enhances data security and protects patient privacy.[27][29]

2.3.2 Interoperability

Cloud computing facilitates the seamless exchange of healthcare data between different stakeholders such as hospitals, clinics, and research institutions. Blockchain can serve as a trusted platform for data exchange, enabling interoperability and ensuring data integrity across disparate systems. [28][30]

2.3.3 Data Access and Control

Blockchain-based solutions enable patients to have greater control over their healthcare data by granting them access rights and permissions. Smart contracts can automate data access management, ensuring that only authorized parties can view or modify sensitive information stored in the cloud.[8][9][31][32]

2.3.4 Regulatory Compliance

Compliance with healthcare regulations such as HIPAA (Health Insurance Portability and Accountability Act) can be facilitated through blockchain-based audit trails and transparent data management practices.[29][33]

2.3.5 Scalability and Performance

Cloud computing infrastructure provides the scalability needed to handle large volumes of healthcare data efficiently. Integration with blockchain technology ensures that as the volume of data grows, the system remains resilient and capable of maintaining performance levels.[28][30]

2.4 Blockchain Medical connectivity

Connectivity in the field health within the framework of activity is based on technical means which make the communication between all actors possible. These actors are mainly health professionals (Doctor, nurse, surgeon..) work in private practice or within establishment. These professionals are increasingly required to manage patient within databases and business tools (hospital information system, medico-technical equipment, practise management software...). We can see the different relationships between the professional's healthcare and the patient in the schema below:

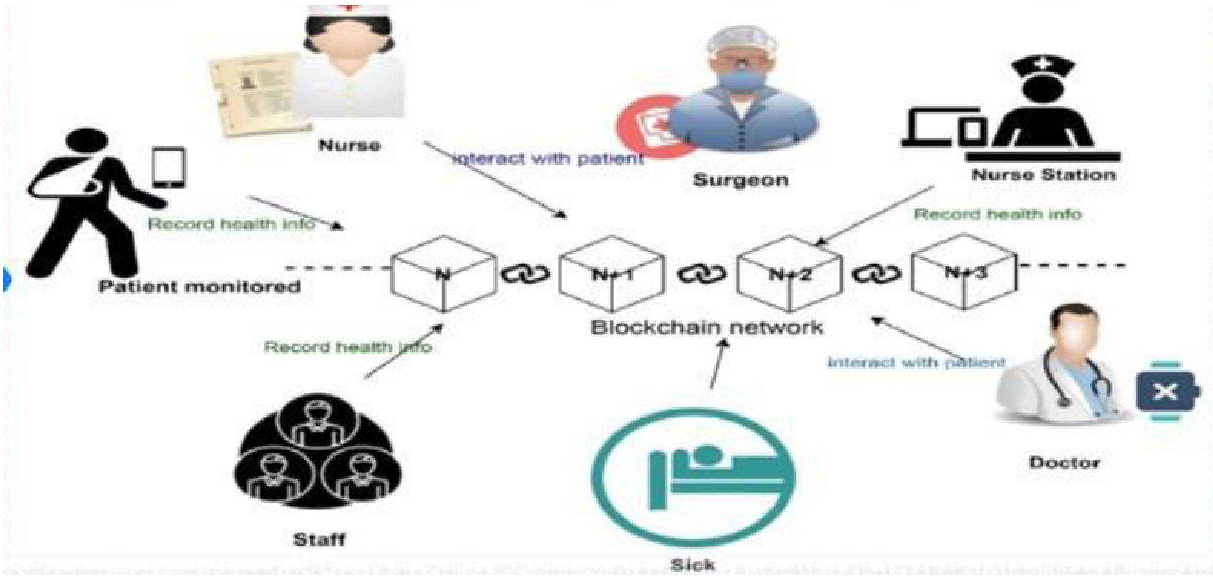


Figure 2.2: Blockchain healthcare data actors [1]

2.5 Blockchain healthcare advantages

2.5.1 Data Security and Integrity

Connectivity in the field health within the framework of activity is based on technical means which make the communication between all actors possible. These actors are mainly health professionals (Doctor, nurse, surgeon..) work in private practice or within establishment. These professionals are increasingly required to manage patient within databases and business tools (hospital information system, medico-technical equipment, practise management software...). We can see the different relationships between the professional's healthcare and the patient in the schema below:Blockchain's decentralized and immutable nature ensures that once data is recorded, it cannot be altered retroactively without the consensus of the network. This feature enhances the security and integrity of healthcare data, protecting it from tampering and unauthorized access.[34]

2.5.2 Interoperability

Blockchain can facilitate interoperability among different healthcare systems and stakeholders by providing a standardized, secure, and transparent platform for sharing data. This interoperability can improve care coordination, reduce administrative burdens, and enhance patient outcomes.[35]

2.5.3 Streamlined Processes

Through smart contracts and automated processes, blockchain can streamline administrative tasks such as claims processing, billing, and insurance verification. This can lead to cost savings, increased efficiency, and reduced errors in healthcare operations.[36]

2.5.4 Patient Empowerment

Blockchain enables patients to have greater control over their health data, allowing them to securely access and share their medical records with healthcare providers as needed. This empowerment can improve patient engagement, enable personalized care, and facilitate medical research participation.[37]

2.5.5 Enhanced Privacy

With blockchain, patients can maintain their privacy while sharing sensitive health information. By granting selective access to their data through cryptographic keys, patients can ensure confidentiality and control over who can view their medical history.[38]

2.6 Conclusion

In conclusion, healthcare blockchain applications offer a promising avenue for transforming the industry by enhancing data integrity, security, and interoperability. Through immutable ledger technology, blockchain ensures the integrity and transparency of patient records, facilitating secure data sharing among healthcare providers while maintaining patient privacy. Smart contracts enable automated processes, streamlining administrative tasks and reducing operational costs. Additionally, blockchain can revolutionize supply chain management, pharmaceutical authentication, and clinical trials, fostering innovation and trust within the healthcare ecosystem. However, challenges such as scalability, regulatory compliance, and interoperability standards must be addressed for widespread adoption. Despite these hurdles, the potential benefits of healthcare blockchain applications are undeniable, promising a future where healthcare delivery is more efficient, transparent, and patient-centric.

Chapter 3

Application Design

3.1 Introduction

The previous chapter highlighted the potential use cases of blockchain technology in the healthcare sector and its advantages over traditional systems. This chapter delves into the architecture and design of a blockchain-based application specifically tailored for managing electronic health records (EHR). The aim is to construct a robust, secure, and efficient system capable of addressing the challenges previously outlined, including the secure sharing of sensitive patient data among various stakeholders in the healthcare ecosystem.

3.1.1 Problem Statement

In the e-health sector, the paramount challenge is the secure and private sharing of sensitive patient data across a diverse network of stakeholders, including laboratories, healthcare providers, insurance companies, and patients themselves. This challenge encompasses not only the technical aspects of secure data transmission but also the broader issues of privacy, data integrity, and access controls.

3.1.2 Objective

The objective of this project is to design and implement a streamlined web-based application leveraging blockchain technology and smart contracts to manage electronic health records. The application aims to ensure that sensitive health data remains confidential while being readily accessible to authorized parties. The design will focus on:

- Identifying key stakeholders and their roles.
- Outlining the processes and interactions within the system.
- Describing the system architecture and the deployment of smart

contracts.

- Ensuring compliance with relevant healthcare regulations and privacy laws.

3.2 Smart contract

Smart contracts serve as the critical infrastructure in a blockchain-based electronic health records (EHR) system, ensuring secure, automatic handling of sensitive medical data. These contracts, embedded with self-executing codes, manage data interactions such as record creation, access, and modification, all while enforcing strict access controls and data privacy measures. For instance, smart contracts validate requests using cryptographic techniques to confirm the identity and authorization of users before processing transactions. They also log every data interaction to provide a secure, immutable audit trail, essential for compliance and transparency. To maintain privacy and security, the contracts handle only encrypted data identifiers, storing actual health records off-chain. Furthermore, the code is optimized for minimal computational load to mitigate the high costs associated with transactions on a Proof of Work (PoW) blockchain, enhancing overall system efficiency and scalability. Through these mechanisms, smart contracts facilitate a robust, secure framework for EHR management, balancing blockchain's transparency with the critical need for confidentiality in healthcare data handling.

3.3 Global Architecture

3.3.1 Global System Architecture

A private Blockchain will be used as the main architecture, only verified nodes will be allowed to participate and hold a copy of the

Blockchain.

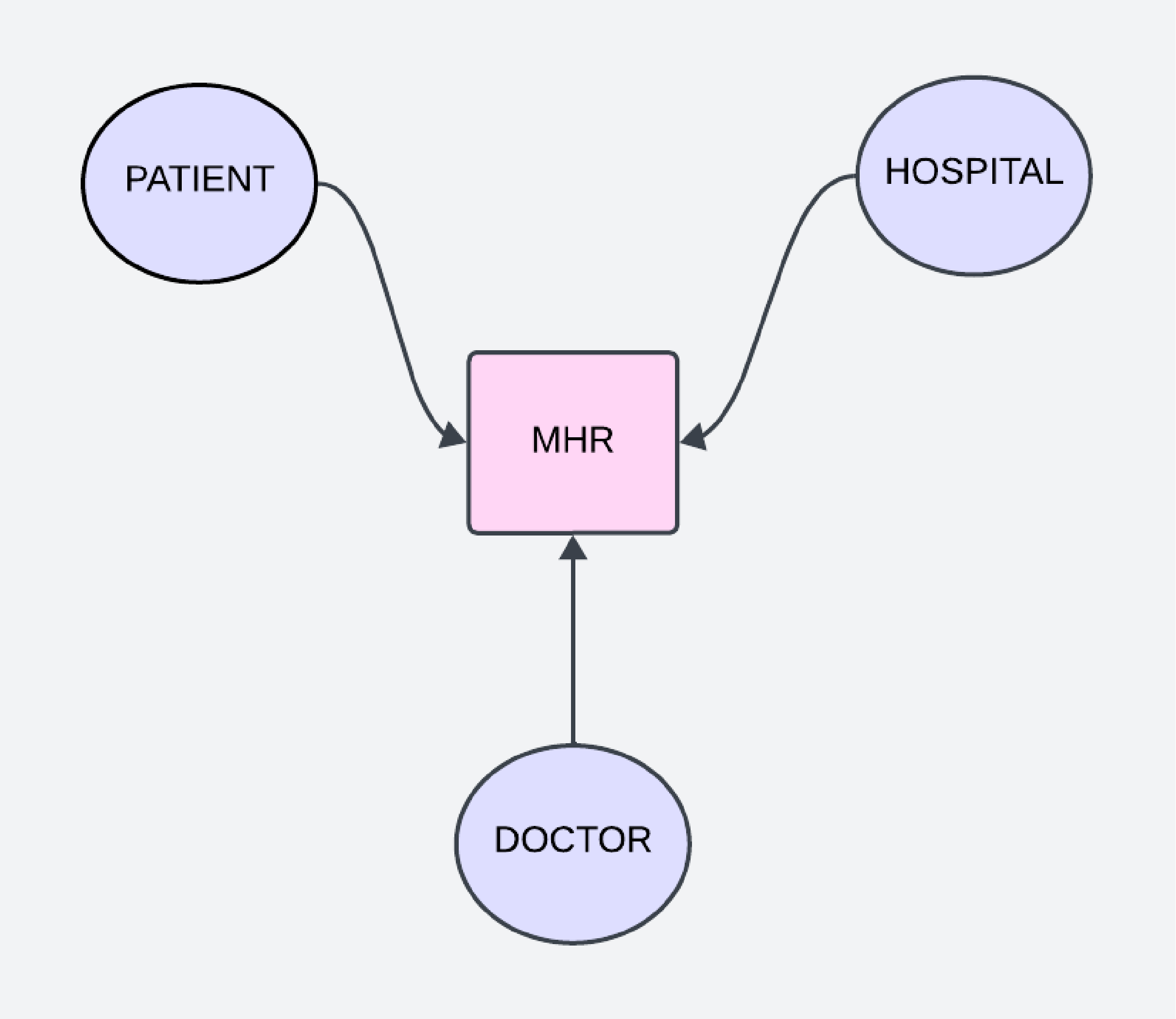


Figure 3.1: Global System Architecture.

3.3.2 Global Network Architecture

The figure 3.2 displays the Global network architecture, which shows the relation that allows the front-end clients to utilize the block-chain back-end through the smart contract, in this process the smart contract acts as a controller.

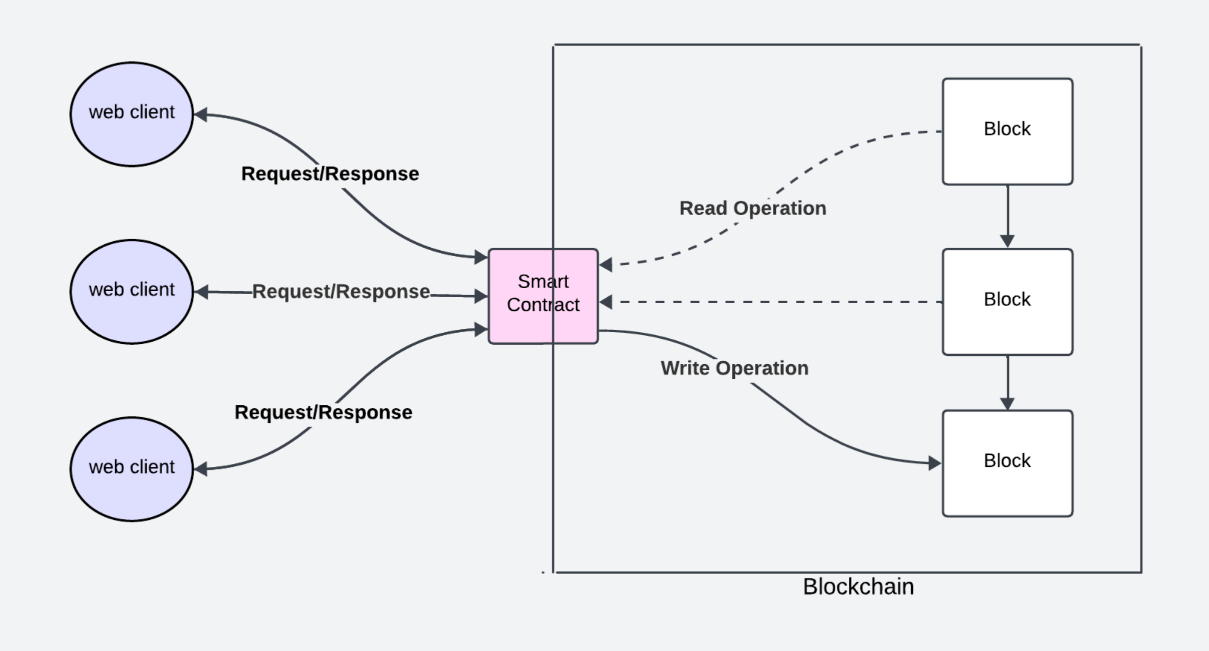


Figure 3.2: Global Network Architecture.

3.3.3 Detailed Network Architecture

The figure 3.3 illustrates the comprehensive network architecture, providing in-depth insights into the interaction between the Front-end and Back-end via smart contracts, alongside the utilization of Truffle for compiling and deploying these smart contracts. Upon compiling the smart contracts using Truffle and its Solidity compiler (Solc), they are then deployed using Truffle, which stores them as machine code on the blockchain through a blockchain transaction. Additionally, with the incorporation of Hyperledger Besu, the smart contracts are now also deployed and stored within the Hyperledger Besu network, enhancing the resilience and privacy of the system. This integration enables interaction with the smart contracts contained within the blockchain (Back-end) using the JavaScript Web3.js library (Front-end), thereby facilitating seamless communication and functionality across the entire network architecture.

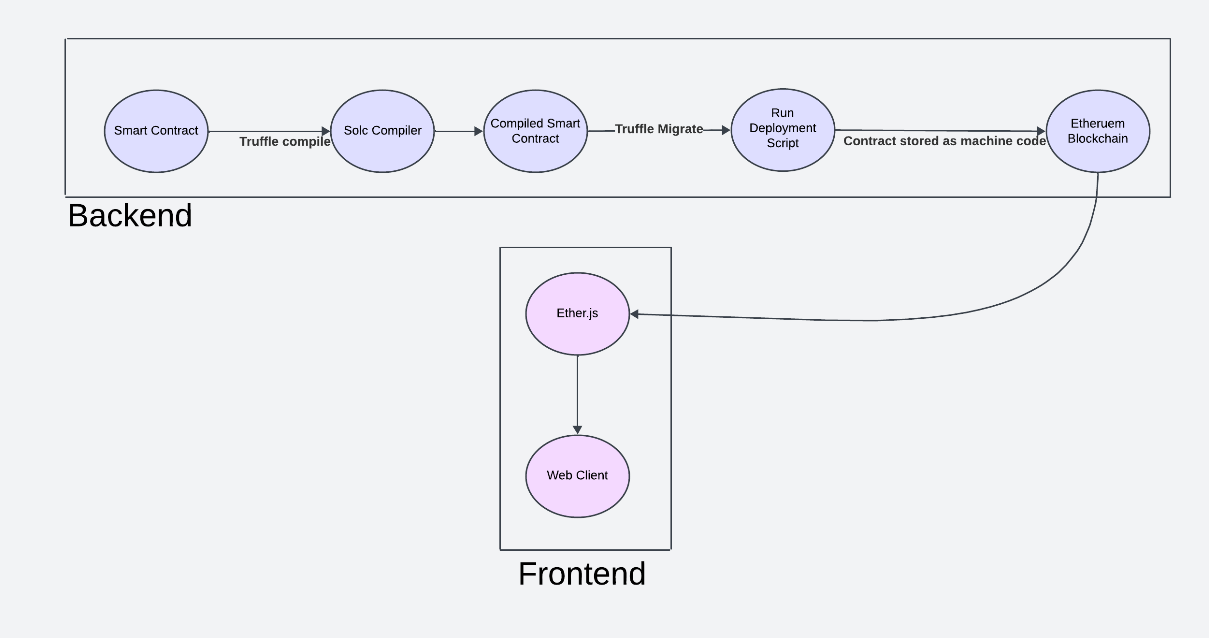


Figure 3.3: Detailed Network Architecture.

3.3.4 Choosing document storage method

For a healthcare application, it is critical to manage two distinct categories of data:

- Lightweight Data: This category encompasses both identification details and basic medical records of patients. Since these items are compact and occupy minimal storage space, they can be directly integrated into the blockchain. This placement not only ensures accessibility but also enhances data security.
- Heavyweight Data: This includes substantial files such as images, videos, and extensive text documents. Due to their significant storage demands, these files are unsuitable for blockchain storage because it would be prohibitively costly and inefficient. Thus, alternative external storage solutions are necessary.

Given that document storage is a core functionality of the application, it is imperative that the chosen method is secure, rapid, and user-friendly. Here are two recommended options to consider:

- IPFS Server: The InterPlanetary File System offers a decentralized protocol and network for data storage and sharing across a peer-to-peer file system. While this method is ideal for decentralized applications, establishing a large user network is challenging without resorting to a public IPFS server.
- SQL Server: This traditional method involves using an SQL server for file storage. It is relatively straightforward to implement and manage. However, it suffers from the critical downside of centralized storage, which could be a potential vulnerability in terms of data privacy and security.

3.3.4.1 Storage method Architecture with IPFS server

Among the proposed solutions, employing an IPFS server is deemed the most appropriate for the application due to its alignment with the principles of decentralization, a key advantage in scenarios requiring distributed access and storage.

Challenges with SQL Server: Utilizing an SQL server reintroduces centralization, consolidating control over the data with a single entity. This centralization conflicts with the application's objective to maintain transparency and independence in data handling.

- Document Upload Process :
  - Initiation by Health Worker: The user (health worker) inputs details of the document such as title and date and selects the document for upload.
  - Transmission to IPFS Server: Upon user confirmation, the document is uploaded from the web client to the IPFS server using the IPFS.js JavaScript library.

- Blockchain Integration: The server returns a unique hash of the file, serving as an identifier. This hash, along with the previously entered document details, is recorded on the blockchain, ensuring its availability and integrity.
- Visualization: The architecture of this process is depicted in Figure 3.4.

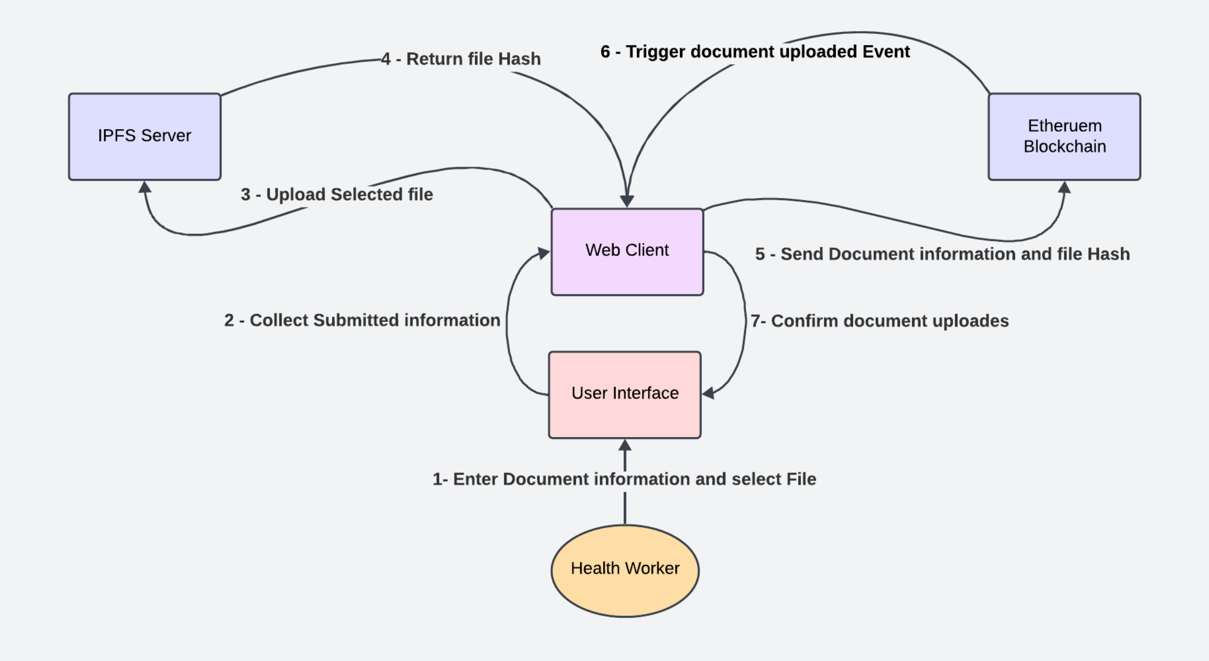

IPFS Server
Etheruem Blockchain
4 - Return file Hash
6 - Trigger document uploaded Event
3 - Upload Selected file
Web Client
5 - Send Document information and file Hash
2 - Collect Submitted information
7- Confirm document uploades
User Interface
1- Enter Document information and select File
Health Worker

Figure 3.4: Document Upload Method

- Document Download Process :
  - Selection by Health Worker: The user selects the desired document from a blockchain-stored index.
  - Retrieval from IPFS Server: The web client retrieves the file's hash from the blockchain and requests the actual file from the IPFS server using IPFS.js.
  - Display to User: Once retrieved, the document is displayed to the user along with associated metadata. This step is graphically represented in Figure 3.5.

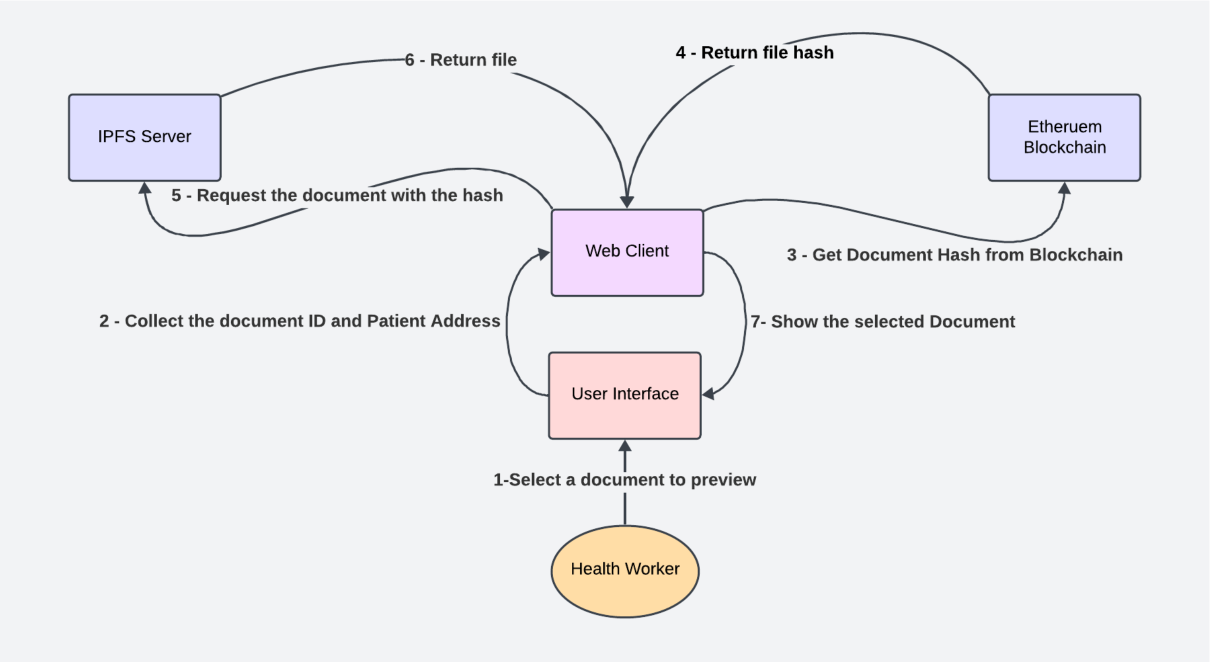

6 - Return file
4 - Return file hash
IPFS Server
Etheruem Blockchain
5 - Request the document with the hash
Web Client
3 - Get Document Hash from Blockchain
2 - Collect the document ID and Patient Address
7- Show the selected Document
User Interface
1-Select a document to preview
Health Worker

Figure 3.5: Document Storage Method

3.3.5 System actors

3.3.5.1 Admin Owner

- Role: Sole administrator and system organizer.
- Responsibilities:
  - Manages all administrative tasks and settings across the system.
  - Grants access permissions to hospitals and controls the operations of various healthcare workers.
  - Responsible for adding hospital accounts to the system.

3.3.5.2 Patients

- Role: Primary users of the system receiving medical care.
- Responsibilities:
  - Access and manage their own medical records.
  - Grant access permissions to doctors or other healthcare workers for viewing and updating their health records.

3.3.5.3 Healthcare Workers

- Doctors:
  - Responsibilities:
    - Add and update medical information in patients' records.
    - Access patient data as permitted by the patient.
- Hospital:
  - Responsibilities:
    - Manage doctors and staff within the hospital.
    - Access and view patient data for authorized cases.

3.3.6 Global use case

The figure 3.6 represents the general use case diagram of the application, it shows every system user and the actions they can enact.

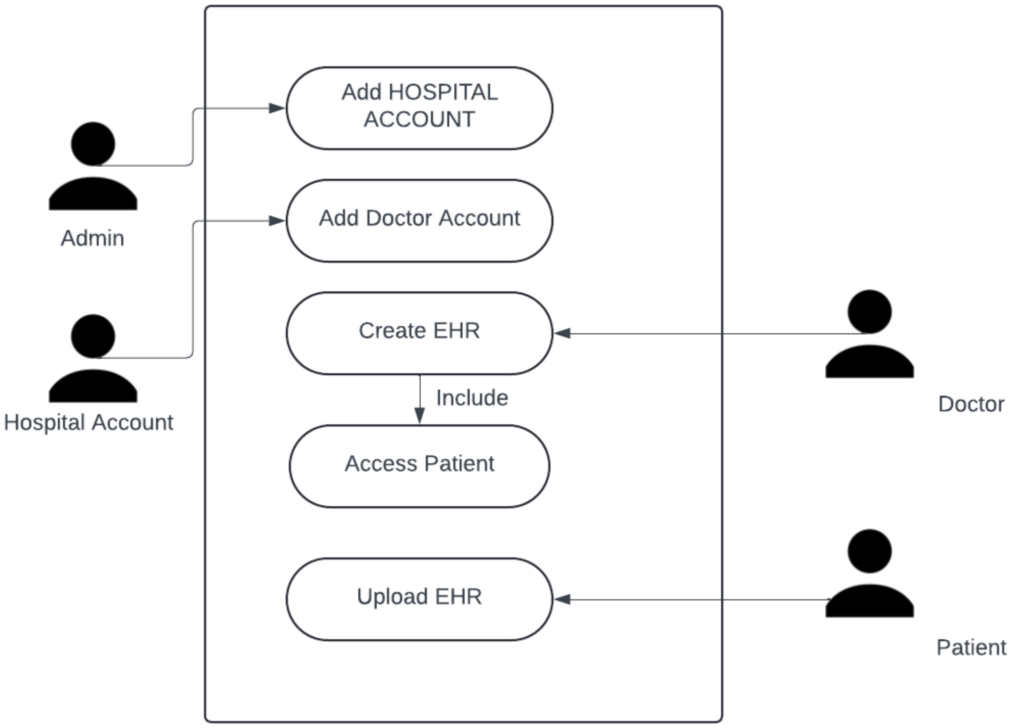


Figure 3.6: Global Use Case Diagram.

3.4 Detailed view

3.4.1 Use Case diagrams

3.4.1.1 Admin Owner (Administrator)

This admin is fixed and doesn't change. Their job is straightforward: they can only add new hospitals to the app. This helps keep the app organized and ensures that users can easily find and access the hospitals they need.

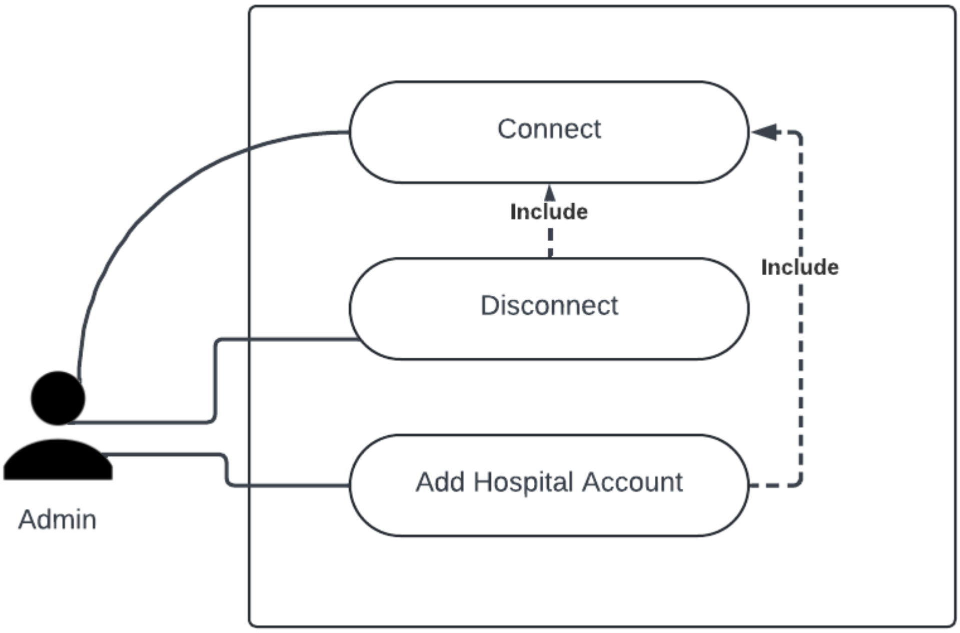


Figure 3.7: Admin Use Case Diagram.

3.4.1.2 Visitor

The visitor is not really an actor in the application, so to become a part of it he have to join by sending registration request. The next 3.8 figure will present the Visitor use case diagram to give more clear picture.

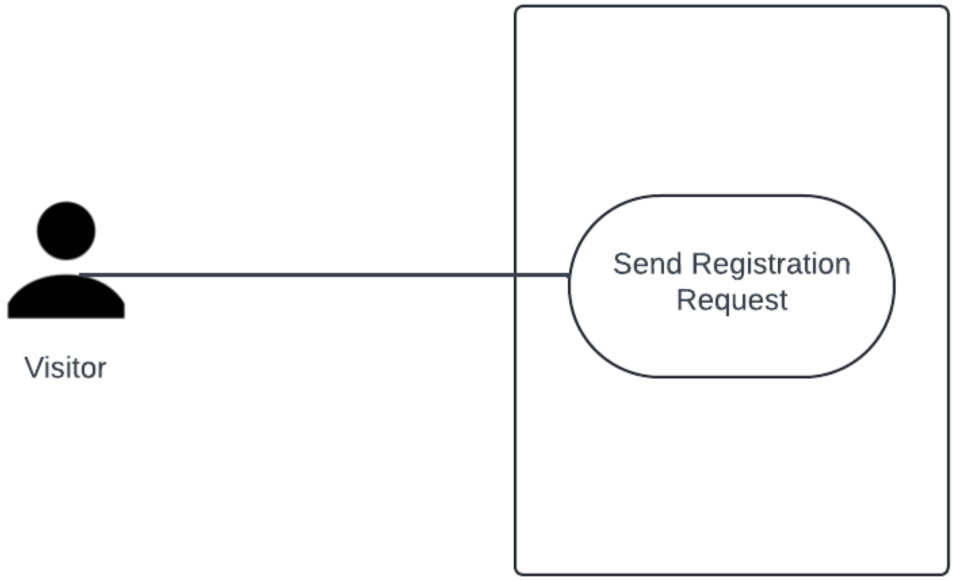


Figure 3.8: Visitor Use Case Diagram.

3.4.1.3 Doctor

The Healthcare worker is the user that can manage the records of the patients. he will able to consult, add and modify on the health records of patients to other health workers. The 3.9 figure next will show the use case diagram of the healthcare worker in the app.

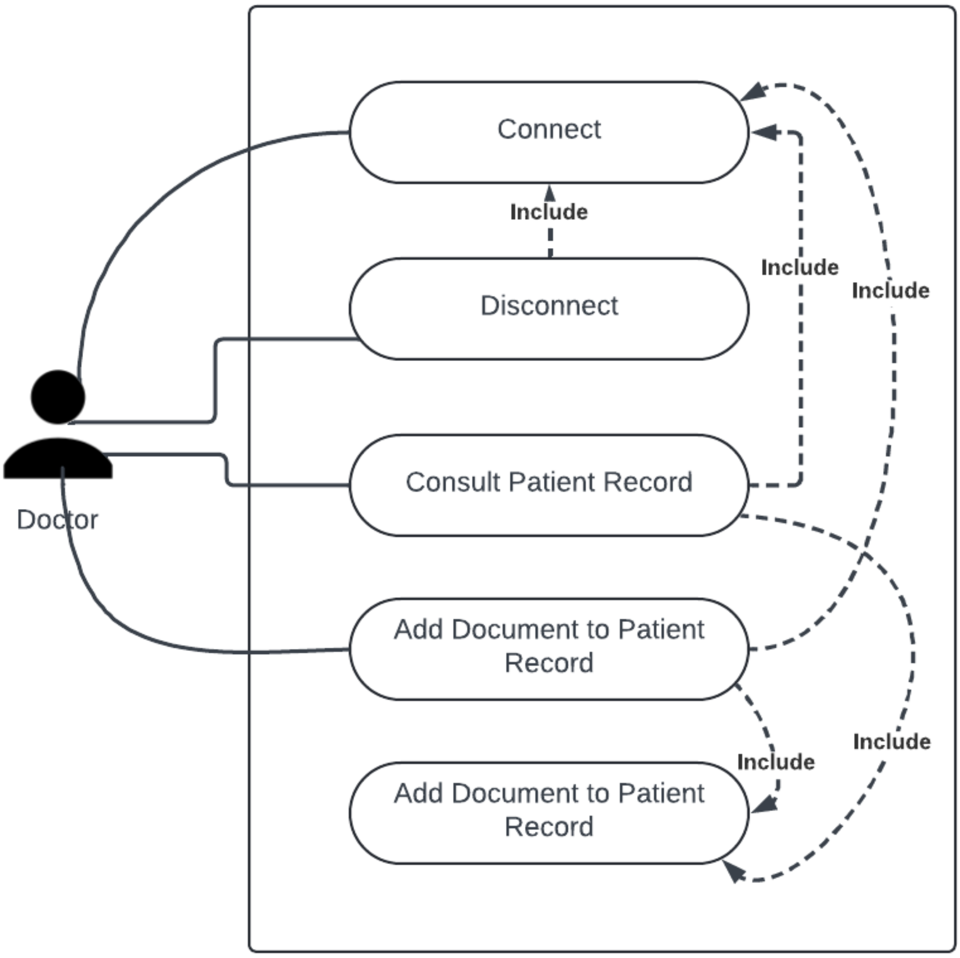


Figure 3.9: Health Worker Use Case Diagram.

3.4.1.4 Patient

The patient will be able to complete simple tasks, such as consulting his own records and edit his own contact information. The next 3.10 figure will present the patient use case diagram to give more clear picture.

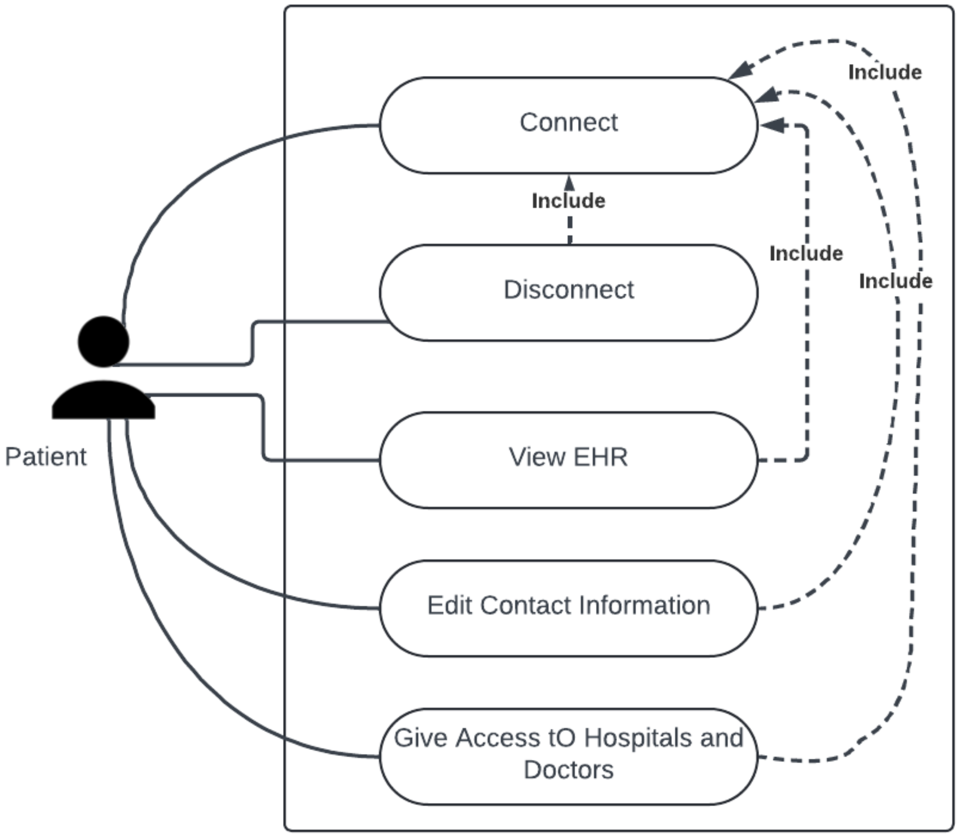


Figure 3.10: Patient Use Case Diagram.

3.4.2 Sequence Diagram

3.4.2.1 Admin Register Hospital Account

the figure 3.11 represents the process there is used to register a new Hospital Account by the admin.

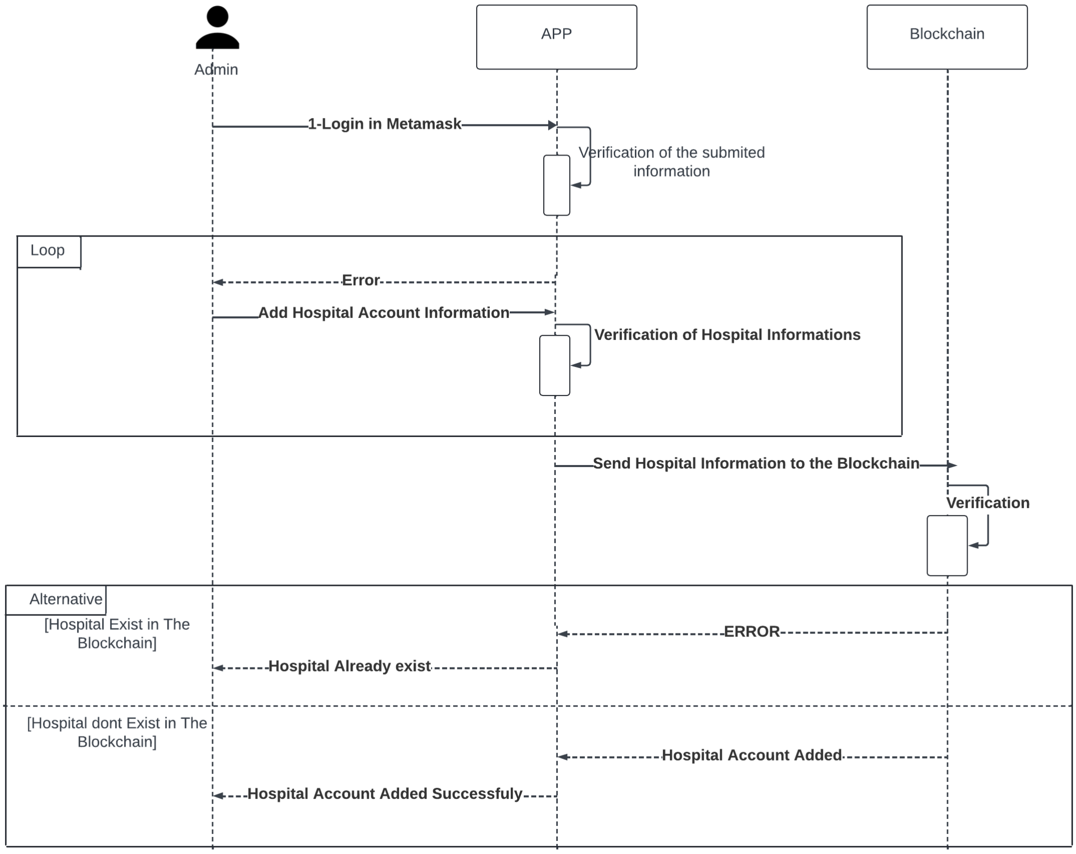

Admin
APP
Blockchain
1-Login in Metamask
Verification of the submited information
Loop
Error
Add Hospital Account Information
Verification of Hospital Informations
Send Hospital Information to the Blockchain
Verification
Alternative
[Hospital Exist in The Blockchain]
ERROR
Hospital Already exist
[Hospital dont Exist in The Blockchain]
Hospital Account Added
Hospital Account Added Successfuly

Figure 3.11: Sequence diagram of Admin

3.4.2.2 Patient Consult Record

the figure 3.12 represents the process the patient takes in order to view his own record.

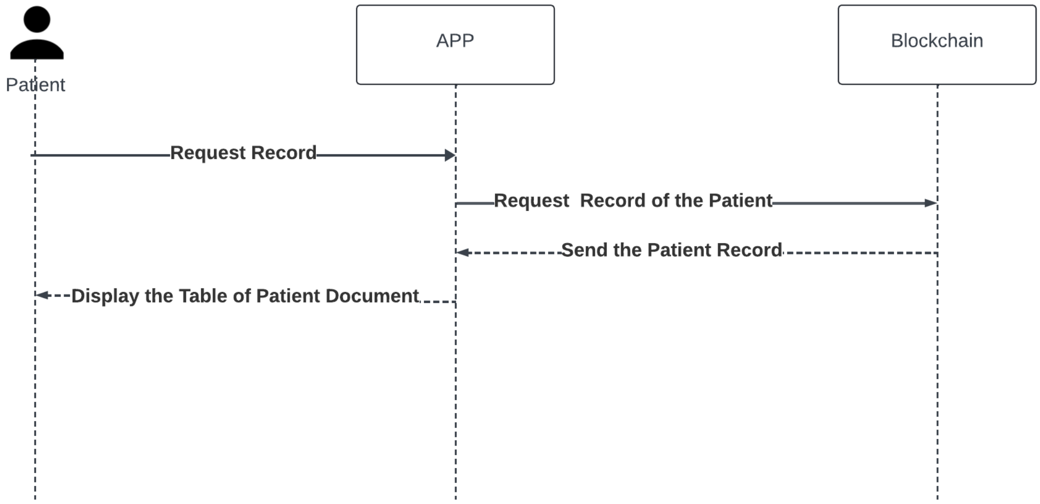

Patient
APP
Blockchain
Request Record
Request Record of the Patient
Send the Patient Record
Display the Table of Patient Document

Figure 3.12: Sequence diagram of Patient Consult Record.

3.4.2.3 Health Worker add document

the figure 3.13 shows the operations the Health Worker performs in order to add a document to a patient record.

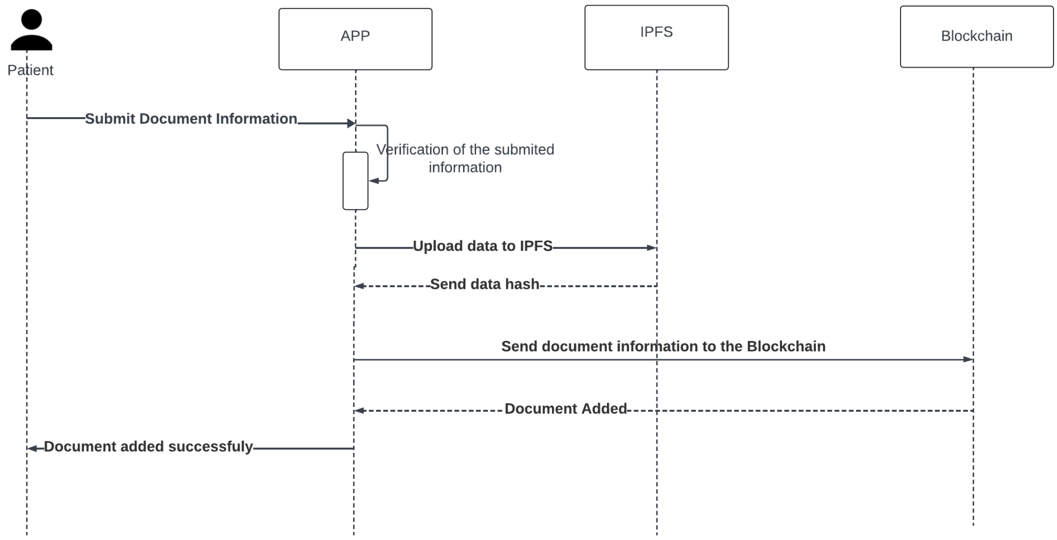

Patient
APP
IPFS
Blockchain
Submit Document Information
Verification of the submited information
Upload data to IPFS
Send data hash
Send document information to the Blockchain
Document Added
Document added successfuly

Figure 3.13: Sequence diagram of Health Worker add document.

3.5 Conclusion

This section has provided a comprehensive overview of the application's architecture, featuring UML diagrams for both use cases and sequence flows. Additionally, it included detailed visual representations of the application's structure and networking components, offering a thorough insight into the application's design. In the following chapter, we will explore the technologies and tools employed during the development process, accompanied by a presentation of the technology stack and visual screenshots of the implemented application.

Chapter 4

Realization and implementation of The applications

4.1 Introduction

The previous chapter covered the theoretical aspects of the application, including the underlying logic and diagrams. This chapter focuses on the practical implementation of the system, detailing the technology stack used, the development tools employed, and providing screenshots of the completed application.

4.2 The Hardware

This application was realized using a single machine with the following specifications:

- CPU: Intel i5 (6th Generation)
- RAM: 16GB
- Operating System: Debian 12

4.3 Software and programming languages used

The application development was divided into backend and frontend components to ensure a more organized and efficient workflow. Multiple programming languages and technologies were employed to build the application. During the initial stages of development, selecting the most suitable approaches for the project was challenging. The plethora of frontend frameworks and storage options made finding the optimal combination of methods quite overwhelming.

4.3.1 Visual Studio Code

Visual Studio Code (VS Code) is a free, open-source code editor developed by Microsoft for Windows, macOS, and Linux. It is known for its speed, lightweight design, and powerful features, including intelligent code completion (IntelliSense), integrated debugging, a built-in terminal, and seamless Git integration. VS Code supports a wide range of extensions and themes, making it highly customizable to suit various development needs. Its versatility and rich feature set make it a popular choice among developers for coding, debugging, and version control.

Figure 4.1: Visual Studio Code (VS Code).

4.3.2 Truffle

Truffle is a development framework for Ethereum, the popular blockchain platform for decentralized applications (dApps). It provides a suite of tools for smart contract development, testing, and deployment, streamlining the workflow for blockchain developers. Key features of Truffle include automated contract testing, network management for deploying to various Ethereum networks, and a built-in script runner that executes JavaScript to perform complex deployments or run scripts within a Truffle environment. By simplifying the development process, Truffle helps developers build and manage blockchain applications more efficiently.

Figure 4.2: Truffle.

4.3.3 Node.js

Node.js is an open-source, cross-platform JavaScript runtime environment built on Chrome's V8 JavaScript engine. It allows developers to run JavaScript code outside of a web browser, making it possible to build scalable and high-performance server-side applications. Node.js uses an event-driven, non-blocking I/O model, which makes it lightweight and efficient, particularly for handling concurrent connections and asynchronous operations. With its vast ecosystem of npm (Node Package Manager) modules, developers can access a wide range of libraries and tools to streamline the development process. Node.js is widely used for building web servers, APIs, microservices, real-time applications, and more. Its flexibility, performance, and large community support make it a popular choice for modern web development.

Figure 4.3: Node.js.

The first dependency needed for Node.js development is the Node Package Manager (NPM) and Interplanetary File System

(IPFS), which comes bundled with Node.js.

- NPM: NPM is the world's largest software registry. Open-source developers from every continent use npm to share and borrow packages, and many organizations use npm to manage private development as well. It is used to adapt packages of code for applications, incorporate packages as they are, download standalone tools ready for immediate use, manage multiple versions of code and dependencies, and much more.
- IPFS: IPFS is a peer-to-peer (p2p) storage network. Content is accessible through peers located anywhere in the world, which might relay information, store it, or do both. IPFS knows how to find what you ask for using its content address rather than its location.

4.3.4 Hyperledger Besu

Hyperledger Besu is an open-source Ethereum client tailored for enterprise-grade blockchain applications. It offers a versatile solution for both public and private network setups, enabling organizations to create permissioned blockchain networks with controlled access and enhanced privacy features. With its focus on scalability, interoperability, and enterprise support, Hyperledger Besu empowers businesses to build secure and scalable blockchain solutions that meet their specific requirements. Its flexible permissioning system and privacy features make it an ideal choice for confidential and regulated environments, providing organizations with a reliable foundation for deploying blockchain-based applications.

Figure 4.4: Hyperledger Besu.

4.3.5 React JS

React.js, commonly known as React, is a JavaScript library developed by Facebook for building user interfaces. It adopts a component-based architecture, allowing developers to create reusable UI components that manage their own state. With its efficient virtual DOM implementation and declarative syntax, React simplifies the process of building and maintaining complex user interfaces for web applications. Its popularity, extensive ecosystem, and large community support make React.js a preferred choice for front-end development.

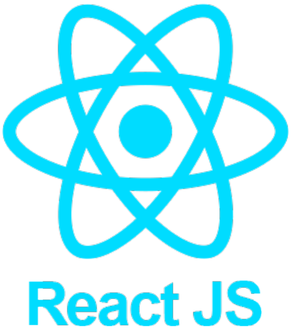


Figure 4.5: React JS.

4.4 MetaMask

MetaMask is a browser extension and mobile application that functions as a cryptocurrency wallet and gateway to the decentralized web. Initially designed for Ethereum, it now supports multiple blockchains and decentralized applications (dApps). MetaMask enables users to manage their digital assets securely, interact with smart contracts, and access decentralized applications directly from their web browser. With its user-friendly interface and seamless integration with popular browsers, MetaMask simplifies the experience of engaging with blockchain technology, making it more accessible to a broader audience.

Figure 4.6: MetaMask.

4.4.1 Preparing the environment

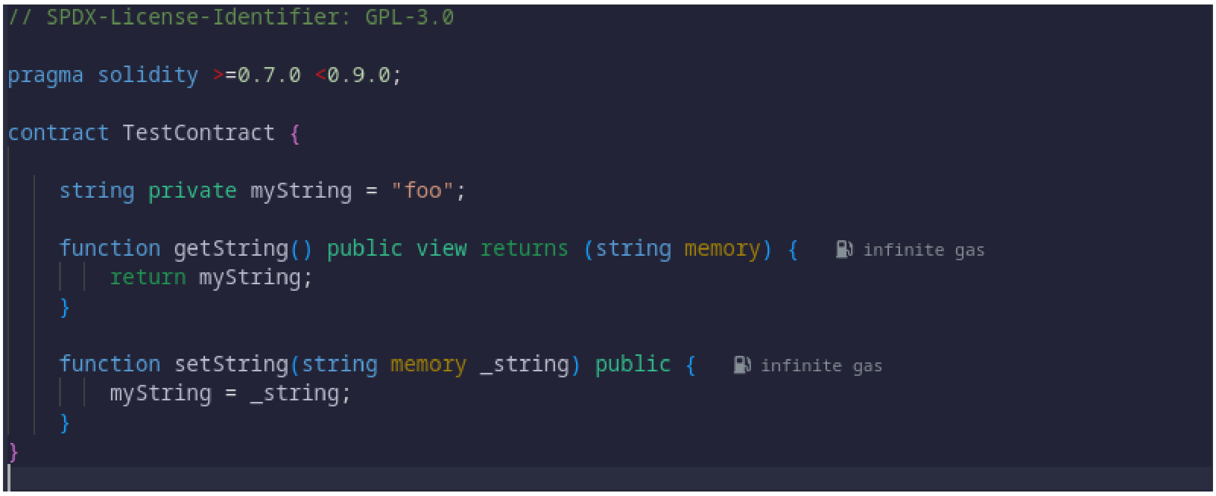
This section presents the description of the general steps needed in order to build a dApp.

4.4.1.1 Installing requirements

- node.js: Can be downloaded and installed from the official Web Site
- Truffle: Can be installed with npm using the command: npm i -g truffle
- Hyperledger fabric: Can be downloaded and installed from the official Web Site

4.4.1.2 Writing the Smart Contracts

Smart Contracts function as the core intelligence of any dApp, executing the desired behavior based on specific inputs. A Smart Contract must be succinct, efficient, and ensure the reliability of the expected outputs. Figure 4.11 illustrates a straightforward example of a Smart Contract named TestContract. This contract includes a global string variable, myString, and features two functions: one that assigns an input value to myString, and another that retrieves the value of myString.

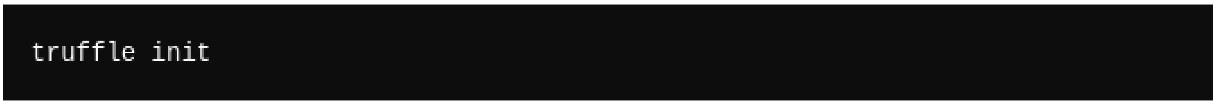


```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.7.0 <0.9.0;

contract TestContract {

    string private myString = "foo";

    function getString() public view returns (string memory) {    infinite gas
        return myString;
    }

    function setString(string memory _string) public {    infinite gas
        myString = _string;
    }
}
```

Figure 4.7: Simple Contract Example.

4.4.1.3 Project Setup

- Initialize a Truffle project: Initialized a Truffle project with:

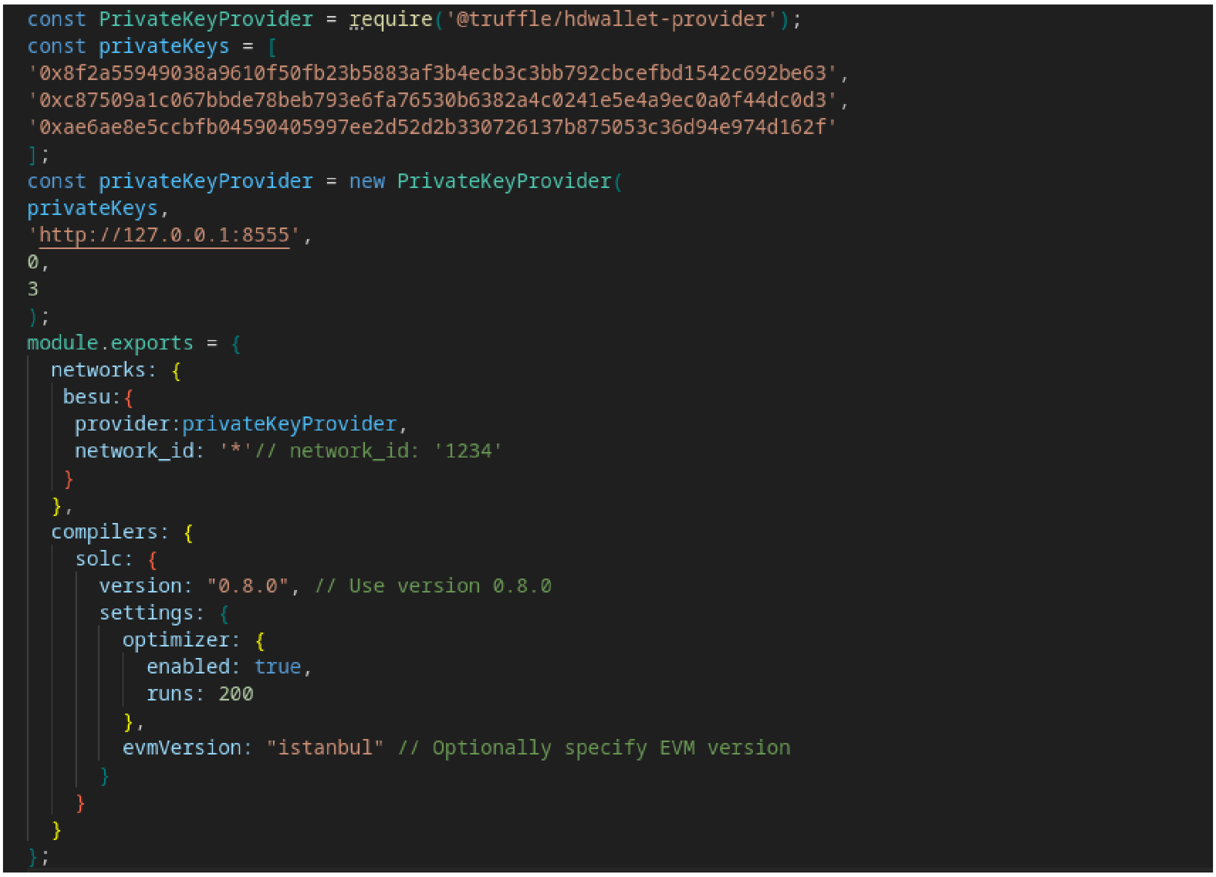


```
truffle init
```

Figure 4.8: Initialize a Truffle project.

- Create Project Structure: Create the contracts directory if it doesn't exist and add your Solidity contracts there and place the `1_deploy_contracts.js` file inside the `migrations` directory.
- Configure the Network: Open truffle-config.js Ensure your network configuration is set correctly. The provided configuration

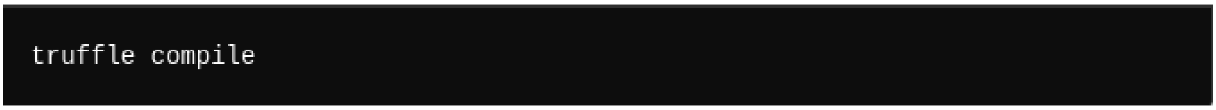
is for a local Besu network:



```
const PrivateKeyProvider = require('@truffle/hdwallet-provider');
const privateKeys = [
'0x8f2a55949038a9610f50fb23b5883af3b4ecb3c3bb792cbcefbd1542c692be63',
'0xc87509a1c067bbde78beb793e6fa76530b6382a4c0241e5e4a9ec0a0f44dc0d3',
'0xae6ae8e5ccbfb04590405997ee2d52d2b330726137b875053c36d94e974d162f'
];
const privateKeyProvider = new PrivateKeyProvider(
privateKeys,
'http://127.0.0.1:8555',
0,
3
);
module.exports = {
  networks: {
   besu:{
    provider:privateKeyProvider,
    network_id: '*'// network_id: '1234'
   }
  },
  compilers: {
    solc: {
      version: "0.8.0", // Use version 0.8.0
      settings: {
        optimizer: {
          enabled: true,
          runs: 200
        },
        evmVersion: "istanbul" // Optionally specify EVM version
      }
    }
  }
};
```

Figure 4.9: Configure the Network.

- Compile Contracts: This command will compile the Solidity contracts found in the contracts directory and create the necessary artifacts in the build/contracts directory.

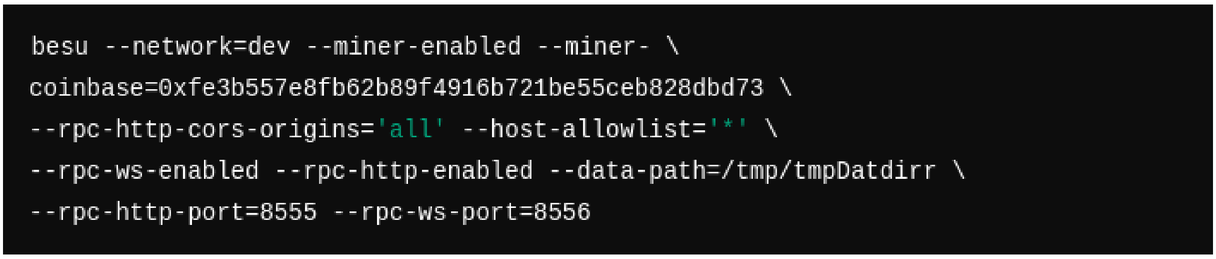


```
truffle compile
```

Figure 4.10: Compile Contracts.

4.4.1.4 Running the Blockchain

- Start Your Local Blockchain: Start a local Ethereum blockchain using Hyperledger Besu, you can run:

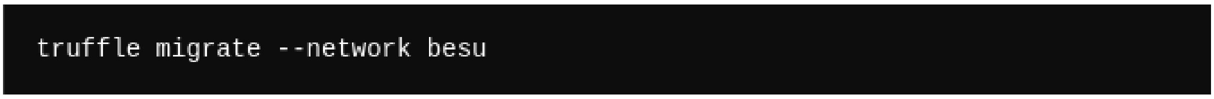


```
besu --network=dev --miner-enabled --miner- \
coinbase=0xfe3b557e8fb62b89f4916b721be55ceb828dbd73 \
--rpc-http-cors-origins='all' --host-allowlist='*' \
--rpc-ws-enabled --rpc-http-enabled --data-path=/tmp/tmpDatdirr \
--rpc-http-port=8555 --rpc-ws-port=8556
```

Figure 4.11: Start Local Blockchain.

4.4.1.5 Deploying the Smart Contracts

After Writing a smart contract, the next step is to deploy it to the blockchain, but before that,compiling it is necessary, Fortunately, truffle condenses these two procedures into one command: Note:deploying a smart contract is represented in the blockchain as a transaction.

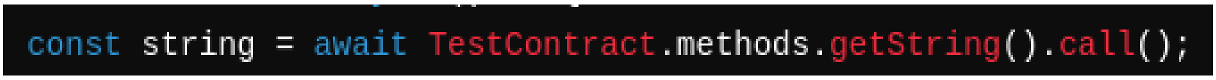


```
truffle migrate --network besu
```

Figure 4.12: Deploying the Smart Contracts.

4.4.1.6 Interacting with The dApp

Now that the smart contract is deployed, Interacting with it from the front-end is possible, JavaScript is used for this purpose, the Web3.js library allows the web client to call the smart contract functions. the figure shows an example of calling the function getString() from the contract that previously seen TestContract.

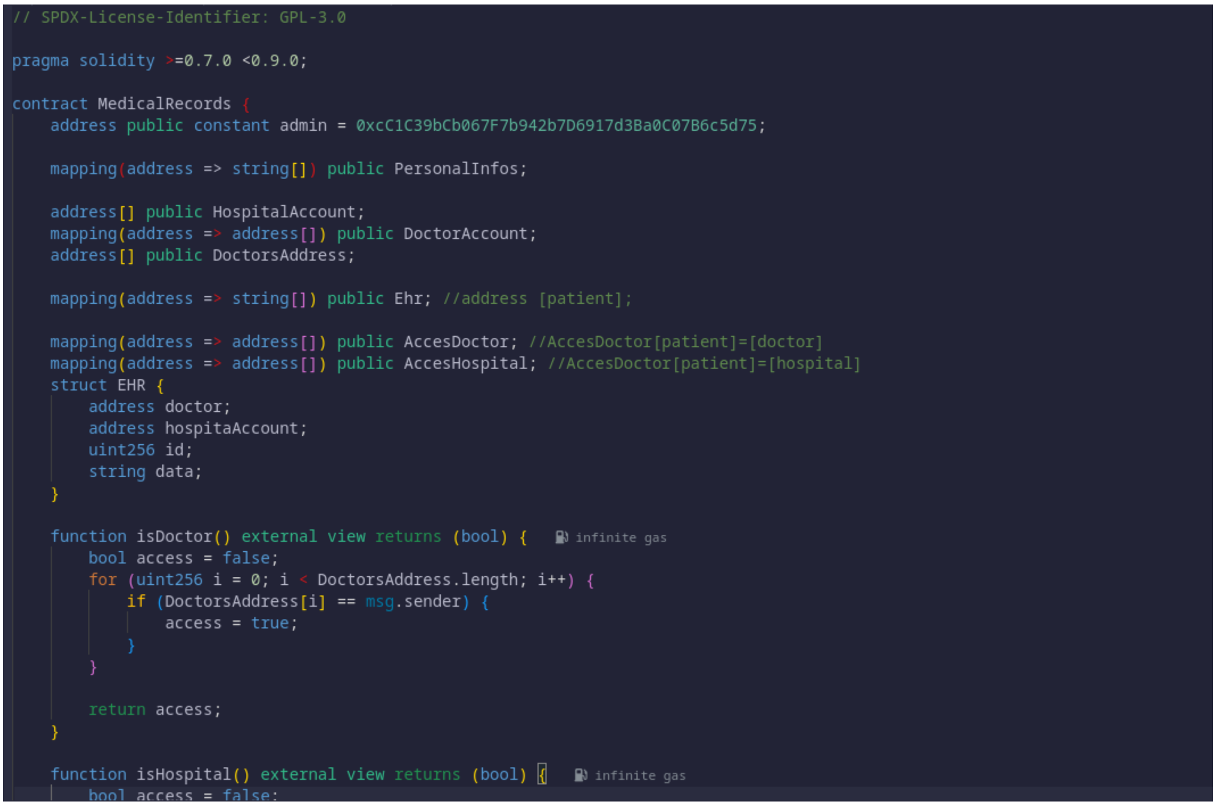


```
const string = await TestContract.methods.getString().call();
```

Figure 4.13: JS function call example.

4.5 The System Smart contracts

The MedicalRecords contract securely manages electronic health records (EHRs), enabling authorized entities to create, modify, and access patient data with utmost privacy and integrity.



```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.7.0 <0.9.0;

contract MedicalRecords {
    address public constant admin = 0xcC1C39bCb067F7b942b7D6917d3Ba0C07B6c5d75;

    mapping(address => string[]) public PersonalInfos;

    address[] public HospitalAccount;
    mapping(address => address[]) public DoctorAccount;
    address[] public DoctorsAddress;

    mapping(address => string[]) public Ehr; //address [patient];

    mapping(address => address[]) public AccesDoctor; //AccesDoctor[patient]=[doctor]
    mapping(address => address[]) public AccesHospital; //AccesDoctor[patient]=[hospital]
    struct EHR {
        address doctor;
        address hospitaAccount;
        uint256 id;
        string data;
    }

    function isDoctor() external view returns (bool) {   infinite gas
        bool access = false;
        for (uint256 i = 0; i < DoctorsAddress.length; i++) {
            if (DoctorsAddress[i] == msg.sender) {
                access = true;
            }
        }

        return access;
    }

    function isHospital() external view returns (bool) {   infinite gas
        bool access = false;
```

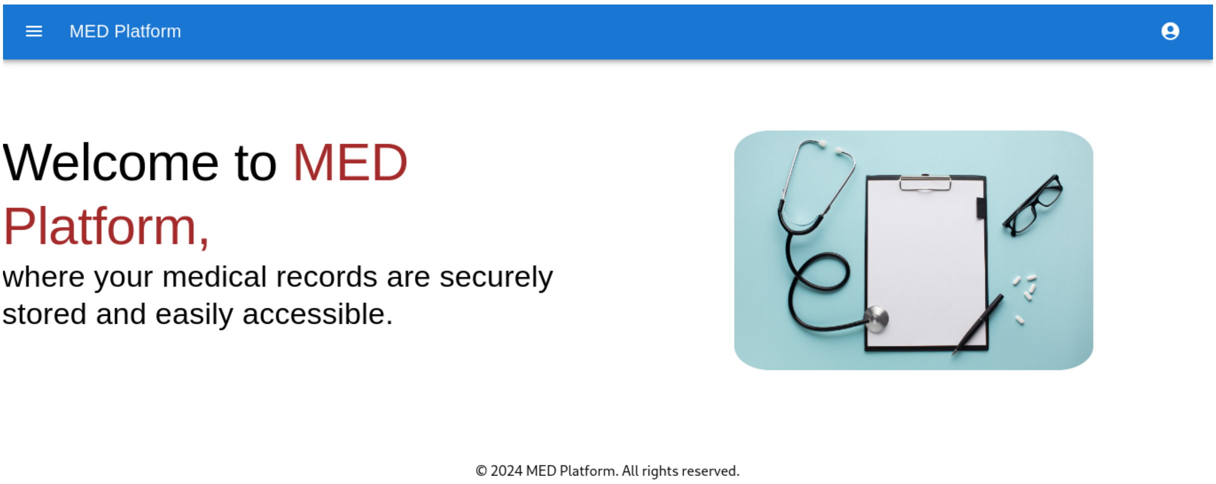
Figure 4.14: MedicalRecords.sol preview.

4.6 The System Interfaces

This part, presents some interfaces, starting with the homepage

4.6.1 Homepage

The homepage of the DAPP serves as the main entry point for users. It provides an overview of the application's functionalities and offers easy navigation to different sections. Users can log in, access different modules, and find general information about the DAPP.



Welcome to MED Platform,

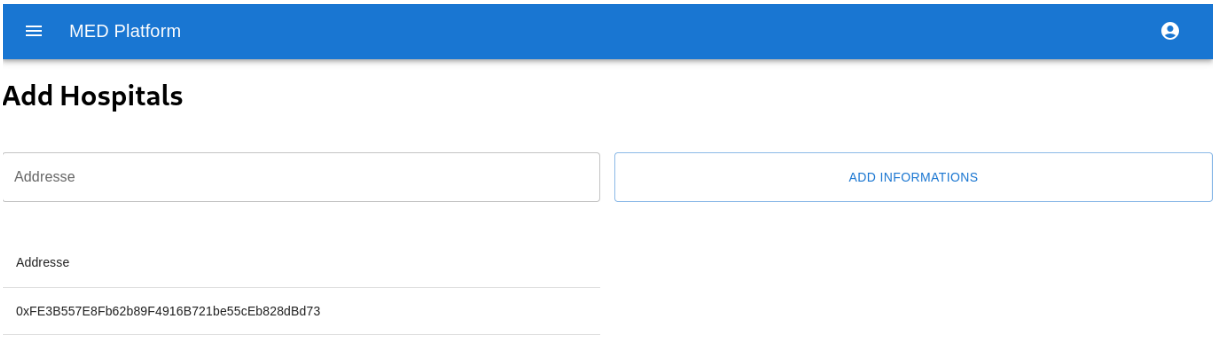
where your medical records are securely stored and easily accessible.

© 2024 MED Platform. All rights reserved.

Figure 4.15: Homepage interface.

4.6.2 Add Hospital

The "Add Hospital" page is designed for administrators. It allows an admin to create and manage hospital accounts within the DAPP. By adding a hospital, the admin enables that institution to manage its doctors and patient records within the system. This ensures that only authorized hospitals can access and modify data.



Add Hospitals

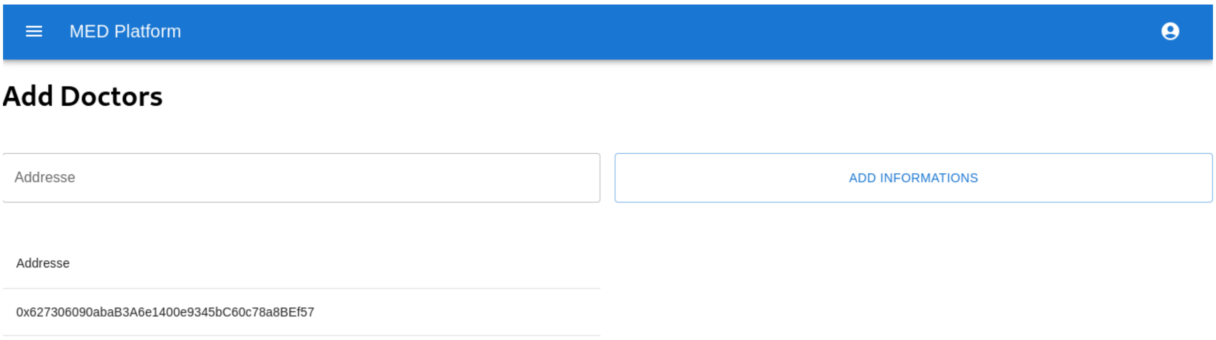
Addresse

Addresse
0xFE3B557E8Fb62b89F4916B721be55cEb828dBd73

Figure 4.16: Add Hospital interface.

4.6.3 Add Doctors

The "Add Doctors" page is accessible to hospital administrators. This page allows a hospital admin to add and manage doctor accounts associated with their hospital. By adding doctors, hospitals can ensure that their medical staff have the necessary access to create and manage patient EHRs (Electronic Health Records).



Add Doctors

Addresse
0x627306090abaB3A6e1400e9345bC60c78a8BEf57

Figure 4.17: Add Doctors interface.

4.6.4 Create EHR

The "Create EHR" page is designed for doctors. This functionality allows a doctor to create a new Electronic Health Record for a patient. The doctor can enter comprehensive medical information, including medical history, current medications, physical examination findings, assessment, and lab results. This ensures that patient information is accurately recorded and easily accessible.

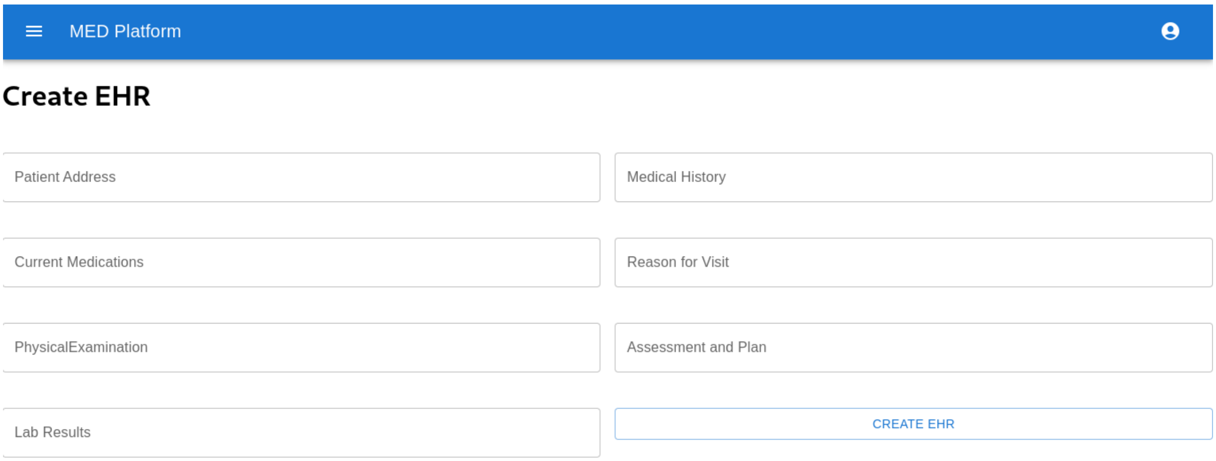
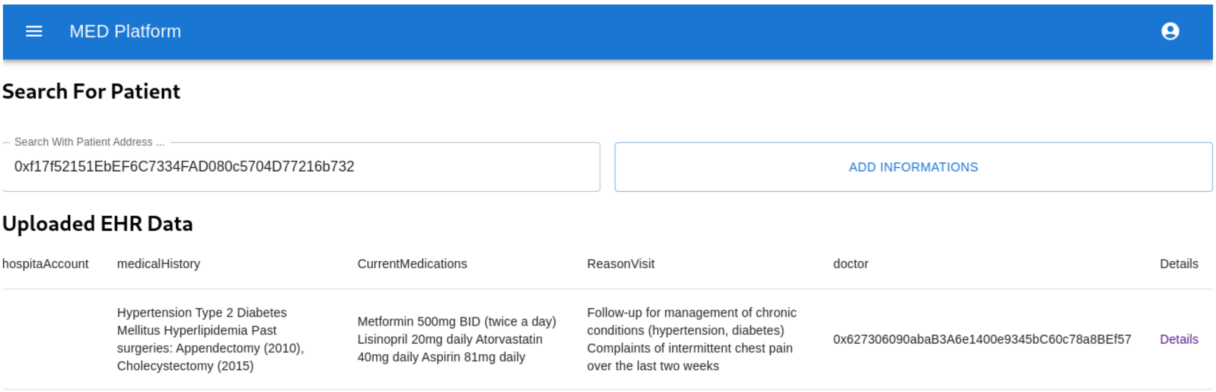


Figure 4.18: Create EHR interface.

4.6.5 Search For Patient EHR

The "Search For Patient EHR" page enables doctors to search for and retrieve Electronic Health Records of their patients. Using this feature, doctors can quickly find a patient's medical history and current health information, which is essential for ongoing treatment and care decisions.



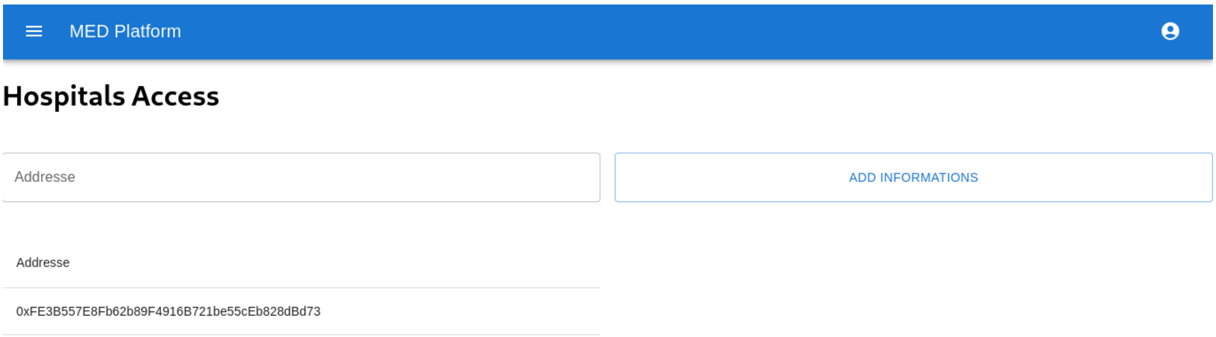
Search With Patient Address ...: 0xf17f52151EbEF6C7334FAD080c5704D77216b732

hospitaAccount	medicalHistory	CurrentMedications	ReasonVisit	doctor	Details
	Hypertension Type 2 Diabetes Mellitus Hyperlipidemia Past surgeries: Appendectomy (2010), Cholecystectomy (2015)	Metformin 500mg BID (twice a day) Lisinopril 20mg daily Atorvastatin 40mg daily Aspirin 81mg daily	Follow-up for management of chronic conditions (hypertension, diabetes) Complaints of intermittent chest pain over the last two weeks	0x627306090abaB3A6e1400e9345bC60c78a8BEf57	Details

Figure 4.19: Search For Patient EHR interface.

4.6.6 Hospitals Access

The "Hospitals Access" page allows patients to manage which hospitals have access to their EHRs. Patients can add or remove hospital accounts, granting them permission to view or update their health records. This feature ensures that patients have control over who can access their sensitive medical information.

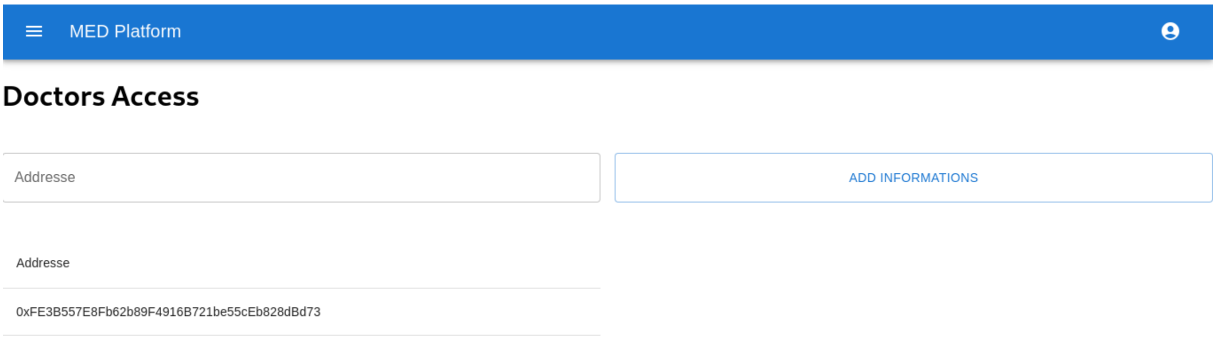


Addresse
0xFE3B557E8Fb62b89F4916B721be55cEb828dBd73

Figure 4.20: Hospitals Access interface.

4.6.7 Doctors Access

The "Doctors Access" page is similar to the Hospitals Access page but is specifically for managing doctor accounts. Patients can give specific doctors permission to access their EHRs, ensuring that only trusted medical professionals can view and update their health information. This allows for a high level of patient control and privacy.



Doctors Access

Addresse

ADD INFORMATIONS

Addresse
0xFE3B557E8Fb62b89F4916B721be55cEb828dBd73

Figure 4.21: Doctors Access interface.

4.7 Conclusion

This chapter presents and explains the implementation of the website and its different features that enable users to interact with it with more privacy.

Chapter 5

Business Model Canvas

5.1 Introduction

This chapter outlines the business model for a blockchain-based electronic health records (EHR) platform aimed at enhancing security, confidentiality, interoperability, and accessibility, thereby improving patient care and streamlining healthcare processes.

5.2 Purpose of the Business

To enhance the security, interoperability, and accessibility of electronic health records (EHRs) through the implementation of blockchain technology, thereby improving patient care and streamlining healthcare processes.

5.3 Customers and Value Propositions

5.3.1 Customer Segments

- Hospitals and healthcare providers (Large, teaching hospitals): These institutions require a scalable solution to manage vast amounts of patient data across multiple departments and locations. They prioritize data security, interoperability with existing systems, and seamless integration with their workflows.
- Patients (Tech-savvy individuals with chronic conditions): These patients actively participate in managing their health and value secure access to their medical records. They are interested in a user-friendly platform that allows them to share data with authorized providers and track their health progress over time.
- Pharmaceutical companies (Large, research-driven organizations): These companies require access to a broad pool of anonymized patient data for clinical trials and drug development. They seek a secure and reliable platform that facilitates

collaboration with researchers and ensures data quality.

5.3.2 Value Propositions

For Hospitals and healthcare providers (Large, teaching hospitals):

- Scalable infrastructure: The system can accommodate the high volume of data generated by large hospitals and seamlessly integrate with existing infrastructure.
- Departmental integration: The platform facilitates data sharing across different departments within a hospital, improving care coordination and reducing redundancies.
- Simplified workflows: Automated processes and a user-friendly interface streamline administrative tasks and free up staff time for patient care.
- User-friendly interface: While the platform offers a user-friendly interface for ease of use by organizations, it is also designed to be integrated into existing systems of these organizations. Comprehensive documentation will be provided to assist with the integration process, ensuring a smooth transition and effective use of the blockchain technology.

For Patients (Tech-savvy individuals with chronic conditions):

- Real-time access: Patients can access their medical records anytime, anywhere, allowing them to participate actively in their healthcare decisions.
- Data sharing control: Patients have complete control over who can access their data and can easily grant or revoke access permissions.
- Personalized insights: The platform can generate personalized health reports and analytics, empowering patients to manage

their chronic conditions more effectively.

For Pharmaceutical companies (Large, research-driven organizations):

- Anonymized data pool: The system provides access to a vast pool of anonymized patient data, suitable for conducting large-scale clinical trials and research studies.
- Secure data collaboration: The platform facilitates secure collaboration between researchers and pharmaceutical companies, accelerating drug development processes.
- Improved data quality: Blockchain technology ensures data integrity and traceability, leading to more reliable research outcomes.

5.4 Channels and Customer Relationships

5.4.1 Channels

- Direct sales force: A dedicated sales team will target healthcare organizations directly, highlighting the benefits of the blockchain platform and addressing their specific needs.
- Online marketing: Developing a user-friendly website and engaging in targeted online advertising can reach a wider audience of healthcare providers and patients.
- Industry partnerships: Collaboration with healthcare IT vendors and industry associations will leverage existing distribution channels and reach healthcare professionals at industry conferences and events.

5.4.2 Customer Relationships

- Onboarding and training: Providing comprehensive training programs and support during the initial implementation phase ensures smooth user adoption across healthcare institutions.
- Dedicated customer support: Our dedicated customer support team exclusively serves Business to Business (B2B) clients, addressing technical inquiries and troubleshooting issues efficiently. This specialized support enhances user satisfaction and strengthens business partnerships by providing tailored assistance to meet the unique needs of our B2B customers.
- Online knowledge base: Developing a comprehensive online knowledge base can empower users to find answers to common questions independently and reduce the burden on customer support.
- User communities: Creating online communities can foster communication and collaboration among healthcare professionals and patients, promoting knowledge sharing and peer-to-peer support.

5.5 Key Resources, Key Activities and Key Partners

5.5.1 Key Resources

- Blockchain platform: A secure and scalable blockchain infrastructure is essential for storing and managing sensitive patient data. This could be a custom-developed platform or a permissioned blockchain network tailored for healthcare applications.
- Data security protocols: Robust security measures are necessary to protect patient data privacy and ensure compliance with relevant data protection regulations. This includes encryption

technologies, access controls, and intrusion detection systems.

- User-friendly interface: An intuitive and user-friendly interface is crucial for both healthcare professionals and patients to interact with the platform seamlessly. This interface should cater to diverse user needs and technical expertise levels.
- Technical expertise: A team with expertise in blockchain technology, healthcare data management, and software development is critical for maintaining and evolving the platform.

5.5.2 Key Activities

- Platform development and maintenance: Continuous development and maintenance of the blockchain platform ensure its security, scalability, and performance. This includes addressing potential vulnerabilities, integrating new features, and optimizing system operations.
- Regulatory compliance: Regularly monitoring and updating the platform to comply with evolving data privacy regulations and healthcare industry standards is crucial. This involves staying informed about changes in regulations and implementing necessary adjustments.
- User adoption and education: Developing targeted strategies and programs to encourage adoption of the platform by healthcare providers and patients. This might include educational workshops, user guides, and ongoing support initiatives.
- Data management: Establishing procedures for data governance, access control, and audit trails to ensure the integrity and traceability of patient data within the blockchain ecosystem.

5.5.3 Key Partners

- Healthcare IT vendors: Collaboration with established healthcare software companies can facilitate integration of the blockchain platform with existing EHR systems and expand the user base. These partners can provide technical expertise and access to existing healthcare provider networks.
- Government agencies: Engaging with government bodies can promote the adoption of blockchain technology for healthcare data management on a national level. Partnerships with government agencies can lead to pilot programs and policy initiatives that support the implementation of the platform.
- Security firms: Partnerships with cybersecurity experts are crucial for implementing robust security measures and safeguarding sensitive medical data. Security firms can provide expertise in risk assessment, vulnerability testing, and ongoing threat monitoring.
- Patient advocacy groups: Collaboration with patient advocacy groups can ensure the platform prioritizes patient privacy and empowers individuals to manage their health information. These groups can provide valuable feedback and insights into patient needs and expectations.

5.6 Cost Structure and Revenue Streams

5.6.1 Cost Structure

- Platform development and maintenance: The ongoing costs associated with maintaining and evolving the blockchain platform, including software development, infrastructure management, and security updates.

- Data security: Costs associated with implementing and maintaining robust data security measures, such as encryption technologies, intrusion detection systems, and regular security audits.
- Regulatory compliance: Costs associated with monitoring and updating the platform to comply with evolving data privacy regulations and healthcare industry standards. This may include legal fees and consulting services.
- User adoption and education: Costs associated with developing and delivering educational materials, user training programs, and support initiatives to encourage user adoption of the platform.
- Sales and marketing: Costs associated with marketing and promotional activities to reach potential customers, including advertising campaigns, attending industry events, and developing sales materials.
- Personnel: Salaries and benefits for the team responsible for managing the platform, including developers, security professionals, and customer support staff.

5.6.2 Revenue Streams

- Subscription fees: Healthcare organizations can pay a monthly or annual subscription fee for access to the blockchain-based medical record management system. This fee could be tiered based on the size and needs of the organization. Prices range from $1000/month for small clinics to $5000/month for large hospitals.
- Transaction fees: A minimal transaction fee could be charged

for specific actions within the system, such as data sharing events, record access requests, or additional storage capacity. This fee could range from $0.05 to $0.25 per transaction.

- Integration services: Fees associated with customized integration services to connect the blockchain platform with existing EHR systems and healthcare IT infrastructure. Prices vary based on the scope of integration, starting from $5000 for basic integration services.
- Data access licenses: Pharmaceutical companies and research institutions could pay licensing fees for access to anonymized patient data for research purposes. This could be a tiered structure based on the volume and type of data accessed. Prices range from $10,000 to $50,000 per year depending on the level of access and usage.

5.7 Linking The Boxes and Tidying Up

5.7.1 Connecting the Promises

5.7.1.1 Value Propositions for Key Activities & Resources

- The secure and scalable platform (Key Resource) enables improved data security and interoperability (Value Propositions) for healthcare providers.
- User-friendly interface (Key Resource) empowers patients with control over their data (Value Proposition).
- Secure data access (Key Resource) supports research activities (Value Proposition) for pharmaceutical companies.

5.7.1.2 Customer Relationships to Cost Structure:

- Dedicated customer support (Customer Relationship) incurs personnel costs (Cost Structure).

- Online resources (Customer Relationship) can reduce support workload and costs (Cost Structure).

5.7.2 Tidying Up

- Color Coding: Assign distinct colors to each customer segment for clarity:
  - Hospitals - Blue
  - Patients - Green
  - Pharma Companies - Red

5.8 Telling The Story

The journey of developing a blockchain-based electronic health records (EHR) platform began with a vision to transform how healthcare data is managed and utilized. Our mission is to enhance the security, interoperability, and accessibility of EHRs, thereby improving patient care and streamlining healthcare processes.

5.8.1 Origin and Vision:

The idea originated from the observed challenges in the current healthcare data management systems, including data silos, security vulnerabilities, and inefficiencies in data sharing among healthcare providers. Blockchain technology emerged as a promising solution due to its inherent security features, decentralization, and ability to provide a single source of truth.

5.8.2 Stakeholders:

We identified three primary customer segments: hospitals and healthcare providers, patients with chronic conditions, and pharmaceutical companies. Each segment had distinct needs that could be addressed through our blockchain platform.

5.8.2.1 Hospitals and Healthcare Providers:

- Large hospitals require scalable solutions for managing vast amounts of patient data.
- They prioritize data security, seamless integration with existing systems, and streamlined workflows.

5.8.2.2 Patients:

- Tech-savvy patients with chronic conditions value secure, real-time access to their medical records.
- They seek control over their data and personalized health insights.

5.8.2.3 Pharmaceutical Companies:

- These companies need access to anonymized patient data for clinical trials and research.
- They require secure collaboration tools to ensure data quality and reliability.

5.8.2.4 Research Laboratories:

- Research laboratories rely on access to anonymized patient data for conducting studies and advancing medical knowledge.
- They require secure and reliable data sources to support their research efforts.

5.8.3 Crafting Value Propositions:

For each customer segment, we crafted tailored value propositions:

- For Hospitals:A scalable, integrated platform that enhances data security and simplifies workflows.

- For Patients:Secure, real-time access to health records and control over data sharing.
- For Pharmaceutical Companies:Access to high-quality, anonymized data for research purposes.

5.8.4 Building the Platform:

We developed a blockchain platform with robust security protocols, an intuitive user interface, and scalable infrastructure. Continuous development and maintenance ensure the platform's performance and compliance with regulatory standards.

5.8.5 Establishing Partnerships:

Collaboration with healthcare IT vendors, government agencies, security firms, and patient advocacy groups was essential. These partnerships helped integrate our platform with existing systems, promote adoption, and ensure robust security measures.

5.8.6 Engaging Customers:

A dedicated sales force, online marketing strategies, and industry partnerships helped us reach potential customers. Comprehensive training programs and dedicated customer support ensured smooth onboarding and user satisfaction.

5.8.7 Revenue Model:

We structured our revenue streams around subscription fees, transaction fees, integration services, and data access licenses. This model ensures sustainable growth while providing value to our customers.

5.8.8 The Future:

As we continue to evolve, our focus remains on addressing the ever-changing needs of our stakeholders, enhancing platform capabilities, and fostering a healthcare ecosystem where data is secure, interoperable, and easily accessible.

5.9 Assumptions Testing

To validate our business model, several key assumptions need to be tested:

5.9.1 Scalability and Integration:

- Assumption: The blockchain platform can scale to handle large volumes of data and integrate seamlessly with existing hospital infrastructure.
- Test: Conduct pilot implementations in large hospitals to monitor performance and integration efficiency.

5.9.2 Data Security and Compliance:

- Assumption: The platform meets all relevant data protection regulations and provides robust security.
- Test: Perform comprehensive security audits and compliance checks, and obtain certifications from relevant regulatory bodies.

5.9.3 User Adoption:

- Assumption: Healthcare providers, patients, and pharmaceutical companies will adopt the platform.
- Test: Implement user trials and gather feedback to assess ease of use, satisfaction, and adoption rates.

5.9.4 Value Proposition Effectiveness:

- Assumption: The value propositions resonate with the target customer segments.
- Test: Conduct surveys and focus groups with representatives from each segment to validate the perceived benefits.

5.9.5 Revenue Streams:

- Assumption: The proposed revenue model is viable and acceptable to customers.
- Test: Introduce pricing trials and gather customer feedback on subscription fees, transaction fees, and other charges.

5.10 Designing New Versions

Based on the feedback and insights gained from assumptions testing, the next steps involve designing new versions of the business model and the platform:

5.10.1 Enhanced Scalability

Develop advanced algorithms and architecture enhancements to improve the platform's ability to handle increasing data volumes and complex integrations.

5.10.2 Security Upgrades

Implement cutting-edge security technologies, such as quantum-resistant encryption and AI-driven threat detection, to further enhance data protection.

5.10.3 User Experience Improvements

Refine the user interface and add new features based on user feedback to make the platform more intuitive and user-friendly.

5.10.4 Expanded Partnerships

Form additional partnerships with industry leaders and innovators to leverage new technologies and expand the platform's capabilities.

5.10.5 Flexible Pricing Models

Consider implementing pay-per-use, pay-as-you-go, and freemium options to broaden your customer base and increase market penetration. These models offer flexibility and cater to diverse needs and usage patterns. With pay-per-use, customers pay for what they use, while pay-as-you-go enables incremental payments. Freemium options provide basic features for free, enticing users to upgrade. By adopting these models, you can attract a wider audience and stay competitive.

5.10.6 Advanced Analytics

Integrate advanced analytics and AI capabilities to provide deeper insights and predictive analytics for healthcare providers and patients.

5.10.7 Conclusion

In this chapter, we have explored the comprehensive business model for a blockchain-based electronic health records (EHR) platform aimed at enhancing security, interoperability, and accessibility. By addressing the needs of hospitals, patients, and pharmaceutical companies, we offer tailored value propositions that ensure scalability, data security, and user control. Through strategic partnerships, robust technical infrastructure, and a focus on user experience, our platform is poised to revolutionize healthcare data management. Moving forward, we will continue to refine and validate our model, ensuring sustainable growth and meeting the evolving needs of the healthcare industry.

General Conclusion

The intersection of blockchain technology and healthcare presents a promising frontier for innovation, addressing many critical challenges faced by modern medical systems. This thesis has delved into the intricate mechanisms of blockchain, explored its diverse applications in healthcare, and proposed a robust system for the secure management of Electronic Health Records (EHRs) using Hyperledger Besu.

Blockchain technology offers a decentralized, transparent, and secure framework, which is especially pertinent in the realm of medical data management. Traditional systems, often plagued by issues of fragmentation, interoperability, and security vulnerabilities, stand to benefit significantly from the adoption of blockchain technology. By leveraging the inherent advantages of blockchain—such as immutability, cryptographic security, and decentralized consensus—this study has demonstrated a viable path towards enhancing the integrity and accessibility of medical records.

In developing a blockchain-based EHR management system, the research has addressed key concerns around patient privacy, data security, and system interoperability. The proposed solution using Hyperledger Besu ensures secure storage and access to sensitive medical information, facilitating seamless sharing of data across various stakeholders in the healthcare ecosystem. This promotes a more integrated and patient-centric approach to healthcare delivery.

Hyperledger Besu, being an Ethereum-based client, offers compatibility with the broader Ethereum ecosystem and smart contract functionality. Its public-permissioned network capabilities make it suitable for applications requiring both transparency and controlled access. The research underscores how Hyperledger Besu can be effectively utilized to create a secure and efficient EHR management system, demonstrating its potential to transform the healthcare industry.

The broader implications of blockchain adoption in healthcare suggest potential improvements in clinical trial optimization, pharmaceutical supply chain integrity, and the mitigation of medical fraud. These applications further illustrate the transformative potential of blockchain technology beyond EHR management.

Looking forward, the research team plans to extend this work by incorporating Hyperledger Fabric into the study and conducting a comparative analysis between Hyperledger Besu and Hyperledger Fabric. Hyperledger Fabric's high performance and privacy features within a permissioned network offer promising advantages for healthcare applications requiring stringent control over participant access and transaction confidentiality. This future comparative analysis will provide deeper insights into the strengths and best use cases for each platform, guiding stakeholders in selecting the most suitable technology for their specific needs.

In conclusion, this thesis contributes valuable insights to the burgeoning field of blockchain technology in healthcare. It provides a compelling case for the integration of blockchain solutions, particularly Hyperledger Besu, to overcome existing limitations in medical record management. The anticipated future work with Hyperledger Fabric will further enrich the understanding of blockchain applications in healthcare, driving advancements, improving patient outcomes, and ensuring the secure and efficient delivery of healthcare services.

References

[1] Abbas Yazdinejad, Gautam Srivastava, Rezam Parizi, and Mohammed Aledhari. Decentralized authentication of distributed patients.

[2] Journal of Industrial Integration Y. Lu and no . 04 p. 1850015 2018 Management, vol. 3. Blockchain: A survey on functions, applications and open issues.

[3] applications M. Mettler, dans 2016 IEEE 18th international conference on e-health networking and p. 1–3 services (Healthcom). IEEE, 2016. Blockchain technology in healthcare: The revolution starts here,.

[4] [Online; Available] https://www.hyperledger.org/projects/iroha, 2021. Hyperledger iroha.

[5] International Journal of Research in Engineering S. A. Abeyratne et R. Monfared and p. 1–10 2016 Technology, vol. 05. Blockchain ready manufacturing supply chain using distributed ledger.

[6] D. Shin M. Bae et E. Jee dans 2019 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE). IEEE 2019 p. 11–21 J. Yoo, Y. Jung. Formal modeling and verification

of a federated byzantine agreement algorithm for blockchain platforms.

[7] https://www.investopedia.com/terms/b/blockchain.asptoc-how-does-a-blockchain work. how does a blockchain work.

[8] Internat. J. Web Grid Serv 2016. H.-N. Dai H. Wang Z. Zheng, S. Xie. A survey. Blockchain challenges and opportunities.

[9] https://blockgeeks.com/guides/what-is-hashing.
Ameer Rosic. What is hashing?

[10] Schmidt-D. C. White J. Dubey A. (2019) 115 181-209. Zhang, P. Consensus mechanisms and information security technologies. advances in computers.

[11] https://www.oracle.com/middleeast/blockchain/what-is blockchain/. what is blockchain?

[12] S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System." Bitcoin Whitepaper. Nakamoto. Activation function.

[13] A. M. (2014). Antonopoulos. Mastering bitcoin: Unlocking digital cryptocurrencies.

[14] V. (2013). Ethereum Whitepaper. Buterin. Ethereum white paper: A next-generation smart contract and decentralized application platform.

[15] M. (2015). Swan. Blockchain: Blueprint for a new economy.

[16] Tapscott A. (2016). Tapscott, D. Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world.

[17] W. (2016). Mougayar. The business blockchain: Promise, practice, and application of the next internet technology.

[18] et al. (2016). Narayanan, A. Bitcoin and cryptocurrency technologies: A comprehensive introduction.

[19] Scheuermann B. (2016). Tschorsch, F. Bitcoin and beyond: A technical survey on decentralized digital currencies.

[20] A. (2018). de Vries. Bitcoin's growing energy problem.

[21] Vigna P. (2018). Casey, M. J. The truth machine: The blockchain and the future of everything.

[22] M. (2015). Swan. Blockchain: Blueprint for a new economy.

[23] A. (2015). Zohar. Bitcoin: under the hood.

[24] https://news-medical/net/health/Blockchain-Applications-in-healthcare. Dr.LijiThomas, MD. Blockchain applications in healthcare.

[25] Mohler-J.-Milojkovic-M.- Marella P. B. (2018). IEEE Access 6 9375-9385. Dagher, G. G. Blockchain in healthcare.

[26] Ravaud P.- Blockchain Consortium-R. (2017). Trials 18(1) 335 Benchoufi, M. Blockchain technology for improving clinical research quality.

[27] Kim-H. E. Ohno-Machado L. (2017). Journal of the American Medical Informatics Association 24(6) 1211-1220 Kuo, T. T. Blockchain distributed ledger technologies for biomedical and health care applications.

[28] Wang H.-Jin D. Li M.- Jiang W. (2016). Journal of medical systems 40(10) 218 Yue, X. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control.

[29] Ekblaw A.-Vieira T. Lippman-A. (2016). In 2016 2nd International Conference on Open Azaria, A. and Big Data (OBD) (pp. 25-30). IEEE. Medrec: Using blockchain for medical data access and permission management.

[30] Xu Z. Ryu-S. Schumacher-M. (2017). AMIA Annual Symposium Proceedings 2017 650. Dubovitskaya, A. Secure and trustable electronic medical records sharing using blockchain.

[31] White J. Schmidt-D. C. Lenz-G. Rosenbloom S. T. (2017). Computational Zhang, P. and 355-364. structural biotechnology journal, 15. Fhirchain: Applying blockchain to securely and scalably share clinical data.

[32] Sifah E. B.-Asamoah K. O.-Gao J. Du X. Guizani M. (2017). IEEE Access 5 14757-14767. Xia, Q. Medshare: Trust-less medical data sharing among cloud service providers via blockchain.

[33] Sifah E. B.-Smahi A. Amofa-S. Zhang X. (2017). Information 8(2) 44. Xia, Q. Bbds: Blockchain-based data sharing for electronic medical records in cloud environments.

[34] Azaria A. Halamka-J. D. Lippman A. (2016). In IEEE Open Big Data Conference (OBD) (pp. 506-513). IEEE. Ekblaw, A. A case study for blockchain in healthcare: "medrec" prototype for electronic health records and medical research data.

[35] Mahmoud Q. H. Eklund J. M. (2019). Healthcare 7(2) 56 Agbo, C. C. Blockchain technology in healthcare: A systematic review.

[36] Applications Mettler, M. (2016). In 2016 IEEE 18th International Conference on e-Health Networking and Services (Healthcom) (pp. 1-3). IEEE. Blockchain technology in healthcare: The revolution starts here.

[37] Deeduvanu R.-Kanjamala P. Boles K. (2019). Healthcare-7(2) 87 Peterson, K. A blockchain-based approach to health information exchange networks.

[38] Ravaud-P. (2017). Trials 18(1) 335. Benchoufi, M. Blockchain technology for improving clinical research quality.