

Hyperledger Fabric Blockchain-Based Medical Document and Prescription Sharing System: Enhancing Data Security and Traceability of the Healthcare Sector in Bangladesh

by

Mohammed Taher Abdullah

19101054

Ikramul Hasan

19101362

Shadab Iqbal

22241138

Srijan Banik

19101062

Merazul Islam Dihan

19101118

A thesis submitted to the School of Data and Sciences
in partial fulfillment of the requirements for the degree of
B.Sc. in Computer Science

School of Data and Sciences

Brac University

January 2023

© 2023. Brac University
All rights reserved.

Declaration

It is hereby declared that

1. The thesis submitted is our original work
2. The thesis does not contain any material previously published or written by other participants.
3. We have acknowledged all main sources of help

Student's Full Name & Signature:

Mohammed Taher Abdullah

Mohammed Taher Abdullah
19101054

Ikramul Hasan

Ikramul Hasan
19101362

Shadab Iqbal

Shadab Iqbal
22241138

Srijan Banik

Srijan Banik
19101062

Merazul Islam

Merazul Islam Dihan
19101118

Approval

The thesis/project titled “Hyperledger Fabric Blockchain-Based Medical Document and Prescription Sharing System: Enhancing Data Security and Traceability of the Healthcare Sector in Bangladesh” submitted by

1. Mohammed Taher Abdullah (19101054)
2. Ikramul Hasan (19101362)
3. Shadab Iqbal (22241138)
4. Srijan Banik (19101062)
5. Merazul Islam Dihan (19101118)

Of Spring, 2023 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on January, 2023.


Examining Committee:

Supervisor:
(Member)



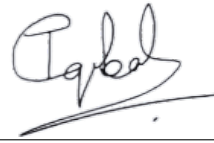
Md. Golam Rabiul Alam, PhD
Professor
Department of Computer Science and Engineering
BRAC University

Co-Supervisor:
(Member)



Md Sadek Ferdous, PhD
Associate Professor
Department of Computer Science and Engineering
BRAC University

Co-Supervisor:
(Member)



Muhammad Iqbal Hossain, PhD
Associate Professor
Department of Computer Science and Engineering
BRAC University

Program Coordinator:
(Member)

MD Golam Rabiul Alam
Professor
Department of Computer Science and Engineering
Brac University

Head of Department:
(Chair)

Sadia Kazi Hamid
Chairperson and Associate Professor
Department of Computer Science and Engineering
Brac University

Abstract

In the current digital age, Blockchain technology has the potential to revolutionize the way sensitive medical information is handled. Blockchain's immutable and encrypted nature makes it an ideal solution for preventing fraud and ensuring the security of essential data. This study aims to utilize an Hyperledger Fabric-based blockchain network for the authentication of individual medical prescriptions, while maintaining a ledger for each patient to reduce drug abuse and promote transparency and traceability. In Bangladesh, the analog nature of medical prescriptions makes it difficult to verify their authenticity, leading to a high rate of counterfeit prescriptions and drug abuse. Our proposed solution utilizes a distributed ledger where records of transactions and data can be remotely stored, providing an open and tamper-proof system. In each transaction, the date and time are embedded with the digital signature of the issuer, creating a clear timeline of the transaction and greatly reducing the possibility of fraud. The current system of using hard copies for medical prescriptions is not only inconvenient for storage and sharing of information but also time-consuming. Our proposed blockchain network can be used to store transaction and documentation data and easily share it with other nodes in the network, eliminating the need for paper exchange. This improves the efficiency of transactions and reduces the need for reconciling different ledgers. Our goal is to assist in the creation of a secure and authentic system for issuing and storing medical prescriptions in Bangladesh, to eliminate drug abuse. This research aims to explore the use of the Hyperledger blockchain system to make patient data more secure, while also enabling private sharing of information within the network. The Hyperledger framework, being a permissioned blockchain system, is well-suited for use cases that require privacy and security. The study will also examine the technical feasibility of building such a system. The outcome of this study will provide valuable insights into the potential of Hyperledger-based systems in the healthcare sector and aid in the design and implementation of similar systems in the future.

Acknowledgement

Firstly, all praise to the Great Allah for whom our thesis have been completed without any major interruption.

Secondly, to our supervisor Md. Golam Rabiul Alam sir and our co-supervisors Md Sadek Ferdous sir and Muhammad Iqbal Hossain sir for their kind support and advice in our work. They helped us whenever we needed help.

And finally to our parents without their throughout support it may not be possible. With their kind support and prayer we are now on the verge of our graduation.

Table of Contents

| | |
|--------------------------------------------------|-------------|
| Declaration | i |
| Approval | ii |
| Abstract | iv |
| Acknowledgment | v |
| Table of Contents | vi |
| List of Figures | viii |
| Nomenclature | viii |
| 1 Introduction | 1 |
| 1.1 Research Problem | 2 |
| 1.2 Research Objectives | 3 |
| 2 Background Study | 4 |
| 2.1 Blockchain | 4 |
| 2.2 Merkle Tree | 4 |
| 2.3 Symmetric key cryptography | 6 |
| 2.4 Asymmetric key cryptography | 6 |
| 2.5 Digital Signature | 7 |
| 2.6 Public Blockchain | 7 |
| 2.7 Private Blockchain | 7 |
| 2.8 Consortium Blockchain | 8 |
| 2.9 Proof of Work | 8 |
| 2.10 Proof of Stake | 8 |
| 2.11 Hyperledger fabric | 8 |
| 2.12 Peers | 9 |
| 2.13 Orderer | 9 |
| 2.14 Certificate Authority | 9 |
| 2.15 Membership Service Provider | 10 |
| 2.16 Shared ledger | 10 |
| 2.17 Private Data | 11 |
| 2.18 World State and Transactional Log | 11 |
| 2.19 Channel | 12 |
| 2.20 Asset | 12 |

| | | |
|----------|---------------------------------------------------|-----------|
| 3 | Literature Review | 13 |
| 3.1 | Related Works | 13 |
| 3.2 | Comparative Analysis with Related Works | 19 |
| 4 | Methodology | 22 |
| 4.1 | Architecture | 22 |
| 4.2 | Data Storage | 26 |
| 4.3 | User Experience | 27 |
| 5 | Implementation | 29 |
| 5.1 | Environment setup | 29 |
| 5.2 | Tech Stack | 30 |
| 5.3 | User Flow Diagram | 30 |
| 5.4 | Doctor Flow Diagram | 30 |
| 5.5 | Pseudocodes and Explanation | 32 |
| 5.5.1 | Upload of encrypted files in IPFS | 32 |
| 5.5.2 | Creation of Prescription | 32 |
| 5.5.3 | API Connection | 33 |
| 5.6 | Designing User-Friendly Interface | 34 |
| 5.6.1 | Doctor’s interaction with the App | 34 |
| 5.6.2 | Patient’s interaction with the App | 34 |
| 5.6.3 | IPFS files | 35 |
| 6 | Results and Discussion | 41 |
| 6.1 | Security and Performance | 41 |
| 6.1.1 | Authentication | 41 |
| 6.1.2 | Authorization | 41 |
| 6.1.3 | Privacy | 41 |
| 6.1.4 | Scalability | 41 |
| 6.2 | Hyperledger Fabric vs Central Database | 42 |
| 7 | Future Works | 44 |
| 8 | Conclusion | 46 |
| | Bibliography | 47 |

List of Figures

| | | |
|------|-----------------------------------------------------------------------|----|
| 2.1 | <i>Merkle Tree</i> | 5 |
| 2.2 | <i>Symmetric key cryptography</i> | 6 |
| 2.3 | <i>Digital signature</i> | 7 |
| 2.4 | <i>CA issuing and revoking certificates</i> | 10 |
| 2.5 | <i>Authorized and Unauthorized Peers</i> | 11 |
| 2.6 | <i>World State and Transactional Log</i> | 12 |
| 3.1 | <i>Authenticating Certificates using QR Code</i> | 16 |
| 3.2 | <i>UniCert System Diagram</i> | 17 |
| 3.3 | <i>Automating the process of certificate storage</i> | 18 |
| 4.1 | <i>System Architecture and workflow from MOHFW Admin control</i> | 23 |
| 4.2 | <i>CA diagram</i> | 24 |
| 4.3 | <i>Process of ordering service</i> | 25 |
| 4.4 | <i>Invalid student account added to the CRL</i> | 25 |
| 4.5 | <i>User request and asymmetric key decryption for file retrieving</i> | 26 |
| 4.6 | <i>User Interaction</i> | 27 |
| 4.7 | <i>Data storing in IPFS</i> | 28 |
| 4.8 | <i>User Permissions</i> | 28 |
| 5.1 | <i>Tech Stack used for our prototype</i> | 29 |
| 5.2 | <i>User flow diagram</i> | 31 |
| 5.3 | <i>Doctor flow diagram</i> | 31 |
| 5.4 | <i>IPFS implementation Pseudo-code</i> | 32 |
| 5.5 | <i>Function for creating prescription: Pseudo-code</i> | 33 |
| 5.6 | <i>Pseudo-code for API connection</i> | 34 |
| 5.7 | <i>Doctor's view 1</i> | 35 |
| 5.8 | <i>Doctor's view 2</i> | 36 |
| 5.9 | <i>Patient's view 1</i> | 37 |
| 5.10 | <i>Patient's view 2</i> | 38 |
| 5.11 | <i>Pharmacist's view and Transactional Log</i> | 39 |
| 5.12 | <i>Medical files stored in IPFS</i> | 40 |
| 6.1 | <i>Our solution vs Other solutions</i> | 42 |

Chapter 1

Introduction

If there is no way to verify the authenticity of medical prescriptions, The proliferation of counterfeit and fraudulent medical prescriptions poses a significant risk to the healthcare industry, as patients may receive ineffective or dangerous medications. Furthermore, this problem not only contributes to the growing issue of prescription drug abuse and illegal distribution of controlled substances, but also leads to financial losses for healthcare providers and insurance companies. To combat this issue, a Hyperledger Fabric blockchain network can provide a secure and tamper-proof method for recording and tracking prescription information. By creating a decentralized database of prescriptions, where each prescription is recorded as a unique transaction on the blockchain, the network can ensure authenticity through the use of digital signatures. Additionally, by limiting access to authorized parties such as doctors, pharmacists, and regulatory authorities, the network can prevent unauthorized alteration or counterfeiting of prescriptions. Real-time tracking of prescriptions from point of origin to point of dispensation can also be enabled, thus providing an effective means of detecting and preventing prescription drug abuse and illegal distribution of controlled substances. Under the blockchain, a block becomes validated only once it has been verified by multiple parties. The data present in the blockchain cannot be modified arbitrarily. Hence, we can ensure the authenticity of the certificates better. Using a Hyperledger Fabric blockchain network to prescribe certificates can be beneficial for doctors in several ways. Improved patient safety: By using a tamper-proof system for recording and tracking prescriptions, doctors can ensure that patients receive the correct medication and dosage. This can help to prevent medication errors and adverse reactions. Streamlined prescription process: With a blockchain network, doctors can easily access a patient's medical history and prescribed medications. This can help to avoid prescribing contraindicated medications, and also can speed up the prescribing process. Enhanced security and privacy: Blockchain technology provides a secure and private way to store and share patient information. With a Hyperledger Fabric network, doctors can ensure that only authorized parties have access to patient information, which can help to protect patient privacy. Improved regulatory compliance: By using a blockchain network to prescribe certificates, doctors can ensure that they are compliant with regulatory requirements related to prescription tracking and reporting. Better tracking and reporting: With real-time tracking of prescriptions from point of origin to point of dispensation, doctors can have a better understanding of prescription drug usage and can detect any potential issues. Overall, using a Hy-

hyperledger Fabric blockchain network to prescribe certificates can provide a secure, efficient, and compliant way for doctors to prescribe and track medications, which can help to improve patient safety and care, streamline the prescribing process, and meet regulatory requirements.

1.1 Research Problem

In Bangladesh, despite a High Court directive issued in 2019 [1] to prohibit the over-the-counter sale of antibiotics without a prescription from registered physicians, such sales continue to occur in violation of the directive [2]. This illegal practice has been identified as a major contributor to the rising problem of antimicrobial resistance (AMR) in the country. Public health experts have warned that the failure of the authorities to effectively enforce the HC directive has led to an increase in AMR-related deaths. The illicit sale of antibiotics without prescription is a major public health concern and the continuation of this practice despite the court directive highlights the need for stricter enforcement measures to be implemented. And this still remains a huge problem as there is no active system to prevent it. Not having a secure and authentic system for issuing and storing medical prescriptions in a country can lead to several problems:

Patient safety: Without a way to verify the authenticity of prescriptions, patients may receive counterfeit or fraudulent medications, which can lead to ineffective treatment or even harm. **Prescription drug abuse:** Without a way to track prescriptions, it can be easier for individuals to obtain and abuse prescription drugs.

Illegal distribution of controlled substances: Without a way to track prescriptions, it can be easier for individuals to obtain and illegally distribute controlled substances. **Financial loss:** Without a way to verify prescriptions, healthcare providers and insurance companies may incur financial losses from fraudulent or counterfeit prescriptions. **Lack of transparency and traceability:** Without a system for recording and tracking prescriptions, it can be difficult to detect and prevent fraud and abuse.

Difficulty in sharing information and tracking patients history: Without a digital system for storing and sharing information, it can be difficult for healthcare providers to access important patient information, such as their medical history, allergies, and current medications. **Lack of regulatory compliance:** Without a system for recording and tracking prescriptions, healthcare providers may have difficulty meeting regulatory requirements related to prescription tracking and reporting.

Overall, not having a secure and authentic system for issuing and storing medical prescriptions can have serious consequences for patients, healthcare providers, and the overall healthcare system of a country. It can lead to unsafe treatment, drug abuse, financial loss and lack of transparency and traceability. For our research, we aim to create a blockchain-based hyperledger fabric network where the authority will be able to easily monitor and trace this to eradicate the mentioned problems.

1.2 Research Objectives

This project aims to develop a system that can authenticate individual medical prescriptions and medical documents while boosting authenticity, and effectiveness, and minimizing clutter. The way prescriptions are issued in Bangladesh ,and most other countries are still analog- written on paper and shared. This system makes verifying prescriptions next to impossible. Furthermore, this system also makes it inconvenient to store and keep track of all the medical reports and data for both the hospitals and the patients; which is a very important part of medical investigation. As a result, this system will benefit the doctors and the majority of the people in this country by assuring that their medical documents will not be manipulated, and it will have credibility across the border, allowing them to deal with international standards. However, in this discipline, a more accurate system with the maximum level of precision is required.

The following are the objectives of this study:

- **RO1:** To increase security and authenticity by generating a record that cannot be altered and keeping it safe.
- **RO2:** Develop an application to eradicate prescription forgery in Bangladesh.
- **RO3:** To study the technical feasibility of building a Hyperledger-based system for private data sharing with individual nodes in the network.
- **RO4:** To guide the design and implementation of similar Hyperledger-based systems in the future.
- **RO5:** To provide recommendations for areas of further research, based on the results of the study.

Chapter 2

Background Study

2.1 Blockchain

A blockchain can be visualized as a chain of blocks, where each block contains a certain amount of information or data. The blocks are connected in a linear fashion, with each block containing a unique code, known as a "hash," that links it to the previous block in the chain. The entire chain is secured using complex cryptography, making it nearly impossible to alter or tamper with any of the data contained within the blocks. Each block in the chain also contains a record of the previous transactions that have taken place on the blockchain, allowing users to track the history of the data and ensure its integrity. The decentralized nature of a blockchain means that it is distributed across a network of computers, rather than being stored in a central location, making it resistant to tampering and censorship.

2.2 Merkle Tree

A Merkle tree, also known as a binary hash tree shown in Figure 2.1, is a data structure used in computer science and cryptography to verify the integrity of large amounts of data. It allows for efficient and secure verification of data without having to transmit the entire data set. In a Merkle tree, data is represented in the form of leaf nodes, and each non-leaf node is the hash of its children. This creates a tree-like structure with a single hash, called the root hash, at the top. When data is added or removed from the tree, the affected hashes are recalculated and the root hash is updated. This allows for the efficient verification of the integrity of the data by only transmitting the root hash. Merkle trees are widely used in distributed systems and blockchain technology to verify the integrity of data being transmitted between nodes.

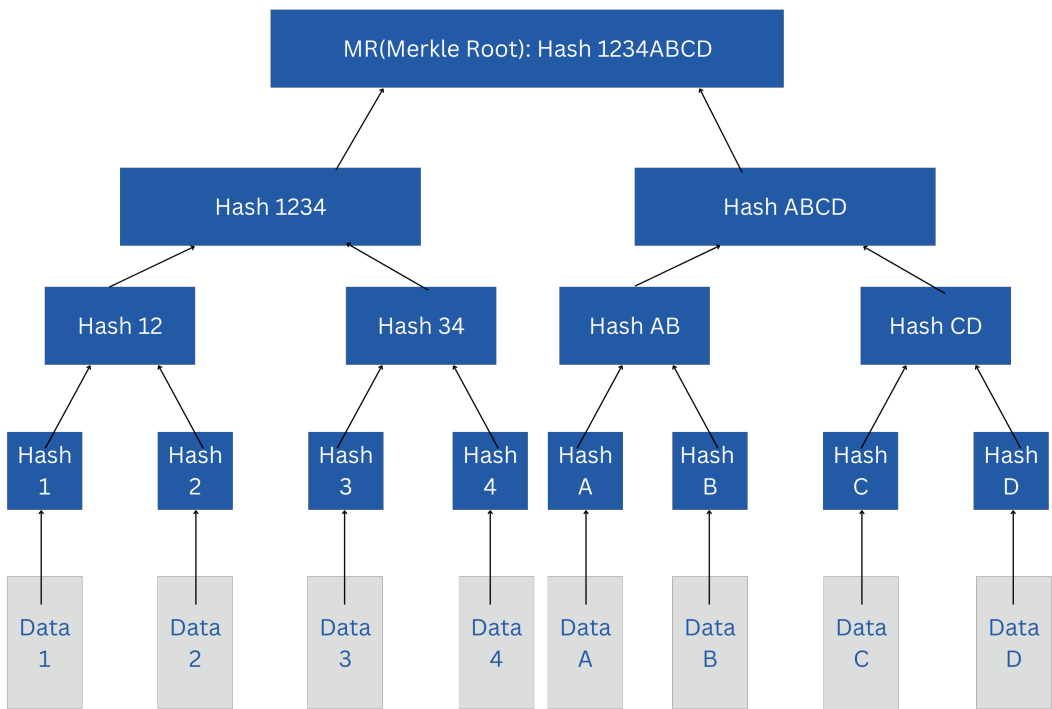


Figure 2.1: *Merkle Tree*

2.3 Symmetric key cryptography

Symmetric key cryptography, also known as shared secret cryptography, is a method of secure communication that uses the same key for both the encryption and decryption of a message. The sender uses the key to encrypt the message, and the receiver uses the same key to decrypt the message, which is shown in Figure 2.2. Some examples of symmetric key algorithms include AES (Advanced Encryption Standard), DES (Data Encryption Standard), and Blowfish. One of the main advantages of symmetric key cryptography is that it is relatively fast compared to other methods of encryption. However, it also has some disadvantages, such as the need to securely exchange the key between the sender and the receiver, and the possibility that the key could be discovered by an attacker.

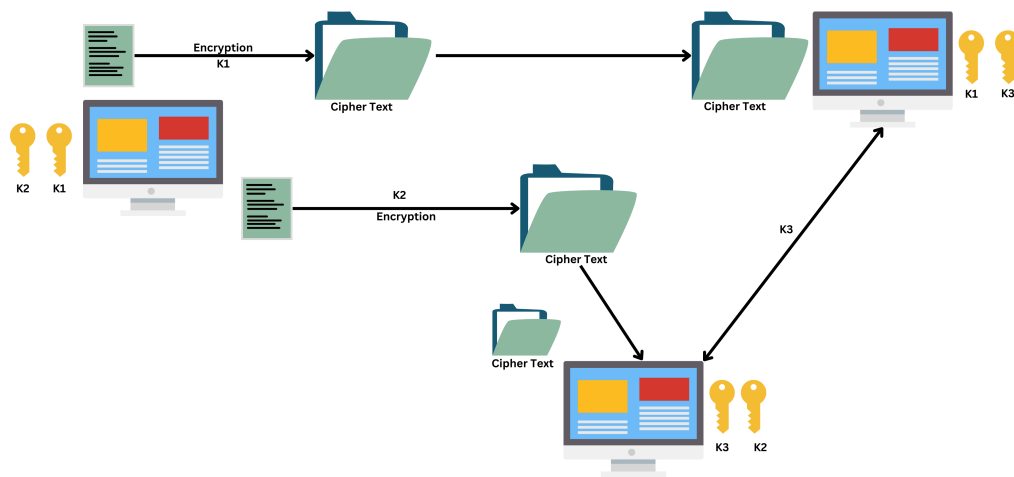


Figure 2.2: *Symmetric key cryptography*

2.4 Asymmetric key cryptography

Asymmetric key cryptography, also known as public key cryptography, is a method of encrypting and decrypting messages using a pair of keys. One of the keys, called the public key, is used to encrypt the message, and the other key, called the private key, is used to decrypt it. The public key can be shared with anyone, while the private key must be kept secret. This allows individuals to send messages to each other without the need to exchange keys beforehand. The security of this method relies on the fact that it is computationally infeasible to deduce the private key from the public key. This makes it difficult for an attacker to intercept and decrypt the message without access to the private key. Asymmetric key cryptography is commonly used in a secure communication over the internet, such as in the transport layer security (TLS) protocol that is used to secure web traffic.

2.5 Digital Signature

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software, or digital document. Digital signatures use a combination of private and public keys to sign and verify the identity of the sender or signer. The private key is used to create the digital signature, while the public key is used to verify it. The process is shown in Figure 2.3. Digital signatures provide several benefits, including non-repudiation (preventing the sender from denying the authenticity of the message or document), authentication (verifying the identity of the sender), and data integrity (ensuring that the message or document has not been altered).

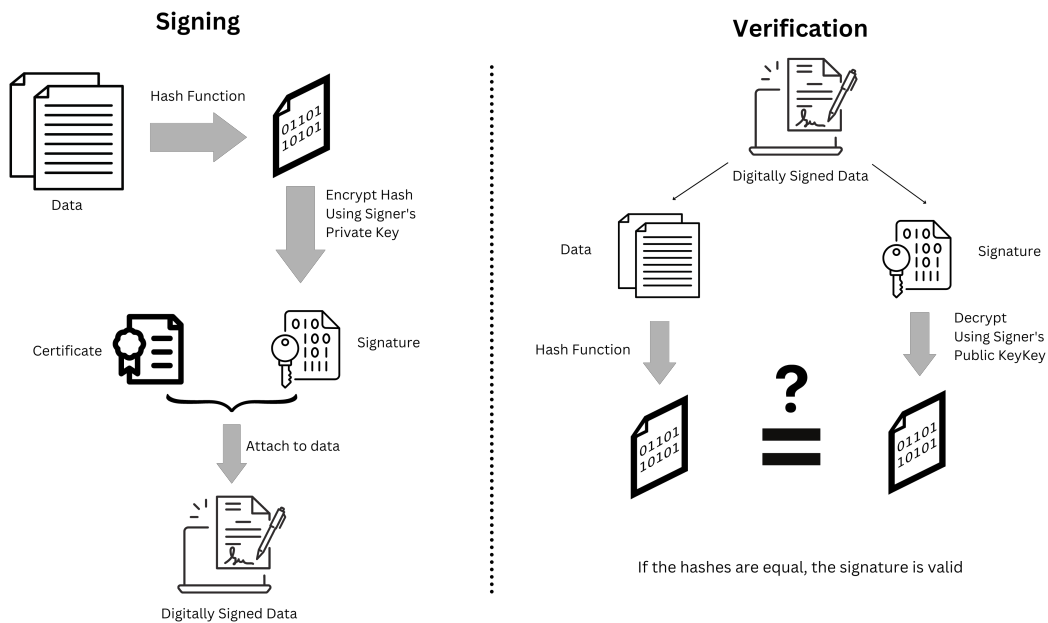


Figure 2.3: *Digital signature*

2.6 Public Blockchain

A public blockchain is a decentralized and distributed digital ledger that is open to the public and is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network. The public blockchain allows anyone to read or write to the ledger, provided they follow the rules of the network. Bitcoin and Ethereum are examples of public blockchain networks.

2.7 Private Blockchain

A private blockchain is a type of blockchain that is restricted to a specific group of individuals or organizations. In a private blockchain, only the members of the group that the blockchain belongs to can access the data stored on the blockchain. This is in contrast to a public blockchain, which is open to anyone and can be accessed

by anyone on the internet. Private blockchains are often used by organizations that want to keep their data secure and private, such as banks, healthcare organizations, and government agencies.

2.8 Consortium Blockchain

A consortium blockchain is a type of blockchain platform that is owned and operated by a group of organizations, rather than by a single entity. Consortium blockchains are typically used for specific business or industry purposes, and the members of the consortium work together to develop and maintain the blockchain. Unlike public blockchains, which are open to anyone to join and participate in, consortium blockchains are typically permissioned, meaning that only member organizations are allowed to participate in the network and validate transactions. This can make consortium blockchains more efficient and secure, as the members of the consortium can be trusted to act in the best interests of the network. However, it also means that consortium blockchains are less decentralized than public blockchains, as the member organizations have more control over the network.

2.9 Proof of Work

In the context of blockchain technology, proof of work (PoW) is a mechanism used to ensure that new transactions added to the blockchain are valid and secure. It is a computation process that requires a lot of effort and time to solve a complex mathematical problem, also known as a "puzzle." The puzzle is designed in such a way that it becomes increasingly difficult to solve as more transactions are added to the blockchain. Once the puzzle is solved, the transaction is considered to be verified and added to the blockchain. The proof of work mechanism is used to prevent malicious actors from altering or tampering with the transactions on the blockchain. It ensures that the transactions are secure and can be trusted.

2.10 Proof of Stake

Proof of stake (PoS) is a type of algorithm used by some blockchain networks to achieve distributed consensus. In PoS, the creator of a new block is chosen in a deterministic way, depending on their stake in the network. Stake refers to the number of coins that a miner has committed to the network as collateral. The idea behind PoS is that the more stake a miner has, the more invested they are in the success of the network, and the less likely they are to engage in malicious behavior. PoS is an alternative to proof of work (PoW), which is used by networks such as Bitcoin and Ethereum. In PoW, miners compete to solve a mathematical puzzle in order to create a new block.

2.11 Hyperledger fabric

Hyperledger Fabric is a permissioned blockchain platform that is designed to support the development of smart contracts and applications that can be run on top of the

blockchain. It is an open-source project under the Hyperledger umbrella, which is an umbrella project of the Linux Foundation for open-source blockchains. Hyperledger Fabric is intended to support a wide range of industries and applications, including supply chain management, financial services, and digital identity, among others. It is modular in design and can be configured to meet the needs of different organizations and applications. One of the key features of Hyperledger Fabric is its support for private and confidential transactions, which allows organizations to share data and conduct transactions without revealing sensitive information to the public.

2.12 Peers

In Hyperledger Fabric, a peer is a node in the network that can perform certain functions such as endorsement, committing transactions to the ledger, and serving as a lookup for transaction and block information. Peers can be divided into three categories: endorsement peers, commit peers, and anchor peers. Endorsement peers endorse transactions and return an endorsement to the client. Commit peers validate the endorsement and commit the transaction to the ledger if it is valid. Anchor peers are used for discovery and serve as the entry point for other peers to interact with the network.

2.13 Orderer

In Hyperledger Fabric, an orderer is a special type of peer that is responsible for ordering and delivering transactions to the correct peers in the network. The orderer receives transactions from clients and other peers, validates them, and then delivers them to the appropriate peers in the correct order. The orderer plays a central role in ensuring that transactions are processed and recorded consistently across the network.

2.14 Certificate Authority

In Hyperledger Fabric, a Certificate Authority (CA) is a service that issues digital certificates to identify network members, such as peers and clients. These digital certificates are used to establish trust and enable secure communication among network members. The CA is responsible for issuing and revoking digital certificates, as well as managing the certificate revocation list (CRL), depicted in Figure 2.4. A Certificate Authority (CA) in Hyperledger is responsible for issuing and managing digital certificates. The CA can also revoke certificates if necessary.

In Hyperledger, CA can work in two ways:

- **External CA:** It is an external third-party service that issues the certificates. It's not a part of the Hyperledger fabric but it can interact with it to issue the certificate.
- **Fabric CA:** It is a built-in CA service that is a part of the Hyperledger fabric network. It issues certificates for the members of the network.

Both External CA and Fabric CA are responsible for issuing certificates, but Fabric CA is tightly integrated into the Hyperledger fabric network and can be used to manage the identities of the members of the network.

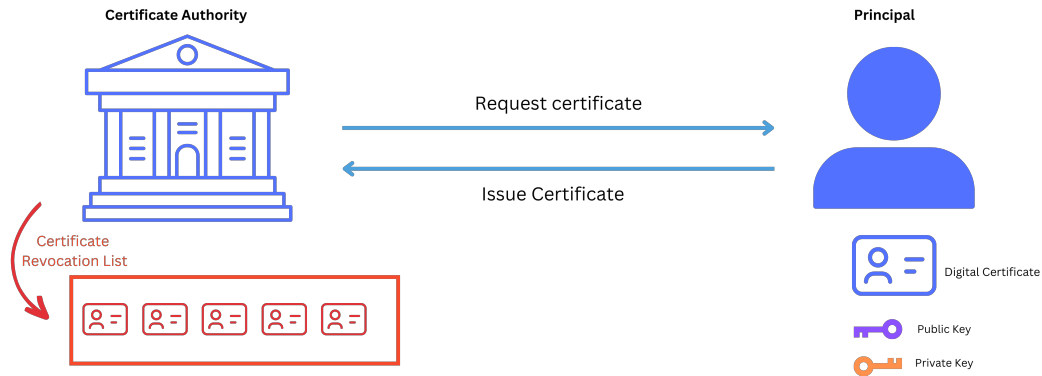


Figure 2.4: CA issuing and revoking certificates

2.15 Membership Service Provider

In Hyperledger, a Membership Service Provider (MSP) is responsible for managing the identities and permissions of entities on the network. It is used to authenticate and authorize access to the network and its resources.

MSP is implemented as a set of components that work together to manage the identities of members on the network. These components include:

- Identity: A digital certificate that is issued by a certificate authority (CA) and is used to authenticate the identity of a member.
- Policy: A set of rules that define the permissions of a member on the network.
- Role: A collection of policies that define the access rights of a member to different resources on the network.
- MSP Config: It contains the configuration information for the MSP, such as the CA certificate, CRL (Certificate Revocation List), and the identities of the members.

MSP is responsible for validating the identity of members, enforcing policies, and managing access to the network resources. It ensures that only authorized members can access and perform operations on the network, and that members can only access the resources for which they have been granted permission.

2.16 Shared ledger

In Hyperledger Fabric, a shared ledger is a database that records transactions across a distributed network of computers. It is maintained by a consortium of participants

and is used to track and verify the status of transactions within the network. The ledger is an append-only data structure, which means that new data can be added to it, but existing data cannot be modified or deleted. This helps to ensure the integrity and immutability of the data stored in the ledger. The shared ledger is an important component of Hyperledger Fabric and is used to facilitate the exchange of information and value between different parties within the network.

2.17 Private Data

In Hyperledger Fabric, private data refers to sensitive information that is only accessible to a certain subset of network participants. This data is stored on a separate ledger, known as a private data ledger, and is only shared among authorized members of the network, as shown in Figure 2.5. Access to the private data ledger is controlled through a set of predefined access controls, which are defined by the network administrator. This allows for certain parties to have access to certain parts of the ledger while others do not. This allows for sensitive data to be shared with only those who need to see it, while keeping it confidential from others.

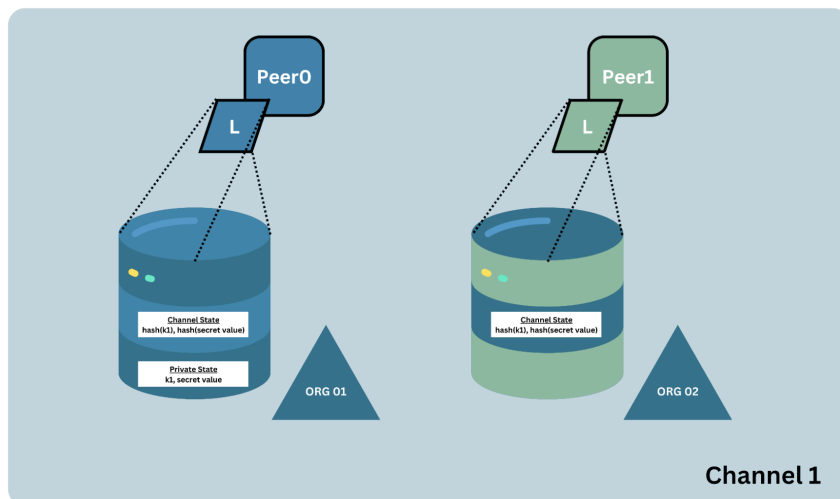


Figure 2.5: *Authorized and Unauthorized Peers*

2.18 World State and Transactional Log

In a Hyperledger Fabric blockchain, the world state represents the current state of the network. It is implemented as a key-value store, where the keys are the unique identifiers of the assets and the values are the current state of the assets. The keys are generated based on the unique attributes of the assets and are used to look up the current state of the assets in the world state database. The transactional log, on the other hand, is a record of all the transactions that have occurred on the network. It is a series of blocks, each containing a list of transactions that have been committed to the network. The transactional log is used to ensure the integrity of the world state, as it allows the network to determine the valid state of an asset at any given point in time. Figure 2.6 shows an overview.

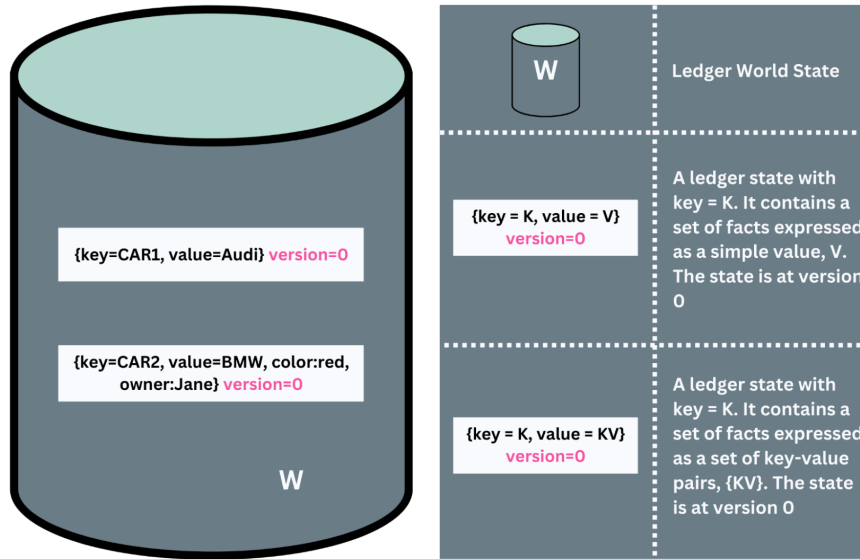


Figure 2.6: *World State and Transactional Log*

2.19 Channel

In Hyperledger Fabric, a channel is a private, secure communication link between two or more organizations that participate in a blockchain network. The channel is used to exchange confidential information and transactions between the participating organizations. Each channel is isolated from the other channels and only the organizations that are part of the channel can access the information and transactions within that channel. Organizations can create multiple channels to share different types of information and transactions with different sets of organizations.

2.20 Asset

In Hyperledger Fabric, an asset represents a tangible or intangible item of value that is tracked on the ledger. Examples of assets could include physical goods such as a car or a house, financial assets such as a bond or a currency, or intangible assets such as a patent or a trademark. The ledger is used to track the ownership and movement of these assets as they are transferred from one entity to another.

Chapter 3

Literature Review

There is a greater need than ever for a blockchain-based certificate authentication mechanism. The problems with hard copies of certificates can be readily fixed by employing blockchain-based document authentication. Organizations can use the system to issue and authorize their certificates, and anyone can readily share those accreditations with other individuals for verification. It is simple to confirm someone's credibility, and the hassle of amending the certificate can be reduced. In light of everything, a blockchain-based certification system is a significant step toward a world with more transparency and accountability.

3.1 Related Works

In this research paper [3], the authors suggest a decentralized application that makes use of blockchain technology to provide smart contract-based document authentication and verification. This methodology creates a distinct fingerprint of each input file that utilized a cryptographic hash function, as opposed to the typical method of storing the entire input digital document. In order to verify the document in the future, this fingerprint is stored on the blockchain network. This blockchain-based technology enables businesses to validate the papers they produce and enable third parties to confirm them. This article discusses several crucial issues, including how to guarantee flexibility and processing efficiency, how IoT may connect billions of items together, and how to address the real-time and compliance standards for industrial applications. It also includes a thorough discussion of the complexity of adopting Blockchain for 5G-Enabled IoT.

The authors of the study [4] describe a distributed web app for digitized validation in peer-to-peer cloud storage that makes the inspection more accessible, transparent, and auditable by utilizing Ethereum blockchain technology. The suggested model incorporates a number of techniques, including peer-to-peer networks, digital signatures, hashing, online storage security, public/private key cryptography, and proof of work, which makes it easier and faster for any organization or authority to verify any uploaded documents with just one click. Additionally, each document is given its own hash value. By filling in the gaps and overcoming the challenges in the current document verification methods, the authors claim that their suggested model successfully satisfies all the requirements for a digital document verification system.

Here in [5] of the given reference, the authors use a blockchain-based drastic supervision system to generate e-certificates based on the documentation submitted by each student and user. The system is broken down into four sections. First, they define the user's ability to upload documents or educational certificates, and this documentation from recognized organizations will be verified by the middleware authority known as the Third Party Auditor (TPA). If all of the documents have been approved, a QR code and unique ID are dynamically generated for an e-certificate. Once this process is complete, the data is stored in various data nodes, and the student is given a QR code and a UID. Additionally, any entity can use the QR code or request a Unique Id number in order to authenticate student documentation. Following safe authentication, blockchain will deliver consistent information once these companies have verified the student data. The authors used an open Smart contract throughout the execution, with a generic approach based on the SHA family of algorithms, a mining algorithm to generate valid hashes, and a consensus algorithm to assess the proof of work.

The proposed framework in this paper [6] aims to establish a secure and private method for sharing medical data. This is achieved through the incorporation of multi-authority attribute-based encryption, blockchain technology, and smart contract integration, in addition to utilizing software-defined networking. The framework encrypts and stores patients' medical records in hospital databases with stringent access controls enforced through attribute-based encryption and privacy level classification. The architecture employs smart contracts to facilitate the economic logic of clinical data consumption, blockchain technology to connect and integrate dispersed private databases from participating hospitals, and software-defined networking to revoke access permissions. The evaluation system of the prototype shows that the corresponding computational expenses are practical.

A blockchain-based digital certificate verification system that uses an owner authentication scheme and stores the students' time and space as blocks, is proposed in the paper- "The Impact of the Blockchain on Academic Certificate Verification System-Review" [7]. A decentralized, public ledger that is resistant to tampering and alteration, preserving the integrity of the document and ensuring the security of the digital asset. This stated clearly that such an innovation is necessary to keep digital properties secure and available to anyone without data loss while requiring the least amount of maintenance.

The goal of this research [8] is to - optimize public e-documents in a cutting-edge and safe way by using the capabilities of Blockchain technology. Presenting a Blockchain-based documentation qualitative methodology that is used in conjunction with a literature review study, and which also makes use of DAOs (Decentralized Autonomous Organizations) and smart contracts to guarantee the quick execution of the system. As a result, contemporary, secure government e-documents used for document verification can greatly preserve transparency and boost public trust.

The potential benefits and issues resolved by a blockchain-based system for transferring ownership of land have been explored in this paper [9]. The authors are attempting to develop a system that is built around Ethereum. On a blockchain,

every transaction made during the transfer of land ownership will be documented. By utilizing the blockchain's smart contract idea, they may set off a number of different events, such as a money transfer event from the buyer to the seller upon the successful validation of the transfer of land ownership and the access of land records to a land inspector. This approach will address the issues that all three parties faced during the asset registration system and get rid of middlemen like real estate brokers. It also strengthens the land registration procedure and reduces instances of fraud, according to them. The system makes it easy to validate the lands because the public ledger stores immutable transactions.

The paper [10] aims to present a model for using blockchain technology to issue and verify academic certificates. The proposed model demonstrates that blockchain technology can be effectively used for academic certificate authentication, meeting the requirements of a modern verification system and addressing the challenges of current methods. To verify the authenticity of an issued certificate using blockchain technology, the following steps are taken: First, the hash of the certificate is generated. Then, the certificate is encrypted using the issuer's private key and provided to the recipient with a digital signature embedded in it. The issuer also uploads the hash of the digital signature to the blockchain. When the employer receives the certificate, they can decrypt the digital signature using the recipient's public key and generate a hash of the decrypted certificate. The employer can then compare this hash to the hash stored on the blockchain to check the authenticity of the certificate. If the hashes match, the certificate is considered valid. If the hashes do not match, the certificate is considered invalid.

The authors of the paper [11] proposed to address the issue of counterfeiting certificates by leveraging the immutable nature of blockchain. To verify the authenticity of a certificate using blockchain technology, the following steps are taken: First, an electronic file of the certificate is generated. The file's hash value is then calculated and stored on the blockchain. The system creates a QR code and inquiry string code for the certificate and provides them to the student, as depicted in Figure 3.1. The student can send the certificate's serial number and QR code to the company for verification. The company can then scan the QR code using a phone and verify the certificate by checking the serial number and QR code against the information stored on the blockchain. If the QR code and serial number match the information on the blockchain, the certificate is considered valid. If there is a discrepancy, the certificate is considered invalid.

The concern of [12] is also that these documents are often stored in centralized databases, requiring physical presence at the issuing office to access them. This system is vulnerable to natural disasters such as floods and earthquakes, which could result in the permanent loss of all documents. So, the authors mentioned the following steps to mitigate the problem. First, a private network is created using a bottle server. The authorized issuer then uploads the e-certificate file to the blockchain. The issuer provides the hash of the certificate to the recipient, who can use an API to query the hash. An OTP is generated and sent to the API and a random node in the network, allowing the recipient to download the e-certificate file. This process enables the recipient to verify the authenticity of the e-certificate using the private

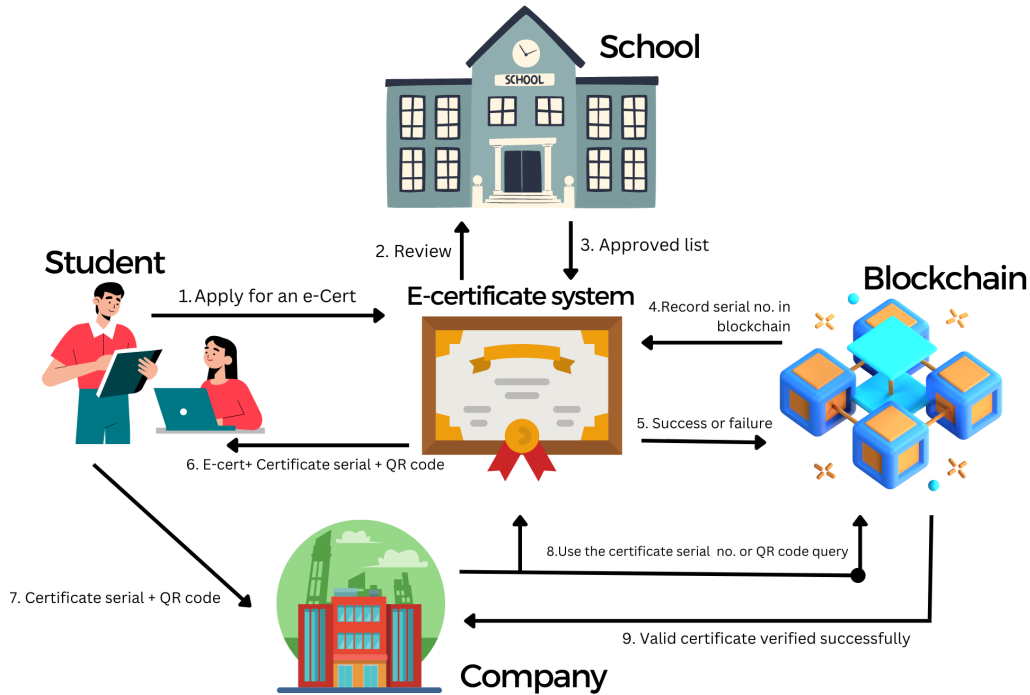


Figure 3.1: *Authenticating Certificates using QR Code*

network and blockchain technology.

This [13] research introduces UniCert, a model for issuing and verifying documents and certificates using UniCoin, a digital currency constructed on blockchain technology. According to the authors, this model can be extended to tackle various issues such as counterfeiting, copyright protection of music, and patents, all of which are implemented using blockchain technology, shown in Figure 3.2. In this process for issuing and verifying certificates using UniCert and UniCoin, the following steps are taken: First, the issuer collects information for the certification process. The hashed certificates are stored in the metadata of the transaction using the Merkle tree hash algorithm. These transactions are pushed into the UniCert system for validation. Once the transactions are validated by UniCert, recipients receive a certificate identity number for the certificate. Recipients can use this identification number to view the issued certificates and verify their authenticity through the UniCert system. To retrieve the original certificate, the identification number and the transaction identity of the original certificate must be provided to query the transaction in UniCert.

In the paper [14], the following steps are taken to issue and verify a certificate. First, the issuer generates a signed e-certificate, sets the default access control, and uploads the information to the central system server. The issuer then sends the certificate to the student via email. The student downloads the e-certificate, verifies and validates it, and uploads it to the central system server's subsystem using an access token. The student can set the access control for their certificate and send it to the employer via email. The employer can then download the certificate, access the central server's subsystem using the access token, and verify the authenticity of the certificate.

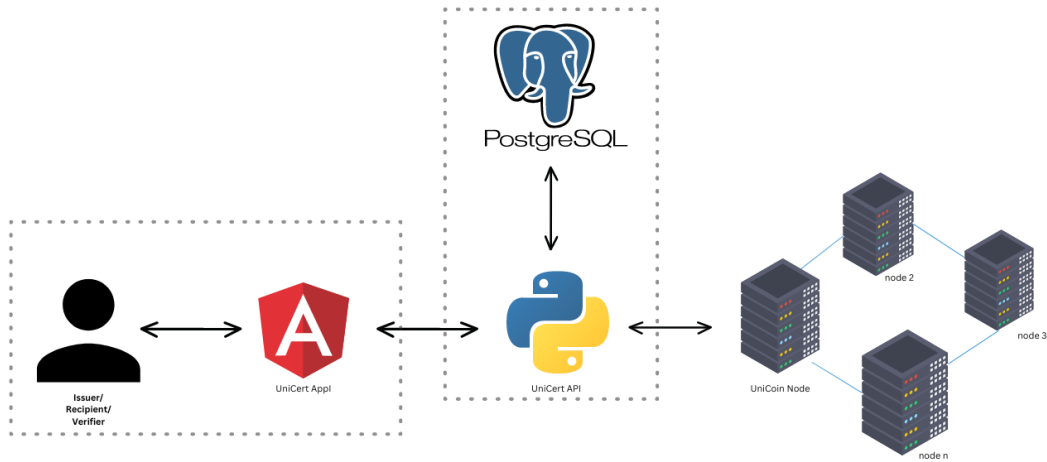


Figure 3.2: *UniCert System Diagram*

The solution proposed in reference [15] includes a web-based interface for registration and initiation of transfer requests, with a backend architecture built on Hyperledger Fabric and Hyperledger Composer. The backend infrastructure is employed to store and maintain the hash of the records on the blockchain for authentication purposes. To facilitate the transfer of transcripts between universities using a web application, the following steps are proposed: Utilize a web-based interface as the primary medium for the transfer process. Transform the transcript, being off-chain data, into a hash and record the hash on-chain as part of the transaction. Invoke a function, named `sendTranscript()`, to execute the transfer of proprietorship of the transcript to the addressee university, and at the same time, records the hash of the transcript as part of the transaction on the blockchain. The addressee university can then retrieve the transcript and confirm its authenticity by comparing it to the hash recorded on the blockchain. Implement access controls to regulate user access and permissions as required.

In the paper [16], to create a secure system for storing and verifying documents using a web application and the Hyperledger network, the following steps are taken by the authors: First, a web application is created for various types of users. Each user is assigned a unique identity on Hyperledger by the system administrator. The owner of the document uploads it and links it to their identity to ensure ownership. Encrypted API (REST API) endpoints are used to ensure that only authenticated users can access the flow of data to and from Hyperledger. When data is transferred from the web interface to the blockchain, the hash of the file is calculated and stored in the Hyperledger network, while the actual file is stored in an off-chain database. The verifier can perform document verification, but only they can see unverified documents to ensure privacy and confidentiality. Data is only visible to authorized entities with permission to access it. The issuer, who is also the administrator of the system, is responsible for physically verifying new organizations or users and issuing identities to them after verification.

In this system [17], members including universities, companies, police, and doctors are part of the Hyperledger network. Each member has at least three entities: a Peer, an Admin, and a Certificate Authority. The Peer submits a certificate to the Admin for verification. If the certificate is approved, the Admin sends the hash values of the certificate and the student’s SSN and last name to the orderer, who updates the entry in the blockchain. The student then sends their documents to the recruiter, who can verify their authenticity by querying the web app with the student’s SSN and last name, as well as the certificate file. The recruiter receives a message indicating whether the documents are validated or not.

To ensure the authenticity of educational transcripts, in the paper [18], the authors make use of a system that utilizes blockchain technology to store and verify grades. Teachers submit signed grades to the institution’s database, and the institution then sends the data to the Hyperledger network, as shown in Figure 3.3. The Smart Contract on the network checks if the student is eligible to pass and, if so, adds the information to the student’s transcript on the blockchain. The issuing institution is then notified and can provide a certificate to the student. A verifier can use a web app to validate the certificate on the Hyperledger network. This process ensures the integrity and security of the educational transcripts.

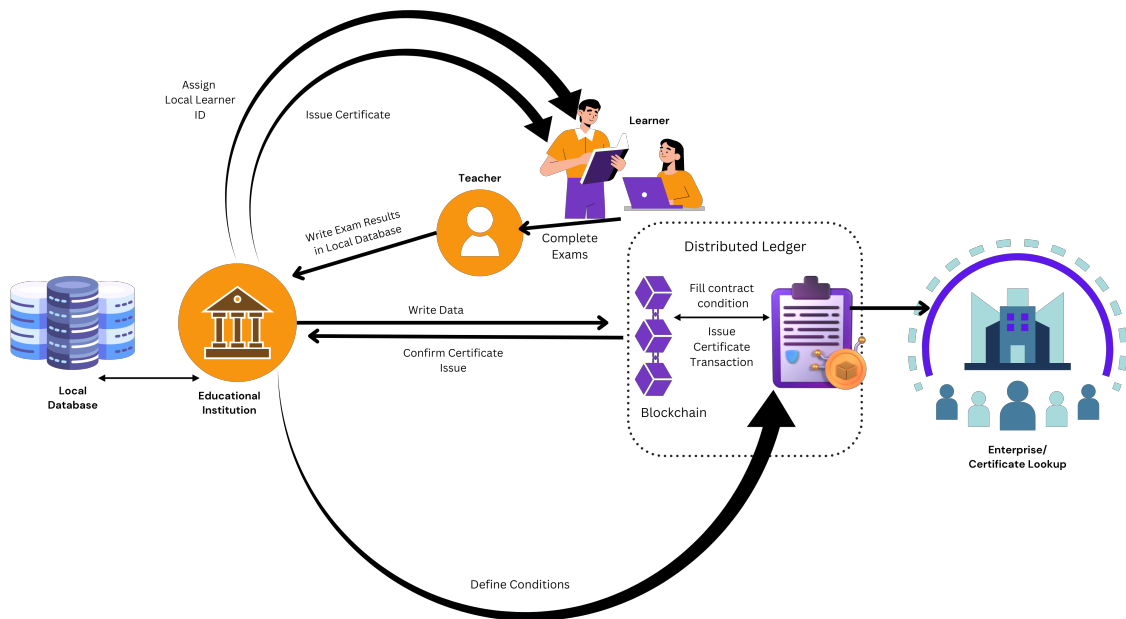


Figure 3.3: Automating the process of certificate storage

3.2 Comparative Analysis with Related Works

The methodology employed in this paper [10] for the graduation certificate verification model via utilization of the blockchain technology involves generating a hash of the certificate, encrypting the certificate with a private key, providing the encrypted certificate with a digital signature to the recipient, uploading the hash of the digital signature to the blockchain, and verifying the authenticity of the certificate by decrypting the digital signature with the recipient's public key, generating a hash of the decrypted certificate, comparing the generated hash to the hash on the blockchain, and determining the authenticity of the certificate based on the comparison. However, a major shortcoming of this methodology is that if the private key used to encrypt the certificate is lost or compromised, the certificate cannot be decrypted and verified. Additionally, as the blockchain is public, the transactions may be slow and additional gas fees may be added. Our solution to address these issues is to encrypt the medical files using a symmetric key and store the key on the Hyperledger Fabric network. This approach eliminates the need for gas fees as the nodes in the network will be composed of hospitals and the Ministry of Health and Family Welfare.

The methodology of this paper, [11] involves the generation of an electronic certificate file, calculation of its hash, storage of the hash in a blockchain, creation of a QR code and inquiry string, and provision of the QR code to the student. The student then sends the serial number and QR code to the company, which verifies the certificate using the QR code and serial number by checking against the blockchain. However, this approach has certain limitations. One major limitation is that if the QR code or inquiry string is lost or becomes damaged, the student may not be able to provide it to the company for verification. Additionally, as the blockchain is public, the transactions may be slow and incur extra costs in the form of gas fees. To address these limitations, the proposed solution in our paper eliminates the need for an extra QR code by allowing for direct sharing of the file with the verifier, and eliminates the need for gas fees by limiting the nodes to hospitals and the Ministry of Health and Family Welfare. Overall, this paper presents a promising approach for digital certificate verification using blockchain and smart contract technology, but further improvements in security and efficiency are necessary to ensure its practical implementation.

In the paper titled [12] the authors propose a method for storing and verifying electronic documents using a private blockchain network set up on a bottle server. The process involves an authorized issuer uploading an e-certificate file to the blockchain and providing the recipient with the certificate's hash. The recipient then uses an API to query the blockchain with the hash, generating an OTP which allows them to download the e-certificate file. However, this method has several shortcomings including the unnecessary on-chain data, lack of automation due to the absence of smart contracts, and the possibility of losing the OTP, rendering the e-certificate file inaccessible. Additionally, the API may not be compatible with certain devices, making it difficult for some users to retrieve their e-certificate files. In contrast, our proposed solution addresses these shortcomings by storing the files on IPFS instead of directly on the fabric network, implementing smart contracts for automation,

sharing the files directly through a webapp, and ensuring that the webapp is accessible through any browser.

The methodology presented in the [13] paper involves collecting information for certification by the issuer, storing hashed certificates in transaction metadata using a Merkle tree, and undergoing validation through the UniCert system. The recipients receive a certificate hash as an identity number, and certificates can be viewed and validated through the UniCert system. However, this methodology has several limitations. Firstly, if the issuer does not collect complete or accurate information for the certification, the resulting certificate may not be reliable. Secondly, the mining process is expensive, as the paper uses one single transaction to upload a certificate batch, with the transaction meta-data containing a Merkle tree that contains all the certificate hashes. This results in the use of more computational power. Our proposed solution to these shortcomings is that the issuer themselves creates the prescription transaction with the necessary details, and only one single hash per file is needed to calculate, resulting in much less computational power.

The methodology presented in the paper [14] involves a central server-based approach for the issuance, storage, and verification of digital certificates. The issuer generates a signed e-certificate, sets default access control, and uploads it to a central server. The certificate is then sent to the student via email, who is responsible for downloading, verifying, and uploading the certificate to the central server's subsystem using an access token. The student can then set access control and send the certificate to an employer via email. The employer can then download the certificate, upload it to the central server's subsystem using an access token, and verify it. However, this approach is not without its shortcomings. One major limitation is that it stores unnecessary on-chain data. Additionally, if the email containing the certificate is not delivered or is lost, the student will not be able to access the certificate. The use of an access token also introduces the potential for loss or compromise, rendering the student unable to upload the certificate to the central server's subsystem or the employer unable to verify it. Furthermore, the approach is not straightforward for end-users. Our proposed solution addresses these shortcomings by utilizing IPFS for direct storage and sharing of files, eliminating the need for any third-party apps and simplifying the process through the use of a single webapp for all tasks including sharing, retrieving and verifying. Additionally, the issuer himself will upload the medical files to IPFS and store its hash on the chain.

The methodology of [15] is to utilize a web app for university transcript transfer, where off-chain transcripts are hashed and stored on-chain, and ownership and records of the transcript hash are transferred via the `sendTranscript()` function. The recipient university verifies the transcript with the saved hash and access control limits (ACL) are used to restrict user permissions. However, one major drawback of this system is the risk of losing the off-chain transcript, which may prevent the generation of a valid hash to be stored on-chain. To address this issue, our proposed solution is to store the files decentrally, which reduces the likelihood of the file getting lost forever.

The methodology outlined in the paper [16] involves a web application for various users, where each user receives a unique identity from the system administrator. The documents are uploaded and linked to the owner’s identity, and encrypted API endpoints are used to ensure secure data transfer. The hash of the file is calculated and stored on Hyperledger, while the actual file is stored in an off-chain database. The verifier performs document verification, and the data is only visible to authorized entities. The system administrator is responsible for physical verification and issuing identities to new users. However, a shortcoming of this approach is that it entrusts students with the responsibility of uploading their own certificates. Additionally, the ownership of the certificate is kept with the issuer itself, rather than being shared with the student. To address these issues, our proposed solution suggests that hospitals nodes/peers upload the prescription on the ledger and share the ownership with the patients.

The methodology presented in the paper [17] involves a process in which a peer submits a certificate to an admin for verification and approval. The admin then sends the hash values of the approved certificate to an orderer, who updates the entry in the blockchain. The student then sends the documents to a recruiter, who queries a web application with the student’s SSN and last name to receive a validation message. However, this approach has several shortcomings, namely that the ownership of the certificates is not shared with the students, students have no control over who can access their certificates and for how long, and multiple hashes are generated unnecessarily. Our proposed solution addresses these issues by sharing ownership of the certificates with the patients, giving patients control over who can access their certificates and for how long using Hyperledger Access Control Limit (ACL), and generating one single hash/file that is stored on-chain. This approach ensures security, transparency, and control for the students while maintaining the integrity of the information stored on the blockchain.

The methodology proposed in the [18] paper involves a process in which teachers submit grades and digitally sign them using their private key. The institution then sends the grade data and private key signature to the Hyperledger network, where it is verified to determine if the student is eligible to pass. If the student passes, the data is stored in the blockchain and mapped to the student’s transcript. The institution then issues a certificate to the student, and verifiers can use a web application to validate the certificate against the Hyperledger network. However, this methodology has several shortcomings, including a lack of proper authentication of roles, the storing of unencrypted transcripts on the blockchain which breaches the confidentiality of the student, and the lack of ownership and control for the students over who can verify the certificate and for how long it can be seen. Our proposed solution addresses these shortcomings by implementing authentication using a Certificate Authority (CA), encrypting the files before uploading them to IPFS and giving patients control over who they share their certificates with and for how long, using Hyperledger Access Control Limit (ACL).

Chapter 4

Methodology

4.1 Architecture

The increasing prevalence of counterfeiting and forging documents, such as prescriptions and IDs, has made it difficult to trust the authenticity of these important documents. Traditional methods of verification are often costly and time-consuming, leading to a need for a more efficient and secure solution. This problem statement aims to address the issue of ensuring the authenticity of documents through the use of blockchain technology and the Hyperledger Fabric platform.

The proposed solution aims to address the issue of authenticating documents through the use of a web application and the Hyperledger Fabric platform. This application, which will be accessible to clients, allows for the retrieval and verification of prescriptions within the Hyperledger Fabric network. The app will be connected to the network via a gateway, which will facilitate the transmission of commands from the user to the network.

The Ministry of Health and Family Welfare (MOHFW) of Bangladesh is responsible for overseeing all hospitals in the country, which can be seen in Figure 4.1. In order to ensure the authenticity and security of documents, such as prescriptions and IDs, the MOHFW will oversee a Hyperledger Fabric network. The MOHFW will act as the root Certificate Authority and Membership Service Provider, granting access and roles to new hospitals and patients seeking to join the network. By using this system, the MOHFW can effectively verify the authenticity of documents and maintain a secure system for storing and accessing them.

When a new hospital wants to join the network, the MOHFW will grant the hospital's admin nodes access and a role in the network. Patients who want to join the network will also need to be granted access. However, it is practically impossible for the MOHFW nodes alone to provide a role to every patient at every hospital. That's where intermediary CAs come in. The MOHFW will make some nodes from each hospital, intermediary CAs, allowing each hospital to handle and have Access Control Limit (ACL) for their own patients, illustrated in Figure 4.2. This makes the process of access control in the network faster and more secure. In our proposed plan, the MOHFW has full control over who can access the network and how each node can interact with it. This is only possible with a permissioned consortium

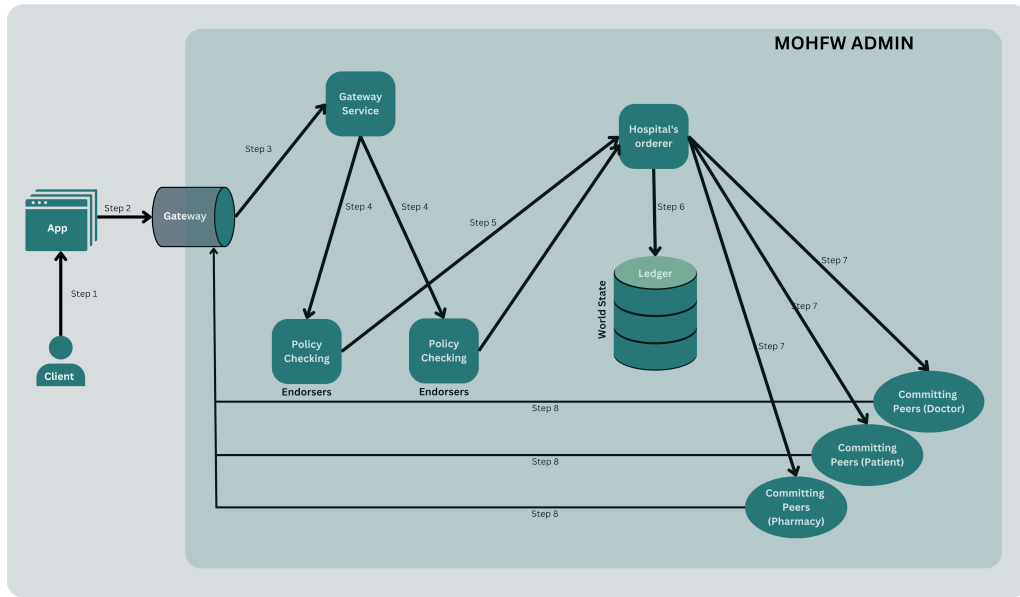


Figure 4.1: *System Architecture and workflow from MOHFW Admin control*

blockchain, not with a public or fully private blockchain, which is why we chose to solve the problem using Hyperledger Fabric.

The application will utilize the gateway to access the network from the user end. Upon accessing the network, the gateway service will forward the request to enter the network to the endorsers. The endorsers will evaluate the request using a chaincode to determine whether it is suitable for acceptance into the network. The endorsers will simulate the request in order to determine its validity and suitability for acceptance into the network.

When the gateway service forwards a transfer request to the hospital node within the Hyperledger Fabric network, the hospital node will generate a Transfer Proposal Response (TPR) message in response. The TPR message will indicate whether the transfer proposal has been accepted or rejected, based on the evaluation of the request by the endorsers. The TP message is a request to transfer a specified number of assets from one party to another. The TPR message is a response to the TP message, indicating whether the transfer proposal has been accepted or rejected.

In the Hyperledger Fabric network, a transaction proposal must be signed by all necessary endorsers before it can be added to a block. The list of required endorsers is determined by the membership service provider and may include one or more endorsers or none at all, depending on the configuration set by the network administrators.

After all the necessary signatures have been obtained, the gateway service retrieves the proposal and verifies that all required signatures are present. If the signatures are valid, the gateway service sends the proposal to the orderer for commitment to

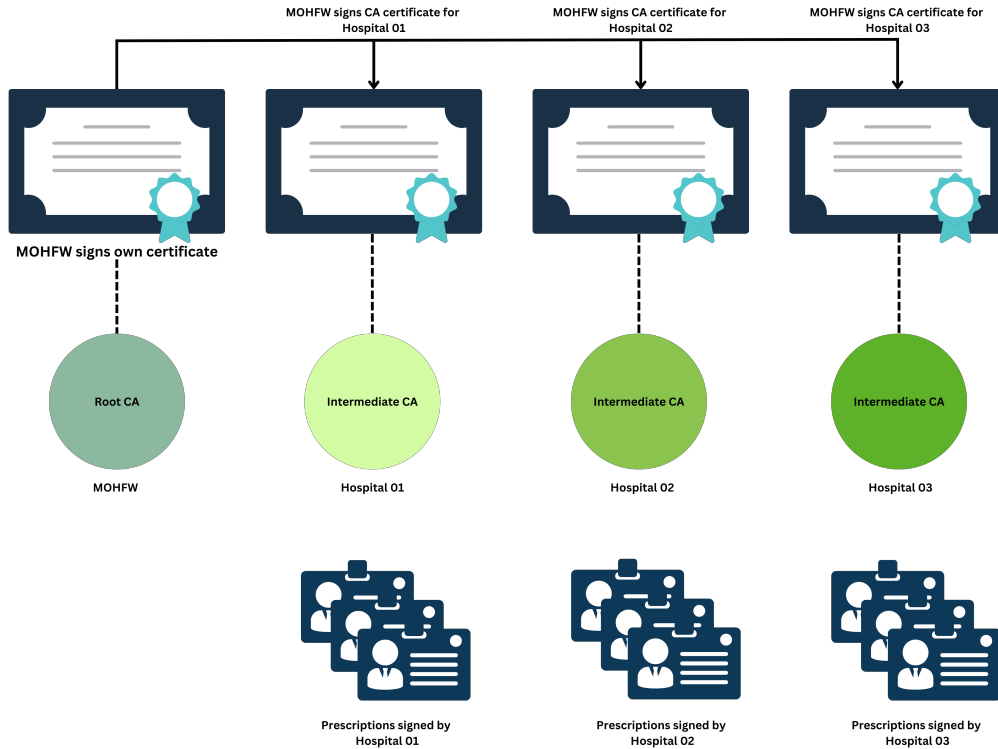


Figure 4.2: *CA diagram*

the block. If any signatures are missing or an unauthorized peer has signed, the gateway service rejects the entire transaction and notifies the client.

If the transfer proposal is accepted by the endorsers, it will be forwarded to the hospital orderer for further processing, along with a unique key and version identifier. The orderer will use this information to verify the validity of the request and update the relevant block in the distributed ledger accordingly. The orderer will verify the validity of the digital signature and update the block accordingly. The orderer will also update the world state and broadcast a confirmation message to the peers in the network, enabling them to record the data in their respective ledgers.

Upon receiving the confirmation message from the orderer, the peers on the network will verify that all endorsers have endorsed the request, check the version number of the early request first, and update their ledgers accordingly. Orderers will distribute the transaction to committing peers, shown in Figure 4.3, who will verify the version and record it in the ledger. It is important to check the version in order to track the order in which the transaction was created. When a later version is requested after an earlier version, the ledger will still be updated with the earliest version that was requested. If the version of the transaction that is being simulated by the endorsing peers does not match the version of the transaction being committed by the committing peers, then there will be a discrepancy in the data, defeating the purpose of using a blockchain. These updates will then be relayed to the gateway, where the user can access the original request that was submitted. This constitutes the complete process within the network.

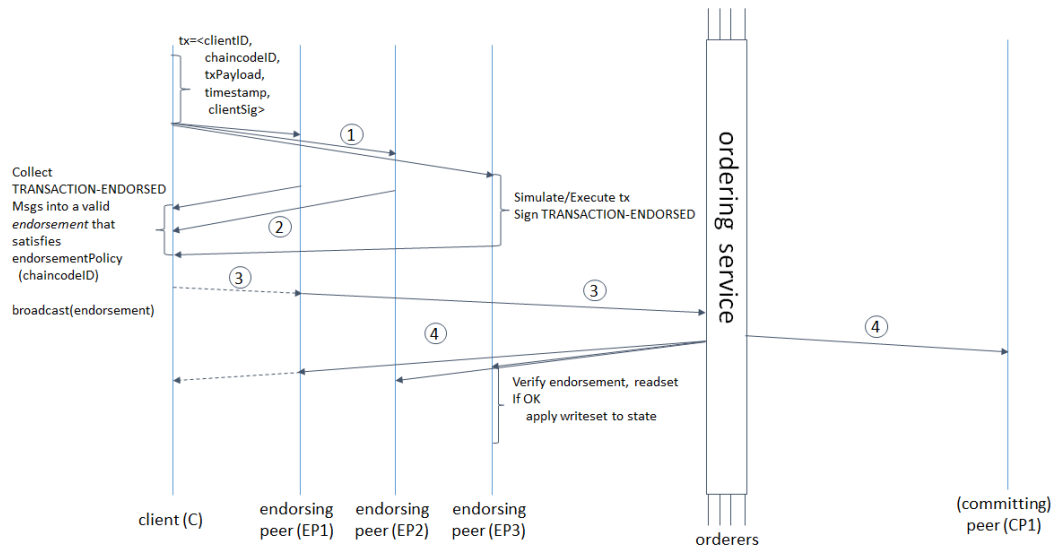


Figure 4.3: *Process of ordering service*

In the event that a patient's account has been compromised or their certificate becomes invalidated, the Certificate Authority admins can add the certificate to the Certificate Revocation List (CRL). When a verifier attempts to validate or verify the certificate, it will be flagged as invalid, shown in Figure 4.4.

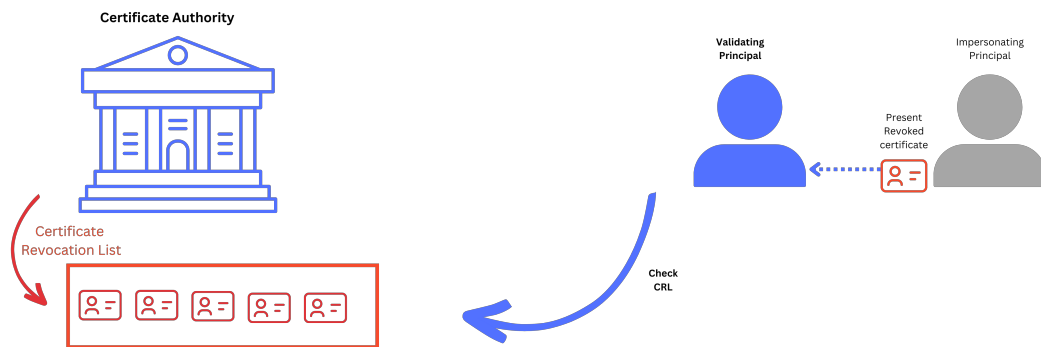


Figure 4.4: *Invalid student account added to the CRL*

4.2 Data Storage

In our proposed system, data will be primarily stored in two locations: the Inter-Planetary File System (IPFS) and the Hyperledger Fabric network. In the IPFS, all medical images of a patient will be saved and encrypted using a unique private key for each user and their respective prescriptions. These public keys are stored in the private ledger and is not accessible to outside of the network. The encryption and decryption processes are carried out in the backend, with only the necessary data displayed on the front end, like in Figure 4.5.

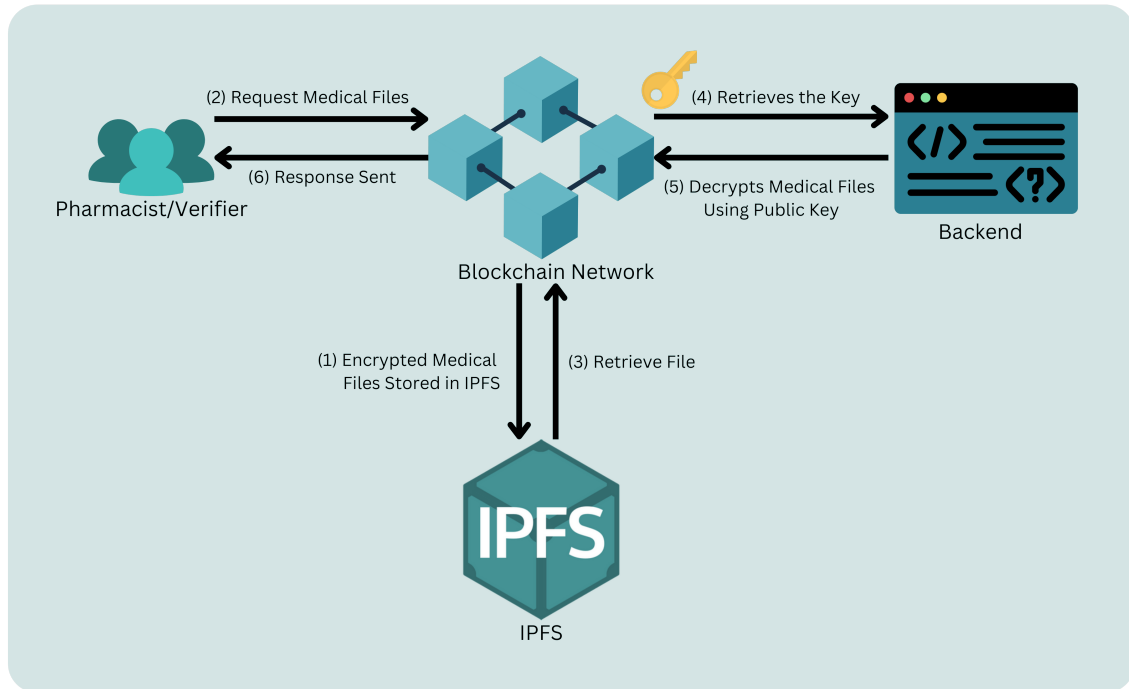


Figure 4.5: *User request and asymmetric key decryption for file retrieving*

On the other hand, the prescription data and hash of the medical images will be stored on the Hyperledger Fabric network. A hash is a unique value that is generated by running the contents of a file through a mathematical function. If the contents of the file are modified in any way, the resulting hash will be different. Therefore, by comparing the hash stored on the Hyperledger Fabric network with the hash of the medical files stored on the IPFS, it is possible to verify the authenticity of the files. If the two hashes match, it can be concluded that the files are valid. If the hashes do not match, it may indicate that the medical files have been tampered with or is otherwise invalid. To facilitate this process, the hash of the files will be mapped to the user in the shared ledger of the Hyperledger Fabric network.

4.3 User Experience

Our system’s backend will be powered by both LevelDB and the Hyperledger network. The front end will feature a web application with distinct interfaces for admins, patients, and verifiers. Patients can view their own prescriptions and download or print them after logging in. Login credentials are verified by the network, shown in Figure 4.6, and patients can also log in using a web3 wallet. After logging in, patients can share their prescriptions with a specific wallet address or a verified user.

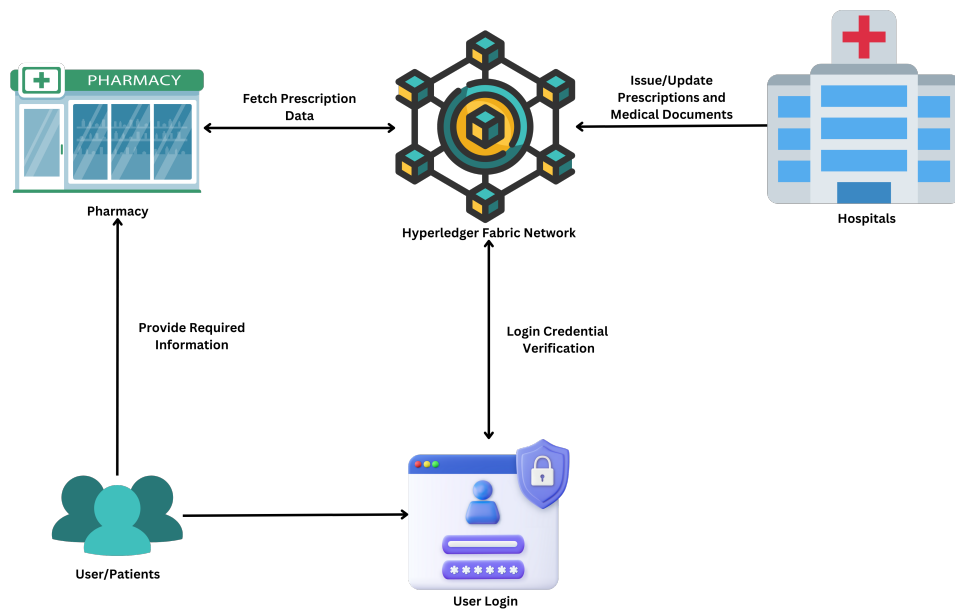


Figure 4.6: *User Interaction*

The process for uploading and storing medical information on a blockchain network using Hyperledger Fabric and IPFS is shown in Figure 4.7 and it involves the following steps:

- Prescriptions are directly written in the hyperledger fabric network.
- Medical images are uploaded by the doctors from local database to the IPFS and their hash is also calculated.
- The hash of the medical files is then stored on the Hyperledger network through the use of a smart contract.
- Patients and doctors are notified of this event and authorized individuals are able to view the prescriptions and medical images.

The verifier/pharmacist will then be able to access and verify the authenticity of a prescription shared by a patient through a login process on the web application interface. Upon logging in, the verifier will be notified of any shared prescriptions and

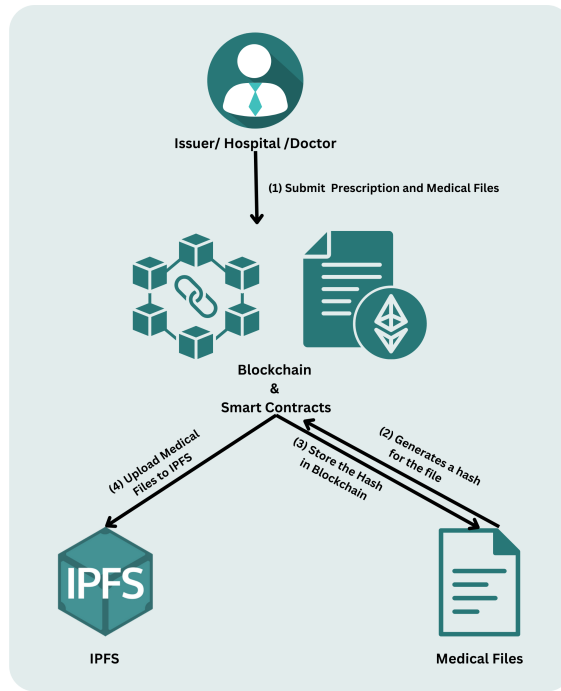


Figure 4.7: *Data storing in IPFS*

will have the ability to view them. Again if a doctor wants to see the previous medical files of a patient, which are stored in IPFS, they need to request to view those files. If the patient is willing to share those files with the doctor, only then they will be able to view those medical files. The validity of the files will be determined by comparing the hash of the file to the hash stored in the blockchain for that specific patient. If the hashes match, the medical files will be considered valid, otherwise, it will be deemed invalid. This is the process by which a doctor/pharmacist can verify the authenticity of a prescription or medical files shared by a patient. Permissions for different entities are shown in Figure 4.8.

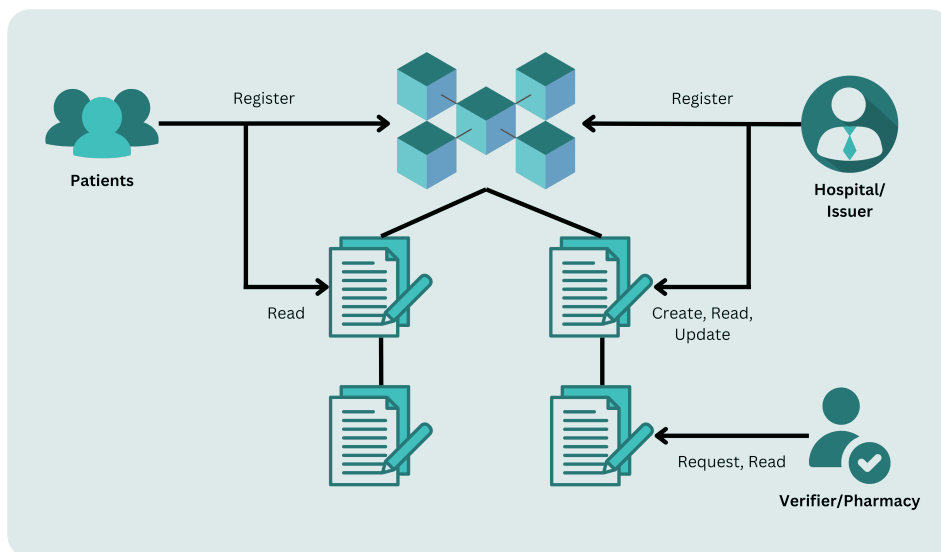


Figure 4.8: *User Permissions*

Chapter 5

Implementation

5.1 Environment setup

To set up the development environment for this prototype, a number of software and tools were installed and configured. The Hyperledger Fabric SDK was used to provide the necessary tools and libraries for building and deploying the blockchain application. The back-end of the prototype was built using Node.js and Express.js, which are open-source JavaScript run-time environments and web application frameworks that allowed for the creation of a RESTful API. The front-end of the prototype was developed using Flutter and Dart, which are open-source mobile application development frameworks that provided a user-friendly and responsive interface. The LevelDB was used as the database to store the medical records and other related data on the blockchain network. The InterPlanetary File System (IPFS) was used to store and retrieve medical files. A local blockchain network was set up to test and deploy the prototype. All the components depicted in Figure 5.1 were configured and integrated to ensure that the system is working as expected.

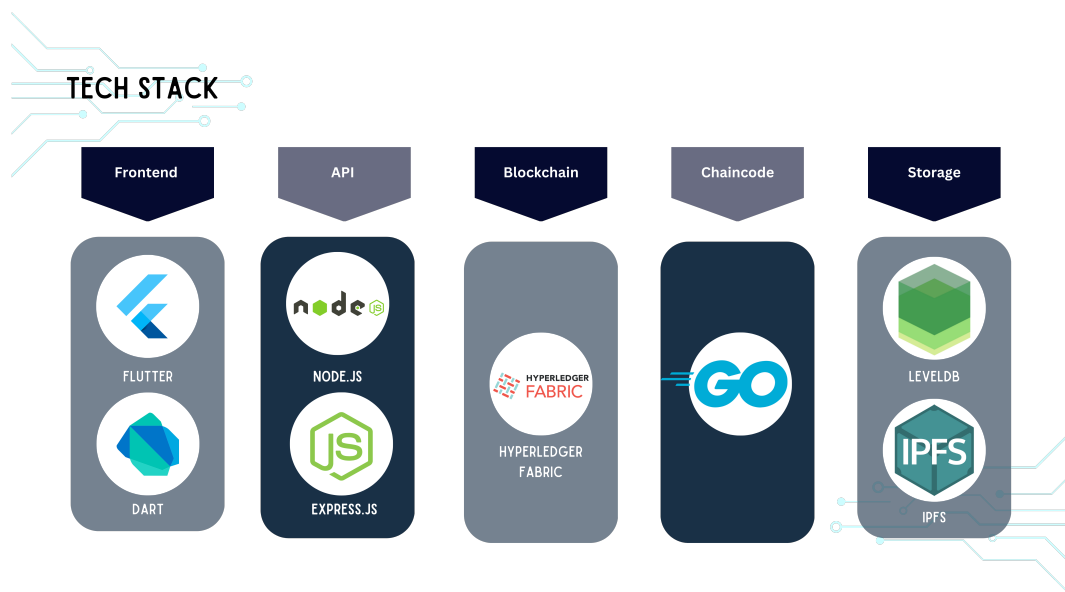


Figure 5.1: *Tech Stack used for our prototype*

5.2 Tech Stack

The technology stack used for this prototype and thesis project includes the following:

Web Application Framework: The front-end of the prototype was developed using Flutter and Dart, which are open-source mobile application development frameworks. This allowed for the development of a user-friendly and responsive interface for patients and doctors to access and manage medical records.

API: The back-end of the prototype was developed using Node.js and Express.js, which are open-source JavaScript run-time environments and web application frameworks. These technologies were used to create a RESTful API that enables communication between the front-end and the blockchain network.

Blockchain Platform: The prototype is built on Hyperledger Fabric, an open-source blockchain platform that is specifically designed for enterprise use cases. Hyperledger Fabric was used to create a secure and decentralized network that allows patients, doctors, and pharmacies to share and access medical records in a confidential and tamper-proof manner.

Database: The prototype uses LevelDB, a fast and lightweight key-value store that is built on top of the file system. LevelDB was used to store the medical records and other related data on the blockchain network.

File Storage: The prototype uses IPFS (InterPlanetary File System) to store and retrieve medical files. IPFS is a distributed file system that enables the permanent and secure storage of files on a peer-to-peer network.

The above technology stack was chosen for its scalability, security, and flexibility to meet the requirements of the medical record tracking system. It ensures that the system is tamper-proof and the data is secure and private. It also allows the system to be scalable and easily adaptable to changing requirements.

5.3 User Flow Diagram

The system utilizes a network server connected to the Hyperledger Fabric network, which comprises of chaincode and LevelDB. The patient uses an app to interact with the server, and medical files are encrypted and uploaded to IPFS via the Hyperledger network. These files can be retrieved and decrypted through the same network when needed, as shown in Figure 5.2.

5.4 Doctor Flow Diagram

The doctor initiates the process by creating a prescription and associating it with the patient's email address, depicted in Figure 5.3. The system then verifies if the

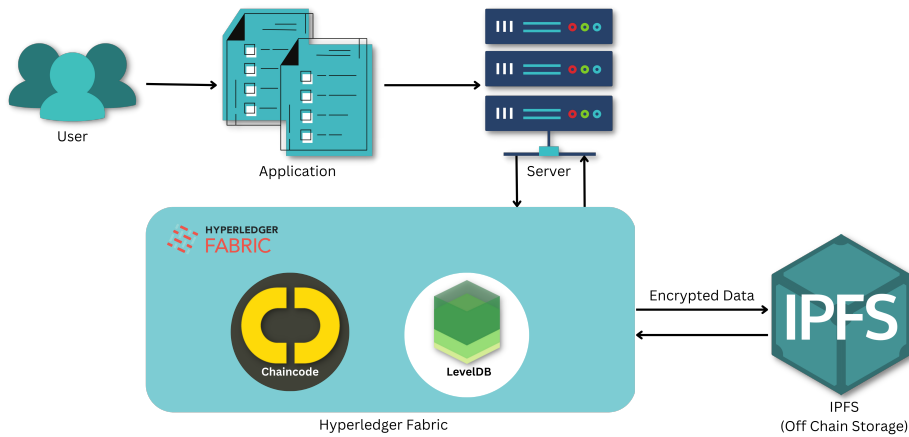


Figure 5.2: *User flow diagram*

email is already registered within the system. In case the email is already registered, the prescription creation transaction is directly submitted to the Hyperledger Fabric network. If the email is not registered, an auto-generated password, encrypted using the SHA-256 algorithm, is created. The patient is then enrolled in the system using the email and the encrypted password. The email and the password combination are then sent to the patient's email address for reference. Subsequently, the prescription creation transaction is submitted to the Hyperledger Fabric network for processing.

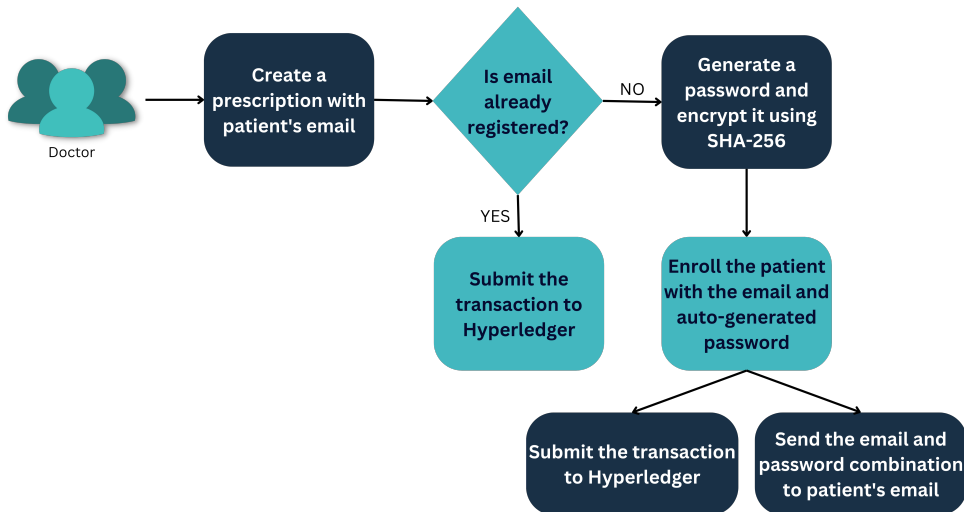


Figure 5.3: *Doctor flow diagram*

5.5 Pseudocodes and Explanation

5.5.1 Upload of encrypted files in IPFS

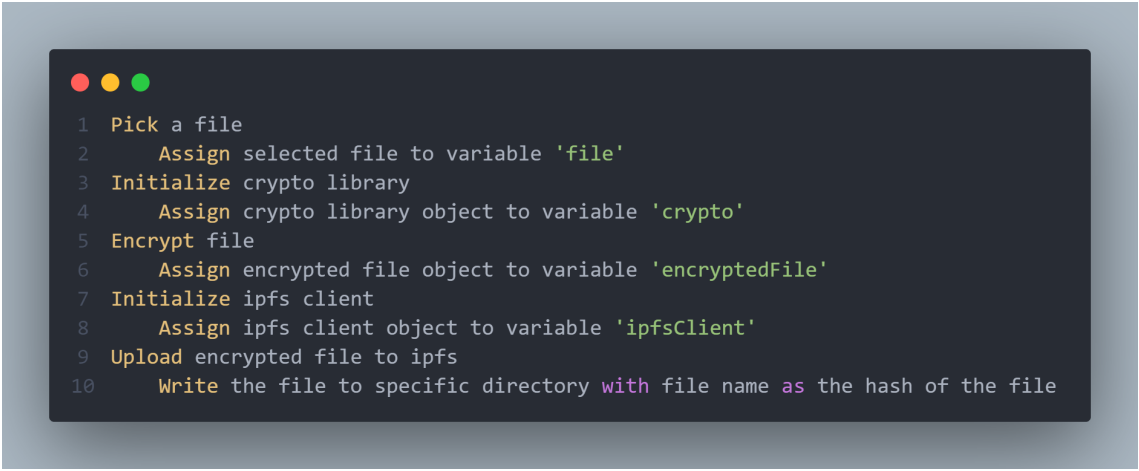
The process of transferring medical records from the physician's local database to our web application and then to the InterPlanetary File System (IPFS) for secure storage will involve several steps.

The physicians will first access their local medical records database, and select the relevant records that need to be transferred.

Once the records are selected, they will be transferred to our web application. This can be done through a variety of methods, such as through a secure file transfer protocol (SFTP) or by using an API to connect the physician's database with our application.

Once the records are received by our web application, they will be encrypted for added security. This can be done using a variety of encryption methods, such as AES or RSA, and a unique key will be generated for each set of records.

After the records are encrypted, they will be directly uploaded to the IPFS network for storage. The pseudo-code is shown in Figure 5.4.



```
1 Pick a file
2   Assign selected file to variable 'file'
3 Initialize crypto library
4   Assign crypto library object to variable 'crypto'
5 Encrypt file
6   Assign encrypted file object to variable 'encryptedFile'
7 Initialize ipfs client
8   Assign ipfs client object to variable 'ipfsClient'
9 Upload encrypted file to ipfs
10  Write the file to specific directory with file name as the hash of the file
```

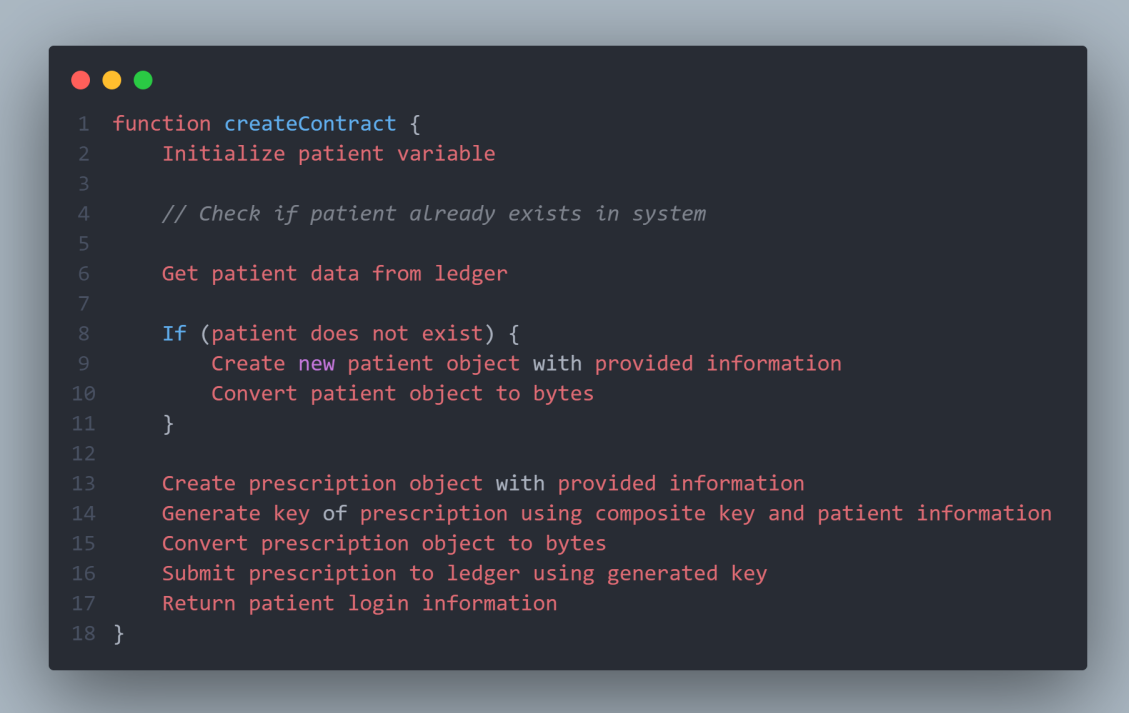
Figure 5.4: *IPFS implementation Pseudo-code*

5.5.2 Creation of Prescription

The proposed code is designed to facilitate the creation of prescriptions for patients by authorized medical professionals. The process begins by checking if the patient in question is already registered in the database. If the patient is already present in the system, the code proceeds to the next step of creating the prescription. However, if the patient is not yet registered, the code creates a new patient profile with the relevant information.

The next step in the process is the creation of a composite key for the prescription. A composite key is a unique identifier made up of multiple fields or attributes that together serve to uniquely identify the prescription in the database. In this case, the composite key is generated using information from both the patient and the prescription.

Once the composite key is generated, the prescription is submitted to the ledger using that key. This ensures that the prescription is securely stored and easily retrievable using the unique identifier. The pseudo-code is shown in Figure 5.5.

A screenshot of a code editor with a dark background and light-colored text. The code is a function named 'createContract' with 18 lines of pseudo-code. The code includes comments and logical steps for initializing a patient variable, checking for its existence, creating a new patient object if it doesn't exist, generating a prescription object and key, and finally submitting the prescription to a ledger and returning login information.

```
1 function createContract {
2     Initialize patient variable
3
4     // Check if patient already exists in system
5
6     Get patient data from ledger
7
8     If (patient does not exist) {
9         Create new patient object with provided information
10        Convert patient object to bytes
11    }
12
13    Create prescription object with provided information
14    Generate key of prescription using composite key and patient information
15    Convert prescription object to bytes
16    Submit prescription to ledger using generated key
17    Return patient login information
18 }
```

Figure 5.5: *Function for creating prescription: Pseudo-code*

5.5.3 API Connection

Upon receiving a POST request for a prescription, the API performs several checks to ensure the validity of the data and the identity of the administrator. Specifically, it verifies that the POST data meets the required specifications and that the administrator is authorized to make such a request. Once these conditions are met, the API submits the transaction using the administrator's identity and establishes a connection to the "Medisafe" application channel. It then constructs a Transaction Proposal Request (TPR) with the necessary parameters and sends it to the network for processing. Finally, it retrieves the login information and returns an appropriate response to the client. The pseudo-code is shown in Figure 5.6.

```

1 Receive POST request to '/api/prescribe'
2   Get user and prescription from request body
3
4   Validate request
5     If (data is missing)
6       return error with status 400 "Invalid request!"
7
8   //Check if doctor admin peer is connected to network
9
10  Check for specific file system wallet
11
12  If (admin identity does not exist)
13    throw error "An admin identity is required to process this transaction"
14
15  Submit transaction with admin identity
16
17  Initialize Hyperledger Fabric client
18  Generate new transaction ID
19  Connect to application channel 'MediSafe'
20
21  Send transaction proposal request to Fabric network with
22  chaincode ID, version, function, and transaction ID
23
24  Get login info from payload
25
26  If (login info present)
27    send response with status 201 "success" and login info
28
29  Else
30    send response with status 500 "Error occurred while submitting transaction"

```

Figure 5.6: *Pseudo-code for API connection*

5.6 Designing User-Friendly Interface

5.6.1 Doctor's interaction with the App

Upon logging into the app, the doctor will have access to a form for entering the patient's information, including their email address which will serve as the patient's identification. The doctor will also have the capability to add medication information or attach medical files. The medication information will be recorded on the Hyperledger network, while the medical files will be uploaded to IPFS for storage. Screenshot from app is shown in Figure 5.7 and Figure 5.8.

5.6.2 Patient's interaction with the App

Upon logging into the system using their email, patients will have the ability to view any prescriptions provided to them by their physician. They will also have the option to view any medical files attached by the physician. If desired, patients will have the option to share their medication information with a pharmacist, who will

then have access to view the prescriptions. Screenshot from app is shown in Figure 5.9, Figure 5.10 and Figure 5.11.

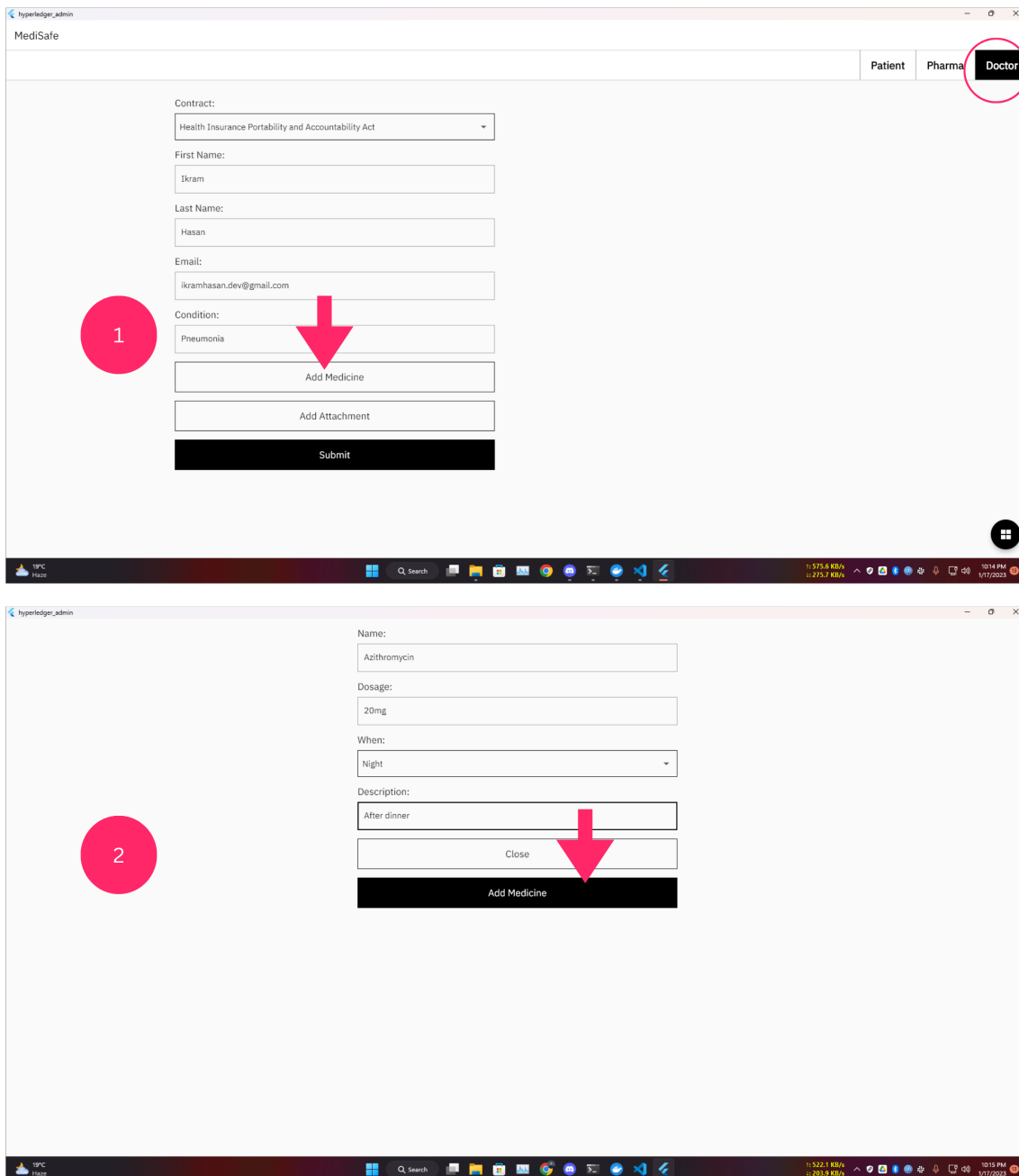


Figure 5.7: Doctor's view 1

5.6.3 IPFS files

Medical files attached by the doctor will be stored on IPFS where anyone can view the existence of any files. However, the medical files uploaded from our system will be encrypted, making them unreadable directly from IPFS. Access to these files can only be granted by the patient, and will only be possible through the use of our system. Screenshot from the app is shown in Figure 5.12.

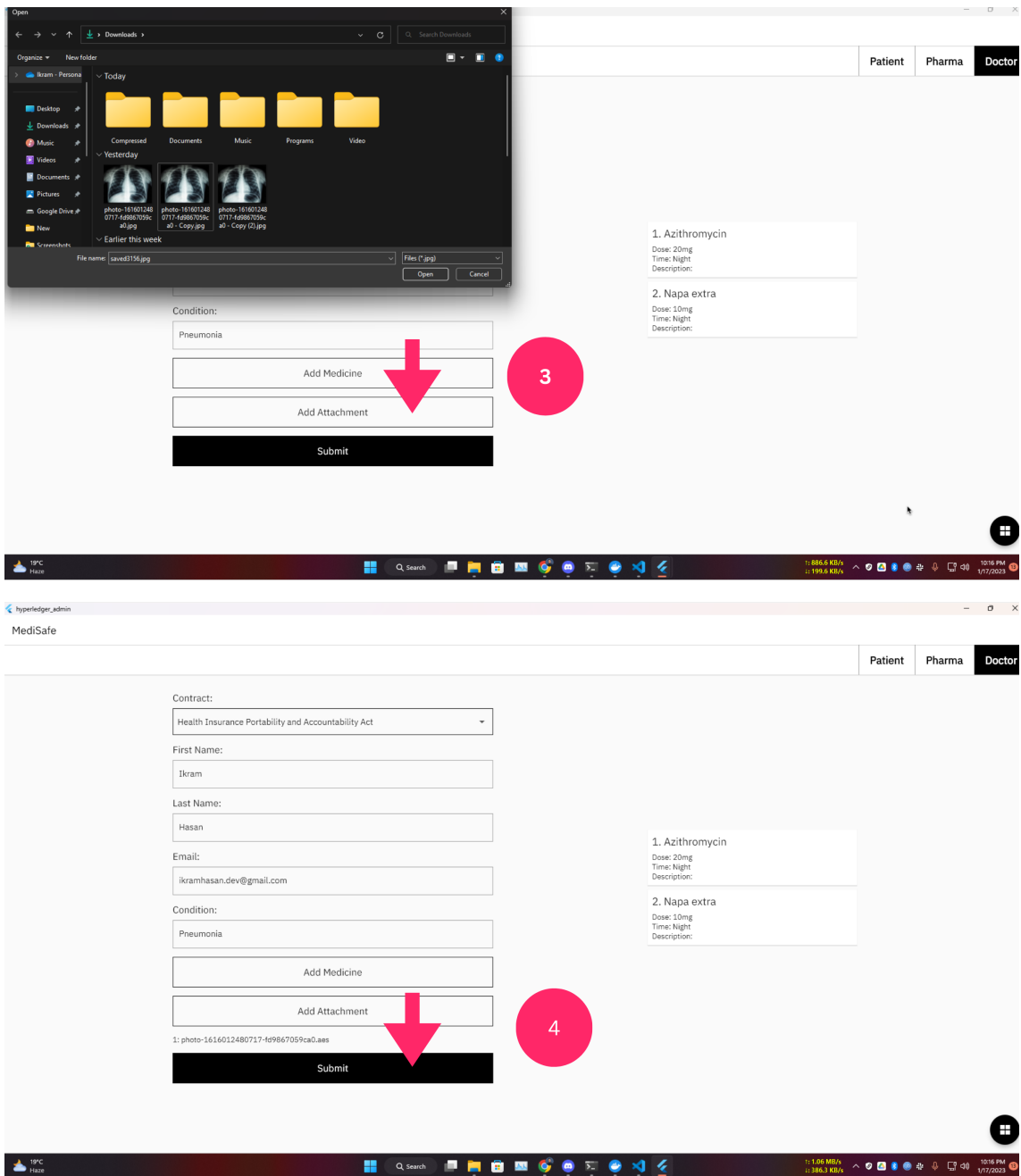


Figure 5.8: Doctor's view 2

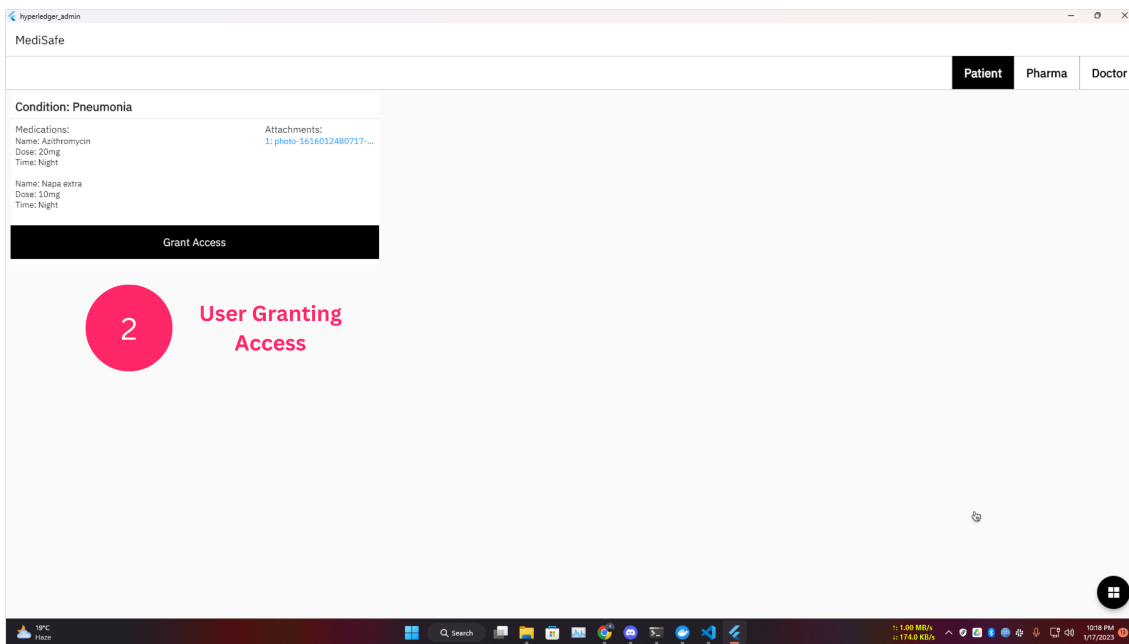
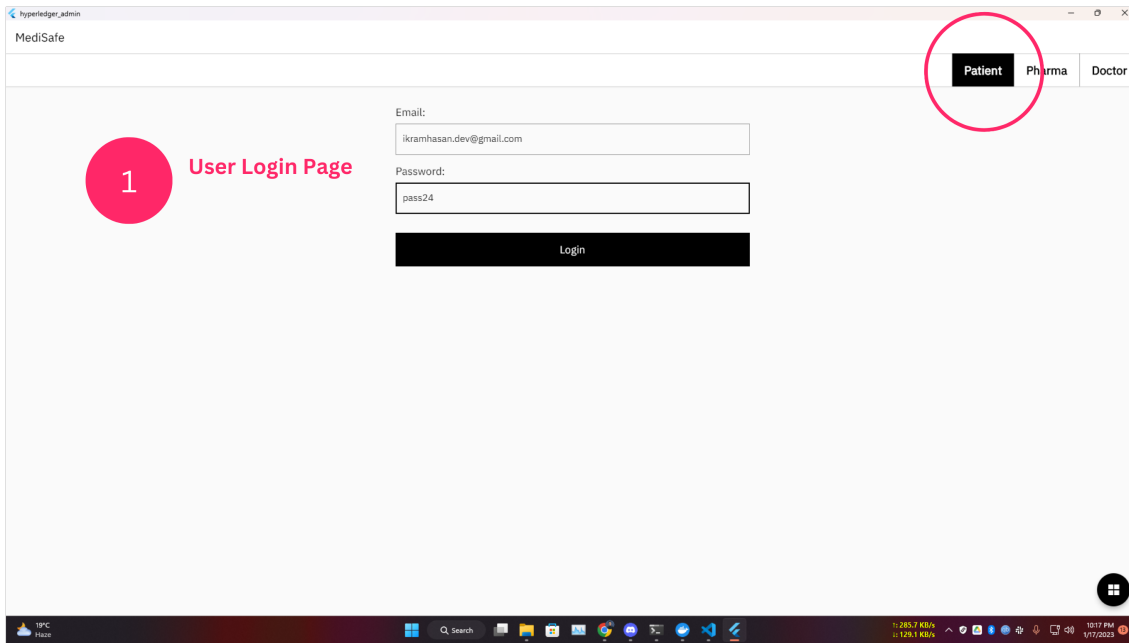


Figure 5.9: Patient's view 1

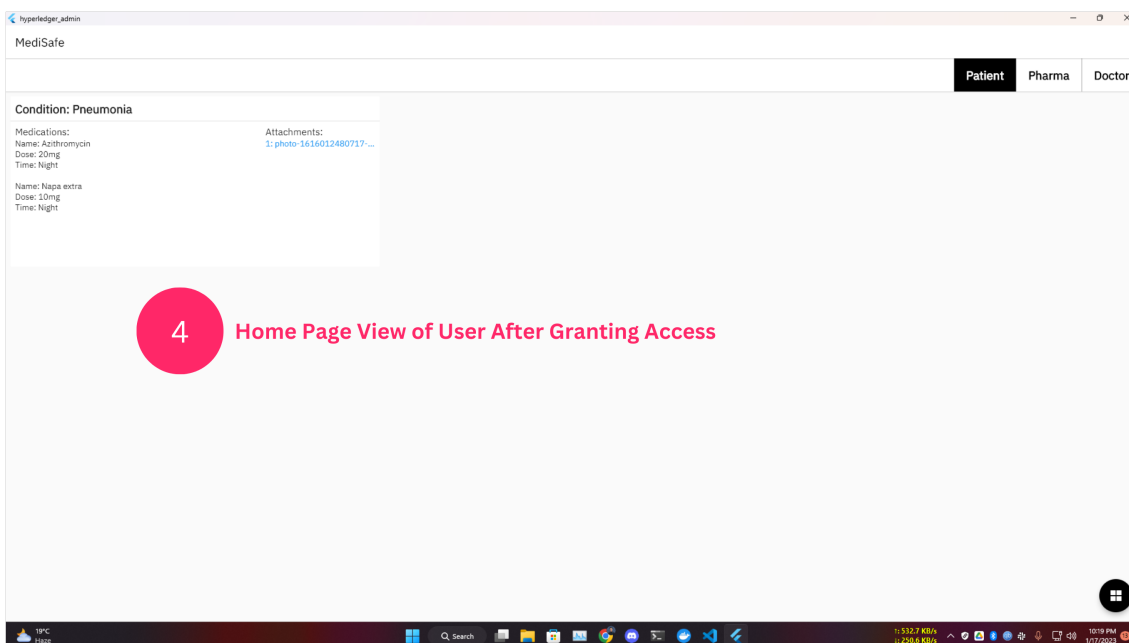
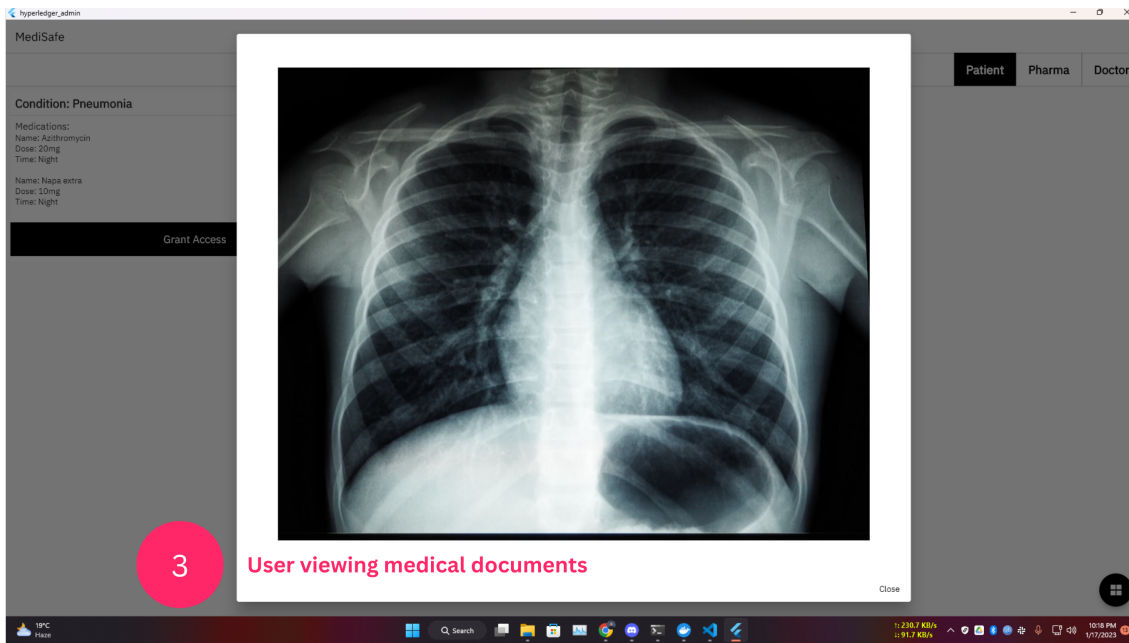


Figure 5.10: *Patient's view 2*

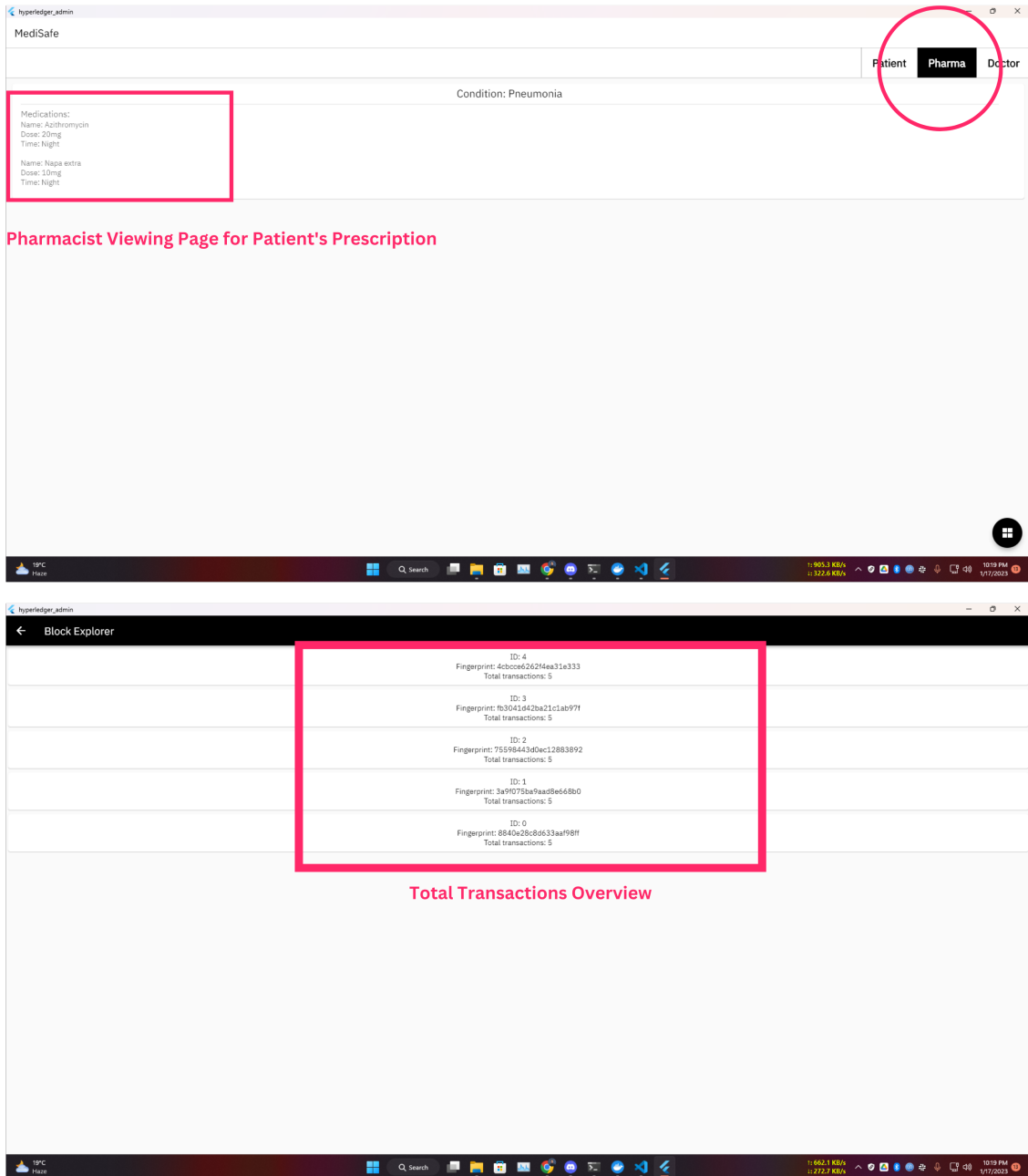


Figure 5.11: *Pharmacist's view and Transactional Log*

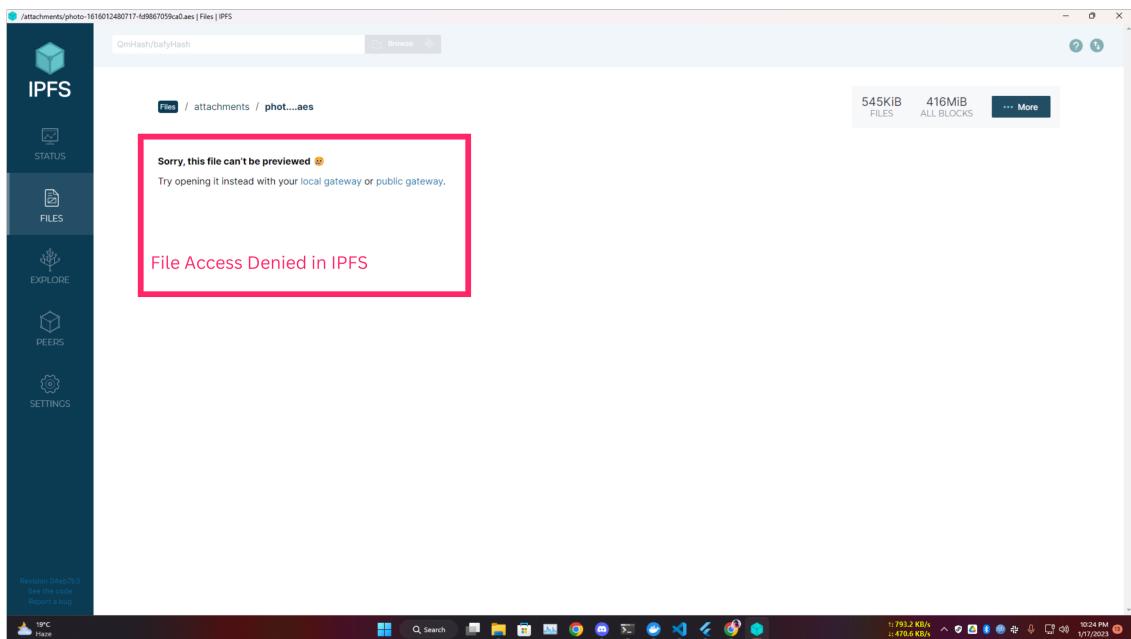
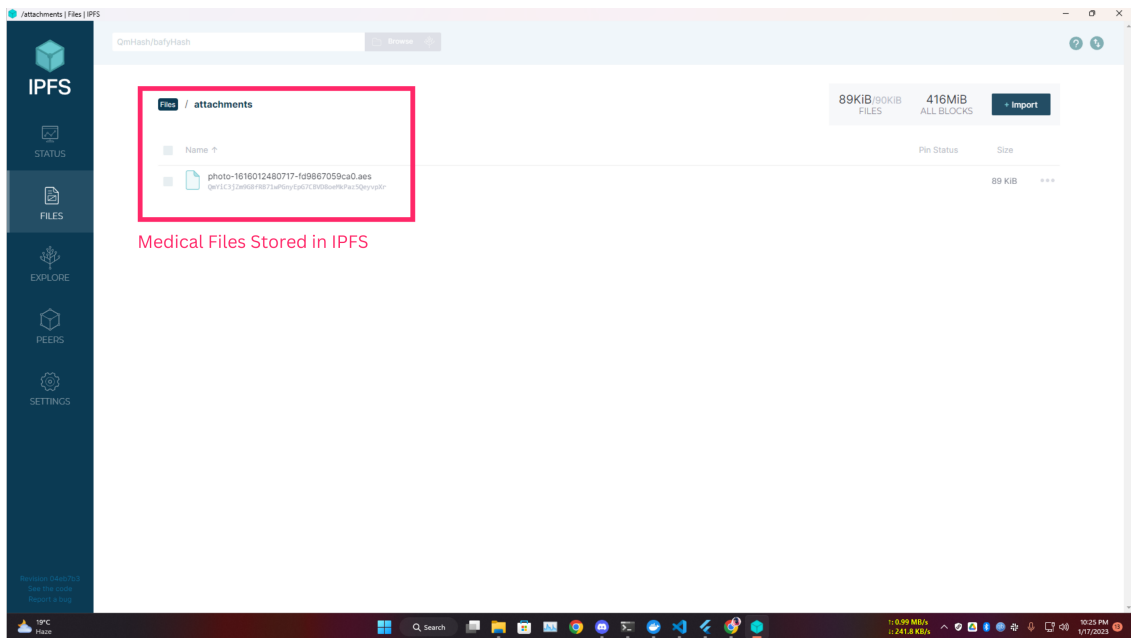


Figure 5.12: Medical files stored in IPFS

Chapter 6

Results and Discussion

6.1 Security and Performance

6.1.1 Authentication

Ensuring the validity and authenticity of users, such as patients, hospitals, and pharmacies, is crucial in utilizing a blockchain system for document verification. This can be achieved through various forms of user authentication, such as username and password, or biometric methods. In this system, before a pharmacist is able to view and verify a prescription, they must first join the blockchain network and be authorized by the MOHFW.

6.1.2 Authorization

The system ensures that the appropriate users have the necessary permissions to carry out actions within the blockchain network. This includes allowing a patient to share their prescription with a pharmacist, or granting the issuer of a prescription the ability to authorize the patient to have control over the prescription once it has been issued. All of these actions and permissions must be granted through proper authorization within the system.

6.1.3 Privacy

Ensuring the protection of sensitive information is a crucial aspect of our system, particularly in regard to the personal data of patients. This includes information held by hospitals as well as the individual patients themselves. To maintain this confidentiality, patients are granted the authority to selectively share their information with authorized pharmacies, for the purpose of verification.

6.1.4 Scalability

Hyperledger Fabric addresses scalability through the use of membership services providers (MSPs) that handle the onboarding process for new members and the use of pluggable consensus. The use of MSPs allows for the delegation of certain responsibilities to trusted third-party organizations, which can help to simplify the onboarding process and reduce the resources required to join the network. Pluggable consensus allows network to choose the consensus algorithm according to their needs.

Also, the modular design of Hyperledger Fabric allows for the separation of concerns, which means that different components of the network can be scaled independently. The use of channels, which are private subnetworks within the overall Fabric network, allows for different groups of participants to transact in parallel, increasing the overall throughput of the network. Our comparison on the above points is shown in Figure 6.1

| Comparison Chart | | | | |
|---------------------------|----------------|---------|---------------|-------------|
| ORGANIZATION/ SOLUTION | AUTHENTICATION | PRIVACY | AUTHORIZATION | SCALABILITY |
| MIT Media Lab | ✗ | ✓ | ✓ | ✓ |
| SmartCert | ✗ | ✗ | ✓ | ✓ |
| Records Keeper | ✓ | ✗ | ✗ | ✓ |
| UNIC | ✗ | ✓ | ✗ | ✗ |
| KMI-OU UK | ✗ | ✓ | ✗ | ✓ |
| BlockCert | ✗ | ✗ | ✗ | ✓ |
| MediSafe (Our Solution) | ✓ | ✓ | ✓ | ✓ |

Figure 6.1: *Our solution vs Other solutions*

6.2 Hyperledger Fabric vs Central Database

In terms of document authenticity:

Immutable Hyperledger Fabric uses a distributed ledger, which is an immutable record of transactions. Once a transaction is recorded on the ledger, it cannot be altered, which ensures the authenticity of the data.

Private Digital Signature It is a method of authenticating and ensuring the integrity of digital communications and transactions through the use of a private key. This private key is used to encrypt a message, generating a signature that can be verified by anyone with access to the corresponding public key. It is a widely employed technique in fields such as blockchain technology and cryptography.

In terms of Data Availability

Decentralized: Hyperledger Fabric is a decentralized system, which means that data are stored across multiple nodes in the network. This can help to improve the authenticity of the data, as it is less vulnerable to tampering by a single point of failure.

In terms of authorization

Access control: Hyperledger Fabric allows for the use of access controls, which can be used to restrict access to certain parts of the network to specific participants. This allows for fine-grained control over who can access, view, or modify the data, which can help to ensure that only authorized participants can access sensitive information.

Membership service providers (MSPs): Hyperledger Fabric allows for the use of MSPs, which are trusted organizations that handle the onboarding process for new members. This can help to ensure that only authorized participants can join the network and access the data.

Identity management: Hyperledger Fabric has built-in support for identity management, which allows for the creation, management, and revocation of digital identities. This can be used to ensure that only authorized participants can access the network and the data.

In terms of privacy

Private data collections: Hyperledger Fabric allows for the creation of private data collections, which are separate ledgers that are only accessible to a specific subset of network participants. This allows for the storage of sensitive information in a secure and private manner.

In terms of scalability

Modularity: Hyperledger Fabric is designed to be modular, which means that different components of the network can be scaled independently. This allows for more granular control over the scalability of the network, and enables specific parts of the network to be scaled up or down as needed.

Pluggable consensus: Hyperledger Fabric allows network to use different consensus algorithms, such as Kafka, Solo and Raft. These consensus algorithms can help to ensure the authenticity of the data by ensuring that all transactions are validated by multiple participants before they are recorded on the ledger.

Chapter 7

Future Works

It is our intention to implement this Hyperledger Fabric-based network as the primary infrastructure for the sharing and issuance of medical data and prescriptions in Bangladesh, thus addressing the challenges of verifying the authenticity of prescriptions and preventing counterfeit or fraudulent prescriptions and providing a secure and tamper-proof system for recording and tracking prescription information for the entire country.

The first area of future work for the Hyperledger Fabric-based system for recording and tracking medical prescriptions is scalability. The system must be optimized to handle a large number of prescriptions and network participants, as the healthcare ecosystem is complex and dynamic. One way to achieve scalability is by implementing sharding, which is the process of dividing the network into smaller segments called shards. Each shard can process transactions in parallel, increasing the overall throughput of the system. Another way to achieve scalability is by implementing off-chain solutions, such as state channels and sidechains, which allow for certain transactions to be conducted off the main blockchain, reducing the load on the network and improving performance. This is particularly relevant to our work as scalability is a crucial aspect in any blockchain-based system, and it is especially important in healthcare where the volume of data and transactions can be high.

The second area of future work is interoperability. The system must be able to integrate with existing healthcare systems, such as electronic medical records, to provide a seamless experience for users and to improve the sharing of information between different systems. This can be achieved by using standard protocols and data formats, such as FHIR, that allow for easy integration with other systems. Additionally, the system can be designed to support different data models, such as HL7 and CDA, to ensure compatibility with existing systems implementing API like “Metriport” for accessing and managing health and medical data through a single open source API. This is relevant to our work as interoperability is crucial in healthcare to ensure that different systems can communicate and share data effectively.

Finally, we can also implement Self-sovereign identity (SSI) which is a concept that aims to give individuals control over their own digital identity and the ability to share their identity information in a secure and private way. It can be a great area of future work for the Hyperledger Fabric-based system for recording and tracking medical prescriptions by providing decentralized identities, improved privacy, traceability, and interoperability. Implementing SSI can be done by using the open-source Hyperledger Indy and Aries projects. SSI aligns well with the main goal of the project which is to create a secure and tamper-proof system for recording and tracking medical prescriptions, and it can improve the security and privacy of the system by giving individuals control over their own identity information, improve traceability and interoperability, and improve the user experience.

Chapter 8

Conclusion

In conclusion, this research aimed to address the problem of verifying the authenticity of medical prescriptions in Bangladesh by creating a secure and tamper-proof system for recording and tracking prescription information using Hyperledger Fabric blockchain technology.

Research Objective 1 (1.2) was to increase security and authenticity by generating a record that cannot be altered and keeping it safe. We addressed this objective by implementing a decentralized ledger system on Hyperledger Fabric, where each prescription is recorded as a unique transaction on the blockchain. The prescriptions are recorded with a digital signature, ensuring that the prescription has not been altered and that it is authentic. This provides a secure and tamper-proof system for recording and tracking prescription information.

Research Objective 2 (1.2) was to develop an application to eradicate prescription forgery in Bangladesh. We addressed this objective by creating a decentralized database of prescriptions, where only authorized parties such as patients, doctors, and pharmacists have access to the read, write and view medical documents and prescription. This can prevent unauthorized parties from altering or counterfeiting prescriptions.

Research Objective 3 (1.2) was to study the technical feasibility of building a Hyperledger-based system for private data sharing with individual nodes in the network. We addressed this objective by investigating the potential of using the Hyperledger platform to create an immutable and tamper-proof record of prescriptions and other medical documents, and creating an efficient and scalable system for private data sharing.

Research Objective 4 (1.2) was to guide the design and implementation of similar Hyperledger-based systems in the future. We addressed this objective by developing a working prototype that can guide future implementation of this system in different scenarios in the future like building a network to provide authentic certificates. We also provided insights into the potential of Hyperledger-based systems in the healthcare sector and guidance for the design and implementation of such systems in the future.

Research Objective 5 (1.2) was to provide recommendations for areas of further research, based on the results of the study. We addressed this objective by analyzing the potential impact of such a system on security, understanding the limitations, trade-offs, or challenges when using Hyperledger technology in such a use case. And providing recommendations for areas of further research, based on the results of the study.

Overall, this research demonstrates the potential of Hyperledger Fabric technology to address the problem of verifying the authenticity of medical prescriptions in Bangladesh by providing a secure and tamper-proof system for recording and tracking prescription information. The implementation of the system shows the technical feasibility of building a Hyperledger-based system for this purpose, and the research provides insights into the potential of Hyperledger-based systems in the healthcare sector and guidance for the design and implementation of such systems in the future. The research also highlights the importance of considering security, privacy, and interoperability when designing and implementing such systems, and the need for further research in these areas.

Bibliography

- [1] S. Correspondent, “New law to curb misuse of antibiotics,” Oct 5, 2022, 17jan, 2023. [Online]. Available: <https://www.thedailystar.net/health/healthcare/news/new-law-curb-misuse-antibiotics-3135381>.
- [2] R. Ahamad, “Sale of antibiotics without prescription goes unabated across bangladesh,” Jul 03,2022, 17jan, 2023. [Online]. Available: <https://www.newagebd.net/article/174931/sale-of-antibiotics-without-prescription-goes-unabated-across-bangladesh>.
- [3] P. Chauhan, J. P. Verma, S. Jain, and R. Rai, “Blockchain based framework for document authentication and management of daily business records,” in *Blockchain for 5G-Enabled IoT*, Springer, 2021, pp. 497–517.
- [4] I. T. Imam, Y. Arafat, K. S. Alam, and S. A. Shahriyar, “Doc-block: A blockchain based authentication system for digital documents,” in *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, IEEE, 2021, pp. 1262–1267.
- [5] M. J. R. Mahale and E. Chirchi, “Modeling and simulation for digital document verification scheme using blockchain in p2p network,”
- [6] H. Jin, C. Xu, Y. Luo, P. Li, Y. Cao, and J. Mathew, “Toward secure, privacy-preserving, and interoperable medical data sharing via blockchain,” in *2019 IEEE 25th International Conference on Parallel and Distributed Systems (ICPADS)*, IEEE, 2019, pp. 852–861.
- [7] R. F. Ghani, A. A. Salman, A. B. Khudhair, and L. Aljobouri, “Blockchain-based student certificate management and system sharing using hyperledger fabric platform,” *Periodicals of Engineering and Natural Sciences (PEN)*, vol. 10, no. 2, pp. 207–218, 2022.
- [8] I. Meirobie, A. P. Irawan, H. T. Sukmana, D. P. Lazirkha, and N. P. L. Santoso, “Framework authentication e-document using blockchain technology on the government system,” *International Journal of Artificial Intelligence Research*, vol. 6, no. 2, 2022.
- [9] R. Khan, S. Ansari, S. Jain, and S. Sachdeva, “Blockchain based land registry system using ethereum blockchain,” *Journal of Xi’an University of Architecture & Technology*, vol. 12, pp. 3640–3648, 2020.
- [10] O. Ghazali and O. S. Saleh, “A graduation certificate verification model via utilization of the blockchain technology,” *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, vol. 10, no. 3-2, pp. 29–34, 2018.

- [11] J.-C. Cheng, N.-Y. Lee, C. Chi, and Y.-H. Chen, "Blockchain and smart contract for digital certificate," in *2018 IEEE international conference on applied system invention (ICASI)*, IEEE, 2018, pp. 1046–1051.
- [12] A. S. Ghanghoria, A. S. A. Raja, V. J. Bachche, and M. N. Rathi, "Secure e-documents storage using blockchain," *Int. Res. J. Eng. Technol.(IRJET)*, vol. 7, pp. 1972–1974, 2020.
- [13] T. T. Huynh, T. T. Huynh, D. K. Pham, and A. K. Ngo, "Issuing and verifying digital certificates with blockchain," in *2018 International conference on advanced technologies for communications (ATC)*, IEEE, 2018, pp. 332–336.
- [14] N. Gopal and V. V. Prakash, "Survey on blockchain based digital certificate system," *International Research Journal of Engineering and Technology (IRJET)*, vol. 5, no. 11, 2018.
- [15] A. Badr, L. Rafferty, Q. H. Mahmoud, K. Elgazzar, and P. C. Hung, "A permissioned blockchain-based system for verification of academic records," in *2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, IEEE, 2019, pp. 1–5.
- [16] O. S. Saleh, O. Ghazali, and M. E. Rana, "Blockchain based framework for educational certificates verification," *Journal of critical reviews*, vol. 7, no. 03, pp. 79–84, 2020.
- [17] V. Marella and A. Vijayan, "Document verification using blockchain for trusted cv information.," in *AMCIS*, 2020.
- [18] B. M. Nguyen, T.-C. Dao, and B.-L. Do, "Towards a blockchain-based certificate authentication system in vietnam," *PeerJ Computer Science*, vol. 6, e266, 2020.