

ELECTRONIC HEALTH RECORDS USING BLOCKCHAIN

Project report submitted in partial fulfillment of the requirement for
the degree of Bachelor of Technology

in

Computer Science and Engineering/Information Technology

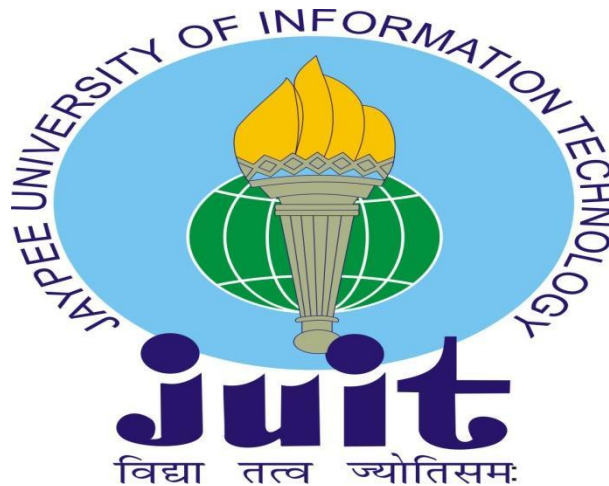
By

Rohit Sharma (181345)

Under the supervision of

Dr. Amit Kumar

to



Department of Computer Science & Engineering and Information
Technology

**Jaypee University of Information Technology Waknaghat,
Solan-173234, Himachal Pradesh**

(I) CERTIFICATE

This is to certify that the work which is being presented in the project report titled “**Electronic Health Records using Blockchain**” in partial fulfilment of the requirements for the award of the degree of B.Tech in Computer Science And Engineering and submitted to the Department of Computer Science And Engineering, Jaypee University of Information Technology, Wagnaghat is an authentic record of work carried out by “**Rohit Sharma (181345)**” during the period from January 2022 to July 2022 under the supervision of **Dr. Amit Kumar**, Department of Computer Science and Engineering, Jaypee University of Information Technology, Wagnaghat.

Rohit Sharma (181345)

The above statement made is correct to the best of my knowledge.

Dr. Amit Kumar

Assistant Professor (SG)

Computer Science & Engineering and Information
Technology Jaypee University of Information
Technology, Wagnaghat

(II) ACKNOWLEDGEMENT

Firstly, I express my heartiest thanks and gratefulness to almighty God for his divine blessing makes it possible to complete the project work successfully.

I am really grateful and wish my profound indebtedness to Supervisor **Dr. Amit Kumar, Assistant Professor (SG)**, Department of CSE Jaypee University of Information Technology, Wakhnaghat. Deep Knowledge & keen interest of my supervisor in the field of “**Blockchain Technology**” to carry out this project. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior drafts and correcting them at all stages have made it possible to complete this project.

I would like to express my heartiest gratitude to **Dr. Amit Kumar**, Department of CSE, for his kind help to finish my project.

I would also generously welcome each one of those individuals who have helped me straightforwardly or in a roundabout way in making this project a win. In this unique situation, I might want to thank the various staff individuals, both educated and non- instructed, who have developed their convenient help and facilitated my undertaking.

Finally, I must acknowledge with due respect the constant support and patience of my parents.

Rohit Sharma(181345)

(III) TABLE OF CONTENT

Content No.	Page
Certificate	I
Acknowledgement	II
Table of Content	III
List of Abbreviations	IV
List of Figures	V
List of Tables	VI
Abstract	VII
Chapter 01: Introduction	1
Chapter 02: Literature Survey	14
Chapter 03: System Development	17
Chapter 04: Performance Analysis	42
Chapter 05: Conclusion	59
References	61

(IV) LIST OF ABBREVIATIONS

BFT	Byzantine Fault Tolerant
CA	Certificate Authority
EHR	Electronic Health Record
EMR	Electronic Medical Record
EVM	Ethereum Virtual Machine
HL	Hyperledger Fabric
MSP	Membership Service Provider
WHO	World Health Organization
PBFT	Practical Byzantine Fault Tolerant
PKI	Public Key Infrastructure
PoW	Proof of Work
PoS	Proof of Stake
REST	Representational State Transfer

(V) LIST OF FIGURES

● Figure 1: Architecture of Hyperledger	10
● Figure 2: Composer Playground	11
● Figure 3:Composer’s Users	12
● Figure 4: Composer’s define page	12
● Figure 5: Composer’s test page	13
● Figure 6: Participants, Assets, and Transactions in Blockchain Network	28
● Figure 7: Class Diagram of the proposed framework	29
● Figure 8: Create a new blockchain user	31
● Figure 9 (a and b): List of Transactions	32
● Figure 10: UML use case diagram for Basic Scenario	35
● Figure 11: UML use case diagram for Permissioned Scenario	37
● Figure 12: UML use case diagram for Purging Scenario	39
● Figure 13: Code snapshot of transaction	44
● Figure 14: Code Snapshot of Access Control Language	44
● Figure 15: Doctor A has no access to Medical Records	46
● Figure 16: Patient A grants medical record access to Doctor A	46
● Figure 17: Doctor A has access to the Medical Record	47
● Figure 18: Doctor A can Update the Medical Record	47
● Figure 19: Patient views Medical Records	49
● Figure 20: Patient removing Doctor ID: #111, from their Medical Record	50
● Figure 21: Successful Transactions List.	50
● Figure 22: Patient deleting his/her Medical Record	51
● Figure 23: Doctor cannot delete patient's Medical Record	52
● Figure 24: Patient A requests an Appointment from Doctor A.	53
● Figure 25: Doctor A confirms the Appointment	54
● Figure 26: Doctor A creating MedPresc Asset.	54
● Figure 27: Doctor A creating Prescription Asset	55
● Figure 28: Doctor A providing consultation to Patient A	55
● Figure 29: Status of Appointment changes to “Consulted”	56
● Figure 30: Patient A’s debt gets updated.	56

(VI) LIST OF TABLES

- Table1 : Participants, Assets, and Transactions in Blockchain Network 28
- Table 2: Participant's Permissions 30
- Table 3 : Notations used in the procedure 1 40
- Table 4: A comparative analysis of the proposed framework 48

(VII) ABSTRACT

Healthcare data is crucial and sensitive because it contains information about patients' medical history, treatments along with actions. This information is frequently shared among different stakeholders of the system. As patients' information is vital, therefore, it must be kept accurate, up to date, secret, and available only to those who are authorized to access the specified information. Still, centralized systems are commonly used to maintain healthcare records which increases the security risk. Therefore, this study focuses on protecting the privacy and security of sensitive healthcare documents while sharing them across multiple healthcare participants. In this work, we proposed a privacy-preserving access control framework based on blockchain technology that uses consensus-driven decentralized data management on top of peer-to-peer distributed computing platforms to ensure the privacy, security, accessibility, and integrity of healthcare data. Blockchain technology helps to protect transactions from manipulation due to its irreversibility and immutability features. Furthermore, we comprehensively investigate the blockchain-enabled security requirements by including patients, doctors, chemists, and pathology labs as entities of the system that can share information through a proper channel. We have evaluated the proposed framework using Hyperledger Fabric and identified that the developed framework reveals promising benefits in security, regulation compliance, reliability, flexibility, and accuracy.

Chapter 01: INTRODUCTION

1.1 Introduction

Over the decade, the healthcare sector such as medical institutions, insurance organizations, etc., are handling patients' records very carefully. These records are considered an extremely critical asset in terms of privacy and security. This asset includes information, like names, addresses, unique identities (UID), medical history, medical history of family members, medication procedures, prescribed medications, and other related data, known as Electronic Health Records (EHRs). As EHRs contain very sensitive and personal data related to a person and it should be kept secret during the system design from unauthorized access. However, cyber-attackers have performed a number of attacks on medical institutions to steal the health records of millions of patients in the past decades [1]. The Indian government introduces two regulation acts in the Health Insurance Portability and Accountability Act (HIPAA) 1996 [2] and General Data Protection Regulation (GDPR) Act 2018 [3] that covers the numerous guidelines on how to store, process, and secure the medical data in order to prevent scam and theft in the healthcare domain. The target hackers obtain personal data using unlawful ways very easily even after specifying the clear regulations for the healthcare sector by the government. Certainly, the main reason behind this insecurity is the lack of technological understanding within the sector. This leads to many challenges including data security that may result in some common attacks including ransomware and phishing for retrieving personal data. It may also reveal some other characteristics of the system like backup and updates [4]. As per GDPR guidelines, the patient records must be handled by data controllers and should be visible only to the respective departments after generating consent through a proper channel (exceptions may be handled separately for serious health issues or emergency conditions). The information stored in the database should be accurate, trustworthy, and comprehensive. Specifically, in emergency circumstances, the hospital personnel require some necessary and personal health information regarding the patients for better and faster treatment to save their life. The entire system works on the access control mechanisms due to sensitive and confidential information stored in the system and unauthorized access is restricted for anyone. Therefore, the emergency medical team cannot access the health

record of the patient and even the patient is also not in the sense to change the access control for his/her EHRs.

Another significant challenge could be that his/her personal and medical records will be at high risk because in the black market the value of a single EHR is approx \$50 which is very much higher as compared to \$0.25 for credit card details [5]. A number of medical staff have released the EHRs to the black market only for financial gains but this ratio has dropped significantly because of the new litigations formed by governments all over the globe. Still, attackers can get the records by phishing attacks in which they masquerade as an authority to get the personal data. This attack is extremely successful, especially, in this pandemic situation when everything is going online and everyone is receiving numerous phone calls and emails from different agencies representatives and they ask for some personal details like name, address, unique id, etc. for verification to process further. For instance, the hacker successfully obtained significant information about staff at Magnolia Health Corporation (MHC) using a spoofed email from the CEO. On the other hand, the National Health Service (NHS) was attacked and encrypted with NHS files in 2017; as a result, all 6900 appointments got canceled [6] and there are many such examples reported in the literature for these kinds of thefts.

In one case, in 2012, a medical technician at Howard University Hospital sold the patients' names, addresses, and Medicare numbers on the black market for monetary gain. Another threat to the healthcare industry is phishing assaults, in which a hacker acts as an authoritative figure to induce users to give sensitive information. Because the exposed data might include patient or employee information such as social security numbers, addresses, earnings, and other personal information, these assaults have a significant impact. Consider the hacking of Magnolia Health Corporation (MHC), in which a hacker obtained considerable information about employees through a falsified email from the CEO. In 2017, hackers used malware to encrypt data at the National Health Service (NHS) (NHS).

Many scholars feel that blockchain is a disruptive technology that may be used in the healthcare business to guarantee the highest level of data protection. The major goal of this research is to create a framework that allows only authorised users, such as doctors, pathologists, and chemists, to access a patient's important information on a blockchain

network. We evaluate numerous scenarios to assess healthcare application needs as part of the study.

1.2 Problem Statement

Accessing health care services across various hospitals or clinics for diagnosis and treatment has become quite widespread, especially for patients with chronic conditions like cancer, due to greater specialisation of health care services and high levels of patient mobility. Physicians can make wiser, safer, and more efficient clinical judgments if they have a thorough understanding of a patient's history. Due to the high sensitivity and privacy of electronic health records (EHR), most EHR data transfer is still done via fax or mail due to a lack of systematic infrastructure support for safe, trustable health data sharing, which can create significant delays in patient care.

1.3 Objectives

The following aspects must be supported in order to construct an efficient healthcare system:

- **Protection**

The information must be kept private, correct, and only available to authorised users. When numerous entities are asked to access and alter databases at the same time, the problem gets even worse. As a result, adhering to the right route of transmitting information is critical for ensuring security.

- **Verification**

Each user of the EHR system will be issued a unique identity that will be used to authenticate them. While accessing any information on the network, any user may be recognised by their identity. To guarantee data privacy, distinct responsibilities and privileges are granted to participants according to the system architecture.

- **Flexibility**

An effective EHR system should be grown in accordance with the amount of blockchain users, ensuring that the entire network is competent and reliable.

- Access control and privacy

It is accomplished by the identification of each network participant. Only those with sufficient authorisation to view certain types of information, such as a doctor, can access and change a patient's record with the patient's consent. Every interaction between a patient and a physician will also be recorded and later tracked through log files.

- Information sharing

A patient has the option of seeking better care in a variety of hospitals and clinics, including specialist ones. As a result, the healthcare system should make it easier to set up secure data exchange channels for all intended receivers.

- Patient autonomy

Patients may access their own data and combine them with tagged notes and other pertinent information in their account, which is especially useful for chronic disease patients. The technology should also provide consumers total control over healthcare data and allow them to view information other than in an emergency.

- Collaboration

The above-mentioned features must be included into a new system. In reality, blockchain-based EHR management solutions are designed to integrate and supply needed functionality in a more effective manner, rather than simply replacing existing systems.

- GDPR Regulation [3]:

The government prohibits the following privacy and security requirements from being implemented anywhere in the globe. GDPR is a set of legislation that covers a wide range of themes, including the protection of healthcare workers, standard procedures, and

health-record transfer techniques. According to the GDPR, data subjects have the following rights:

Personal information should be managed in a lawful and transparent manner.

Right to be forgotten: Data subjects will have the right to request that personal data on them be erased.

Right to rectification: Personal information should be accurate and up to date, and people should be able to amend inaccurate information about them.

Right of access: Personal information should be accessed safely and kept safe from unlawful processing, misuse, damage, or destruction.

Right to restrict access: Data subjects have the right to object to the processing of their personal information (e.g in case of inaccuracy).

The data subject has the right to object to their personal information being used for marketing or profiling purposes.

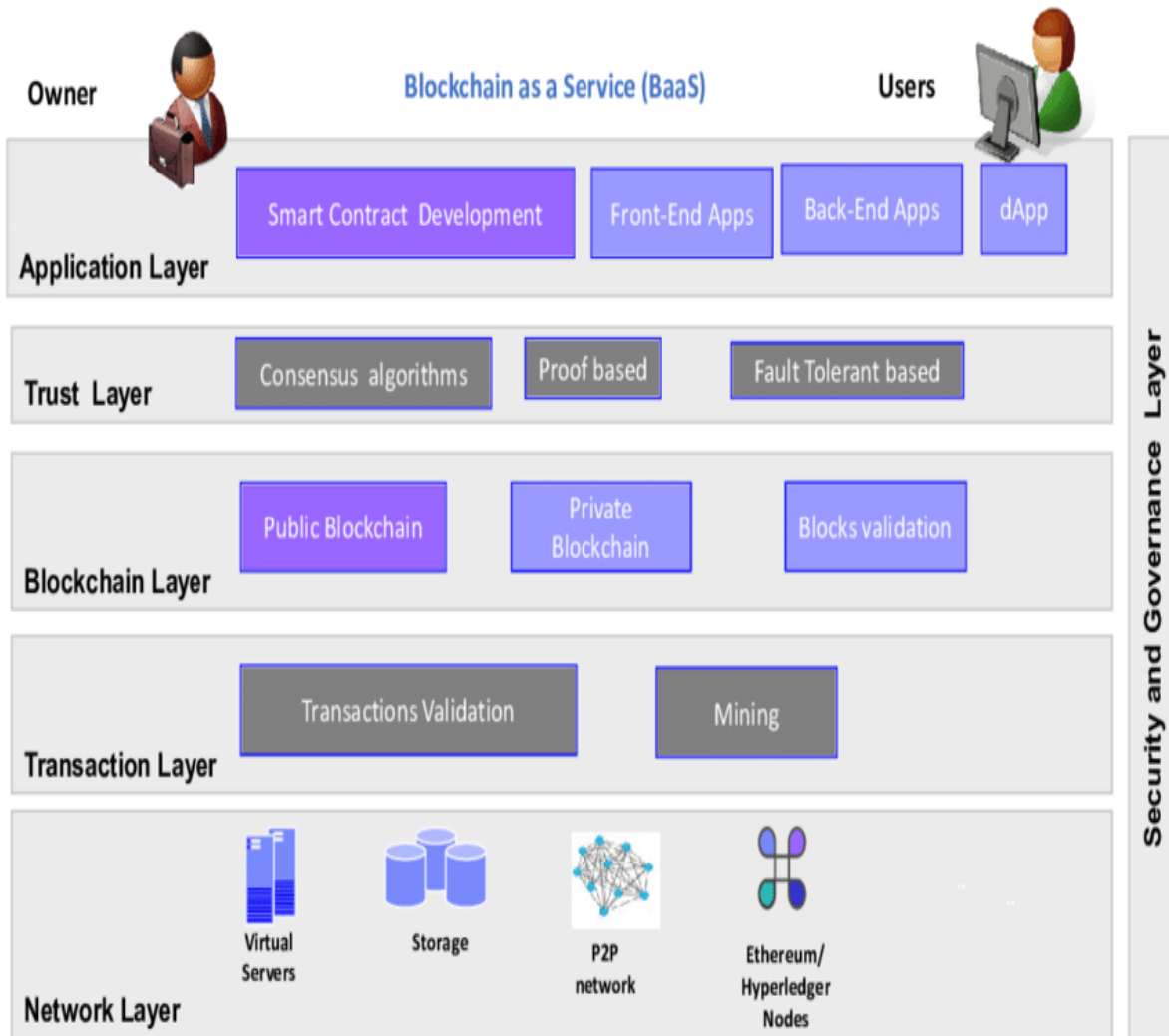
1.4 Methodology

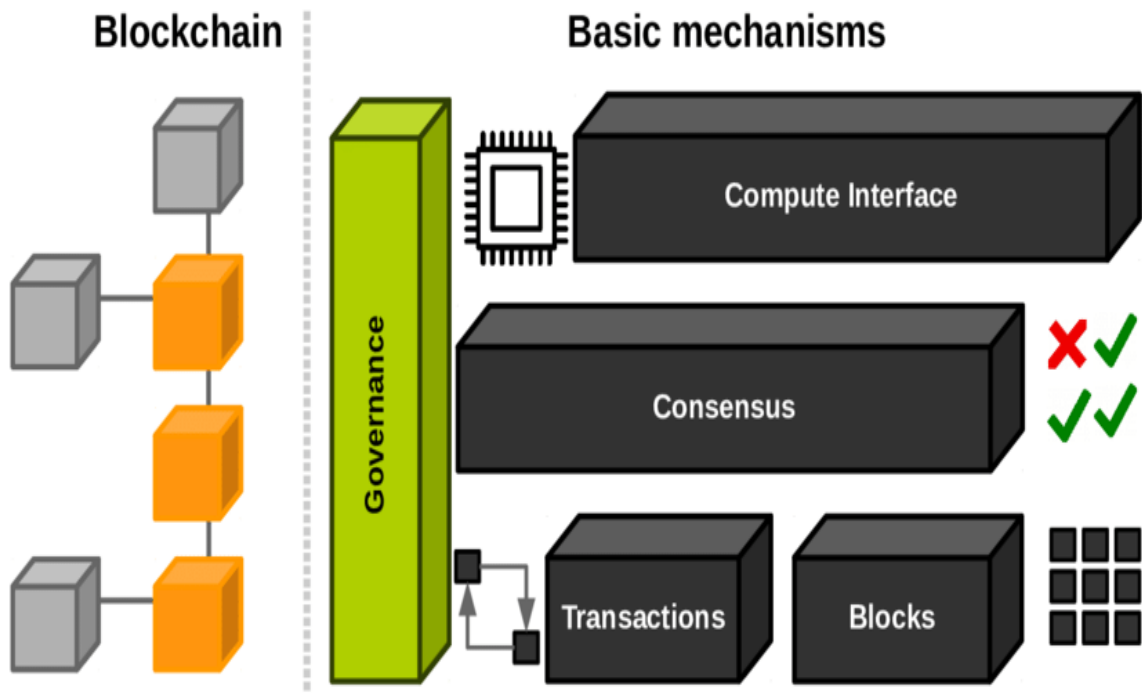
Blockchain Technology

A peer-to-peer platform is a distributed architecture that distributes the network's resources among a number of nodes that work together to make choices on the network's behalf. No centralised authority operates as an agent for all communications in a decentralised system [20], instead each node is free to execute peer-to-peer services known as transactions. The blockchain is a decentralised architecture that consists of a distributed unchangeable ledger that records all transactions. The blockchain, in general, is an undeniably creative innovation by an unidentified individual or group of persons known only as SATOSHI NAKAMOTO. Although the famous cryptocurrency BITCOIN [21] helped to popularise blockchain in the financial sector, the blockchain is a distributed shared ledger for storing transaction information.

Because having many ledgers is a method for fraud, mistakes, and incompetence. The goal is to peer-to-peer monitor a transaction and eliminate vulnerabilities. The blockchain keeps track of an ever-growing set of immutable and widely dispersed documents. All cryptocurrencies make use of what can be adequately characterised as a public ledger that

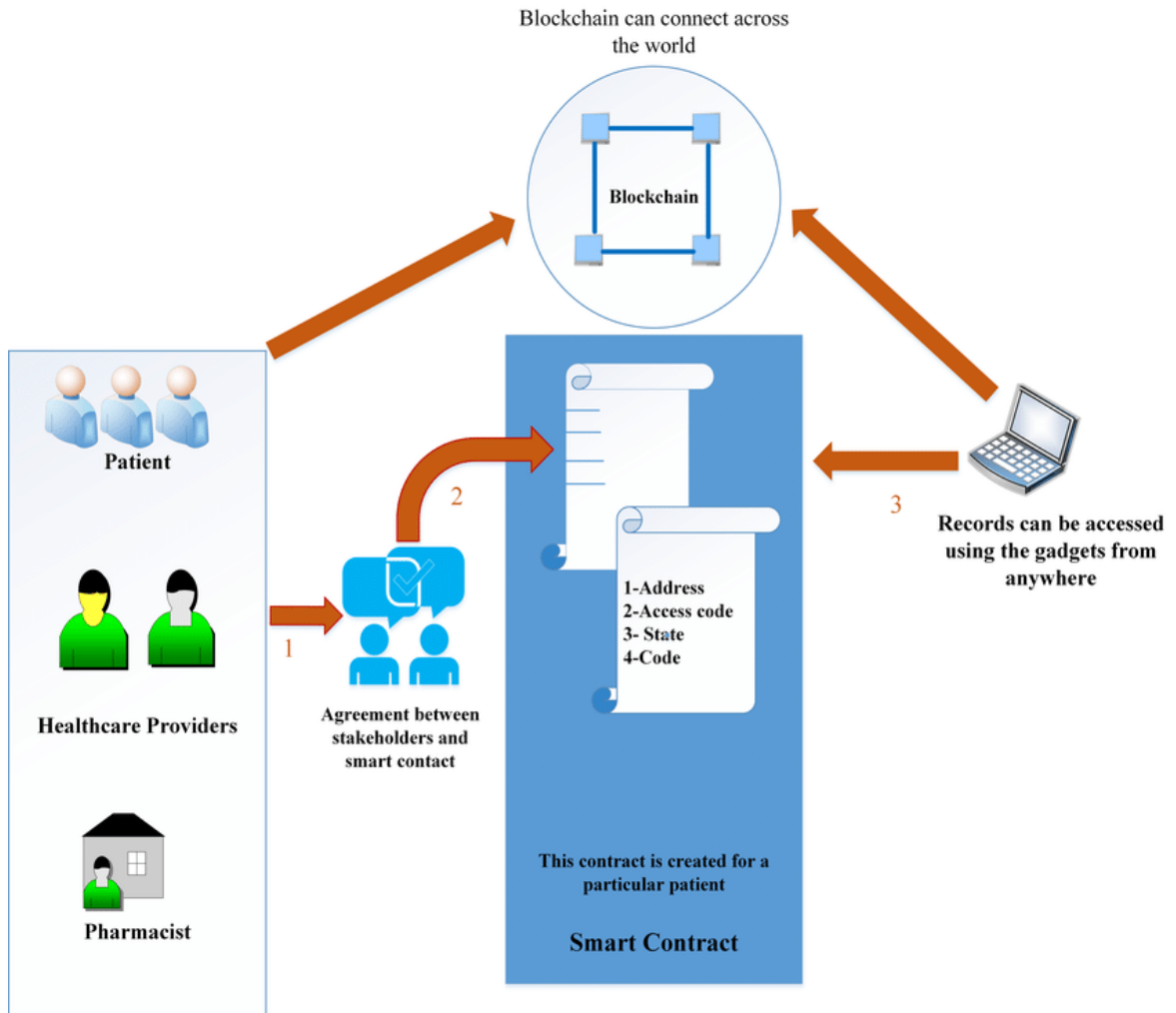
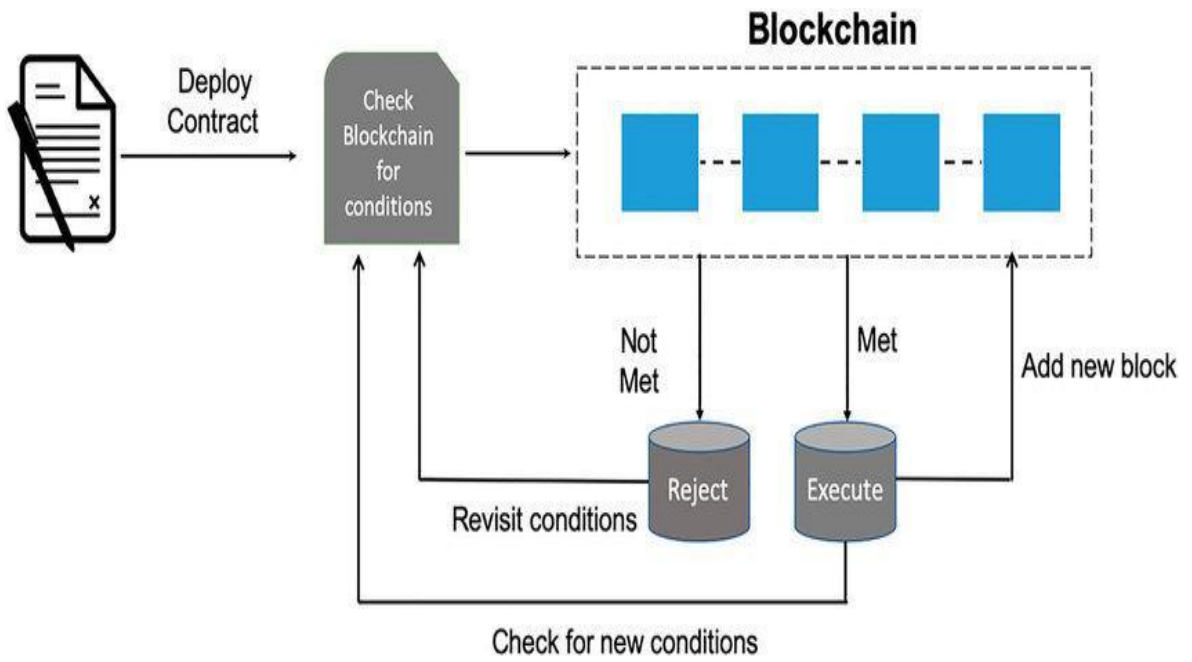
is difficult to falsify. Each participant or node entity in the system network has the same accounting ledger as the other participants or entity nodes. In related currencies blockchain [22], [23], this ensures complete consensus from all participants or nodes. Multiple methods are planned to be built on the blockchain technology platform to ensure the secure exchange of resources between untrustworthy parties.





Smart Contract:

A smart contract is a self-executing contract in which the terms of a two-party agreement are written directly into lines of code. A decentralised blockchain network disseminates the code and agreements contained inside it. Transactions are traceable and irreversible, and programming controls how they are carried out. Simply said, this is the place where business logic is written. Smart contracts are depicted in the diagram below.



1.5 Tools for Implementation

This section describes the basic tools and techniques used to implement our proposed framework.

Hyperledger Fabric:

The Hyperledger Fabric is a permissioned blockchain technology and open-source blockchain effort developed by the Linux Foundation. It is now one of the most prominent blockchain networks, allowing interested parties to join the network in order to change the ledger or initiate transactions. The Hyperledger Fabric Network may be built with many nodes representing different enterprises. In the Hyperledger Fabric network, which is frequently linked with an enterprise, an MSP assigns each node's identification. The MSP sends the client the enrollment and transaction certificates. It also provides for a far less computationally demanding consensus procedure than the POW.

Hyperledger Fabric also adds the ability to build trusted subnetworks called channels, which may generate shared ledgers with a set number of nodes while keeping secrets hidden from the rest of the blockchain. The fabric's smart contract component, Chaincode, enables parties to carry out complicated transactions with established permissions.

Hyperledger Composer:

Hyperledger Composer is a free and open-source blockchain application framework. It supports the Hyperledger Fabric framework and runtime, which makes business network modelling, application implementation, and interfacing with existing systems easier. When the business network definition is complete and ready to deploy, it is archived (.bna file). Refer to Fig. 1 for the four key files that make up the network definition: model, script, access control, and query.

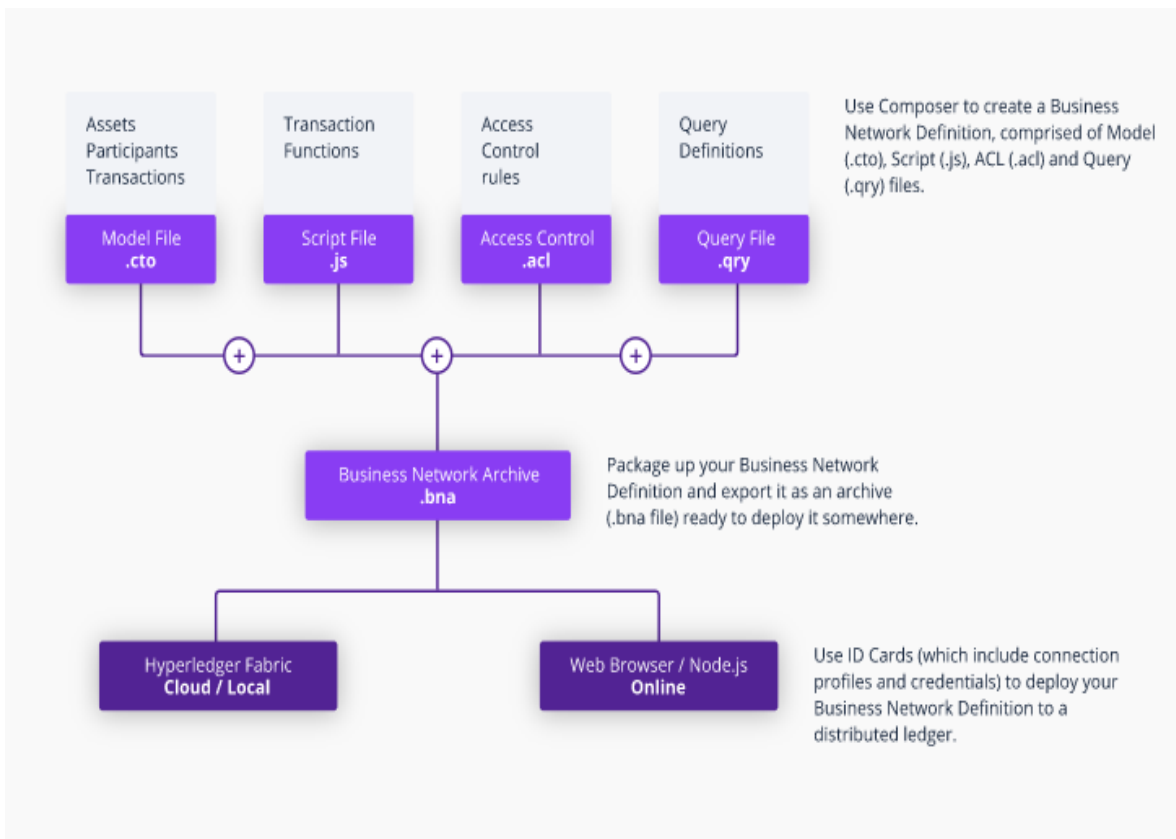


Figure 1: Architecture of Hyperledger

- The *model file*

Assets, participants, and transactions are the three essential components of the model file, which is in charge of sketching out the network's structure. Participants are the network's nodes, while assets are the network's variables. Transactions allow them to communicate. Network transactions are functions that keep the network up to date (e.g., transferring an asset).

- In the network, the script file handles transaction logic and defines several transaction routines in JavaScript. It also divided the participants into groups based on their access permissions for the network's transaction processing and asset transfer.

- In a business network, the access control file describes the user's scope and role, which decides whether they may create, read, update, or delete network items.

•By keeping a ledger of all previous transactions in the system, the query file determines the form and purpose of network enquiries.

Once defined, the network may be exported as an archive, downloaded, and activated on another PC. A network card in the shape of a participant or an administrator is required to connect to the system. The administrator can do complex activities such as adding new participants or removing current ones, whereas participant cards have a restricted scope and role in the network.

Composer's Playground user interface for configuring, testing, and deploying business networks was utilised for implementation. Developers may use Playground to model business networks employing assets (also called blockchain commodities or services), participants (sometimes called blockchain members), and transactions (known as methods allowing participants to interact with assets). The playground is being used to test the scenarios developed for this project (as presented in Figs. 2 and 3). The Define page is used to create each scenario, as shown in Figure 4, and the Test page is used to test the current system, as shown in Figure 5.

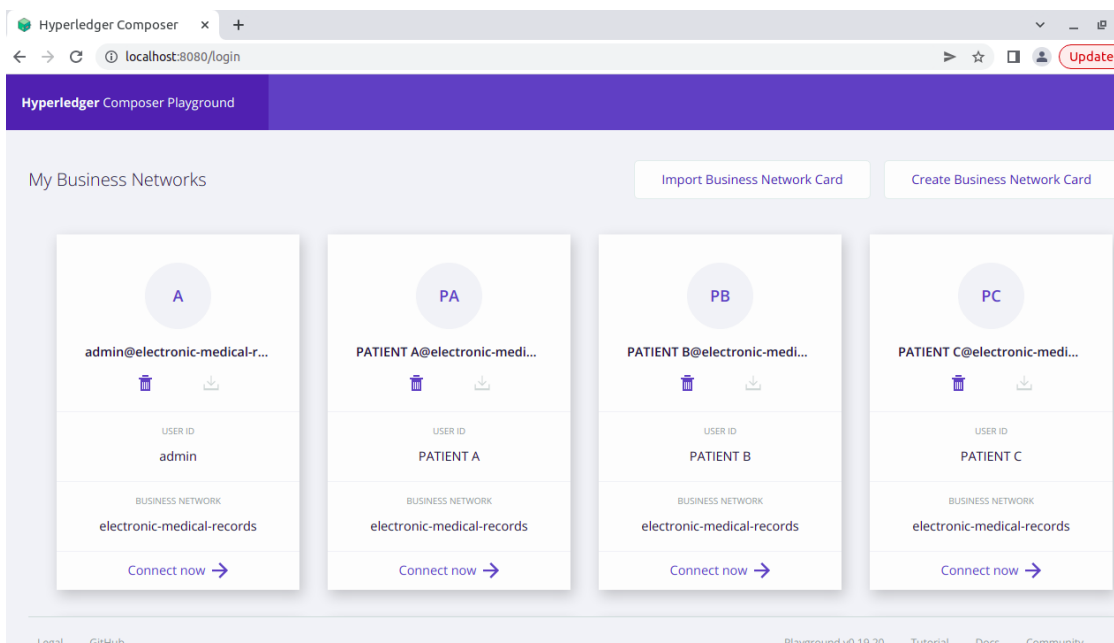


Figure 2: Composer Playground

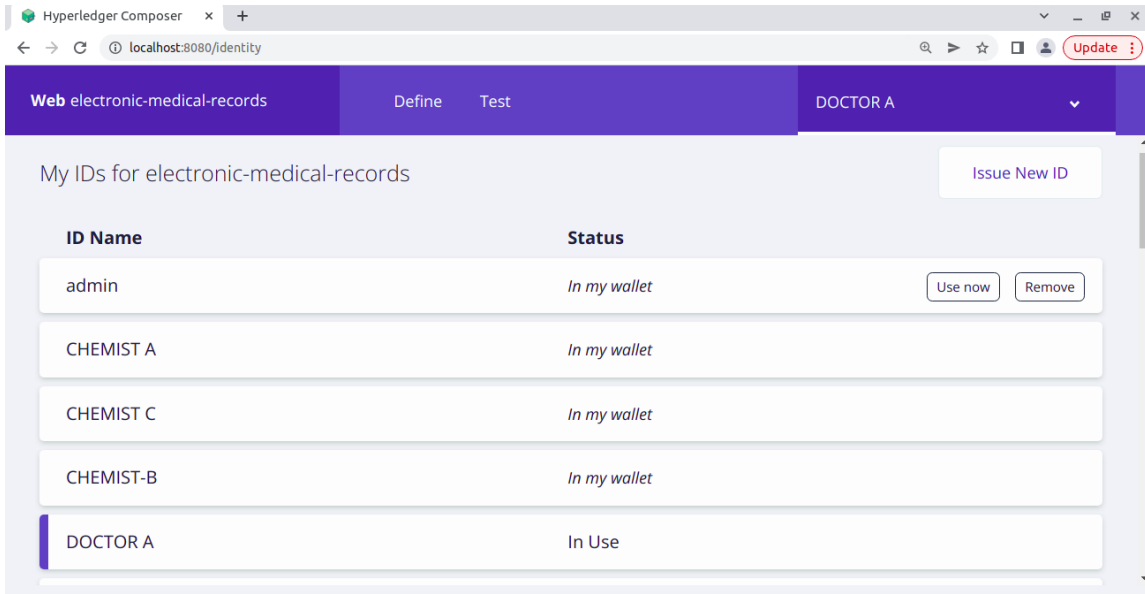


Figure 3:Composer's Users

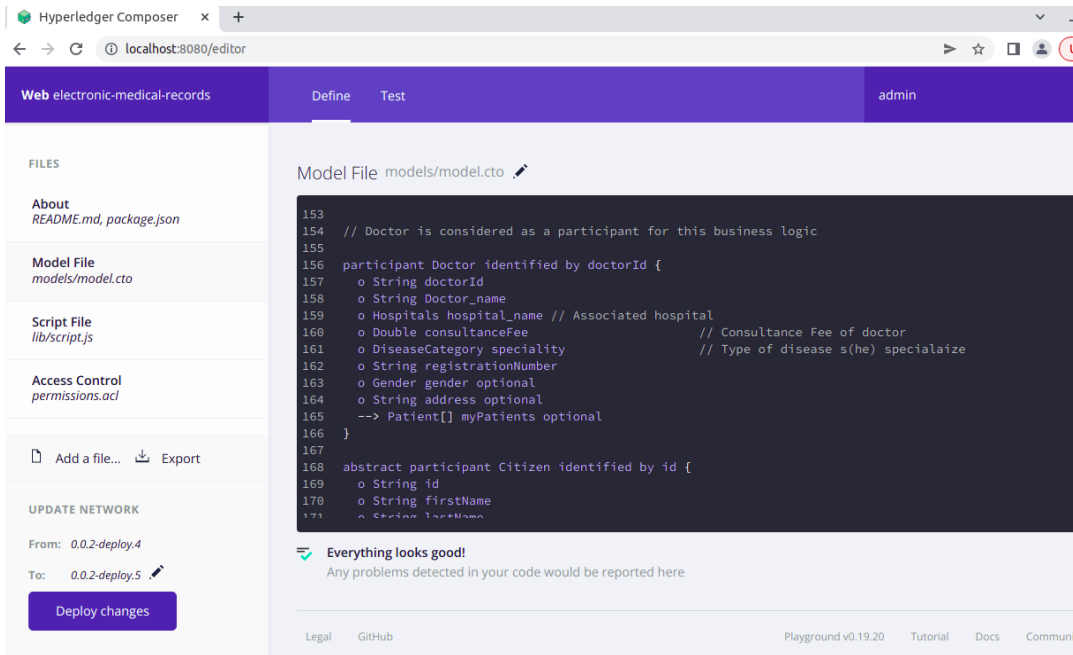


Figure 4: Composer's define page

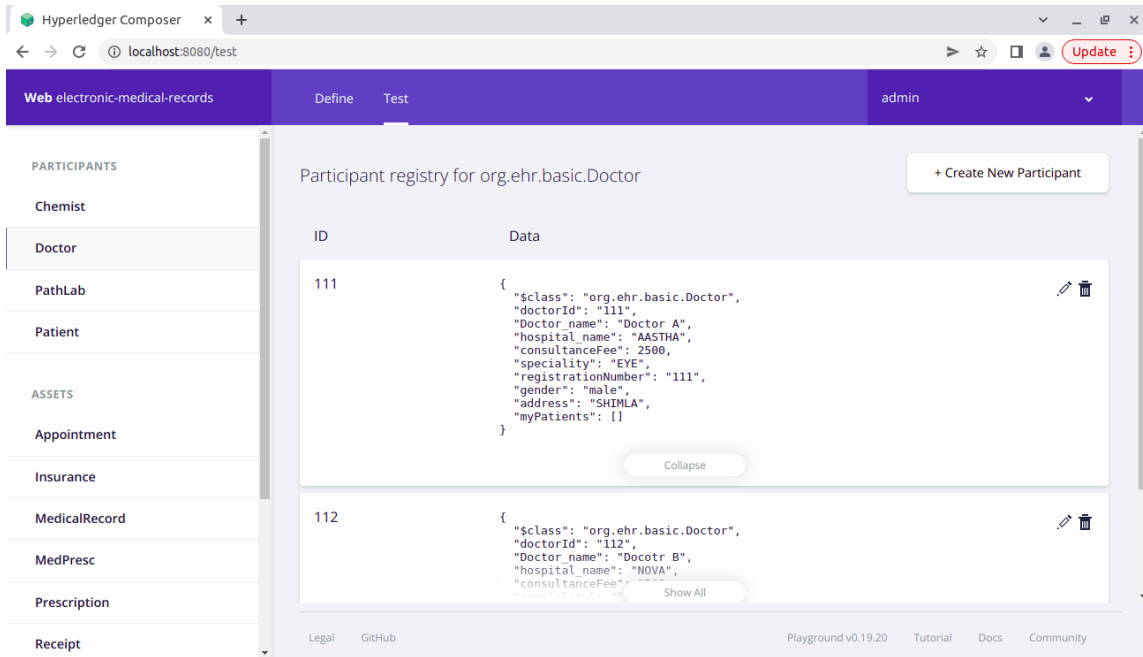


Figure 5: Composer’s test page

1.6 Language Used

- TypeScript
- JavaScript
- Bespoke Query Language
- Object Oriented Modelling Language

Chapter 02: LITERATURE SURVEY

This section goes through the basics of blockchain technology, such as Hyperledger Fabric.

2.1 Working of Blockchain Technology Network

The blockchain is a peer-to-peer platform with a decentralised (no centralised authority) and distributed design that assigns duties to a set of nodes and makes decisions on behalf of the network. Transactions are functions that each node is authorised to do. All approved transactions are recorded in the form of a block in a distributed immutable ledger. Blockchain rose to prominence in the financial realm because to the famous cryptocurrency BITCOIN [9]. Many actions occur in real time on the blockchain, and each user carries his or her own distributed ledger to detect fraud and verify at any time. The global and unchangeable blockchain network continues to add fresh verified blocks of transactions. In the comparable blockchain [10-11], all participants or nodes have equal possibilities for accounting ledger in the network, and it ensures perfect consensus among all nodes. For some commercial transactions, blockchain technology creates a trust layer without the use of a third party [12]. Blockchain applications have expanded and formed the backbone for several applications in the present context, including the healthcare industry. This new technology is particularly useful in this arena for creating podiums for storing, assessing, and retaining private healthcare information in a secure manner. The appropriate blockchain network may be determined based on the use-cases and is classed as public (permissionless), private (permissioned), hybrid, or federated/consortium blockchain.

A individual, an organisation, or a collection of organizations/people are allowed to share information and preserve a record of transactions in the Permissioned blockchain network. This network add-on uses a privileged layer to select who may join the network using a unique identity that is visible to all other users [13]. By exposing each user's identify, the risks of fraud are reduced. Byzantine Fault Tolerance (BFT) is commonly utilised in permissioned or private blockchain networks [14].

Permissionless or public blockchain, on the other hand, is a distributed ledger in which all users' identities are pseudonymous or unknown, and any member can add a new block. BITCOIN is a permissionless and public network in the same way that anybody may create a website on the internet. The mining algorithms allow any node to participate in the verification of transactions on the blockchain. Ethereum is a permissionless blockchain network, which means that anybody may create and execute code [15-16]. Proof of Work (POW) is commonly utilised in this type of network to combat the issue of network anonymity.

A single entity manages the private blockchain, whereas numerous organisations administer the consortium blockchain. A hybrid blockchain is a blend of public and private blockchain characteristics in which users have control over their data and just a fraction of it is exposed in the public domain or for a specific group of individuals.

Hyperledger Fabric

The Permissioned blockchain is implemented with the Hyperledger Fabric and it is also an open-source blockchain project hosted by the Linux Foundation [17]. It allows only the concerned participants and confines others to initiate, temper, or invoke any transactions by making a network with various nodes like the client, peer, and ordering nodes that are related to the different organizations. Every node has its own unique identity on the Hyperledger Fabric network and it is provided by Membership Service Provider (MSP) [18]. The role of the MSP is to generate the enrolment and transaction certificates for the clients and utilizes a specific consensus protocol that requires much lighter computational power than the POW. The Fabric has the capability to form trusted sub-networks, called channels, and has a smart contract functionality that enables users to execute complex transactions as per their permissions.

This section presents some existing literature in which some techniques have already been proposed to cope with the issues related to security in the healthcare domain in order to keep data secure in the network. Primarily, healthcare sector application solutions can be segregated into two main categories: 1) Cloud-based architecture solutions and 2) blockchain-based architecture solutions. At first, different cloud-based solutions have been proposed, especially, for managing the patient record in the healthcare industry by

minimizing the cost and improving the services [19]. For example, with cloud-based services, expenses related to prescription have likely to be reduced by 80% because it is centralized and ubiquitous in nature with complete accessibility of data anywhere at any time. Koufi et al. proposed a cloud-based system in which doctors can access patients' data whenever it is required for improving and prompt the treatment process [20].

On the other hand, blockchain-based solutions address the issues related to the healthcare industry more effectively, such as BitHealth and MedRec supporting data security and maintaining privacy [21-22]. Bitcoin uses POW consensus algorithms and it makes the entire network slow and energy inefficient. If the size of the network is large and a lot of transactions are taking place then the whole network will turn out to be time-consuming. MedRec was designed by MIT to allow the storage and tracking of EHRs records more efficiently [23]. In this model, patients have some degree of flexibility to restrict the permissions that are given to professionals/doctors to access their information. This project is also based on Ethereum, and uses the POW consensus algorithm as Bitcoin, making the whole network inefficient in terms of cost and energy. In some other work [24], the authors proposed an efficient blockchain-based model to keep medical records with different data formats.

All in all, with the intensive literature review, we get a great insight into blockchain technology, especially in the healthcare sector. By the entire conclusion made at the above-said methods with relevant information specified in the healthcare systems, we can form an effective evaluation strategy and conclude whether blockchain should be used in this domain. In this work, while analyzing the blockchain applications with findings and specifying the shortcomings of the existing work, we proposed a framework to eliminate some of the issues efficiently in the medical domain with proper access control mechanisms. Ultimately, the medical records of a patient can be shared over the network with proper consent given by the patient to doctors, path labs, and chemists in a more secure way to fill out the inconsistencies of the existing frameworks. The subsequent section explains the detail of healthcare application requirements to achieve the objective of the proposed work.

Chapter 03: SYSTEM DEVELOPMENT

This section describes the proposed framework for secure healthcare data management.

3.1 System Architecture

A blockchain is just a collection of blocks connected together by hashes and linked to previous blocks in the chain. So, regardless of the use case, the information set for each blockchain is made up of those blocks.

Because blockchain is decentralised, there is no central repository for it. That's why it's scattered over the network on computers and devices. Nodes are the systems or computers that make up the network. Each of the nodes has a copy of the blockchain, which contains all of the network's transactions.

As a result, you'll be able to think of the blockchain system as a spreadsheet with the data contained in each row representing the value of an address. The spreadsheet is also updated anytime something changes.

The blockchain, on the other hand, is ideal for storing large volumes of data. Yes, if you want to establish a video streaming platform similar to Twitch for YouTube, it can't be a database.

It's best for storing little bits of data in huge numbers of transactions, though. Blockchain networks are extremely scalable, and there are several blockchain variations that are also quite efficient in terms of accessibility.

Blocks

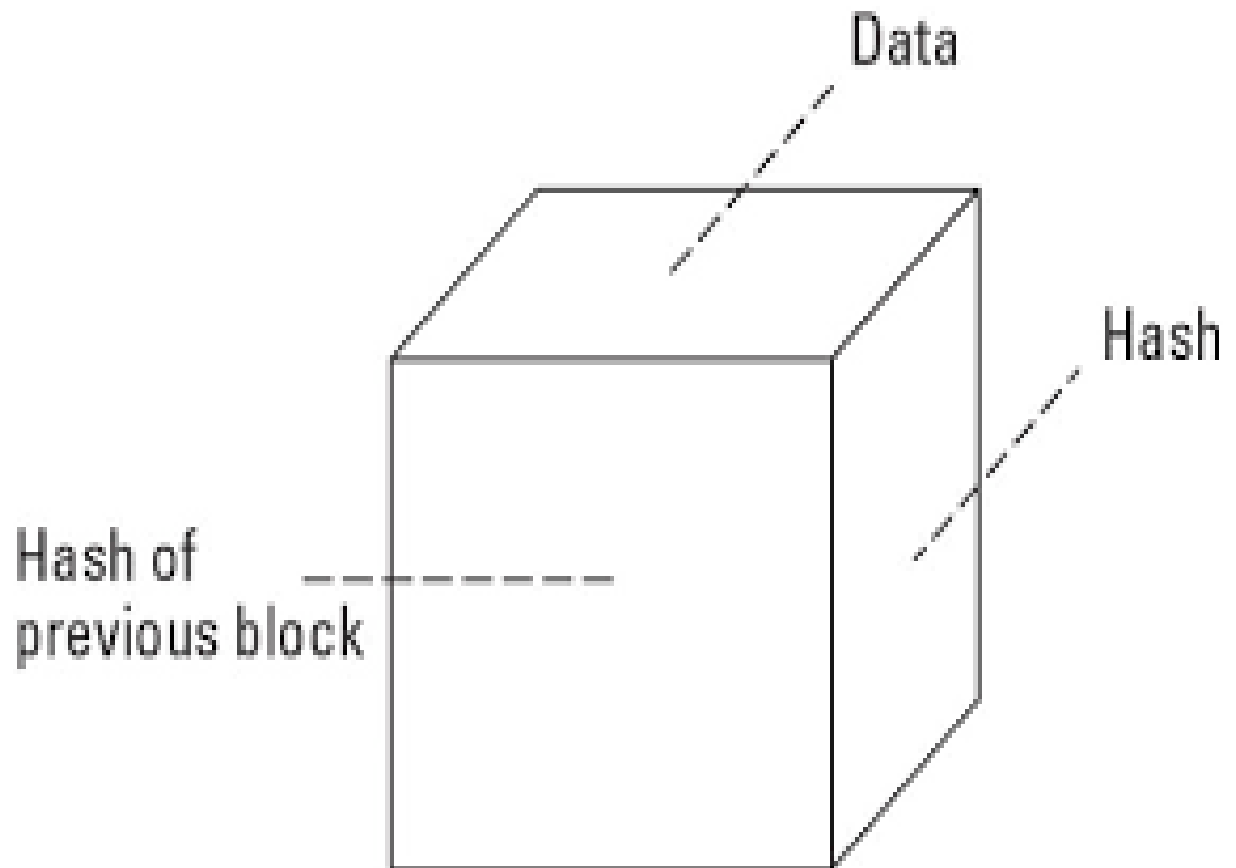
New information is added to a new block as it is received. When a block is full of information, it is linked to the preceding block, producing a chronological chain of data.

Every chain is made up of several blocks, each of which has three basic components:

- a) the data included within the block
- b) A 32-bit number called a nonce. When a block is constructed, a nonce is generated at random, and a block header hash is created.
- c) The hash might be a 256-bit integer that is linked to the nonce. It must begin with a large number of zeros (i.e., be extremely small).

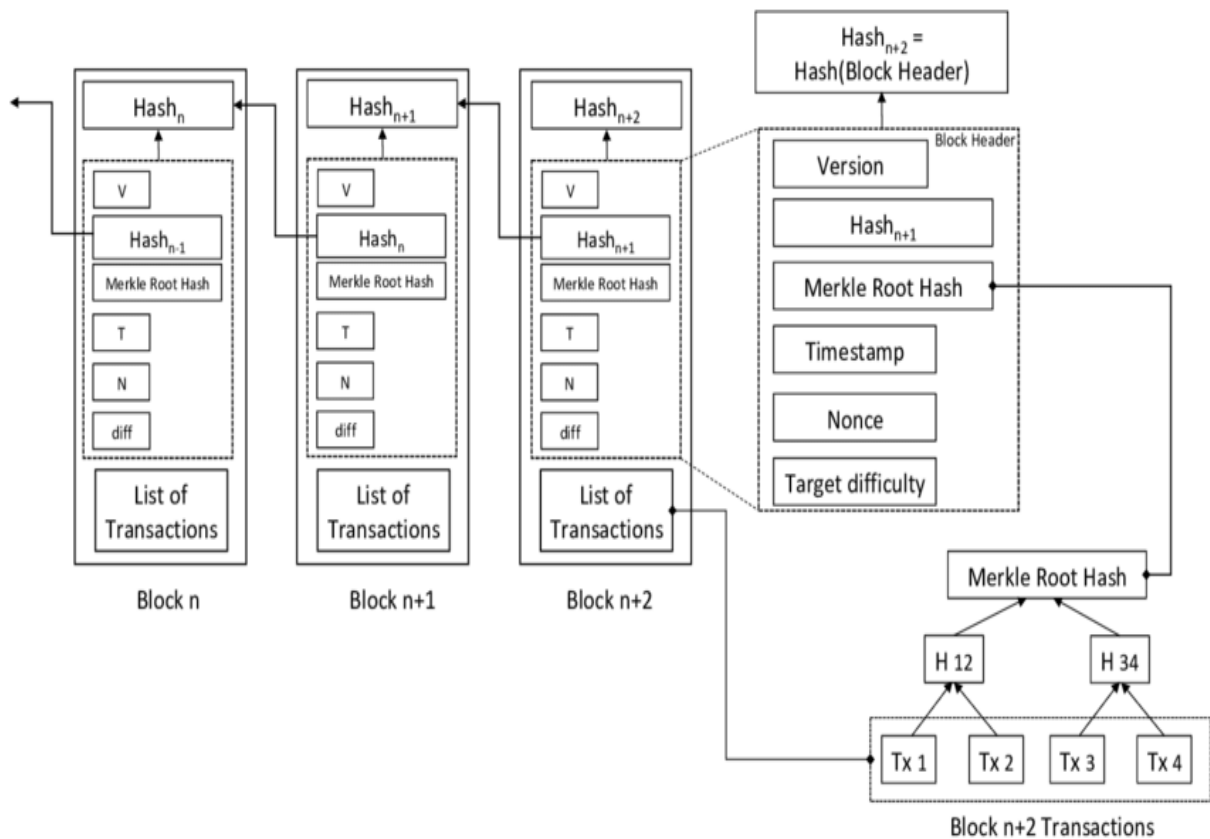
The next part usually has a more extensive explanation.

This is a common way of seeing a block's core structure.



This is how the basic structure of a block can be visualized.

As we discussed, the data-set comprises of the blocks.



A header, an identifier, and a long list of transactions comprise each block. To put it plainly, we have

1) Block header:

It contains the metadata information for the block in question. Metadata again consists of three sets of data at the foremost basic level.

Metadata:

->Previous hash.

->Mining competition for network. (it consists of timestamp, nonce and difficulty, all of which helps to take care of the integrity of the data)

->Merkle tree root. (this is that the root node of the tree used for storing the transactions of a block, it's what makes it possible to spot the full set of transactions for a given block with the assistance of one root node)

2)Block identifier:

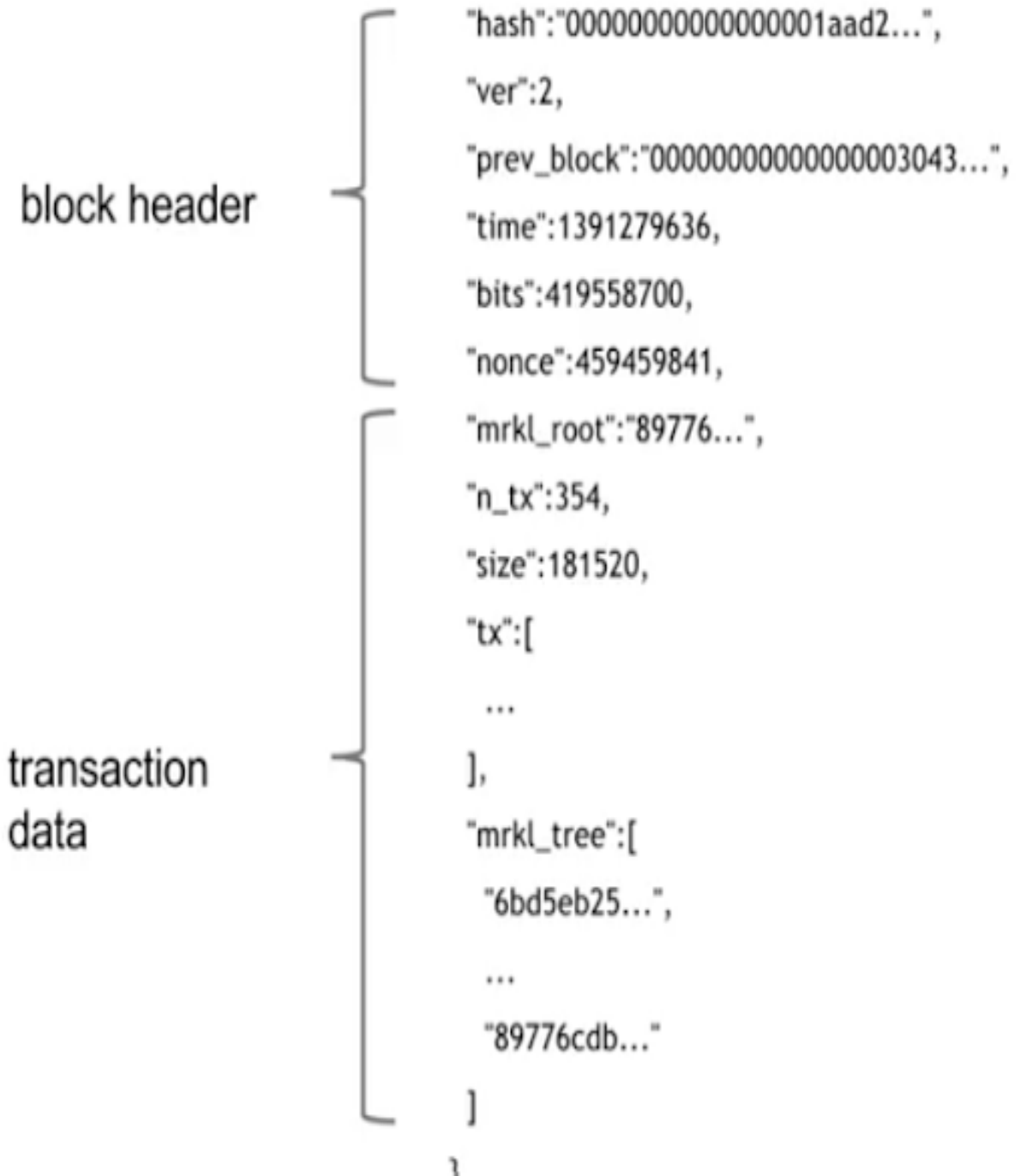
To identify a block, we'd want to have a cryptographic hash of all the information included within the block (which also includes prior block hashes) that can be used as a digital signature.

The block header can be hashed twice with the SHA-256 or SHA-512 methods to achieve this.

(SHA-256 is used in some of the most widely used authentication and encryption protocols, including SSL, TLS, IPsec, SSH, and PGP.) SHA-256 is used for secure password hashing in Unix and Linux.

SHA-256 is used to verify transactions in cryptocurrencies like Bitcoin.)

Another method of identification was the supported block height. However, due to the numerous problems it placed on the system, this came is no longer in use.

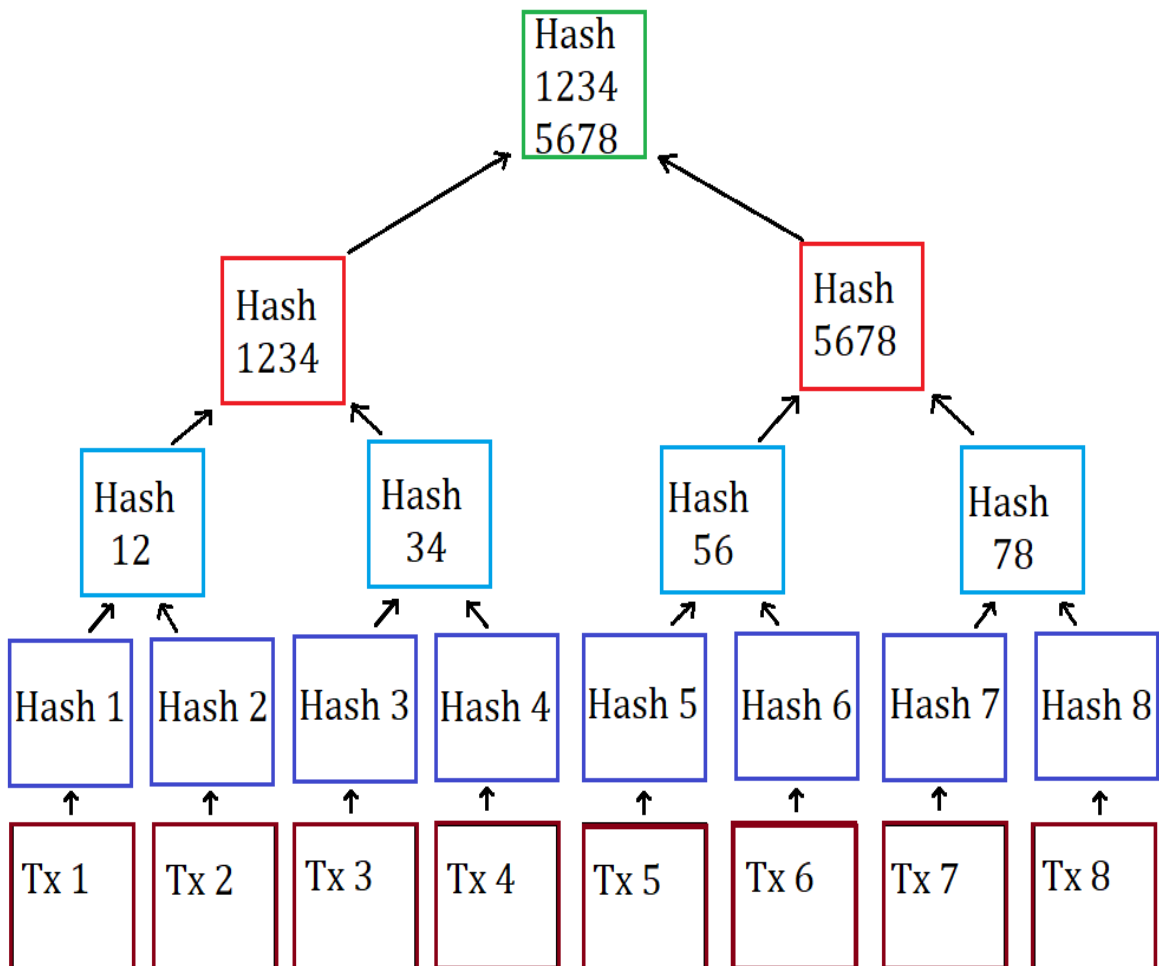


The above diagram shows how the various data structure and their data fields.

3) Merkle Tree:

To summarise all transactions in a specific block, it produces a digital fingerprint for the whole collection of incoming or leaving transactions. By inspecting the tree's leaf nodes, the user may determine whether or not a transaction is part of a certain block. Merkle trees are created by hashing two nodes until there is only one left. Every non-leaf node might be a hash of its previous hashes, and each leaf node could be a hash of its prior hashes (which is Merkle root and is kept in block header).

Because Merkle trees are binary, the amount of transactions we have is hashed with the number of transactions we have.



The size of the fields may usually be modified to meet the needs. The following are the default characteristics size that are implemented by all blockchain platforms:

For reference we have the original structure of

block

The **block** message is sent in response to a `getdata` message which requests transaction information from a block hash.

Field Size	Description	Data type	Comments
4	version	int32_t	Block version information (note, this is signed)
32	prev_block	char[32]	The hash value of the previous block this particular block references
32	merkle_root	char[32]	The reference to a Merkle tree collection which is a hash of all transactions related to this block
4	timestamp	uint32_t	A Unix timestamp recording when this block was created (Currently limited to dates before the year 2106!)
4	bits	uint32_t	The calculated difficulty target being used for this block
4	nonce	uint32_t	The nonce used to generate this block... to allow variations of the header and compute different hashes
1+	txn_count	var_int	Number of transaction entries
?	txns	tx[]	Block transactions, in format of "tx" command

Bitcoin Block Structure

Field	Description	Size
Magic no	value always 0xD9B4BEF9	4 bytes
Blocksize	number of bytes following up to end of block	4 bytes
Blockheader	consists of 6 items	80 bytes
Transaction counter	positive integer VI = VarInt	1 - 9 bytes

*from bitcoin reference paper.

3.2 Algorithm at work

We're utilising Hyperledger fabric and using a tool called Hyperledger composer to push code to it.

The algorithm's many stages are as follows:

- 1) Establish a business network.
- 2) Establish a business network.
- 3) Make a business network success file.
- 4) Use a runtime environment to deploy a business network (FABRIC).
- 5) Using composer, create a rest server.

1) Create a business network

Using Yeoman, create a skeletal business network. A business network name, description, author name, author email address, licence selection, and namespace are all required for this command.

```
"yo businessnetwork hyperledger-composer"
```

For the network name, type "EHR-network," and for the description, author name, and author email, type "desired information."

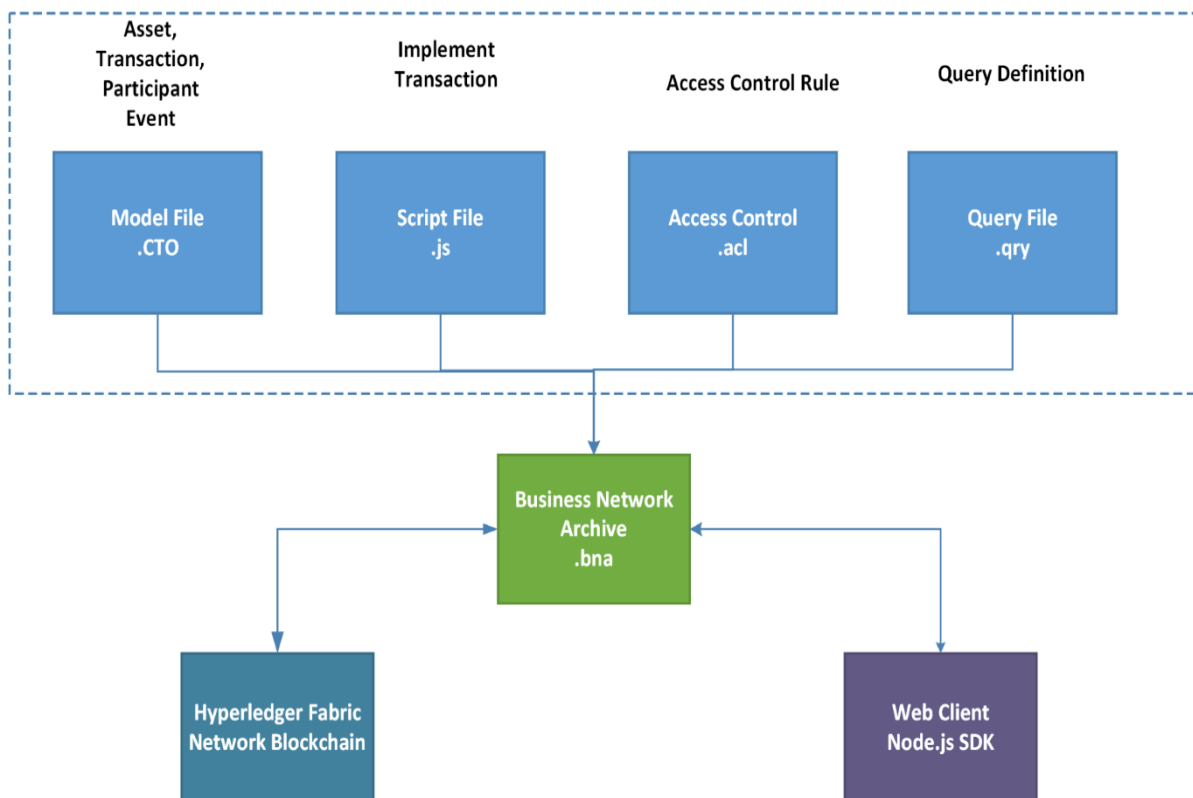
Choose Apache-2.0 as your licencing type.

As the namespace, choose "org.EHR.mynetwork."

On the Hyperledger composer, this builds a business network structure.

2) Define business network

Assets, participants, transactions, access control rules, and, optionally, events and inquiries make up a business network. There is a model (.cto) file in the skeletal business network produced in the previous phases that contains the class definitions for all assets, participants, and transactions in the business network. A basic access control document (permissions.acl), a script (logic.js) file containing transaction processor functions, and a package.json file providing business network metadata are also included in the skeletal business network.



In this step we code the 4 files mentioned above.

3) Create a network archive file for your business.

You'll need to bundle your business network into a deployable business network archive (.bna) file after you've defined it.

Using the command line, navigate to the ehr-network directory.

From the tutorial-network directory, run the command "composer archive create -t dir. -n."

After the process was finished successfully, an EHR@0.0.1.bna business network archive file was created in the ehr-network directory.

4)Deploy over runtime network

After the.bna file is prepared, the business network may be deployed to the Hyperledger Fabric instance. Information from the Fabric administrator is normally required to create a PeerAdmin identity with credentials to install chaincode on the peer and run chaincode on the composer channel.

```
"/createPeerAdminCard.sh"/startFabric.sh"
```

To deploy a business network to the Hyperledger Fabric, first install the Hyperledger Composer business network on the peer, then launch the business network and establish a new network administrator participant, identity, and relevant card. Before the network can be checked for responsiveness, the network administrator's business network card must be imported.

To get the corporate network up and running,

```
"composer network install --archiveFile PeerAdmin@hlfv1" "ehr-network@0.0.1.bna"
```

To begin the business network, first:

```
"composer network start --networkVersion EHR --networkName ehr-network"
```

```
" 0.0.1 --networkAdmin admin --networkAdminEnrollSecret adminpw --card  
--networkAdminAdmin admin --networkAdminEnrollSecret adminpw  
"--file networkadmin.card PeerAdmin@hlfv1"
```

To create a valid business network card from the network administrator identity:

```
--file networkadmin.card composer card import
```

Use the command "composer-playground" to run and test playground.

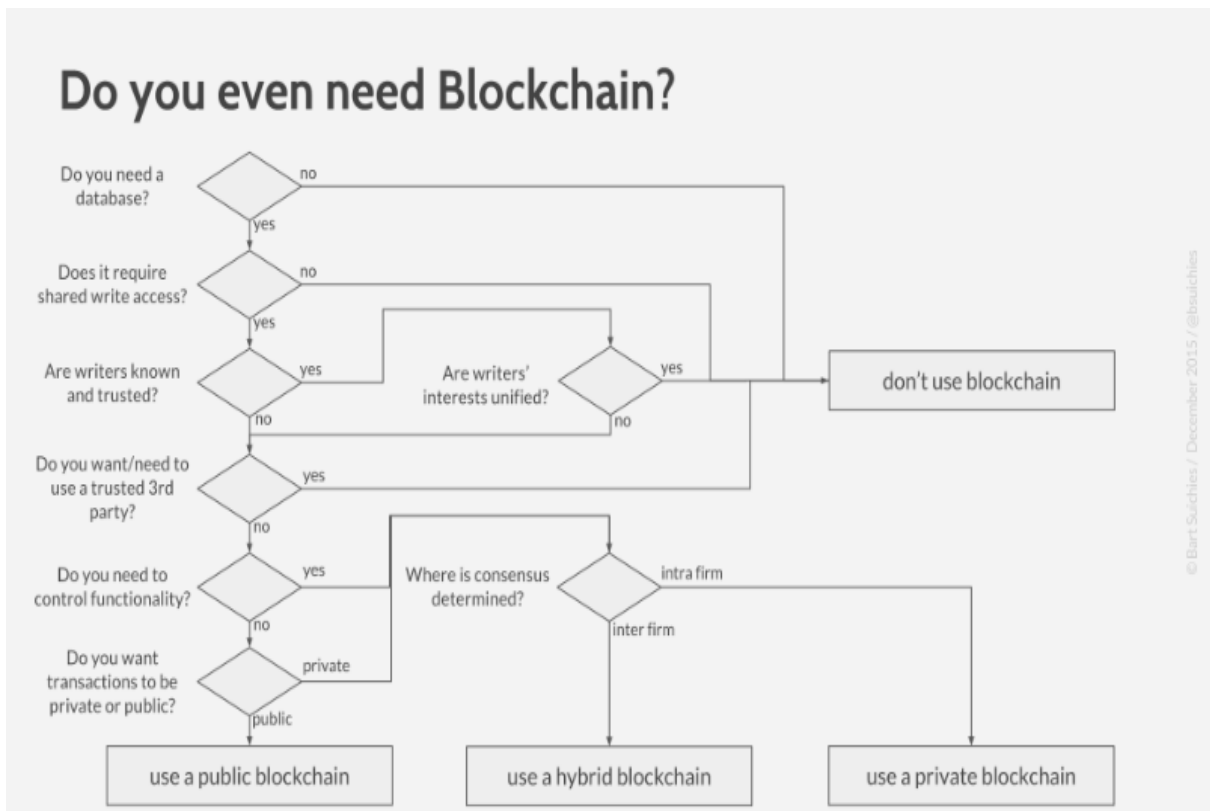
Following that, the composer playground appears, displaying the many participants as well as the various chain codes that we implemented in the files.

5)Generate a Rest server:

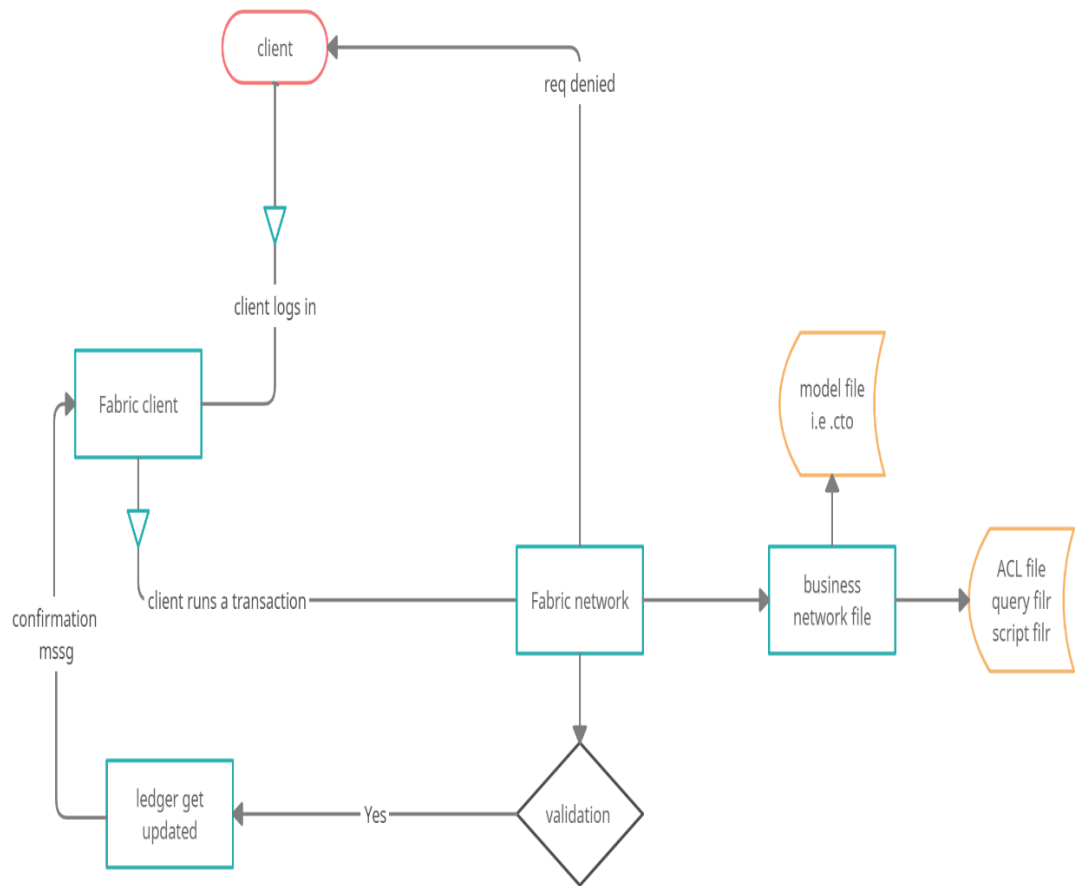
Composer has built in feature which allows this.

Flowgraph

The first flowgraph below is the one which helps us identify whether the blockchain implementation for the given use-case would be successful or not.



Now the below given represents the project in a nutshell:



3.3 Design and implementation

The system is created and deployed from a commercial standpoint, and it demonstrates how different blockchain system users interact with one another. As depicted in Fig. 6, our proposed business network comprises of Participants, Assets, and Transactions.

The class structure of various assets and participants in the blockchain network is shown in Figure 7. Inside the systems, relationships demonstrate how different parties have access to certain transactions. Because in our network, unless the intended participants acquire the required rights, all features of the available information are kept hidden.

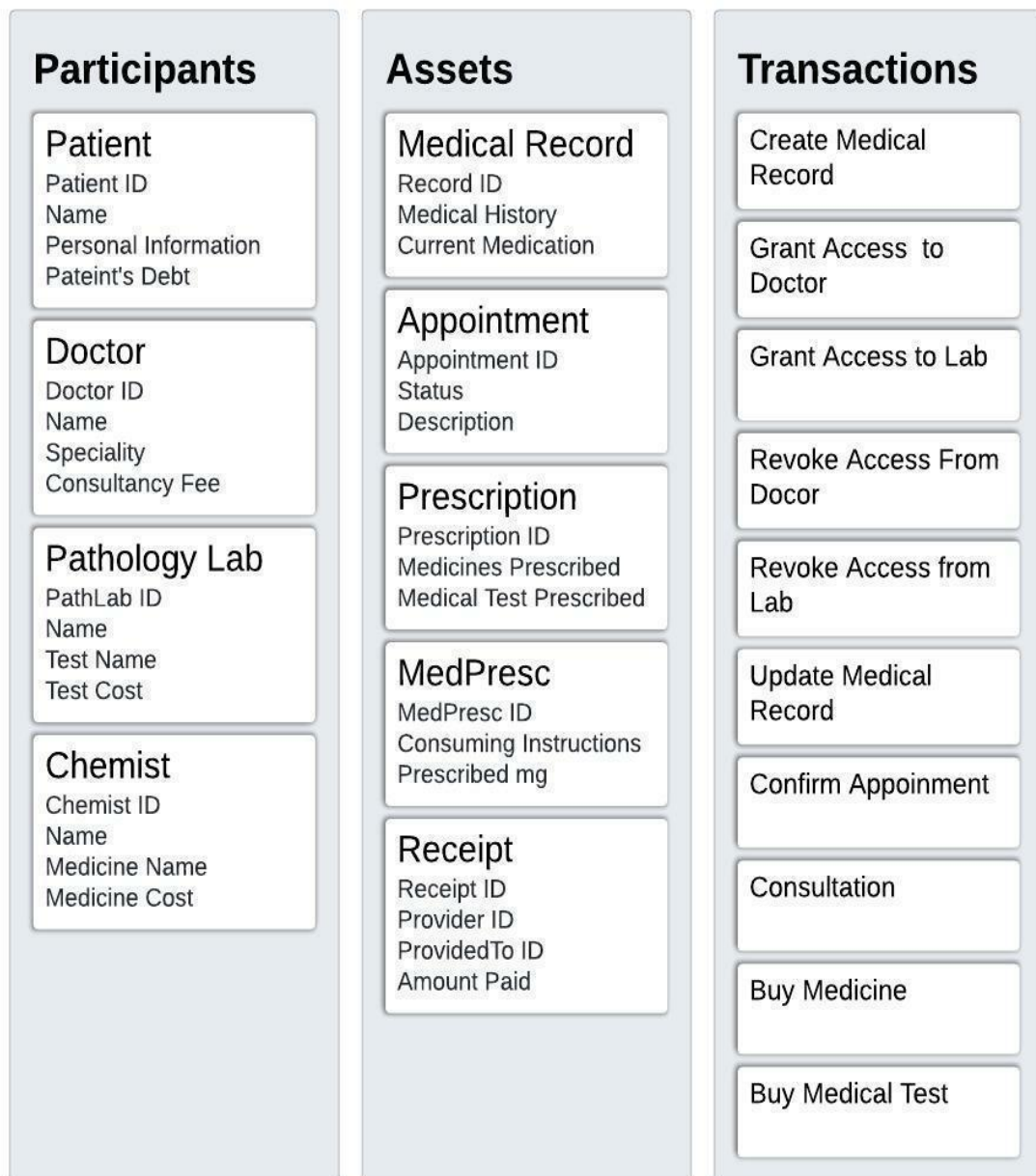


Figure 6: Participants, Assets, and Transactions in Blockchain Network

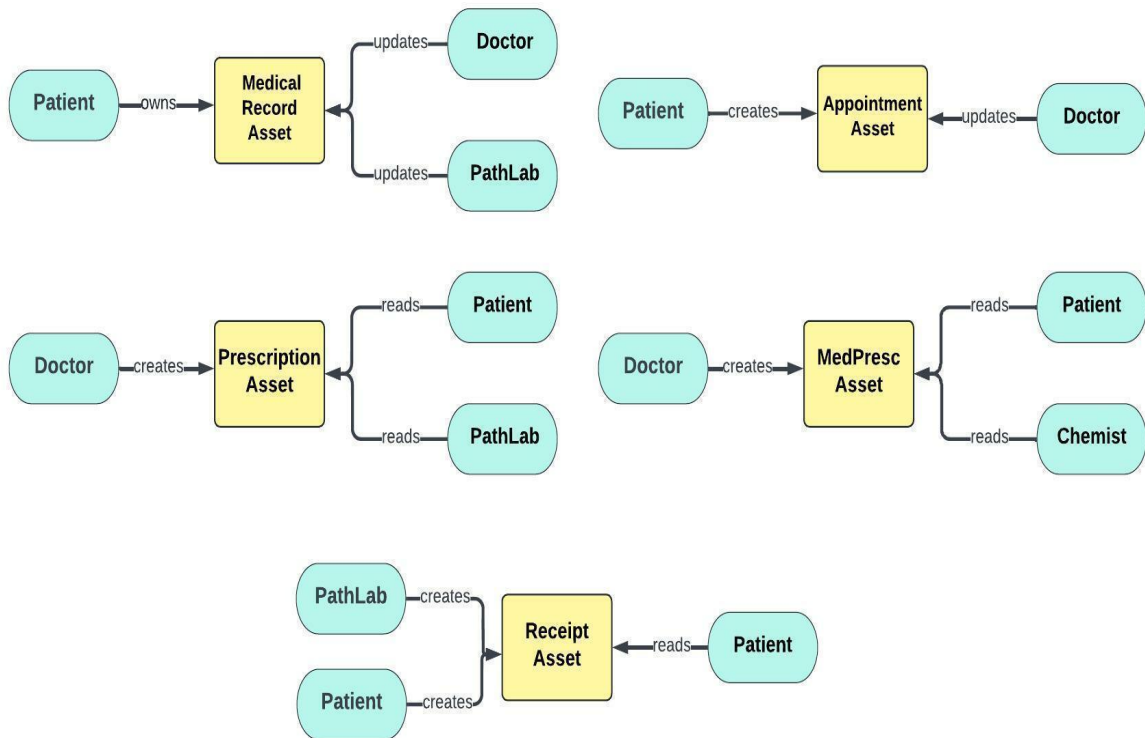


Figure 7: Class Diagram of the proposed framework

3.4 Users and roles

Different entities can access and operate records inside the blockchain network, and our proposed architecture covers the following four types of participants in this work:

Chemist\Doctor\PathLab

Patient

The system administrator has issued each member of the system a unique ID to complete the transactions depicted in Figure 8. Figures 9 (a) and (b) display a list of transactions because each entity inside the system has varied rights and flexibility to complete the operations: some have access to patient information, while others have the ability to edit records. Table 2 explains each participant's role and access control, as well as possible permissions. The numerous responsibilities that can be allocated will be reflected in these permissions.

Table 2: Participant's Permissions

Role	Permissions
Admin Member	<ul style="list-style-type: none"> • Has full access to all users and system resources. • Adds Participants to the blockchain network. • Read, Create, Update, and Delete all participants' information.
Doctor	<ul style="list-style-type: none"> • Read, Create, Update, and Delete his/her information. • All Participants can see all doctors. • A Doctor sees only the list of patients they are authorized to modify. • Read, Update Medical records for which they have permission. • Read, Create, Update Appointment. • Read, Create, Update Prescription. • Read, Create, Update MedPresc. • Confirm an Appointment with the patient. • Make Consultations for assigned patients.
Patient	<ul style="list-style-type: none"> • Read, Create, Update, and Delete their own participant Information. • Read, Create and Update Medical records. • Grant Access to Medical Records to Doctor and PathLab. • Revoke Access to Medical records from Doctor and PathLab • Read all assets, i.e. Appointment, Prescription, MedPresc, Receipt. • Create an Appointment with the Doctor. • Buy Medicine from the Chemist. • Buy a Medical Test from the PathLab.
PathLab	<ul style="list-style-type: none"> • Read, Create, Update, and Delete their own participant Information. • All Participants can see all Labs. • A Lab sees only a list of patients they are authorized to modify. • Read, Update Medical records for which they have permission. • Read Prescription. • Read, Create Receipt.

Chemist	<ul style="list-style-type: none"> • Read, Create, Update, and Delete their own participant information. • All Patients can see all Chemists. • Read MedPresc. • Read, Create Receipt
---------	---

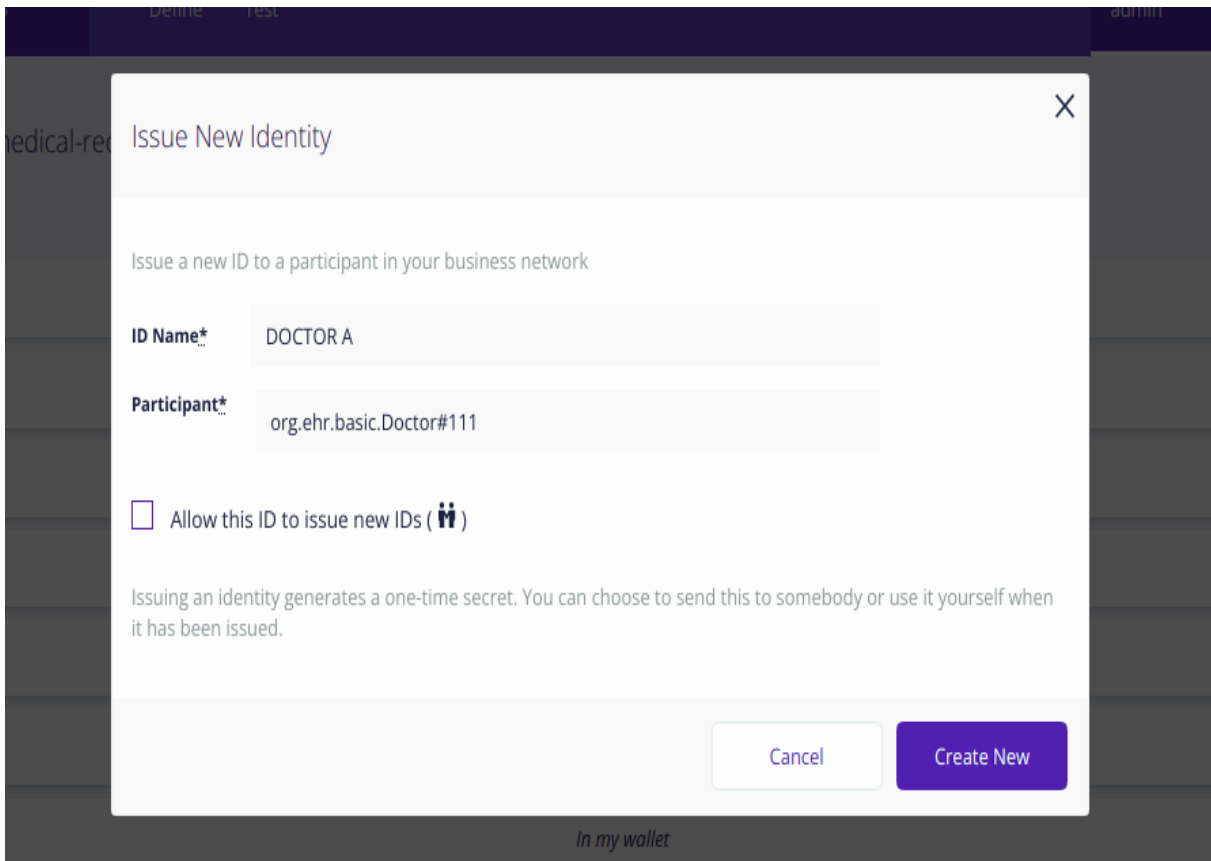


Figure 8: Create a new blockchain user.

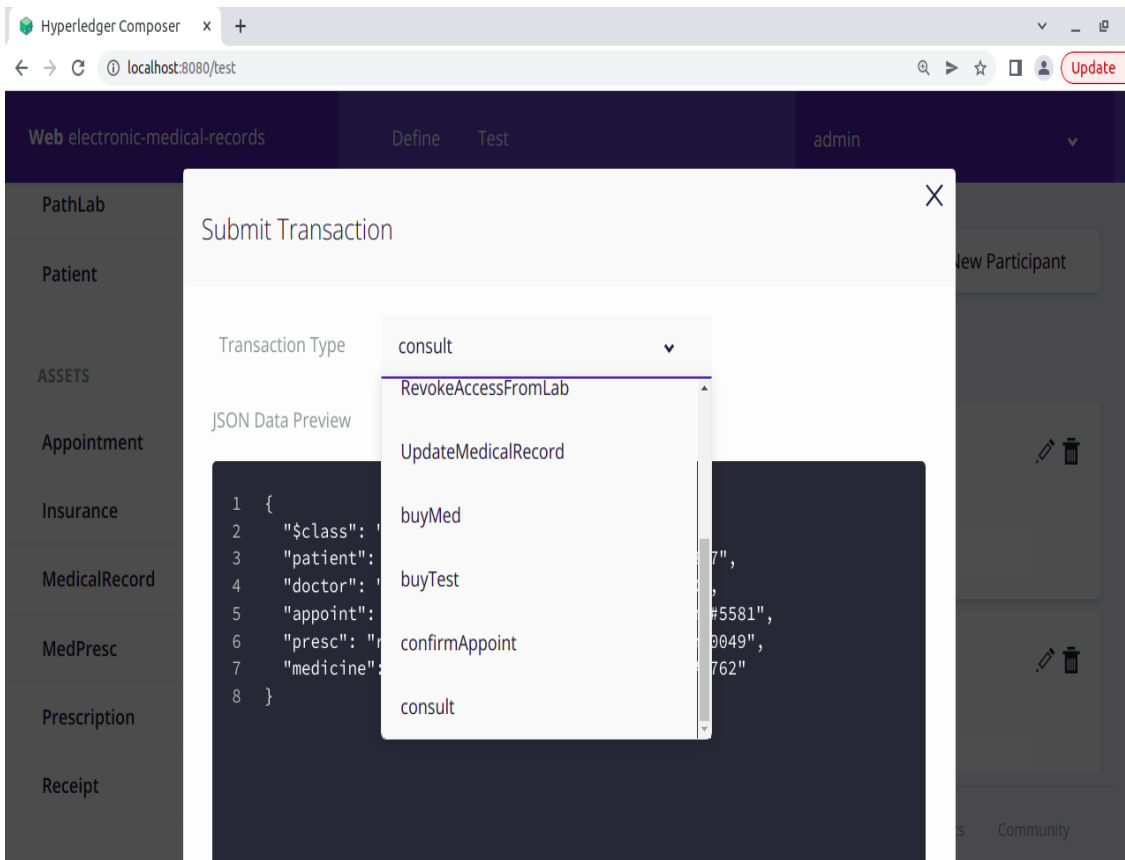
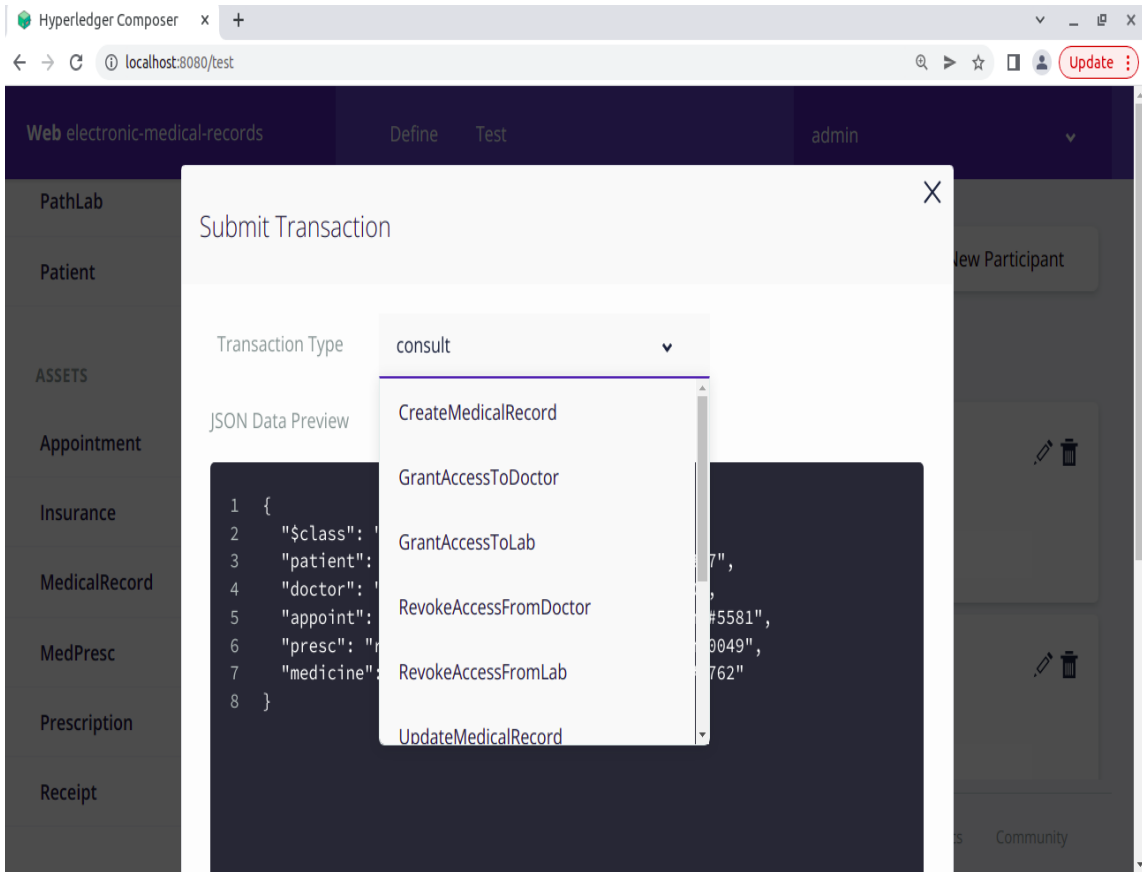


Figure 9 (a and b): List of Transactions

3.5 Operations

The proposed architecture includes a number of security techniques as well as regulations to manage interactions and restrict access inside the blockchain network. The assets (Medical records, Appointment, Prescription, MedPresc, Receipt) are JSON files, and participants interact with them using a smart contract that protects the data model. The contract, in reality, not only reflects the assets, but also the activities that may be done on them.

The smart contract provides the following major functions for interacting with the specified assets:

- **Build Medical Record:** This function allows patients to create their medical records on the blockchain network by establishing a record ID. In the network, only patients are allowed to generate Medical Records.
- **Grant Access:** This feature allows patients to provide doctors and pathology labs access to their medical records. To gain access to their medical records, the patient must submit their DoctorID/PathLabID and RecordID.
- **Update Medical Record:** This feature allows patients and medical professionals to make changes to an existing patient's medical record.
- **Revoke Access:** This feature allows patients to deny access to their medical records to doctors and pathology labs. To cancel access to their Medical Records, the patient must supply their DoctorID/PathLabID and RecordID.
- **Confirm Appointment:** This transaction is used to request an appointment by inquiring about the doctor's availability. According on their schedule, the doctor can approve or deny

the patient's appointment request. The appointment asset is saved to check the appointment's state, and the status changes to "confirmed" when the doctor confirms the appointment.

- **Consultation:** During an appointment, this feature is utilised to capture the interaction between the doctor and the patient. It permits the doctor to prescribe drugs and tests to the patient in exchange for the doctor charging the patient consultation fees. The charge is updated in the debt of the patient. The appointment's status switches to "consulted" when this transaction is completed successfully.
- **Purchasing Medicine:** This transaction is used to track the medications that patients purchase from their designated pharmacists. When this transaction is initiated, the chemist issues a receipt and bills the patient for the drugs.
- **Medical Test Purchasing:** This transaction is used to track medical tests performed by a pathology lab. When this transaction is initiated, the pathology lab issues a receipt, and the patient is charged a fee.

3.6 Scenario Design

3.6.1 Basic Scenario:

A normal user and a blockchain member are compared in this scenario to see how different access control regulations affect them (patients, doctor, chemist, and path lab). Only approved members will be able to study data on the blockchain, and the rest of the world will be uninformed of any transaction participants. In this case, the usage of a powerful hashing mechanism as well as the notion of a shared ledger are both proven. The participants in the transaction should be provided a copy of the transaction, as illustrated in Fig. 10. The participants who are added as non-admin members on the blockchain are Member A, Patient A, Doctor A, Chemist A, and PathLab A.

PathLab A will be able to access Patient A's medical record after Patient A creates one and permits access to it. When Patient A purchases drugs from Chemist A, both Patient A and Chemist A will have access to the receipt. Meanwhile, Member A will have no access to the medical record/receipt or any information about anybody else on the blockchain.

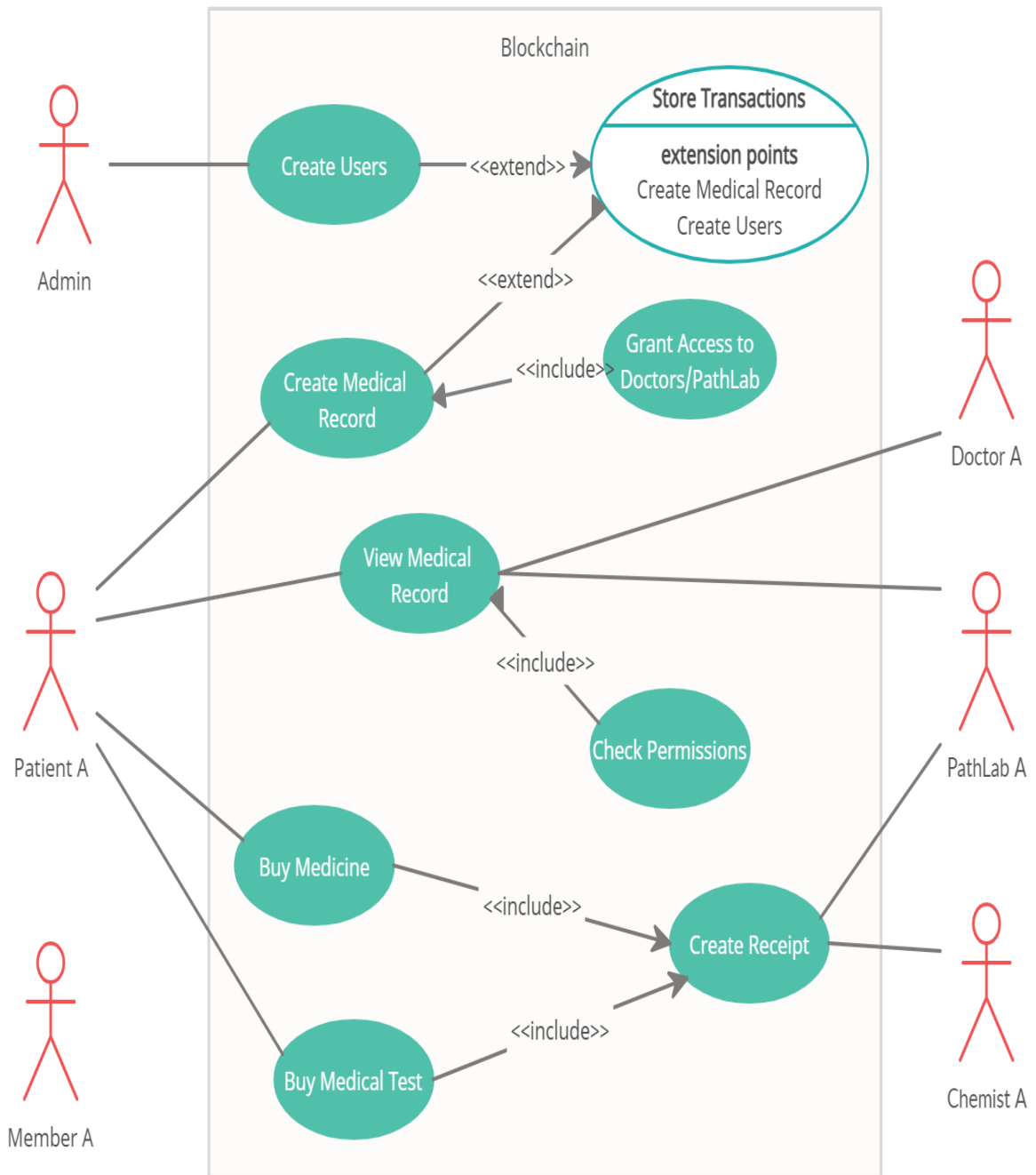


Figure 10: UML use case diagram for Basic Scenario

3.6.2 Permissioned Scenario

This example tests the range of Fabric permissions used to create, read, update, and delete actions. As seen in Table 2, patients, doctors, chemists, and pathologists will all have different permissions depending on the scenario. The goal of this scenario is to explore how Fabric permissions may be used to set up and maintain authorizations and access control for different types of users in the blockchain network, as seen in Figure 11.

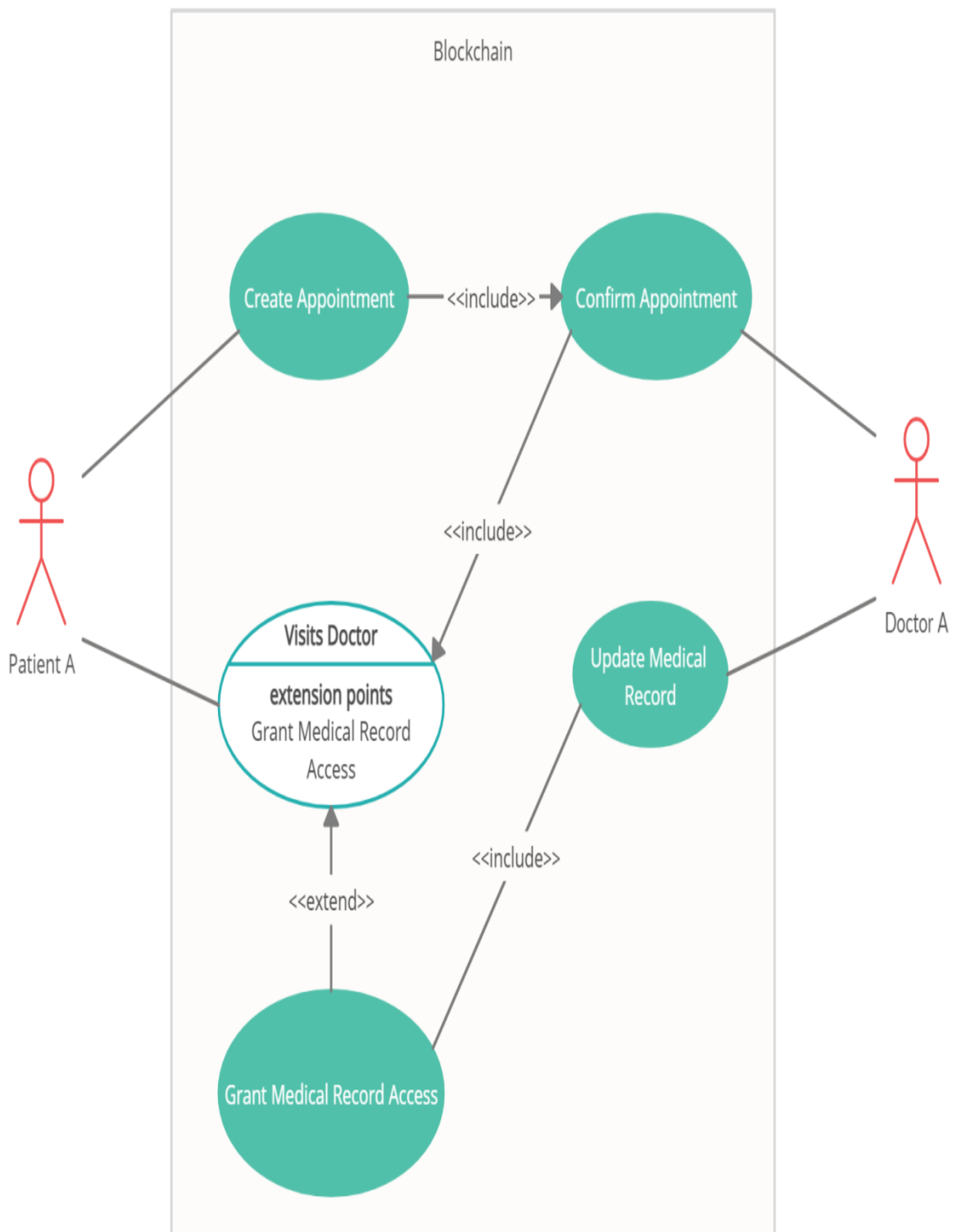


Figure 11: UML use case diagram for Permitted Scenario

3.6.3 Purging Scenario

To be GDPR compliant, patients must have complete control over their medical records, including the ability to grant or withdraw read access to their records as well as the ability to delete them from the network. According to the GDPR, a user's right to be forgotten must be honoured. As a consequence, as illustrated in Fig. 12, this use case investigates the removal of patient information. Patient A had given Doctor A and Doctor B permission to see his or her medical records, but now Patient A has revoked that authorization. Patient B also has the option of deleting his or her Medical Record from the system.

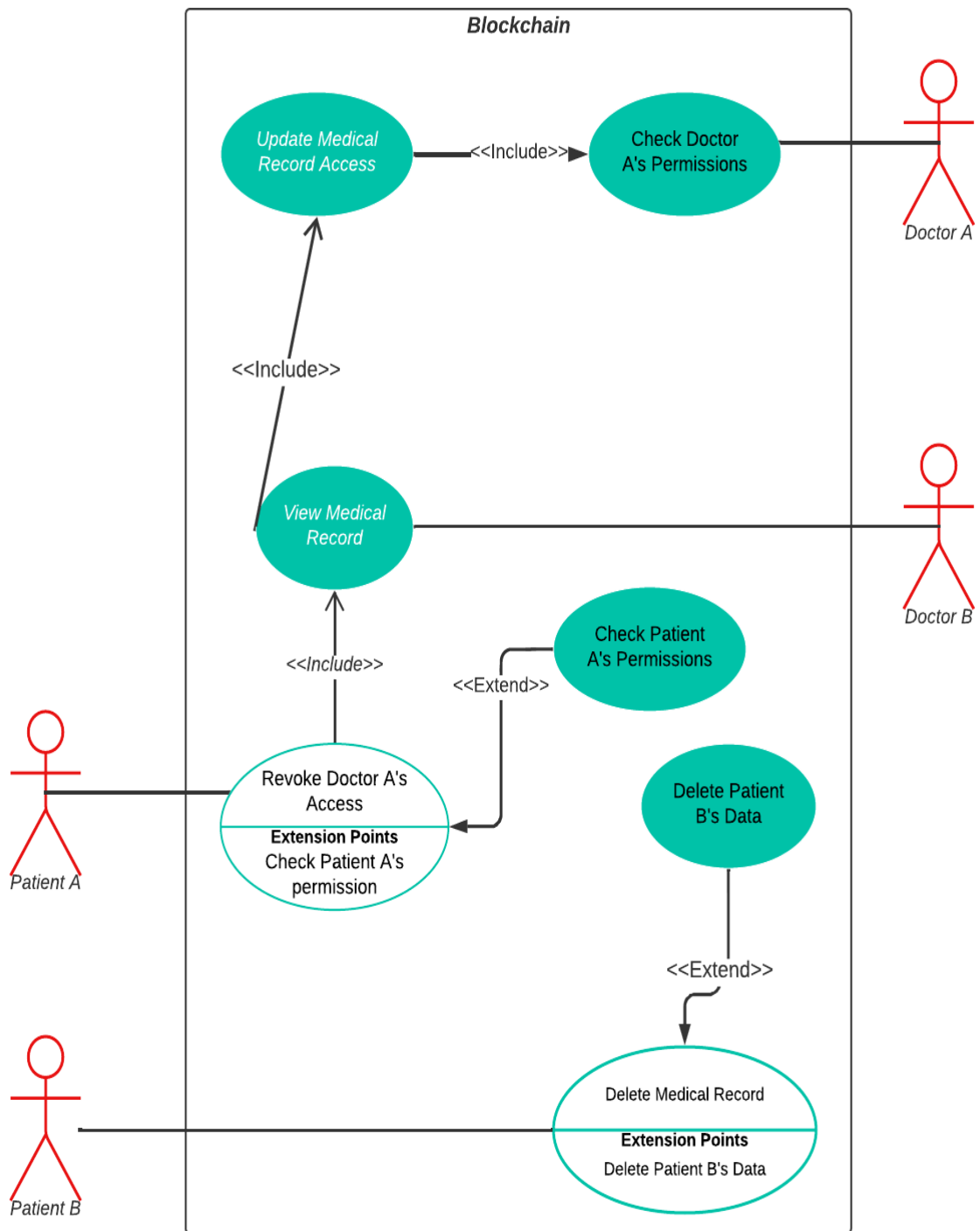


Figure 12: UML use case diagram for Purging Scenario

3.6.4 Encryption Scenario

All other participants are given a Public key and a Private key by Admin members. The notations used in the Algorithm are shown in Table 3, where x denotes the number of network participants (x = 1,2,3..).

Table 3: Notations used in the procedure 1

<u>Notation</u>	<u>Description</u>
Px	Patient
Dx	Doctor
Cx	Chemist
PLx	PathLab
MRx	Medical Record
Ppkx	Patient Public Key
Pprkx	Patient Private Key
Dpkx	Doctor Public Key
Dprkx	Doctor Private Key
UHRx	Updated Health Record

The following procedure describes the steps involved in creation and updation of a medical record.

Procedure 1: Creating and updating Medical Record

Input: A Doctor Dx with their Dpkx

Output: Updation of medical record

1. The procedure of creating and updating Medical records
2. Px with Pprkx creates MRx // Patient with his private key key creates a medical record

3. $P_x \rightarrow MR_x (D_{pk_x})$ // Patient Grants access to medical records using Doctor public key
4. For each user u , given access to MR_x
5. If (Permission == “ALLOWED” and Role = “Doctor” or “PathLab”)
//Algorithm checks whether Access Control permission is ALLOWED or DENIED to access MR_x
6. $D_x \leftarrow \text{Decrypt} (D_{prk_x} (MR_x))$ // Doctor decrypts Medical Record with his Private key
7. $D_x \rightarrow \text{Update } MR_x(D_{prk_x})$ // Doctor encrypts updated Medical Record with his Private Key
8. $P_x \leftarrow \text{Decrypt} (P_{prk_x} (UMR_x))$ // Patient decrypts updated Medical Record with his Private Key
9. Else (Permission = “DENY”)
10. D_x cannot view MR_x
11. End if
12. End for
13. End procedure

CHAPTER 04: PERFORMANCE ANALYSIS

The results of the executed scenarios in the blockchain environment are discussed in this section.

4.1 Experimental Setup

The tests and implementations are done on a laptop with an Core i7 intel CPU and 16 GigaByte of RAM running Ubuntu OS (version 20.04.1LTS). Node: 8.9 or higher, npm: v5.x, Docker-Compose: Version 1.8 or higher, Docker Engine: Version 17.03 or higher,, git: 2.9.x or higher, Python: 2.7.x are the requirements for installing Hyperledger Fabric with Composer.

Composer-cli is the most important of the several components (also known as CLI tools) required to set up the development environment. Components like composer-rest-server, on the other hand, are required for encryption features. Installation of Composer Playground 0.19.20 and VSCode 1.51.1 was done . At last Hyperledger Fabric was installed from github.

4.2 Privacy and Security

The proposed blockchain network protects the privacy of patients by allowing them to establish granular access control throughout their EHRs. It also takes into account access control management by using smart contracts. The given model in the Hyperledger composer network is based on the defined participant's IDs. Figures 13 and 14 demonstrate transaction and access control language code samples, respectively. As a result, no blockchain entity or rogue users will be able to access medical data. Only the list of patients who have been allowed access to their medical records is visible to doctors. Channels in the Hyperledger Fabric are built using access policies that control who has access to the channel's stores, which include smart contracts, transactions, and ledger state. As a result, these channels are made up of nodes where the privacy and confidentiality of medical information are defined. The technology safeguards medical records against

ransomware and other security threats. A blockchain network is a decentralised network with no single point of failure or central repository through which attackers might get access. The concept of a shared ledger ensures that data inside the system is truthful and unchangeable since each peer of the blockchain has its own copy. To assess the performance of the proposed framework, we used the Hyperledger Composer playground because the information is recorded as hash values for every healthcare transaction on the blockchain, the prototype implementation and analysis prove that the technique is tamper-resistant.


```
Script File lib/script.js 
21 * @transaction
22 */
23 async function gettingAppointment(catx) {
24   if (catx.appoint.status === 'CONFIRMED'){
25     throw new Error('Appointment already confirmed');
26   }
27   if (catx.appoint.status === 'CONSULTED'){
28     throw new Error('Appointment already consulted');
29   }
30   if (catx.appoint.status === 'REJECTED'){
31     throw new Error('Appointment already rejected');
32   }
33   if (catx.doctor.speciality !== catx.appoint.group){
34     throw new Error('Doctor is not specialized into the required disease category');
35   }
}
```

Figure 13: Code snapshot of transaction in the Medical Record Blockchain Network

```
ACL File permissions.acl
170
171 rule R1a_DoctorSeeUpdateThemselvesOnly {
172   description: "Doctor can see and update their own record only"
173   participant(t): "org.ehr.basic.Doctor"
174   operation: ALL
175   resource(v): "org.ehr.basic.Doctor"
176   condition: (v.getIdentifier() == t.getIdentifier())
177   action: ALLOW
178 }
179
180 rule R1a_PatientSeeUpdateThemselvesOnly {
181   description: "Patient can see and update their own record only"
182   participant(t): "org.ehr.basic.Patient"
183   operation: ALL
184   resource(v): "org.ehr.basic.Patient"
}
```

Figure 14: Code Snapshot of Access Control Language in the Medical Record Blockchain Network

As described in Section 4, each test case performs validation to increase the fault-tolerance of the developed framework. 4. In the Basic Scenario, access control was used to limit resource utilisation to specific roles (patients, medical practitioners, and medical

institutions). To keep personal information secret from blockchain participants, a thin layer of confidentiality is maintained. In addition, the Basic Scenario highlights two key blockchain concepts: hashing and shared ledger, which are used to achieve a suitable level of integrity. Each transaction is hashed with SHA-2 to ensure that the transaction is valid. Because SHA-2 has never been broken, changing or fabricating a transaction that fits the blockchain is almost impossible.

The Permissioned Scenario expands on the Basic Scenario by incorporating several access constraints that assure anonymity across blockchain participants. By granting distinct permissions to various roles inside the blockchain, the number of people who have access to patients' personal data is considerably reduced, reducing the danger of data breaches. Doctor A is unable to access any patient's medical records, as shown in Figure 15. When Patient A authorises Doctor A medical record access, as shown in Fig. 16, Doctor A can view and update Patient A's medical record, as shown in Figs. 17 and 18. Information is secured from outsiders of the blockchain in the Encryption Scenario, guaranteeing total privacy and security. Every block has a transaction hash, which is updated anytime an asset is changed. As a result, tampering with the ledger is computationally difficult, guaranteeing that the assets are untouchable. Participants in the blockchain are prohibited from acquiring access to health records without the patient's permission due to the rules and degrees of access control.

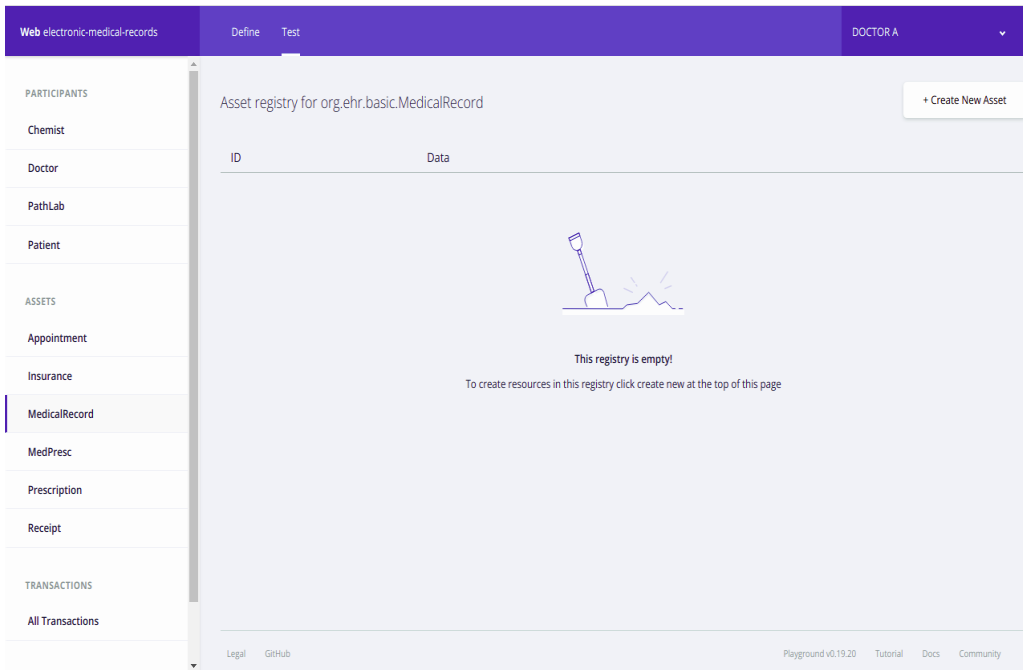


Figure 15: Doctor A has no access to Medical Records

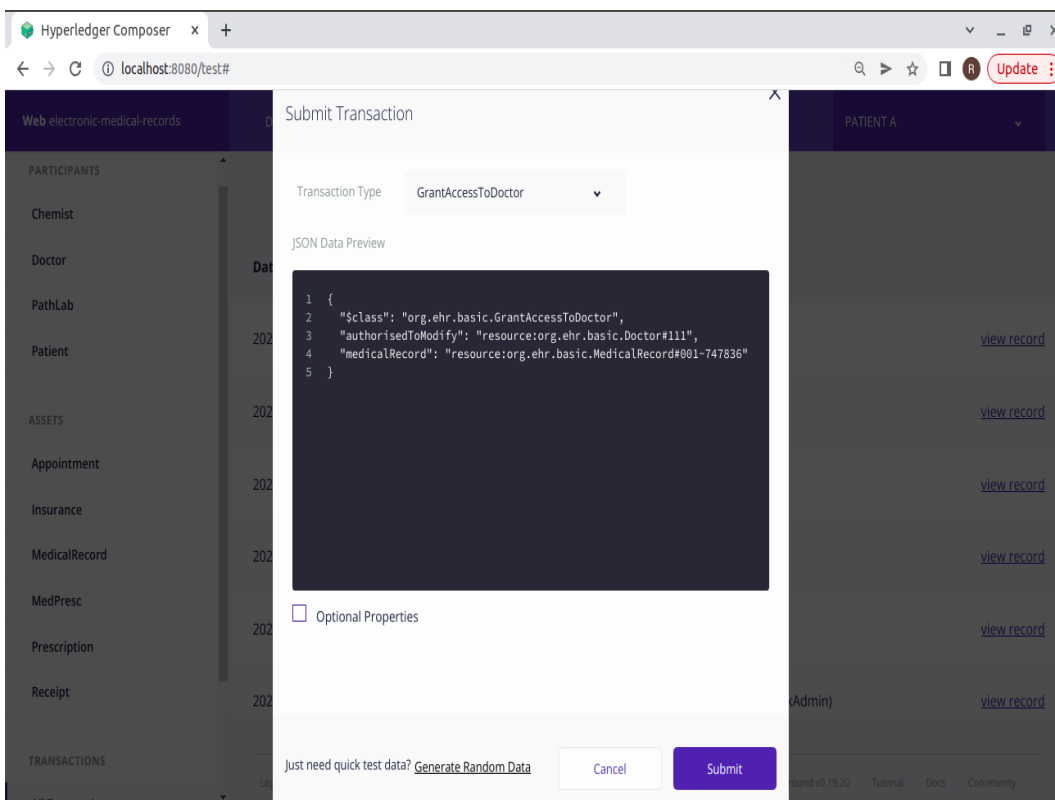


Figure 16: Patient A grants medical record access to Doctor A

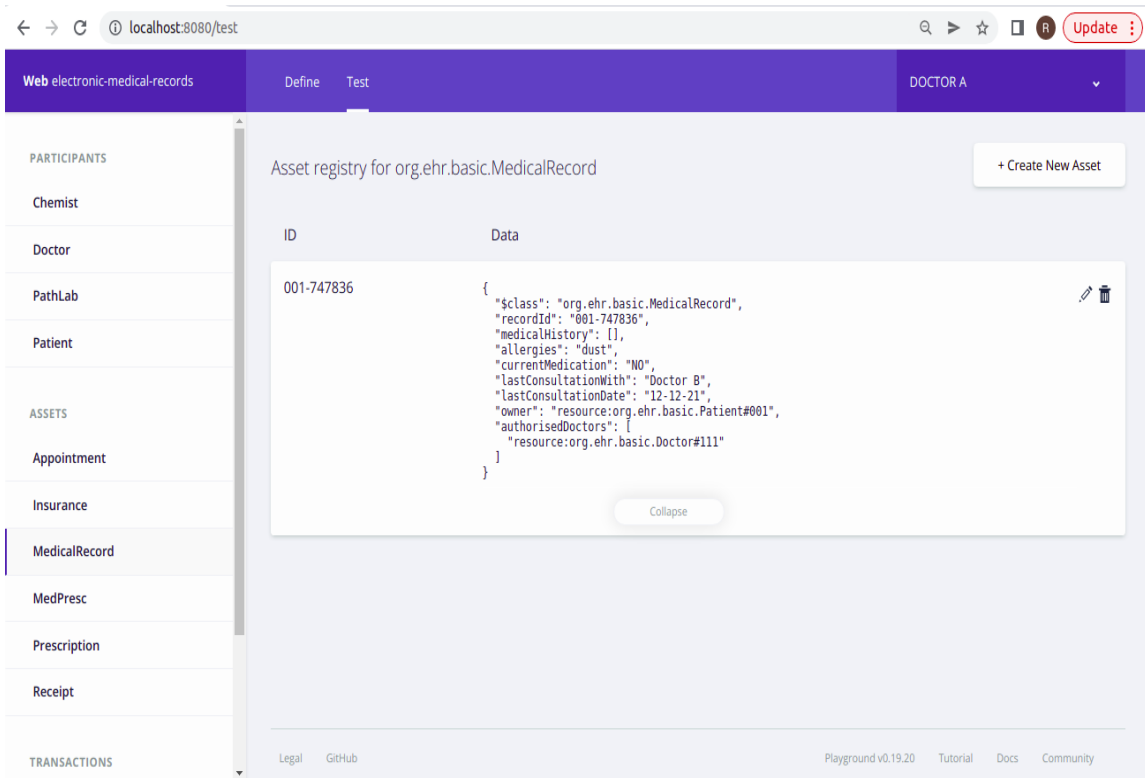


Figure 17: Doctor A has access to the Medical Record

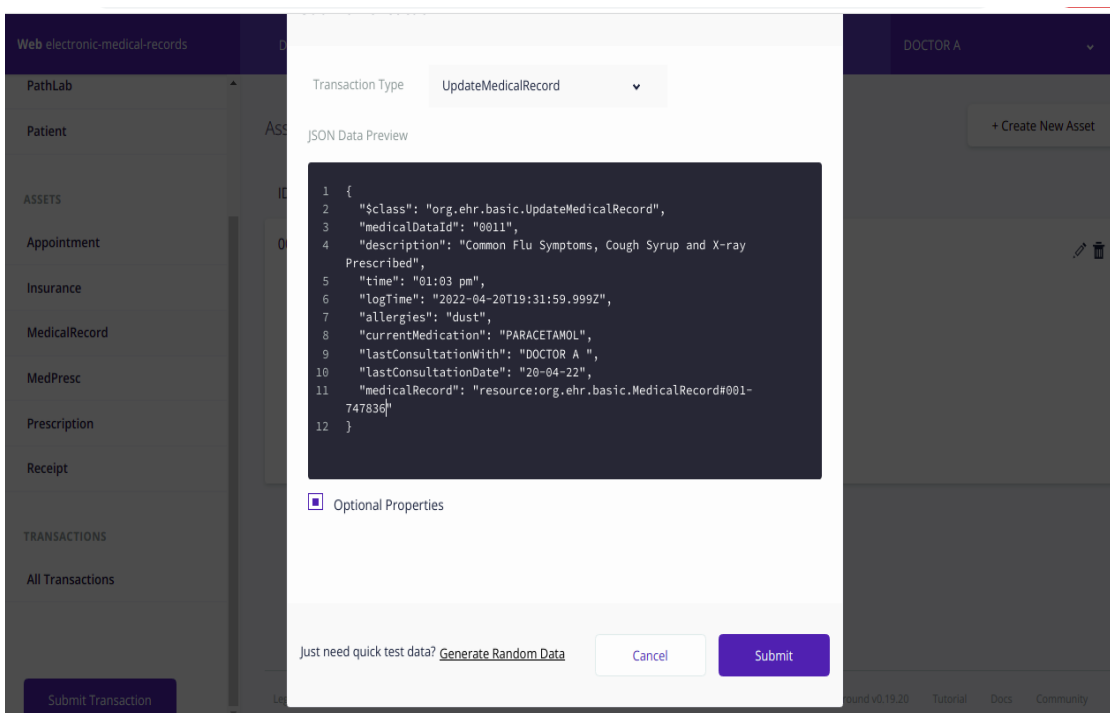


Figure 18: Doctor A can Update the Medical Record

5.3 Comparison with existing healthcare frameworks/systems

We examined current blockchain-based health systems by evaluating their methodologies for creating security rules [32-37] to give a comparative study. We also performed a benchmark research to assess our framework's and other systems' capabilities in the areas of access control, confidential information, data integrity, data security, and patient–user preference. The results of the available benchmark studies are shown in Table 4. During the investigation, we selected critical characteristics that effect system performance and discovered that our framework meets the majority of the requirements that make the system more durable and dependable. Because we built the healthcare data management framework using Hyperledger composer and the aforementioned rules, the total system overhead is reduced.

Table 4: A comparative analysis of the proposed proposed framework with existing blockchain-based frameworks

Models/ Frameworks/ Systems	Confidential Information	Data Security	Data Integrity	Patient–User Preference	Access Control
[32]	✓	✓	✓	×	×
[33]	✓	✓	✓	×	✓
[34]	×	✓	✓	×	×
[35]	×	✓	×	×	×
[36]	✓	✓	✓	×	✓
[37]	✓	✓	✓	×	×
Proposed Framework	✓	✓	✓	✓	✓

4.3 Adherence of regulations

The GDPR standards, which were set in Section 3 and tested in the Basic and Permissioned scenarios, should also be adhered to as the foundation of this activity. Patients may examine their medical data in Figure 19, and in Figure 20, they can restrict or delete data access from a Doctor/PathLab. Figure 21 shows a list of successful transactions. In the permissioned situation, patients may also choose how long the Doctor/PathLab has access to their medical records (Right to erase the records).

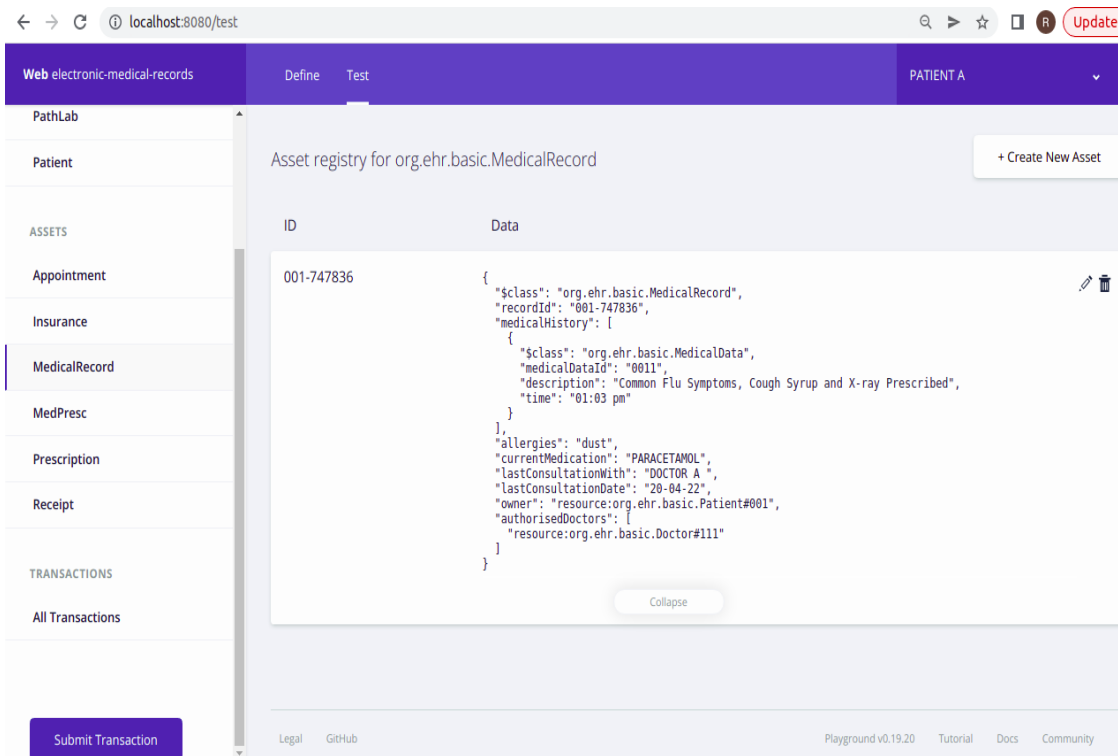


Figure 19: Patient views Medical Records

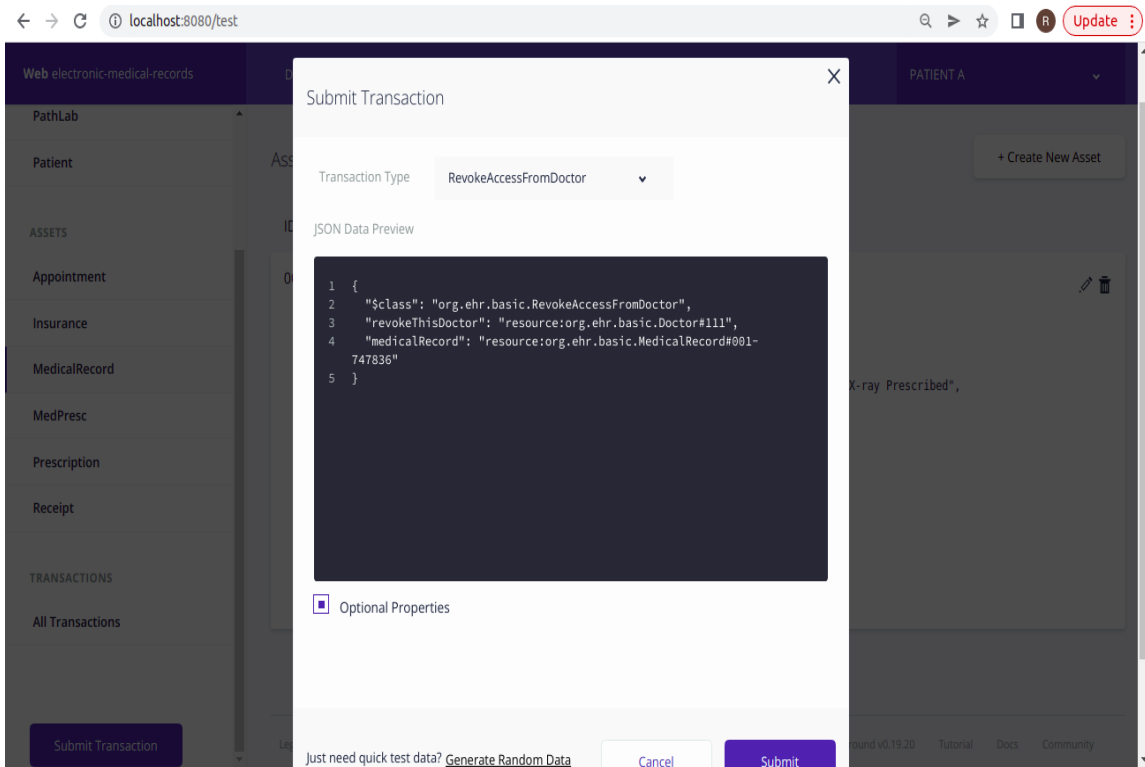


Figure 20: Patient removing Doctor ID: #111, from their Medical Record.

Date, Time	Entry Type	Participant	
2022-04-21, 01:07:01	RevokeAccessFromDoctor	001 (Patient)	view record
2022-04-21, 01:04:40	UpdateMedicalRecord	111 (Doctor)	view record
2022-04-21, 24:59:33	GrantAccessToDoctor	001 (Patient)	view record
2022-04-21, 24:52:38	CreateMedicalRecord	001 (Patient)	view record
2022-04-21, 24:47:56	ActivateCurrentIdentity	none	view record
2022-04-20, 20:06:20	ActivateCurrentIdentity	none	view record

Figure 21: Successful Transactions List.

The GDPR establishes a right to be forgotten for individuals, which Purging Data Scenario investigates. As indicated in Fig. 22, participants can remove their own data in Composer, but no other participant can delete someone's medical record, as shown in Fig. 23. HyperLedger looks to be GDPR compliant and capable of data destruction on the surface. On the other side, Composer is a higher-level toolset that operates on top of Hyperledger Fabric. Transactions are simply marked as destroyed in Composer and seem as such, while the transaction remains unchanged at the Fabric level. If Fabric is the network layer, Composer is the application layer. To comply with regulations, several blockchain application developers stated that Hyper ledger-based apps should not hold any sensitive documents and that any personal data should be kept in an off-chain database. As previously stated, patients have access control over their data, therefore deletion may be replaced by denying access to their medical record data to any other user.

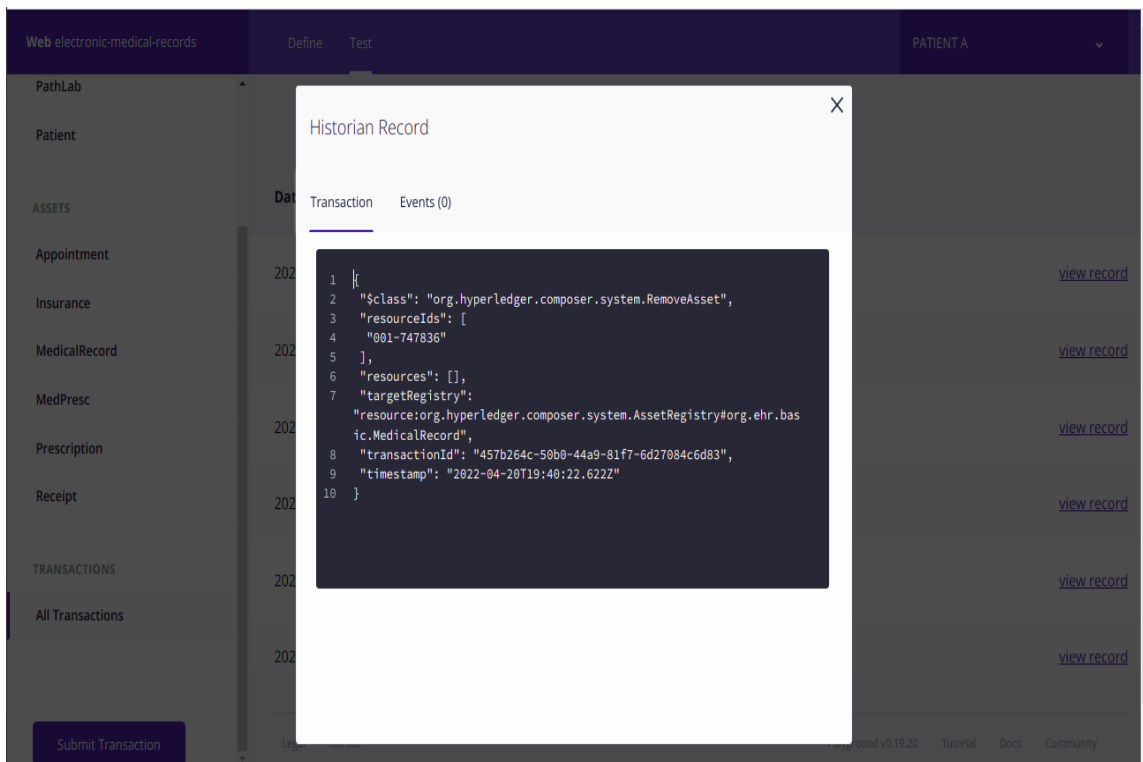


Figure 22: Patient deleting his/her Medical Record

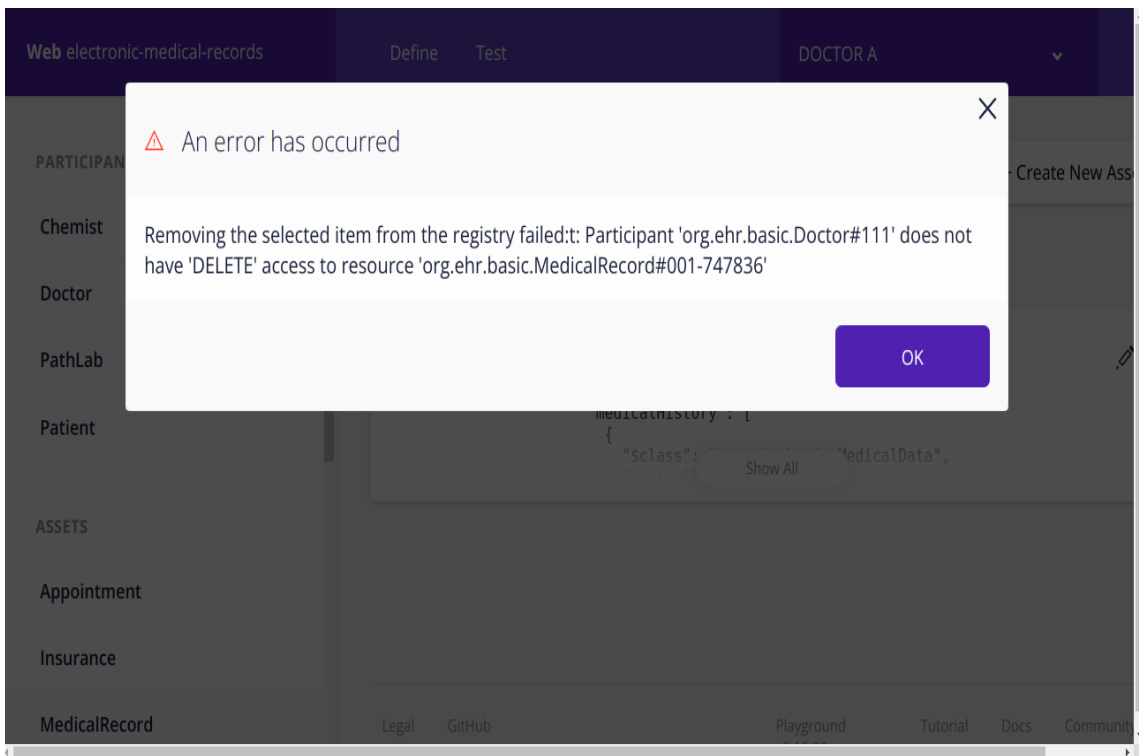


Figure 23: Doctor cannot delete patient's Medical Record

4.4 Accessibility

Under the planned system, medical records, doctor's prescriptions, and invoices should be easy to get. Patients are frequently asked to recall their past drug history from memory or to bring actual copies of their hospital records with them. Using the decentralised ledger system's simple user interface, prescribers may easily update medical histories. When patients visit other medical institutions with their consent, healthcare practitioners can rapidly access prescription histories. The decentralisation of the network eliminates the necessity to deal with a group of private central repositories.

As demonstrated in Figs. 24 and 25, a patient can request an appointment with a doctor of their choosing who is accessible on the blockchain, and the doctor has the discretion to confirm or cancel the appointment depending on availability. If Doctor A confirms Patient A's appointment, then Doctor A must generate assets such as MedPresc and Prescription, as well as give consultation to the patient, as indicated in Figures 26-29. Figure 30 depicts the scenario in which Doctor A gives consultation to Patient A, the appointment status changes to consulted, and Patient A's debt is updated. Similarly, interactions between

Chemists/PathLabs and patients are documented on the blockchain to guarantee that all players have access.

Figure 31 depicts Patient purchasing medication from a pharmacy. The chemist then generates a receipt for the patient, as indicated in fig. 32, and all of these transactions are logged and may be viewed in the historical records (Fig. 33).

Our system also keeps track of transactions done by participants and offers historical data for audits. Overall, the proposed architecture has all of the necessary functionality and security to keep patient data safe and secure in blockchain networks against unwanted access.

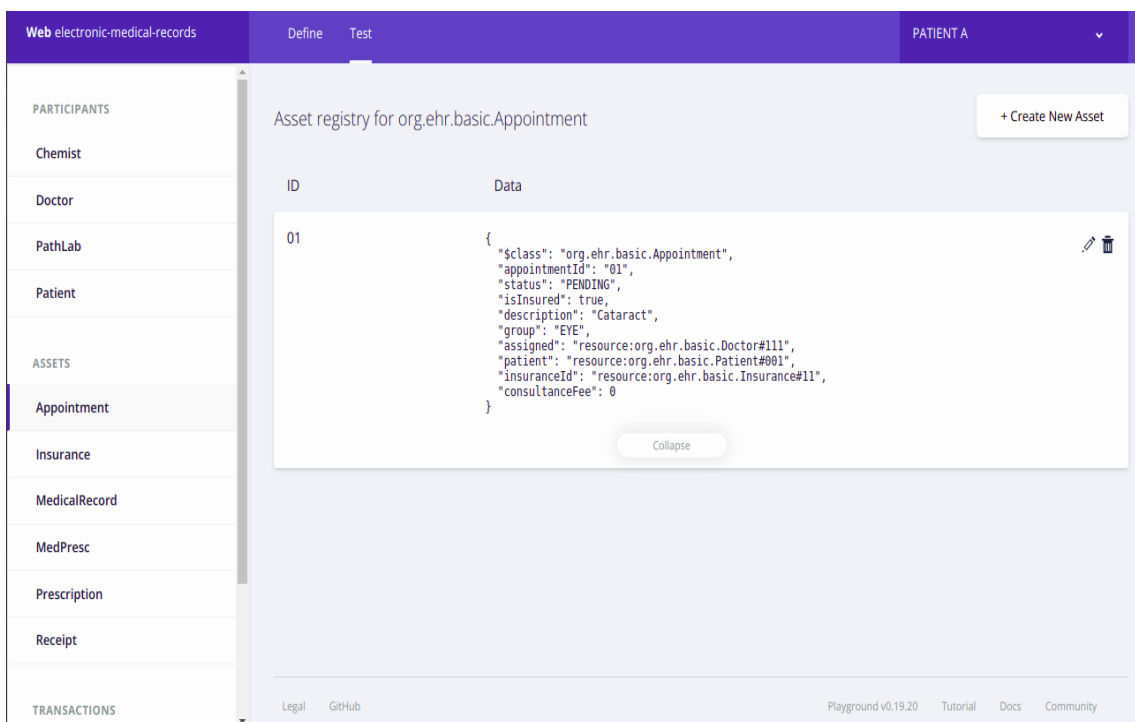


Figure 24: Patient A requests an Appointment from Doctor A.

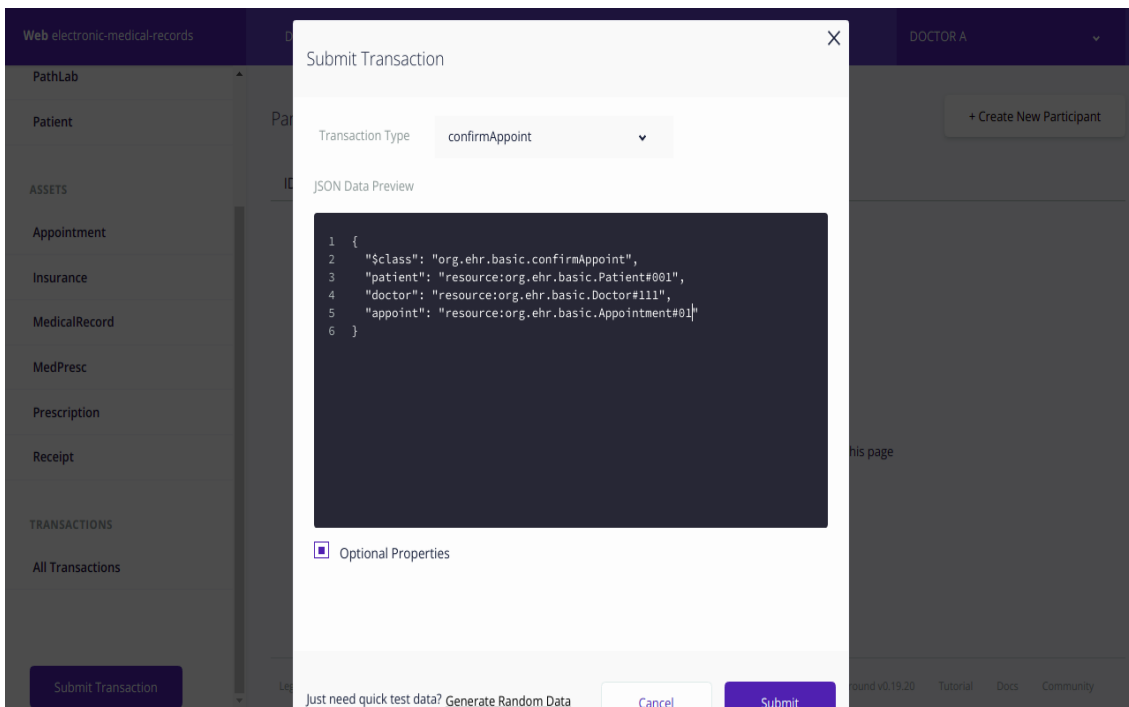


Figure 25: Doctor A confirms the Appointment.

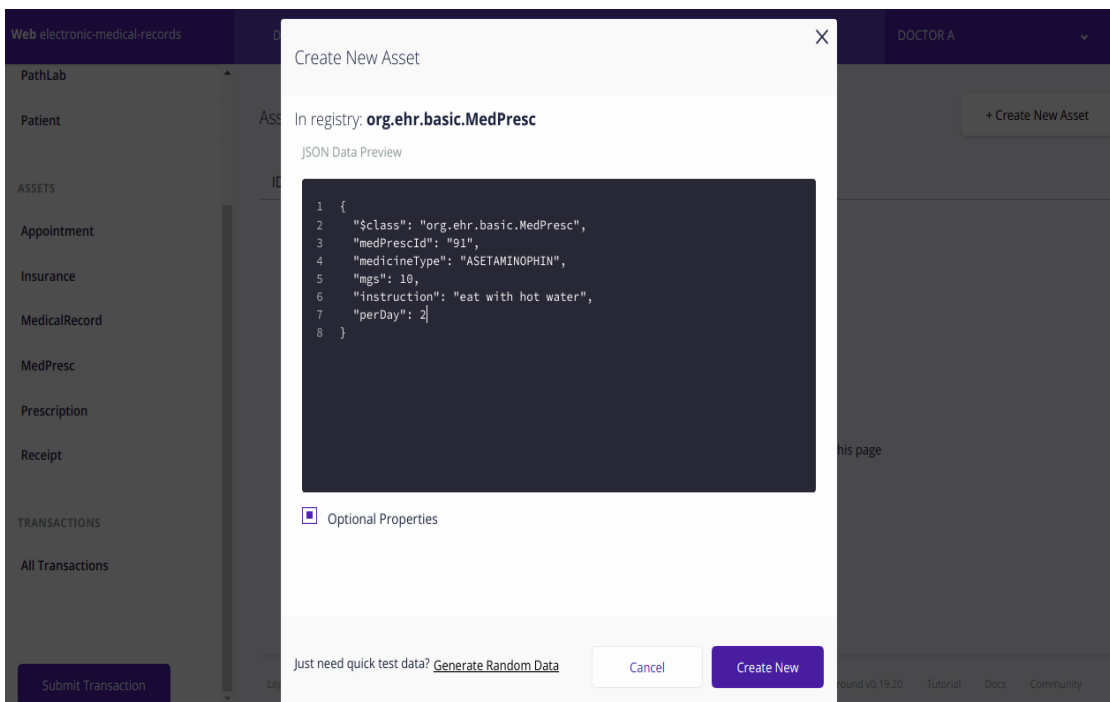


Figure 26: Doctor A creating MedPresc Asset.

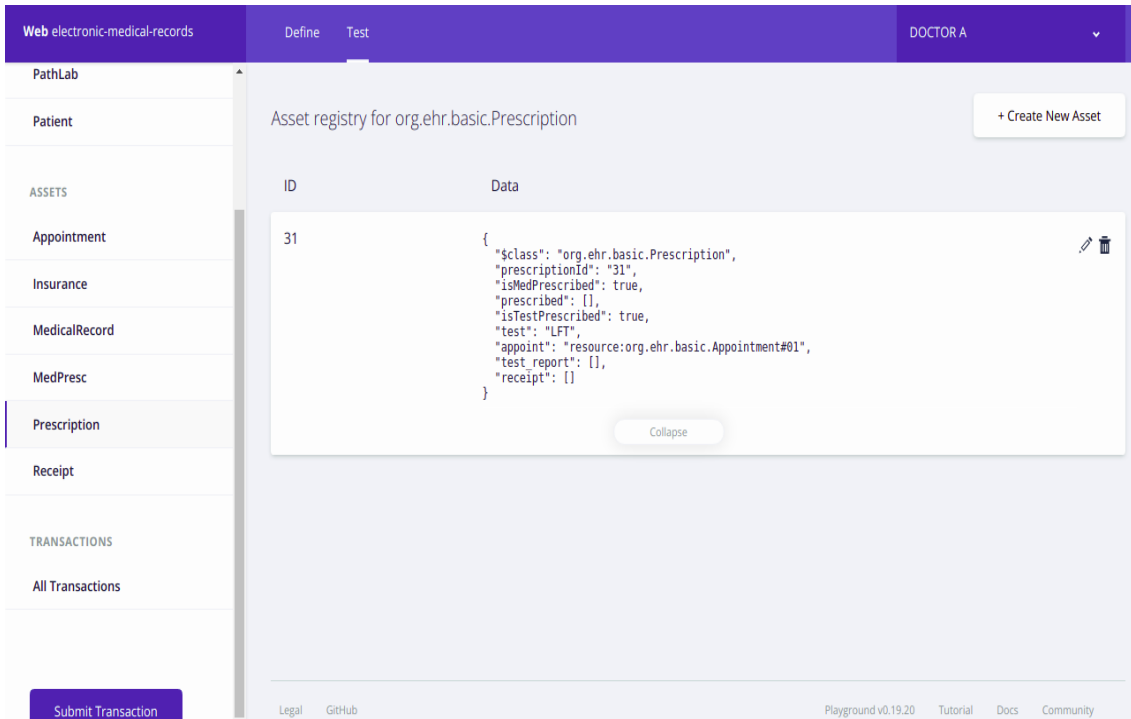


Figure 27: Doctor A creating Prescription Asset.

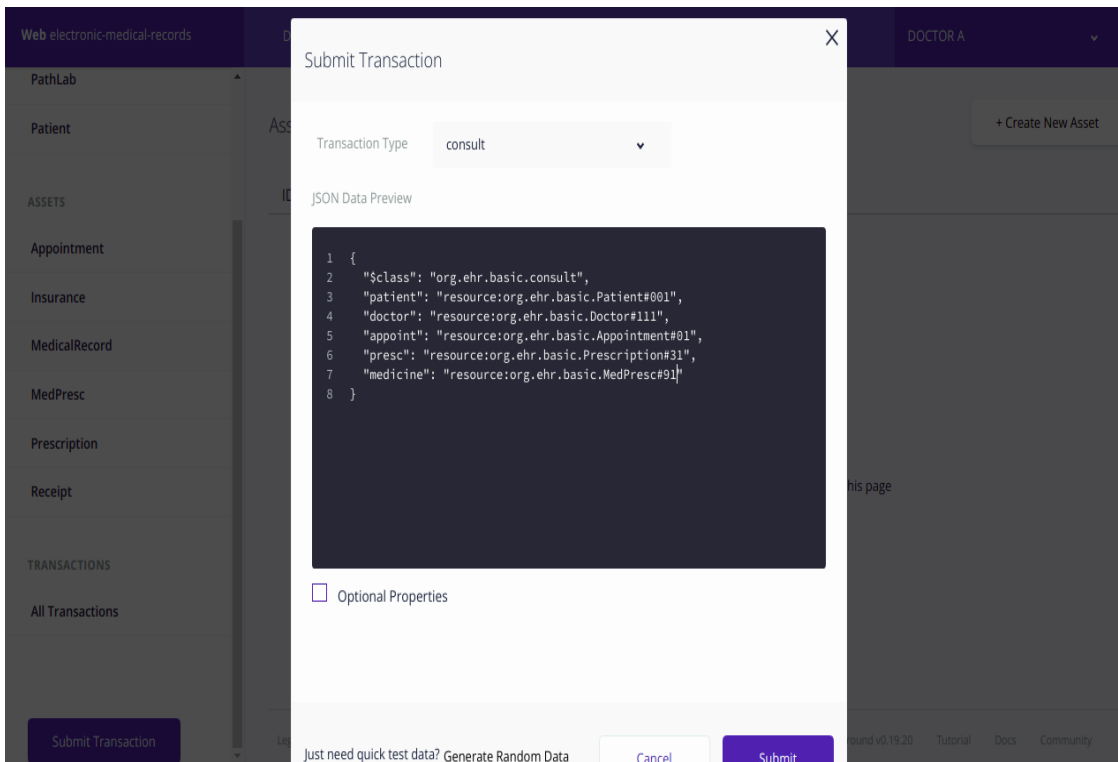


Figure 28: Doctor A providing consultation to Patient A

Define Test PATIENT A

Asset registry for org.ehr.basic.Appointment + Create New Asset

ID	Data
01	<pre>{ "\$class": "org.ehr.basic.Appointment", "appointmentId": "01", "status": "CONSULTED", "isInsured": true, "description": "Cataract", "group": "EYE", "assigned": "resource:org.ehr.basic.Doctor#111", "patient": "resource:org.ehr.basic.Patient#001", "insuranceId": "resource:org.ehr.basic.Insurance#11", "consultanceFee": 2500 }</pre>

Collapse

Figure 29: Status of Appointment changes to “Consulted”

Define Test PATIENT A

Participant registry for org.ehr.basic.Patient + Create New Participant

ID	Data
001	<pre>{ "\$class": "org.ehr.basic.Patient", "patientId": "001", "PatientName": "Patient A", "debt": 2500, "disease": "EYE", "gender": "male", "address": "Shimla, H.P.", "phoneNumber": "9091023049" }</pre>

Collapse

Figure 30: Patient A’s debt gets updated.

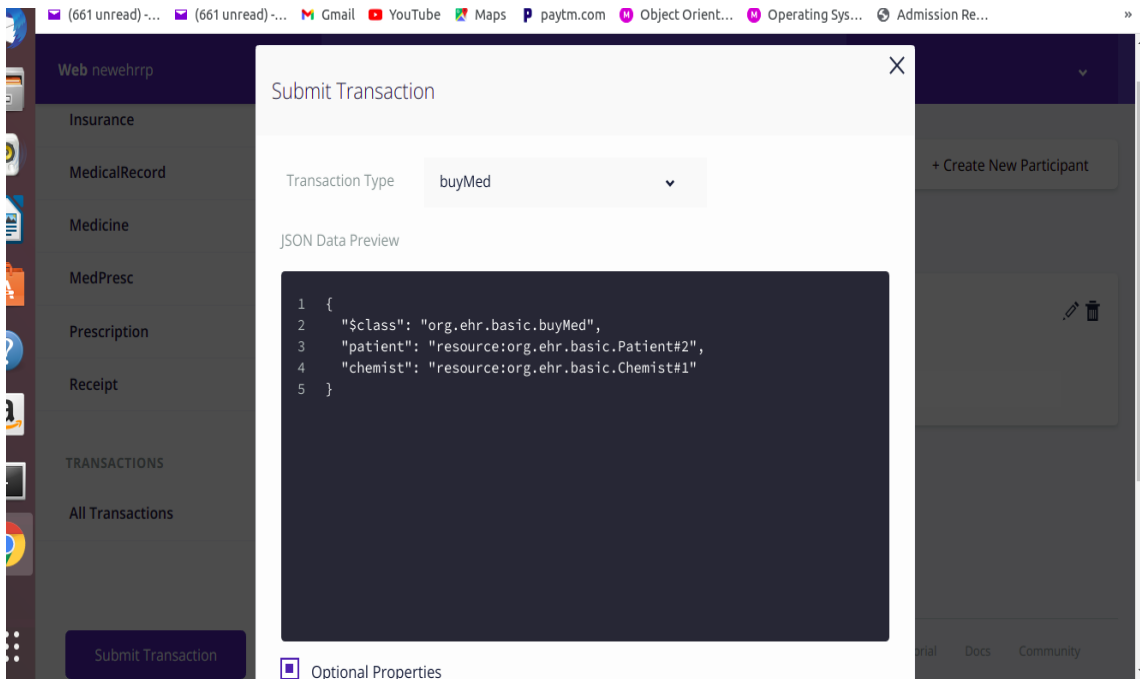


Figure 31: Patient buying medicine from chemist

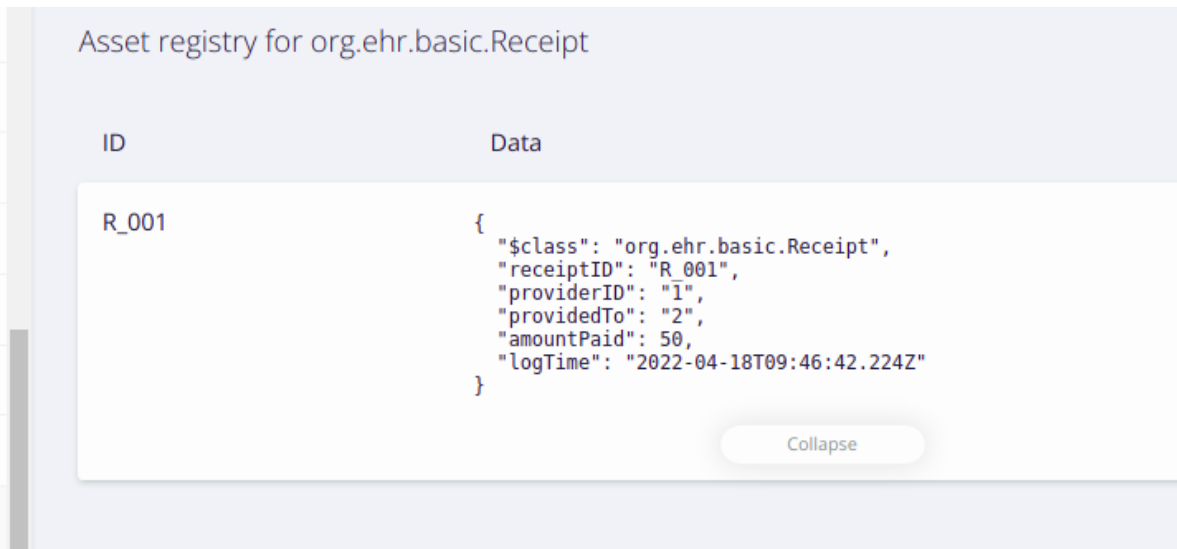


Figure 32 : Chemist generates a receipt for patient

The screenshot shows a window titled "Historian Record" with a close button (X) in the top right corner. Below the title bar, there are two tabs: "Transaction" (which is selected and underlined) and "Events (0)". The main content area displays a JSON object representing a transaction record, with line numbers 1 through 7 on the left side of the code block.

```
1  |{
2  |  "$class": "org.ehr.basic.buyMed",
3  |  "patient": "resource:org.ehr.basic.Patient#2",
4  |  "chemist": "resource:org.ehr.basic.Chemist#1",
5  |  "transactionId": "56cc0b7d-e39d-4770-9631-8db30af72e04",
6  |  "timestamp": "2022-04-18T09:46:42.224Z"
7  | }
```

Figure 33: BuyMed transaction gets recorded on Historian Record

CHAPTER 05: CONCLUSIONS

5.1 Conclusion

In this paper, we present a more secure, efficient, and accessible access control architecture for a Healthcare data management system. Using access control methods and encryption techniques, the research presents an architecture for safe data storage and efficient access management across diverse actors such as patients, doctors, chemists, and pathology labs. In a methodical approach, a permissioned blockchain architecture has been created utilising Hyperledger fabric and Hyperledger composer. Using the consortium model, we used blockchain technology to develop security regulations that give patients influence over other stakeholders' access rules in the healthcare system.

It also has the ability to provide the privacy, security, integrity, timeliness, and confidentiality of healthcare data, as well as accessibility and granular access control management.

5.2 Work for Future

The prototype is a blockchain-based healthcare data management tool that meets some basic requirements. First and foremost, we intend to make our architecture more user-friendly by combining it with a recommendation system that will rate doctors and pathology laboratories based on patient feedback. Second, when patients have completed their therapy, we would want to collect their comments and publish the facts to all stakeholders on the blockchain for efficient treatment.

We want to employ the HyperLedger Explorer tool in the future to investigate blocks, peers consensus, , and energy usage. Utilizing explorer in conjunction with a fully built blockchain will only offer more information about how blockchain may be used in the health-care business. Lastly, blockchain performance will be evaluated against a collection of healthcare-specific benchmark.

References

1. S. Argaw, N. Bempong, B. Eshaya-Chauvin, A. Flahault, The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review, in: BMC Medical Informatics and Decision Making, vol. 19, 2019.
2. Health insurance portability and accountability act of 1996, 104th Congress Public Law 104191.
3. Council of European Union, Reform of Eu Data Protection Rules, European Commission, 2018.
4. A. Le-Bris, W. El-Asri, State of Cybersecurity & Cyber Threats in Healthcare Organizations, 2017.
5. L. Adefala, Healthcare experiences twice the number of cyber attacks as other industries, Fortinet (March 2018). URL www.csoonline.com/article/3260191/healthcare-experiences-twice-the-number-of-cyber-attacks-as-other-industries.html.
6. D. Gayle, A. Topping, I. Sample, S. Marsh, V. Dodd, NHS Seeks to Recover from Global Cyber-Attack as Security Concerns Resurface, Guardian News and Media, 2017.
7. M.S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, M.H. Rehmani, Applications of blockchains in the internet of things: a comprehensive survey, IEEE Communications Surveys Tutorials 21 (2) (2019) 1676–1717.
8. F. Ahmad, Z. Ahmad, C.A. Kerrache, F. Kurugollu, A. Adnane, E. Barka, Blockchain in internet-of-things: architecture, applications and research directions, in: International Conference on Computer and Information Sciences (ICCIS), 2019, pp. 1–6.
9. S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” Tech. Rep., 2008. [Online]. Available: <http://bitcoin.org/bitcoin.pdf>.
10. Ouaddah, A. A. Elkalam, and A. A. Ouahman, “FairAccess: A new blockchain-based access control framework for the Internet of Things,” Secur. Commun. Netw., vol. 9, no. 18, pp. 5943-5964, 2016.

11. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "Towards a novel privacy-preserving access control model based on blockchain technology in IoT," in *Europe and MENA Cooperation Advances in Information and Communication Technologies*. Cham, Switzerland: Springer, 2017, pp. 523-533.
12. W. J. Gordon and C. Catalini, "Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 224-230, Jan. 2018.
13. H. Kakavand, N. Kost De Sevres, and B. Chilton, "The blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies," Jan. 2017. doi: 10.2139/ssrn.2849251.
14. M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Trans. Comput. Syst.*, vol. 20, no. 4, pp. 398-461, 2002.
15. V. Buterin, "A next-generation smart contract and decentralized application platform," White Paper, 2014. [Online]. Available: <https://ethereum.org/>
16. X. Liang, S. Shetty, J. Zhao, D. Bowden, D. Li, and J. Liu, "Towards decentralized accountability and self-sovereignty in healthcare systems," in *Proc. Int. Conf. Inf. Commun. Secur.* Cham, Switzerland: Springer, 2017, pp. 387-398.
17. P. Thakkar, S. Nathan, and B. Vishwanathan, "Performance benchmarking and optimizing hyperledger fabric blockchain platform," 2018, arXiv:1805.11390. [Online]. Available: <https://arxiv.org/abs/1805.11390>.
18. Hyperledger. (2017). *Architecture Explained Read the Docs*. [Online]. Available: <https://hyperledger-fabric.readthedocs.io/en/release-1.2/archdeep-dive.html>.
19. E. Markakis, Y. Nikoloudakis, E. Pallis, M. Manso, Security assessment as a service cross-layered system for the adoption of digital, personalised and trusted healthcare, in: *IEEE 5th World Forum on Internet of Things (WF-IoT)*, 2019, pp. 91–94.
20. V. Koufi, F. Malamateniou, G. Vassilacopoulos, Ubiquitous access to cloud emergency medical services, in: *10th IEEE International Conference on Information Technology and Applications in Biomedicine*, 2010, pp. 1–4.
21. T.D. Smith, The blockchain litmus test, in: *IEEE International Conference on Big Data (Big Data)*, 2017, pp. 2299–2308.
22. J. Cordwell, Blockchain in healthcare: from theory to reality, in: *DXC.Technology*, 2015 available online: <https://blogs.dxc.technology/2015/10/30/blockchain-in-healthcare-from-theory-to-reality/> (Accessed: 9th January, 2020).

23. N. Nchinda, A. Cameron, K. Retzepi, A. Lippman, Medrec: a network for personal information distribution, in: 2019 International Conference on Computing, Networking and Communications (ICNC), 2019, pp. 637–641.
24. S. Wu, J. Du, Electronic medical record security sharing model based on blockchain, in: Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, ICCSP '19, Association for Computing Machinery, New York, NY, USA, 2019, pp. 13–17, <https://doi.org/10.1145/3309074.3309079>.
25. P. Zhang, M.A. Walker, J. White, D.C. Schmidt, G. Lenz, Metrics for assessing blockchain-based healthcare decentralized apps, in: 2017 IEEE 19th International Conference on E-Health Networking, Applications and Services (Healthcom), 2017, pp. 1–4.
26. T.Q. Ban, B.N. Anh, N.T. Son, T. Van Dinh, Survey of hyperledger blockchain frameworks: case study in fpt university's cryptocurrency wallets, in: Proceedings of the 2019 8th International Conference on Software and Computer Applications, ICSCA '19, Association for Computing Machinery, New York, NY, USA, 2019, pp. 472–480.
27. J. Gao, H. Liu, Y. Li, C. Liu, Z. Yang, Q. Li, Z. Guan, Z. Chen, Towards automated testing of blockchain-based decentralized applications, in: Proceedings of the 27th International Conference on Program Comprehension, ICPC '19, IEEE Press, 2019, pp. 294–299, <https://doi.org/10.1109/ICPC.2019.00048>, 10.1109/ICPC.2019.00048.
28. A.E. Gencer, E.G. Sirer, Miniature world: measuring and evaluating blockchains [July 2020], <https://hackingdistributed.com/2017/02/10/miniature-world/>, 2017.
29. W. Gao, W.G. Hatcher, W. Yu, A survey of blockchain: techniques, applications, and challenges, in: 2018 27th International Conference on Computer Communication and Networks (ICCCN), 2018, pp. 1–11.
30. C. Natoli, V. Gramoli, The blockchain anomaly, in: 2016 IEEE 15th International Symposium on Network Computing and Applications, NCA), 2016, pp. 310–317.
31. K. Zile, R. Strazdina, Blockchain use cases and their feasibility, *Appl. Comput. Syst.* 23 (1) (2018) 12–20.
32. Shen, B.; Guo, J.; Yang, Y. Medchain: Efficient healthcare data sharing via blockchain. *Appl. Sci.* 2019, 9, 1207.
33. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A decentralized privacy-preserving healthcare blockchain for iot. *Sensors* 2019, 19, 326.

34. Rajput, A.; Li, Q.; Ahvanooy, M. A blockchain-based secret-data sharing framework for personal health records (2021) in emergency condition. *Healthcare* 2021, 9, 206.
35. Jagadeesh, R.; Mahantesh, K. Blockchain-based knapsack system for security and privacy preserving to medical data (2021) in *SN COMPUT. Scientifur* 2021, 2, 245.
36. Egala, B.S.; Pradhan, A.K.; Badarla, V.; Mohanty, S.P. Fortified-chain: A blockchain- based framework for security and privacy-assured internet of medical things with effective access control. *IEEE Internet Things J.* 2021, 8, 11717–11731.
37. Wang, H.; Song, Y. Secure cloud-based ehr system using attribute-based cryptosystem and blockchain. *J. Med. Syst.* 2018, 42, 152.

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

PLAGIARISM VERIFICATION REPORT

Date: 13-05-2022

Type of Document (Tick): PhD Thesis M.Tech Dissertation/ Report B.Tech Project Report Paper

Name: ROHIT SHARMA Department: CSE Enrolment No 181345

Contact No. 7018081402 E-mail. rohittsharma12@gmail.com

Name of the Supervisor: Dr. Amit Kumar

Title of the Thesis/Dissertation/Project Report/Paper (In Capital letters): ELECTRONIC HEALTH RECORDS USING BLOCKCHAIN

UNDERTAKING

I undertake that I am aware of the plagiarism related norms/ regulations, if I found guilty of any plagiarism and copyright violations in the above thesis/report even after award of degree, the University reserves the rights to withdraw/ revoke my degree/report. Kindly allow me to avail Plagiarism verification report for the document mentioned above.

Complete Thesis/Report Pages Detail:

- Total No. of Pages = 70
- Total No. of Preliminary pages = 60
- Total No. of pages accommodate bibliography/references = 4

Rohit Sharma

(Signature of Student)

FOR DEPARTMENT USE

We have checked the thesis/report as per norms and found **Similarity Index** at 16 (%). Therefore, we are forwarding the complete thesis/report for final plagiarism check. The plagiarism verification report may be handed over to the candidate.

[Signature]

(Signature of Guide/Supervisor)

Vivek Sood

Signature of HOD

FOR LRC USE

The above document was scanned for plagiarism check. The outcome of the same is reported below:

Copy Received on	Excluded	Similarity Index (%)	Generated Plagiarism Report Details (Title, Abstract & Chapters)	
	<ul style="list-style-type: none"> • All Preliminary Pages • Bibliography/Images/Quotes • 14 Words String 		Word Counts	
Report Generated on			Character Counts	
		Submission ID	Total Pages Scanned	
			File Size	

Checked by
Name & Signature

Librarian

Please send your complete thesis/report in (PDF) with Title Page, Abstract and Chapters in (Word File) through the supervisor at plagcheck.juit@gmail.com