

# Medical Applications of Blockchain

Thesis/Report submitted in partial fulfillment of the requirements for the degree of

## Bachelor of Technology in Computer Science Engineering

by

**Swapnil Kole**

(Roll No.: B118060)

under the guidance of

**Dr. Suraj Sharma**



Department of your branch  
International Institute of Information Technology Bhubaneswar  
Bhubaneswar, Odisha, 751003, India  
May 2022

# Medical Applications of Blockchain

Thesis/Report submitted in partial fulfillment of the requirements for the degree of

Bachelor of Technology

in

Computer Science Engineering

by

Swapnil Kole

(Roll No.: B118060)

under the guidance of

Dr. Suraj Sharma



Department of your branch  
International Institute of Information Technology Bhubaneswar  
Bhubaneswar, Odisha, 751003, India  
May, 2022

With the blessings of almighty. To my  
beloved parents, family members, and my  
mother



Computer Science Engineering  
International Institute of Information Technology, Bhubaneswar  
Bhubaneswar-751003, Odisha, India.

## Supervisor's Certificate

This is to certify that the work in the thesis/report entitled “Medical Applications of Blockchain” by Swapnil Kole, bearing roll number B118060, is a record of an original research work/work carried out by him under my supervision and guidance in partial fulfillment of the requirements for the award of the degree of Bachelor of Technology in Computer Science Engineering. Neither this thesis/report nor any part of it has been submitted for any degree or academic award elsewhere.

Date: May 2022

Place: Bhubaneswar

Dr. Suraj Sharma  
Asst. Professor  
Department of Computer Science  
International Institute of Information Technology  
Bhubaneswar, Odisha, India



Department of Computer Science Engineering  
International Institute of Information Technology Bhubaneswar  
Bhubaneswar-751003, Odisha, India.

## Certificate of Examination

Roll: B118060

Name: Swapnil Kole

Title of Thesis/Report: Medical Applications of Blockchain

We the below signed, after checking the thesis/report mentioned above and the official record book (s) of the student, hereby state our approval of the thesis/report submitted in partial fulfillment of the requirements of the degree of Bachelor of Technology in Computer Science Engineering at International Institute of Information Technology, Bhubaneswar. We are satisfied with the volume, quality, correctness, and originality of the work.

Dr. Suraj Sharma  
Supervisor

---

Dr. Rakesh Chandra Balabantaray  
Dean Academics



Department of BRANCH  
International Institute of Information Technology Bhubaneswar  
Bhubaneswar-751003, Odisha, India.

## Declaration of Originality

I, SWAPNIL KOLE, bearing roll number B118060, hereby declare that this thesis/report entitled "MEDICAL APPLICATIONS OF BLOCKCHAIN", presents my original work carried out as a bachelor student of International Institute of Information Technology, Bhubaneswar, and to the best of my knowledge, contains no material previously published or written by another person, nor any material presented by me for the award of any degree or diploma of International Institute of Information Technology, Bhubaneswar or any other institution. Any contribution made to this work by others, with whom I have worked at International Institute of Information Technology, Bhubaneswar or elsewhere, is explicitly acknowledged in the thesis/report. Works of other authors cited in this dissertation have been duly acknowledged under the sections "Reference" or "Bibliography". I have also submitted my original research records to the scrutiny committee for evaluation of my thesis/report.

I am fully aware that in case of any non-compliance detected in future, the Senate of International Institute of Information Technology, Bhubaneswar may withdraw the degree awarded to me on the basis of the present dissertation.

Date: May 2022

Place: Bhubaneswar

Swapnil Kole

Roll: B118060

Department of Computer Science Engineering  
International Institute of Information Technology  
Bhubaneswar, Odisha, India

# Acknowledgement

I take the opportunity to express my gratitude to all who have directly or indirectly made this thesis possible. This dissertation, though an individual work, has benefited in various ways from several people. Whilst it would be simple to name them all, it would not be easy to thank them enough.

A handwritten signature in black ink, appearing to read 'Skole', is written over a horizontal line.

Swapnil Kole

# Abstract

---

With the dramatic increase in the Internet of Things (IoT), remote monitoring of health data and automation of health data to achieve intelligent healthcare solutions has received great attention recently. Due to the limited computing power and storage capacity of IoT devices, users' health data are generally stored in centralized third-party applications, such as the hospital database or cloud databases, and make users lose control of their health data, which can easily result in privacy leakage and single-point bottleneck of getting the data erased, mutated or deleted. In this paper, I propose Doctel, a large-scale health data application based on blockchain technology, where health data are stored with different levels of access controls and privacy policies to give the best benefits. Specifically, admins can effectively revoke or add authorized doctors. Furthermore, by introducing docTel, both IoT data and doctor diagnosis cannot be deleted or tampered with so as to avoid medical disputes and having no change in the history of medical treatments. Theoretical analysis and experimental results show that the proposed Doctel is applicable for smart healthcare systems. This system is ready to be highly scalable and can be massively adopted and what is proposed in this paper is just a prototype of the same.

Keywords: Internet of Things(IOT), cloud database, access control, Blockchain



# Contents

Certificate	4
Certificate Of Examination	5
Declaration of Originality	6
Acknowledgement	7
Abstract	8
List of Figures	11
1 Introduction	12
1.1 Project Motivation. . . . .	14
1.2 Project Objective .. . . .	14
2 Literature Review	15
3 Blockchain Technology and its application areas	28
3.1 Background . . . . .	29
3.2 Technical Background of Blockchain. . . . .	31
3.2.1 Cryptographic Hash Function	
3.2.2 Markle Tree	
3.2.3 Smart Contract	
3.3 Blockchain Architecture . . . . .	32
3.4 Types of Blockchain . . . . .	34
3.5 Application areas . . . . .	35
3.5.1 Supply Chain	
3.5.2 Internet of Things	
3.5.3 Real Estate	
3.5.4 Financial System	
3.5.5 Healthcare System	
4 Healthcare and use cases of Blockchain in Healthcare	39
4.1 Introduction . . . . .	

5	Proposed Work	43
6	Implementation	48
6.1	Technology Implemented. . . . .	
7	Result Discussion, Conclusion & Future Work	66
8	Bibliography/ References	

# List of Acronyms

IT	Information Technology
IoT	Internet of Things
IPFS	InterPlanetary File System
PBFT	Practical byzantine fault tolerance
EHR	Electronic Health Record
EMR	Electronics Medical Record
PHR	Personal Health Record
RPM	Remote Patient Monitoring
PoW	Proof of Work
PoS	Proof of Stake
API	Application Programming Interface

# List of Figures

1. Graphical representation of Differences between centralized, decentralized, and distributed systems
2. Avalanche effect of one way hash functions
3. Basic Structure of blocks in blockchain
4. Proposed blockchain architecture
5. Storing strategy in IPFS via Merkle-DAG
6. Ethereum Dapp instance
7. Screenshot of Homepage
8. Screenshot of Admin Registration Page
9. Details of All Members page
10. Screenshot of Patient Registration page
11. Screenshot of Patient Details page
12. Add Treatment & Reports page
13. Treatment Details page
14. Treatment History page
15. Ganache Application
16. Terminal Page
17. Github Repository
18. Amazon AWS Amplify
19. CI/CD pipeline build

# Chapter 1

---

## Introduction

An Overview of Health Application on Blockchain  
Motivation and Objectives Thesis Organization

# Chapter 1

## Introduction

Blockchain is defined as a ledger system that aids in the management and storage of data in time-stamped blocks that operate mostly decentralized across any computing networks and are linked via encryption. Bitcoin [Nakamoto, 2009], the first electronic payment system to properly exploit the power of blockchain technology, was introduced in the fintech business. Since then, blockchain technology has permeated several industries of information technology (IT). Blockchain technology has the potential to transform several industries, including finance, governance, health care, and supply chain. Its anticipated benefits include lower transaction costs and complexity, more security, greater transparency, and regulation.

Healthcare is considered as one of the blockchain technology's application areas. However, technological adoption in the healthcare industry is slow. Healthcare is characterized as a conventional sector that is difficult to measure due to changing facts and resistant to innovation techniques. Healthcare issues (such as privacy, quality of care, and information security) have received a lot of attention in recent years. Care coordination between patient and health care provider is becoming more difficult as the prevalence of chronic diseases in an aging and rising population rises. In many cases, the technology available in health care is insufficient to record all types of service provided. This is mostly due to the usage of outdated technologies to convey information between parties. To collect and exchange medical data, health care practitioners continue to rely on outdated systems and paper-based medical records.

Health care providers continue to invest significant resources in processing medical claims and administrative data, despite the fact that most of this may be eliminated utilising technology such as BlockChain. Blockchain technology is rapidly being recognised as a means for addressing existing challenges with information distribution.

In this paper, We propose DocTel, an health data application based on blockchain technology, where health data are stored with different levels of access controls and privacy policies to give the best benefits. In DocTel admins (hospital management) or IoT devices can regularly update the users' health data. Doctors and AI health analyzers can anywhere and anytime diagnose these data and this data will build up all the historical data of that particular user and will be connected by a unique identification number (Aadhar no.).

## 1.1 Project Motivation

1. Some medical records are lost, mutated & tampered
2. Some hospitals show wrong results and charge a lot of money to treat it.
3. Health records are not connected to a unique identification no. across the whole country and each hospital is maintaining a different set of records that needs to be unified.
4. The history of a patients' data when trying to retrieve at a later stage takes a lot of time and not everything shows up.

## 1.2 Project Objective

1. Medical records cannot be mutated, deleted, or tampered with anymore as the database is getting decentralized with the help of blockchain technology.
2. Nobody at a later stage can show different results as once written on blockchain nothing can be changed.
3. Each health record is connected to a user's unique identification number or Aadhar no. and we can get a unified & decentralized database all across the country.
4. Easily all the health records of a patient can be retrieved by searching by his aadhar no.

# Chapter 2

---

## Literature Review

Summary of a few papers in the  
same domain



# Chapter 2

## Literature review

- This study[2] offers i-Blockchain, which employs a blockchain which is permissioned to enhance the individual's data sharing experience and protect the privacy of patient health data by using different levels of access control. To prevent malicious activities, it only permits qualified users and Service Providers [Healthcare] to join the network. In addition to a public key and a private key for safe exchange of data, it employs hot storage functions as storage where temporarily users store data that is requested and off-chain storage in the form of off-chain storage.
- Nguyen et al.[3] proposed an Electronic Health Records sharing scheme based on a mobo-cloud platform. They created an access control system for doctors, patients, and healthcare providers which is way far reliable & efficient. They had protected the patient's sensitive information from malicious activities. They have used the Ethereum mainnet blockchain to share real-time data on a mobile application.
- Kai Fan et al.[4] proposed MedBlock, a blockchain-based information management solution, to handle patients' information. MedBlock's distributed ledger allows for quicker Electronic Medical Records access and retrieval in their proposed architecture. Their proposed MedBlock provides a high level of information security

because of the combination of their strategic symmetric encryption and access control methods. Their method avoids the disclosure of the patients' identity information, which has the same effect as the ring signature. They improved the efficiency of information retrieval by using bread crumbs on the ledger. They developed a reliable and effective hybrid consensus technique to reduce unnecessary energy use and power centralization.

- Aujla and Jindal proposed[5] a lightweight private blockchain-based method for healthcare data protection (Privacy of Health Records). It was proposed to use end devices to securely share health data with cloud servers. For the prevention of data redundancy, a "tensor train decomposition model" was provided for storing health data on cloud servers. Blockchain technology was employed for data security as well as to protect the healthcare data privacy. Registration, block generation, validation, data generation, and updates on block were some of the steps in their proposal. The proposed scheme used some Layer 2 solution for optimality ie. zero-knowledge proof (ZKP) protocol to confirm the authenticity of two persons without revealing any confidential information.
- Researchers[6] presented a blockchain-based infrastructure in the healthcare system for remote patients. Every patient has wearable devices (sensors in their watches like heart rate monitor) that obtain health data at regular intervals as specified in their architecture. The blockchain stores the information after it has been pre-processed by the system. A miner mechanism is employed for the generation of blocks. The miner technique is not the same as the miner concept in bitcoin. In the proposed system, only one miner works to generate the hash value of the current block. In the bitcoin system, multiple

miners work together to generate current block's hash value. However, The patient agent chooses an appropriate miner based on a set of criteria (eg, reliability and previous experience of miners). For the sharing of health information across health practitioners, the suggested approach used a patient-centric model.

- Adarsh Kumar[7] et al. has designed a smart healthcare system using Ethereum blockchain framework and healthcare 4.0 processes. In their smart healthcare system, they used an Ethereum virtual machine to run their contracts, meta-mask as a wallet (gateway to the blockchain and do transactions), remix as IDE (to write and test smart contracts), Geth (command-line interface) as Go-Ethereum, Ganache for account creation and running a local blockchain and Athena as a web interface to analyze the performance of the system. To validate the data accessibility they used statistical simulation optimization methods and algorithms. Their proposed smart healthcare system's advantages are that the system can protect from central authorities approach and rather applies a decentralized approach system, data security, and data management.
- The researchers[8] offered a conceptual approach for sharing personal continuous ever-changing health-related info using blockchain. They used Ethereum as a development framework for their system. Cloud storage is used in conjunction with this method to get scalability. The authors recommended employing hashmaps to the location in the storage to tackle the challenge of sharing dynamic, continuously changing, large-sized data while merging blockchain and cloud storage as they came up that hashmaps are the most optimal data structure to accomplish this task. Large quantity of data

may be kept on cloud in an encrypted format, but only metadata and transaction's data can be preserved and shared on the blockchain as the data is on the cloud and the retrieval link is put in the blockchain.

- Chattu et al. [9] discussed disease surveillance system using blockchain technology. They discussed about how blockchain can be used in advance identification of threats and sending reports to healthcare organizations so that preventive measures can be taken. They used ML algorithms to create a disease surveillance system.
- The researchers [10] employed data masking technology to preserve a patient's privacy by transforming and disguising sensitive data into virtual data using masking algos that specialized algorithms. They also employed the InterPlanetary File System to create a secure Electronic Medical Record system, as IPFS connects all nodes to the same file system and prevents file manipulation and duplication. It is important that IPFS not only stores files in several formats, but it also returns the hash of the persistent file. Following hash value and data concealing, the user (a patient or a doctor) distributes medical record data on the blockchain network for storage. This concept addresses the problem of data readily being changed and disappearing throughout the medical record exchange process.
- In this proposal [11], researchers suggested a blockchain framework system named BiiMED. Ethereum blockchain is getting used as a framework. Its usage is to maintain and verify data that is shared between medical service providers who store health data in the cloud and exchange patients' Electronic Health Records. This method introduced the Trusted Third Party Auditor, which is based on

blockchain technology and handles validating of the transferred data. While exchanging EHR, the proposed approach maintains data interoperability and integrity. To identify and authenticate users, the proposed system employs an access management module. As a result, secrecy is ensured. Furthermore, based on scalability analysis, the suggested system supports an enormous population of patients.

- The researchers [12] of this study developed a decentralized storage system by merging Ethereum blockchain, Inter-Planetary File System, and attribute-based encryption technologies to improve data privacy and availability on clouds. To provide fine-grained access control on cloud data, a data owner distributes a secret key to users and encrypts his data using a predetermined access policy. The smart contracts are meant to provide keyword search in de-centralized storage systems, which solves the issue of conventional cloud storage not delivering accurate search results.
- Omar et al. [13] presented a patient-centric data management system for healthcare. A Private Accessible Unit (PAU) is used in this system for safe interaction between users. After registering on the system, users receive a unique Identification (ID), which they may use to securely retrieve data stored on the blockchain.
- The authors [14] mentioned that healthcare data is an important and valuable asset and that there is an urgent need to efficiently preserve it using safe methods. Due to data in healthcare being fragmented the researchers faced a lot of difficulties. As a result, this must be resolved. They believed that by combining blockchain technology and the cloud environment, they might solve the problem to some

extent. They presented a blockchain-based network for storing and managing massive amounts of healthcare data with security, accuracy, and convenience. At the moment, all data related to healthcare is kept on centralized systems. The researchers presented a design that ensures decentralization. This places the data in a dispersed context, which improves interoperability. The data are fragmented in this system, and every transaction is kept on multiple nodes. The proposed architecture uses cryptographic methods to verify the user's identity after a user requests a transaction. The system adds a new block to the current blockchain regarding the transaction when the user has been validated by the system.

- The authors [15] of this research suggested Med-Chain, a blockchain-based session-based healthcare data exchange system. The proposed system allows patients' Electronic Health Records as well as physiological information obtained from the internet of medical things (IoMT) devices linked to their bodies to be managed and shared. Although MedChain ensures data integrity and confidentiality, it has significant limits in terms of availability and scalability. The availability of the sharing service is dependent on the patient's availability to execute these acts due to manually sharing data and uploading data manually to blockchain which can become a disadvantage.
- Garg et al. [16] suggested a model called BAKMP-IoMT an authentication key agreement protocol that uses the Elliptic curve encryption algorithm, signatures, and blockchain to safeguard transmitted data and enable anonymity in an unsecured channel. In

their proposed model the cloud servers keep track of the entire healthcare data on a blockchain. To authenticate between the communicating nodes, they included the identity of the trusted authority as an extra security parameter. The model uses Automated Validation of Internet Security Protocols and Applications (AVISPA) tool for security verification against the different types of possible malicious attacks.

- The authors [17] proposed a IoT-based blockchain framework for safe remote monitoring of patients' vital signs. Hyperledger fabric was used to create the permissioned blockchain framework in the proposed design. The Hyperledger composer is used to define and deploy a smart contract that controls access to the ledger. The suggested approach addresses security problems related to availability, traceability, integrity, confidentiality, and data privacy due to the intrinsic properties of Fabric Blockchain. However, scalability is not met since this system keeps the vital signs of the patients generated by the Internet of Medical Things (IoMT) devices in the blockchain nodes, which needs large storage capacity on the nodes.
- Griggs et al. [18] used a private blockchain based on Ethereum protocol to not only promote secure and safe usage of medical sensors but also to remove security concerns associated with a remote patient monitoring system. For patient data validation, they employ a practical byzantine fault tolerance consensus (PBFT) mechanism.
- Zaabar et al.[19] proposed HealthBlock, a system that provides a secure healthcare management system that involves Remote Patient

Monitoring (RPM) and Electronic Health Record (EHR) sharing and is built on an architecture that combines both IoT and blockchain technologies. Patients may use the HealthBlock system to safely handle their healthcare data on their own. They implemented Practical Byzantine Fault Tolerance (PBFT) in their proposed permissioned blockchain architecture which improves system efficiency while lowering mining costs [6].

- The researchers [20] of this research proposed a Smart Medical System (SMS), a framework which conceptually allows privacy-protected data gathering, storage, and processing for a smart health care system. They employed blockchain to secure medical and personal data against scams that are constantly created by IoT devices and sensors. They used blockchain technology to connect different healthcare groups in order to simplify the sharing of personal health data. The suggested architecture provides patient's health state's real-time monitoring and alerts doctors and healthcare professionals of the patient's condition.
- Madine et.al. [21] described a method for giving patients control over their medical information in their paper. They presented two Ethereum smart contracts with security, transparency, immutability, and traceability as prime features. Their main goal was to maintain decentralized access and control over patients' medical data when they interacted with various entities. For their suggested approach, they have seven categories of entities: hospital, doctor, patient, insurance, trusted re-encryption oracles, regulatory agency, and decentralized database storage. They deployed IPFS for decentralized



storage and oracles to execute operations on medical records of patients.

- Using the blockchain's immutability and built-in autonomous characteristics, Xia et al. [22] suggested a data sharing architecture based on blockchain that adequately solves the access control issues associated with sensitive data kept on cloud. Authors used secured cryptographic methods to enable effective access control to sensitive shared data pool(s) using a permissioned blockchain, and they developed a blockchain-based data sharing mechanism that enables data users/owners to retrieve electronic medical data from a repository that is shared after the user identities and cryptographic keys were verified.

# Chapter 3

---

Blockchain Technology and its application areas

Technology Background  
Technical Background  
Blockchain Architecture  
Types of Blockchain  
Application Areas

# Chapter 3

## Blockchain technology and its application areas

This chapter provides an overview of blockchain, a distributed ledger system. There is discussion of both technical and non-technical aspects.

### 3.1 Background

Blockchain is a transaction processing network with a set of rules (a "protocol") that participants may follow to access a shared transaction log. The implementation of this system in a centralized way would be fraught with difficulty. In 1962 Paul Baran broadly discussed and highlighted the necessity and purpose of decentralised and distributed systems over centralised systems in his paper.(Baran, 1962). The network types are conceptually depicted on the following figure 1:

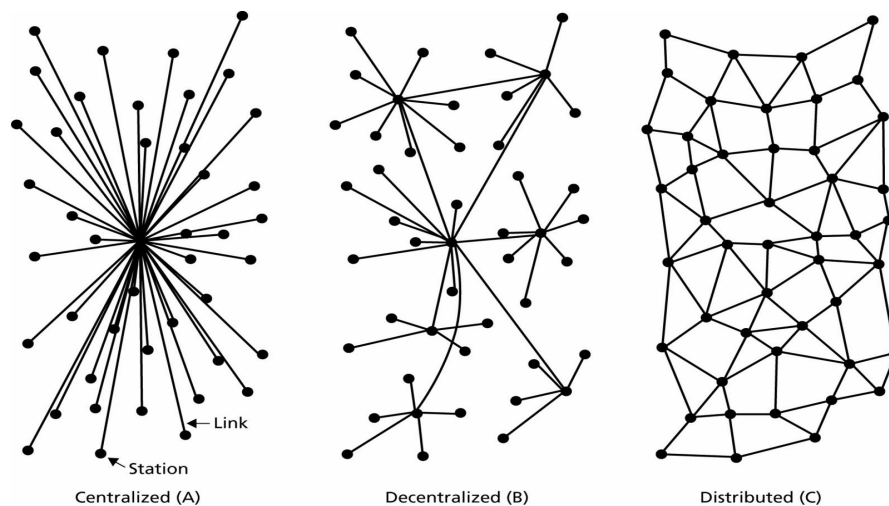


Fig 1 : Graphical representation of Differences between centralised, decentralised, and distributed systems [Baran, 1964]

'Centralized systems,' are the systems which are controlled by a single authority. These systems are simple to manage, develop, and manage, yet they have numerous problems.

The biggest drawback of this centralized system is that it has a single point of failure. This type of technology is less trustworthy in terms of security because if the central node of the system becomes corrupt then all message exchange between other nodes is also affected. Hence, centralized systems are less reliable.

On the other hand , decentralized systems have numerous central coordinators rather than a single central node. This means that no single point makes all the decisions. These nodes interact with one another, and non-coordinators communicate through the coordinators. By introducing this concept a single point of failure is eliminated. In the event that one of the coordinating nodes fails, message communication can continue via other accessible coordinating nodes. In this design, multiple failures can be borne until the network is disconnected.

“A distributed system is a group of autonomous entities that work together to solve an issue that cannot be handled separately ” [Kshemkaya, Singhal, 2011]. In distributed systems, the idea of a centralised coordinator is eliminated, and all nodes collaborate on computation and information sharing. A distributed computer system is one in which the participating nodes share a common physical clock, because they do not share memory. These systems are geographically dispersed, autonomous and heterogeneous.

A blockchain application system can be decentralised or distributed.

The basic concept of blockchain: using cryptographically secure hash function to store information in the form of a block is not a new one. The concept of timestamping a digital document using a series of timestamps that represents the time a document was created or edited was discussed as early as 1991. The authors discussed how the history of a document can be maintained in chains of blocks via hash function using parameters such as sequence number, client ID, timestamp and hash value from the previous block.

## 3.2 Technical Background of Blockchain

To know how blockchain technology works, it is crucial to first know the system's fundamental components and concepts. Three principles that stimulate blockchain are briefly discussed in the below subsections.

### 3.2.1 Cryptographic Hash Functions

Cryptographic hash functions is an algorithm and also a fundamental building block concept that operates information validity and consistency in the blockchain. This hash function takes an arbitrary amount of data input and converts it to a fixed length of output. It produces a unique output. In the blockchain system one way hash functions are used. Let consider the following equation

$$y = F(x)$$

where 'x' is a string of arbitrary data, 'F()' is a one-way hash function, 'y' as result. Given string value 'x' and 'F(x),' one-way hash functions ensure that the value 'y' can be derived. Therefore, no consistent algorithm will be able to evaluate 'x' given 'y' and 'F(x)' [Merkle, 1979]. In figure 2 it shows how a single change in character can change the whole digest. Another important feature of cryptographic hash functions is that they produce an avalanche effect. This effect is defined as "a change in one input bit impacts many output bits and the feature known as diffusion or the avalanche effect." [Paar and Pelzl, 2010, pg. 83]

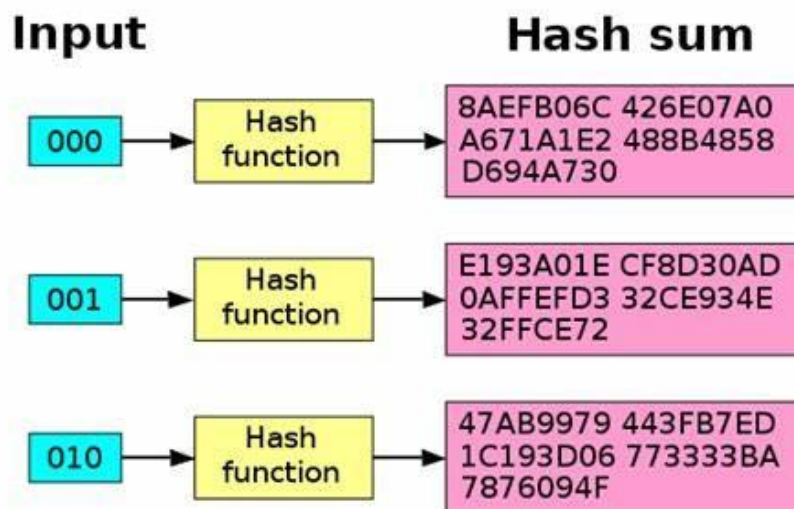


Fig 2: Avalanche effect of one way hash functions

### 3.2.2 Markle Tree

Merkle trees are the backbone of blockchain technology and it plays an important role in verifying the integrity of transactions stored in blockchain system's . It is widely used in theoretical cryptographic constructions and is specifically designed so that a leaf value can be verified with a publicly known root value. Merkle tree is a tree structure in which the document hash is stored in the leaf node and the non-leaf node carries the aggregate hash of the child nodes. The integrity of the documents in the child nodes may be verified using this tree structure. Any modification to one of the leaf nodes affects the root value. As a result, it is simple to verify that none of the leaf nodes (documents) have been altered with using the root value. Merkle trees are also employed in peer-to-peer networks to help in the verification of data blocks that have not been changed.

### 3.2.3 Smart Contract

The smart contract is a computer code agreement made between two individuals. It is executed on the blockchain and is recorded in a decentralized database that can't be modified. A smart contract is a programmable code that runs on the blockchain to enable, execute, and enforce the terms of a contract. The main purpose of a smart

contract is to automatically carry out the terms of an agreement when certain criteria are met. Smart contracts provide low transaction fees in comparison to traditional systems which need a trusted third party to enforce and execute an agreement's provisions.

### 3.3 Blockchain Architecture

First of all, the blockchain structure is made up of three main components:

- Transaction: It refers to the smallest building block of a Blockchain system i.e record or any information.
- Block: It is a data structure used to store all transactions which is distributed to all nodes in the network.
- Chain: A sequence of blocks listed in a specific order that may be viewed as a historical record of all of the ledger.

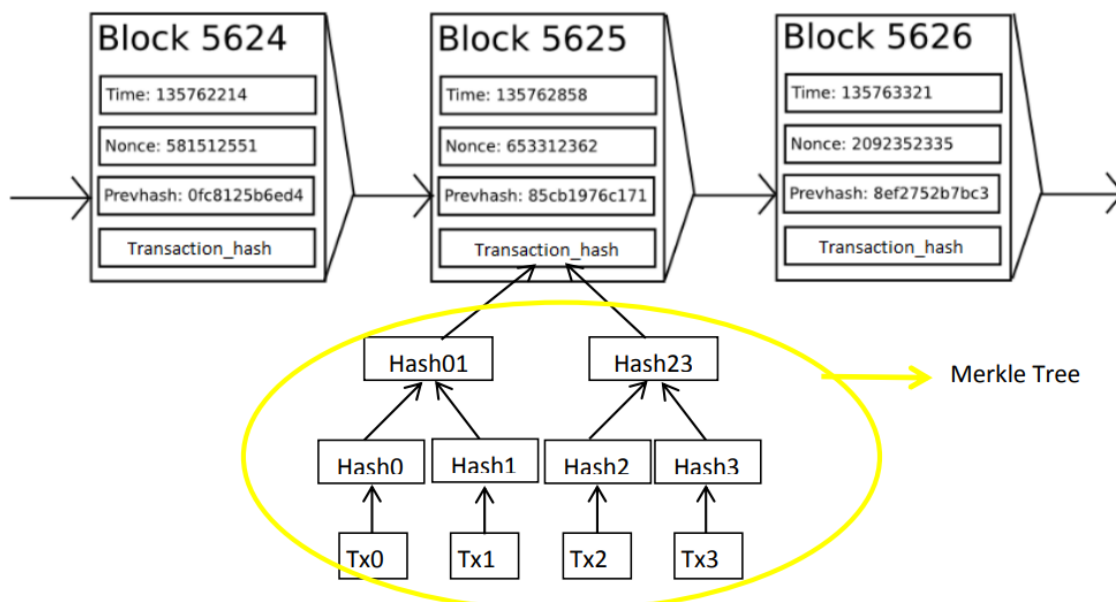


Fig 3: Basic Structure of blocks in blockchain

The simple blockchain structure is depicted in the Figure.3 above, where the later blocks are linked into a chain by recording the hash value of the previous blocks. The

blockchain is designed to pack and add a new block every once in a while, and this block is generated through the consensus protocol that we will mention later.

In the article "Bitcoin: A Peer-to-Peer Electronic Cash System " the user initially sends a request for a transaction through the client, this transaction request then broadcasts to the network and awaits for the confirmation. To construct a block structure, the network node will pack multiple transaction requests and add hash values and other information. The node will next try to find a nonce random string through calculation so that its hash result matches a specified condition; this entire process is commonly referred to as "mining". When a node finds a nonce that meets the condition, it sends a block to the network, and when other nodes get it, they verify it and add it to the local ledger.

It is important to note that once a block is submitted to the local chain, it cannot be erased, which means that the length of the chain only increases and not decreases. That is why the blockchain can provide the feature of no tampering, but it also restricts the overall system's scalability. This consensus process is known as Proof of Work (PoW), and it can prevent malicious nodes from impacting the system to some extent. But the whole process consumes a lot of energy.

### 3.4 Types of Blockchain

It is crucial to know and understand different types of blockchain that exist. A blockchain implementation that needs confidence among interested parties and requires involved parties to have an identity, as opposed to a bitcoin implementation, may be used to address an existing problem in an effective manner. Similarly, a blockchain built specifically for a healthcare system may not be compatible with a blockchain built for financial systems.

There are numerous and often conflicting categorizations of blockchain types. This section of the chapter focuses on blockchain types based on the need for authorisation for data access, as well as the ability to become a node that participates in consensus and block generation. Based on these criteria, we may divide blockchain into three separate categories:



1. Permissionless blockchains allow anybody to join the consensus process and contribute computing power in exchange for a monetary reward.
2. Hybrid blockchains are those in which the information in a block may be accessed but only specific enterprises or entities can participate.
3. Permissioned blockchains require authorization and authentication in order to access information and become a node that participates in consensus.

However, several categorisation of blockchain exist, where the blockchains are broadly divided into public, consortium, and private blockchains:

1. Public: Everyone on the internet can see public Blockchain ledgers, and anybody may verify and add a block of transactions to the Blockchain.
2. Consortium: Only a limited number of organizations (such as banks) may verify and add transactions, however the ledger can be opened to the public or restricted to a select group.
3. Private: Only specific people within the organisation may verify and add transaction blocks to private Blockchains, but everyone on the internet can access it.

To summarise, permissionless blockchains enable public access to data, whereas permissioned blockchains try to limit data access. Hybrid blockchains, on the other hand, exist midway between permissioned and permissionless blockchains, where information reading is public but participation in consensus is not.

### 3.5 Application Areas

With the concept of digital money, blockchain was first used as a solution for the financial sector. However, the power of blockchain extends to other areas such as supply chain, internet of things, financial sectors, real estate and healthcare, which are briefly described below.

### 3.5.1 Supply Chain

The supply chain management system is made up of many transaction levels. Each level has a set of terms and conditions. The supply chain system involves several systems. The various sectors of supply chain systems, such as food preparation, transportation, and shipping. In each of these cases, a digital ledger database makes a system more transparent, reliable, and, most importantly, independent of third parties. When a smart contract is used in combination with a blockchain system, the system becomes both autonomous and secure. Some smart conditions need to be developed in the form of a programme and put into the blockchain system whenever any transaction occurs these smart contracts will be executed. The blockchain nodes are responsible for verification and validation. Smart contract events are triggered when network nodes agree on conditions. Finally, the blockchain system registers the transaction. Making supply chains more transparent with smart contracts helps in the seamless movement of goods and the restoration of trade trust.

### 3.5.2 Internet of Things

One of the most promising areas of research is the internet of things. IoT devices are resource-constrained devices with limited memory and processing capabilities. According to a CISCO research, the number of IoT devices connected to various applications has already exceeded the global population. Some research has already been done on blockchain-based smart home, smart city, smart transportation, and smart environmental monitoring applications. IoT will become more independent if the smart contract concept is combined with the blockchain system.

### 3.5.3 Financial System

The Bitcoin cryptocurrency system pioneered blockchain technology, which was first primarily employed in the banking system. Traditional banking system includes a third party to move money from one account to another account. However, with the blockchain system, transactions are peer to peer and no central storage is employed.

#### 3.5.4 Real Estate

Real estate systems in the traditional way involve lots of risks as well as time taking. It also goes through many levels of legal procedure, requiring numerous paper signatures as well as manual document verification. The real estate sector's problems can be solved with blockchain technology and smart contracts. A centralised system can allow for the buying and selling of properties without the involvement of a third party. The document is also digitally checked and authenticated. All of the papers are also stored in a distributed digital ledger where everyone can see it.

#### 3.5.5 Healthcare System

With the technology growing fast, the human living standard is also growing fastly. Humans can monitor their health status while sitting at home utilising newly developed devices and supporting technologies. Many technologies have previously been developed to read different attributes in the human body. These data may be acquired using a low-cost device and processed locally to get speedy results. Patients' privacy is protected by blockchain technology, which stores data in a digital ledger format. In such system, a smart contract may be utilised to make it more reliable and automated.

# Chapter 4

---

Healthcare and use cases of blockchain in healthcare

Introduction

IoT-based healthcare can improve automation, remote tracking, accuracy, and efficiency. Also connecting it with artificial intelligence (AI) will be able to predict health risks and disease tracking beforehand. A small example can be a simple wearable (smartwatch) tracking your heart rate, blood pressure, your exercises, and so on and syncing all this with your phone where it can be sent to online predictors for health risks (data processing) eventually sending it to the healthcare provider for diagnosis and feedback. This example can be thought of as a very small scale implementation and we should increase the scope of this idea to an extent where we get industry level implementation of the same.

Some limitations for this can be if we go for scalability we have to use a centralized server and database which can be prone to hacking or break down. Healthcare data is very crucial and needs to be protected at all costs from hacking or mutating. Let's say if users want the data to be accessed by only a few doctors but some cloud providers may leak users' data for survey purposes or for monetary benefits.

Blockchain technology is a structure that stores transactional records, also known as the block, of the public in several databases, known as the "chain," in a network connected through peer-to-peer nodes. Though it is getting widely used in cryptography and banking applications, innovating uses of blockchain with IoT is something that is going to be heavily used in the coming stages. As its peer-to-peer network and all participating nodes are equal and collaboratively provide services without a single central point, which can avoid the risk of single-point failure and the database getting compromised. All the transactions can be taken as some kind of data also (the data structure can be changed) are sent to a transaction pool. Some nodes (called miners) take these transactions and adds them to a block and find a nonce for it which is called mining. This block then is broadcasted to all the nodes in the network where a specific consensus mechanism applies and accordingly the nodes accept the block and add to the chain if all transactional data is valid. Once the network accepts the block in the blockchain it cannot be tampered with anymore. The blockchain cannot be forked and all nodes keep working on its extension and it goes by the longest chain rule.

The use of Blockchain Technology is where health data are stored with different levels of access controls and privacy policies to give the best benefits. Admins or doctors can add patients and their data whereas Doctors and AI health analyzers can anywhere and anytime

diagnose these data and this data will build up all the historical data of that particular user and will be connected by a unique identification number (Aadhar no.). The data will continuously keep on growing and blockchain is incapable of storing huge amounts of data as the resource requirements will become too high and complexity will increase to maintain, search and verify. The optimal solution at this point will be to use the InterPlanetary File System (IPFS), which is a content-addressable, distributed file system to store data. The data are distributed over different nodes in the network as there is no central server. Even if some nodes are disconnected still the data is accessible from other running nodes and it can distribute large amounts of data without duplication. Every file uploaded to IPFS has a unique hash string through which the file can be retrieved. Most of the data is stored in the IPFS and that particular hash of that file is stored in the blockchain and helps to verify data integrity and map the data in the ipfs storage.

Blockchain is used in every other field these days due to its wide application across variety of domains and using it in the medical field will be a lot beneficial for all medical applications and all type of users using these systems. If the blockchain is used correctly all these will be very well managed and structured. Also it will be more secure, reliable and faster to use. The major advantage of Blockchain is the hackproof and also the decentralization which aligns with what we are lacking in today's world.

# Chapter 5

---

Proposed Work

# Chapter 5

## Proposed Work

In this paper, I propose DocTel, a blockchain health data application, for storing health data with different levels of access controls and privacy policies to give the best benefits. In DocTel admins (hospital management) or IoT devices can regularly update the users' health data or add new data. Doctors and AI health analyzers can anywhere and anytime diagnose these data and this data will build up all the historical data of that particular user and will be connected by a unique identification number (Aadhar no.) to every patient across the whole country who are part of or can become part of this system. The data will continuously keep on growing as more and more patients get added with them more data will be coming in and blockchain is incapable of storing huge amounts of data as the resource requirements will become too high and complexity will increase to maintain, search and verify the health data. The optimal solution at this point will be to use the InterPlanetary File System (IPFS), a content-addressable (having hash maps that directly maps from the hash to the file location or in simple terms the hash is the location of the file) distributed file system to store data. The data is distributed over different nodes in the network as there is no central server. Even if some nodes are disconnected still the data is accessible from other running nodes and it can distribute large amounts of data without duplication. After uploading file to IPFS it returns a hash string which is unique and can be used to retrieve the file from anywhere. In the DocTel application, most of the data is stored in the IPFS and that particular hash of that file is stored in the blockchain and helps in data integrity verification and link data in ipfs storage. The health data has to be accessed by the doctors and health analyzers so access control is added to the application so only specific groups of people can access the sensitive health data.

In the next section, there is a flow chart and then explaining the whole workflow. Parties involved in this project are as follows:



1. **Patient:** A person who is having to go to the hospital. Should have a unique identification no. such as aadhar number which is already provided by the government to all its citizens.
2. **Doctor:** A doctor who can treat patients and is associated with a hospital or is isolatedly having his own clinic.
3. **Hospital Staff:** A hospital staff helps in the process of registering patients and doctors on the application. Helps in the retrieval of health data of patients and doctors also add treatment for patients.

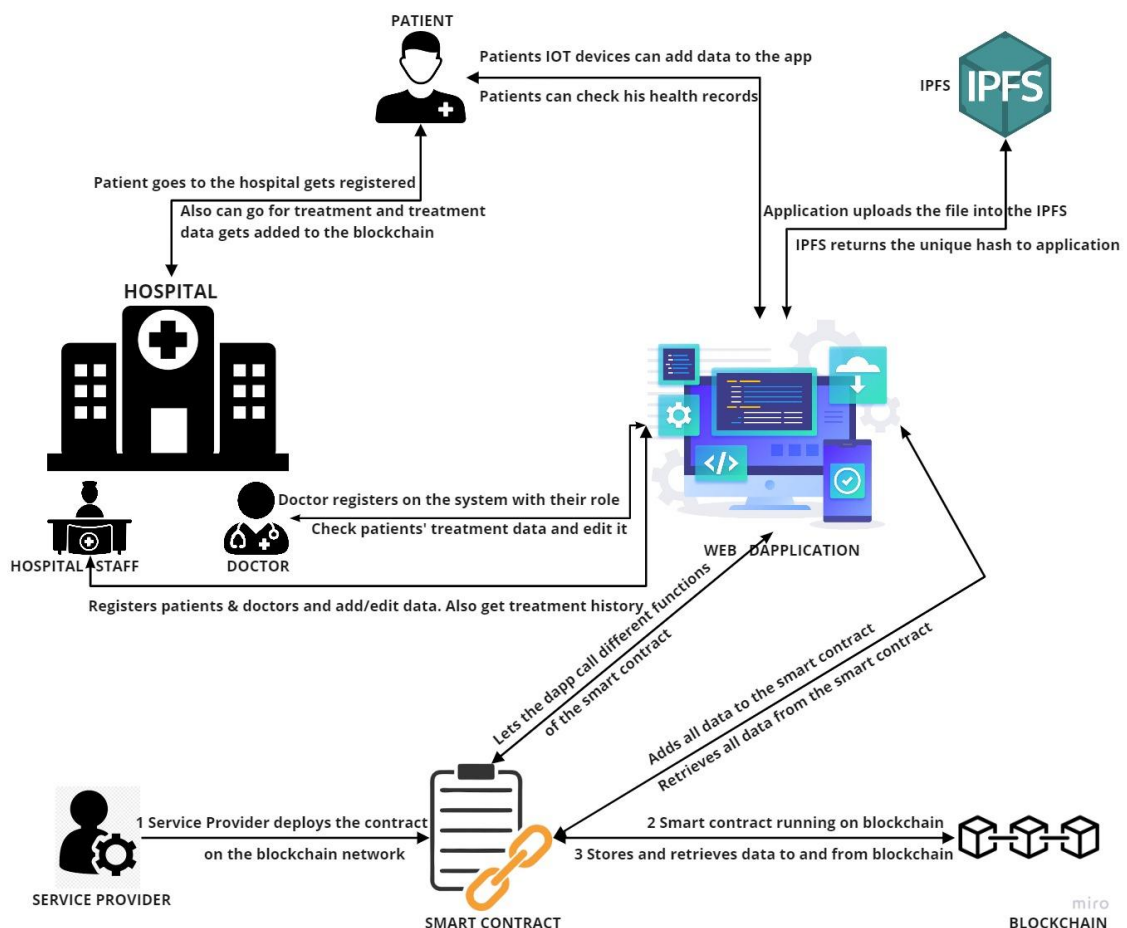


Fig 4 : Proposed blockchain architecture

Figure 4 shows the detailed model of the proposed system. Currently I'm using a local blockchain known as ganache which works exactly as Ethereum blockchain so that all transactions run very fast it is also running on rinkeby & ropsten network of ethereum to

which everybody involved in the system can get connected but is not compulsory and the only difference it has from the ethereum mainnet is that it only requires fake money and not the real one. I developed a smart contract written in Solidity language to manage all these activities. This smart contract is running on the “Code is law” protocol i.e. the functionality under all circumstances will follow whatever is written in the code. This contract is deployed on ganache blockchain, rinkeby and ropsten testnets of Ethereum network also. I created a web dapplication using React.js [A javascript library for building user interfaces] for the frontend creation for all the user interfaces and functionality that can be leveraged for this application, Web3.js [a library that allows you to interact with local or remote Ethereum node using HTTP, IPC, or Websocket] connected with blockchain backend using Metamask[an extension for accessing Ethereum enabled distributed applications, or "Dapps" in your browser] extension that allows you to cover for the gas fees and transaction cost. It is used to be an interface for all the involved parties to access the blockchain network and carry out various activities in the DocTel system. The system strictly follows the decentralized aspects of a private blockchain with a consensus mechanism of entities for every transaction. The detailed steps involved in our proposed Blockchain system are depicted by fig. 4 as follows:

**Mining Continuously:** The process of block production in blockchain is known as mining and is carried out by miners who validate all transactions and check the legitimacy of all functions getting called in the smart contract. In our platform, the mining is continuous in the blockchain and smart contract written in solidity language accomplishes code is law where the functions runs exactly as it is coded in the contract. The service provider can deploy the contract[once and for all] and start mining. The access control is not at the mining level rather it is in the contract layer. So the mining is continuous but the transactions can only be done by a particular agent and the smart contract’s validates all transactions before sending them to the blockchain.

**Users Registry:** This step is to collect all the information about the involved parties, which can be achieved by the registration of all the parties such as hospital staff, doctors, and patients into the platform. The registration can be carried out with a government identity proof(Aadhar number)of the parties and their registration details get stored in Blockchain. While registering the patients all health data is added to the

blockchain and ipfs [and the link is sent into the blockchain] which lets the blockchain store only hashes and ipfs storing all the bigger files which might take a lot of storage.

**Adding Treatment:** Whenever a patient comes for any type of treatment at the hospital, the hospital staff adds a new treatment [the details of all the treatment] and it gets connected to the patient's unique no. [aadhar no.] and the set of doctors doing the treatment also gets connected to that treatment. So everything in this system is strongly interleaved with each other and can be retrieved very easily only by concerned parties.

**Changing Treatment Stage:** Treatment status can only be advanced to next steps and done by only hospital staff and doctors and it tracks the history of the treatment as the history cannot be mutated or deleted in blockchain. We solve the purpose of losing or getting records manipulated. At each stage new doctors might get added, new reports and prescriptions also get added and can be tracked anytime. The system is made robust enough to handle all these.

# Chapter 6

---

Implementation

Implementation  
Technologies implemented

# Chapter 6

## Implementation

### 6.1 Technologies Implemented

The main technologies implemented in this project are: Blockchain, Inter-Planetary File System, Ethereum, Smart Contracts, Ethereum Virtual Machine, Solidity, React Javascript, Ganache, Metamask, AWS Amplify, Github, Consensus Algorithm, and Hashing Algorithm. A brief description of all these technologies follows

**Blockchain:** It is a distributed ledger-based technology that uses consensus-based decisions to come to a single point of truth. It involves three main technologies which are private key cryptography, peer-2-peer network, and Blockchain protocol. The data once entered becomes immutable and hackproof. Blocks in blockchain contain groups of valid transactions that are encoded into a Merkle tree structure and hashed at each step of the merkle tree generation. Each block contains the hash of the parent block in the blockchain, linking the two together so that they cannot be tampered. The linked blocks form a chain. This repetitive process confirms the integrity of the parent or previous block, all the way back to the genesis block. Each block also has a timestamp and a nonce associated with it.

**Inter-Planetary File System:** The Inter-Planetary File System[IPFS] protocol is a peer-2-peer network for sharing and storing data in a distributed system of files. For uniquely identifying each file it uses content addressing in a global namespace in which all computing nodes are connected in a decentralized manner. It uses content-based addressing and Merkle Directed Acyclic Graph data structure.

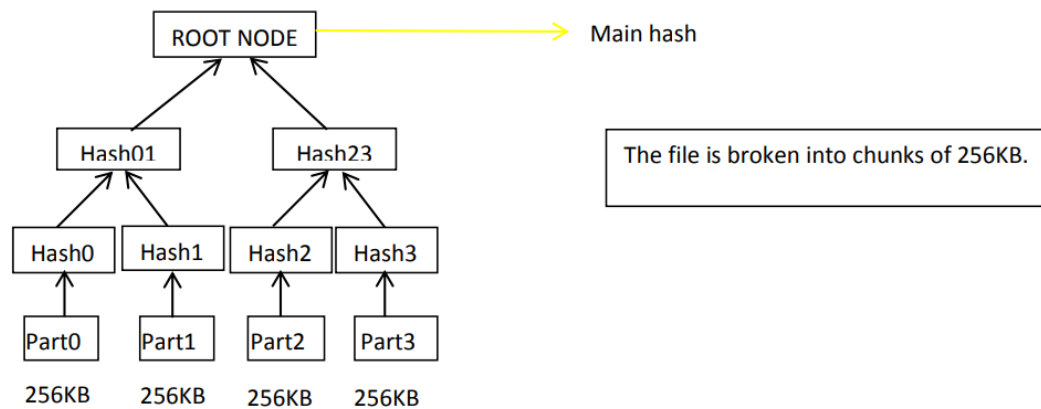


Fig 5: Storing strategy in IPFS via Merkle-DAG

A Merkle-DAG is a Directed Acyclic Graph structure where each node has an identifier and this is the result of hashing the contents of the node. So to get the hash of the any node the children nodes are hashed together and the new hash that comes is the hash of the parent node. The hashing is done using a cryptographic hash function like SHA256.

**Ethereum:** Ethereum is a platform based on Blockchain technology that enables anyone to build and deploy smart contracts and connected decentralized applications. Ethereum's coding language solidity helps write smart contracts. Its native currency is Eth. It was founded by Vitalik Buterin.

**Dapplication:** A decentralized application is a computer application that runs on a distributed computing system. They have distributed ledger [DLT] based technology. It has a web-front in any javascript libraries, smart contract running on blockchain as backend and web3, or some kind of RPC pipelines to connect both of them together as a middleware.

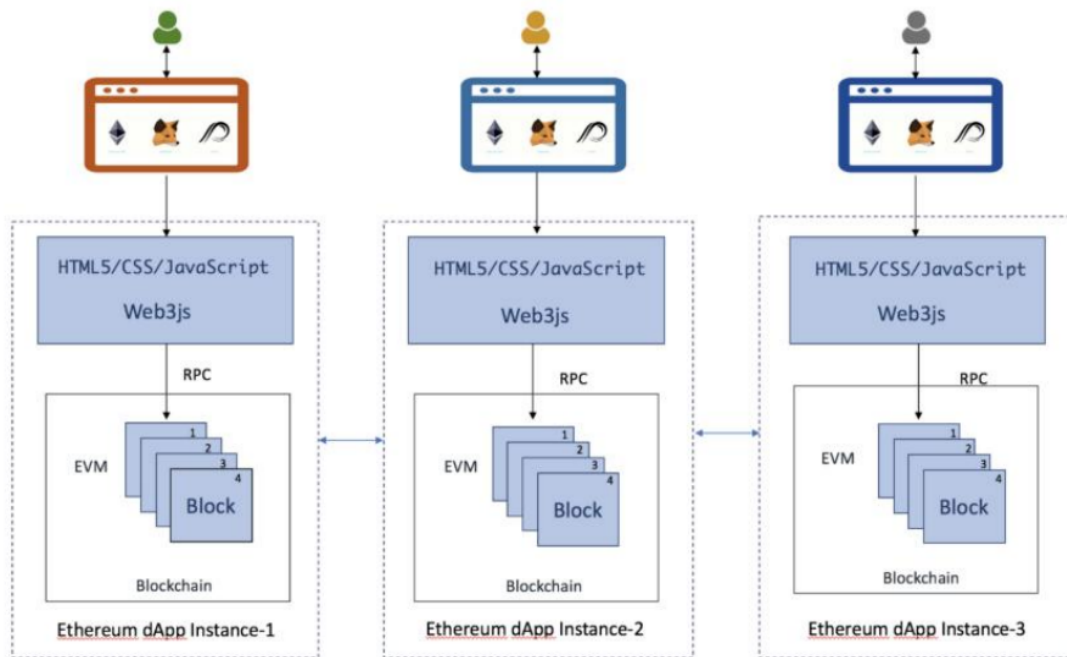


Fig 6: Ethereum Dapp instance

**Solidity:** Solidity is a contract oriented language. It is used mostly for Ethereum Virtual Machine. It is statically typed language so you have define types for each data and functions, supporting inheritance, libraries and complex user defined types. Almost all the applications of solidity are for writing smart contracts.

**Github:** It is a version control software used for versioning and hosting of software, codebases and applications. It offers the distributed version controlling and project code management functionality. In this project github is purely used for version control and first step in CI/CD pipeline.

**AWS Amplify:** AWS Amplify is a set of purpose-built tools and features that lets frontend web developers build full-stack applications, with the flexibility to leverage the breadth of AWS services. In this project it is used for the CI/CD pipeline and hosting the web application.

**React.js:** React is a front-end open-source JavaScript library for building user experience and interfaces based on small components. In this project it is extensive used for the creation of front end and UI.

**Ganache:** Ganache is a copy of Ethereum Blockchain which can be used as a mock for personal use and is used to test and deploy smart contracts , develop applications, run tests and perform other functionalities free of cost. It is used in this project as the blockchain running locally.

**Metamask:** MetaMask is a cryptocurrency wallet for interacting with the Ethereum blockchain. It enables users to access their Ethereum wallet through a mobile app or browser extension, which can then be used to interact with decentralized applications. In this system it acts as a gateway to the blockchain world and to carry on all the transactions.

**Consensus Algorithm:** A voting mechanism where all the nodes connected to a network vote on the validity of a block only then the block is confirmed over the blockchain. The consensus algorithms that can be used for this project are Practical Byzantine Fault Tolerance, Proof of Work and Proof of stake.

**Hashing Algorithm:** It plays a crucial role in the blockchain process and also in the integrity of the transaction and confidentiality of data. It transforms and maps an arbitrary length of input arbitrary data value to a unique fixed-length value. The algorithm should be one-way and collision-free. Some majorly used hashing functions are SHA-256 and Keccak.

The implementation is done in the form of a small working prototype application. Here is a link for the workflow of each type of user and each functionality that I created for a better understanding of how the application works:

[Part 1](#)

[Part 2](#)

A detailed explanation with the help of screenshots follows for each webpage of my system.



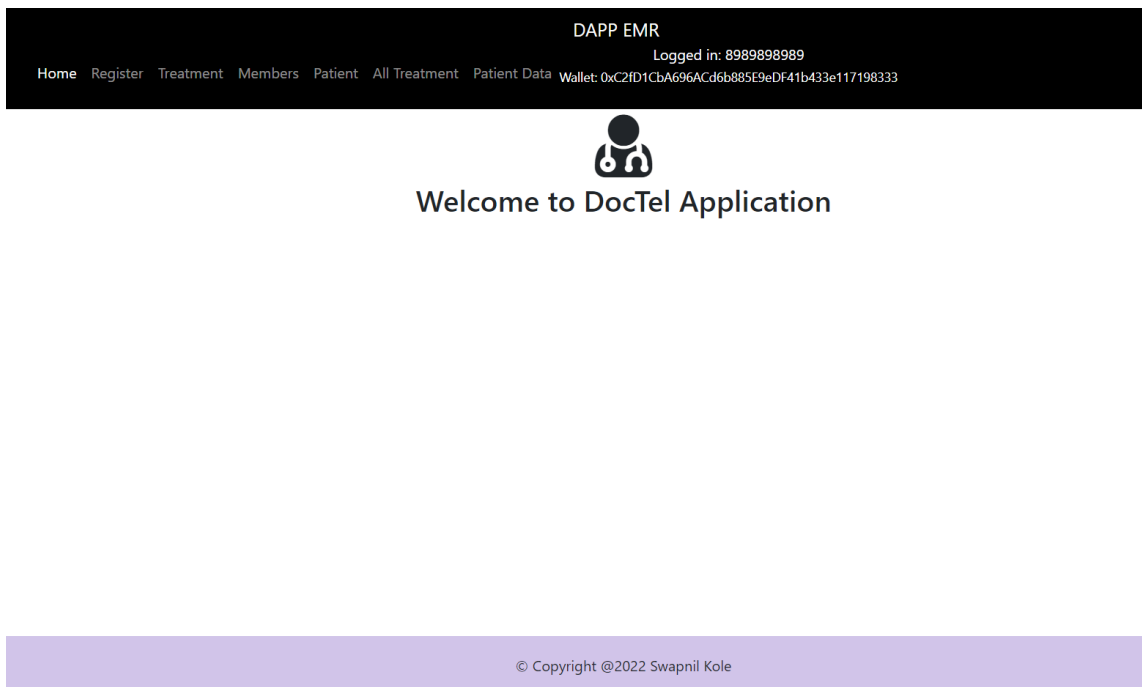



Fig 7: Screenshot of Homepage

This is a very basic homepage I have made just to show that the web application exists and can be customized a lot to make it more professional. The homepage moving forward will have some more features and will have a help center where people will get to know how to use this application.

## SignUp Page

Admin




Aadhar Number:  
8989898989

Role:  
Hospital Staff

SIGN UP

Log In Log Out

Doctor



Wallet Address:  
0xc22c6B37dc526833D09Bb8e1247D966815238186

Aadhar Number:  
5656565656

Speciality:  
Cardiologist

Location:  
Hyderabad

SIGN UP

Log In Log Out

Fig 8: Screenshot of Admin Registration Page

This is the registration page where the admin can signup/login/logout and they require a wallet to be connected to do all these transactions. The admin can join and input his aadhar no. and role in the system and his wallet should be connected to get the account address of the admin. If the admin clicks on “Sign up” button all these admin data will go into the blockchain as a transaction and this admin will be registered into this system. With the same inputs the admin can click on “Log In” and the header will reflect the wallet and logged-in aadhar no. of that admin. If he clicks on “Log Out” his account gets disconnected from the current log in. A doctor can sign up on his own or the hospital staff can make the sign up for him. The doctor has to provide his wallet address, aadhar number, his specialty, and his location and he/she will be registered into the system. The Log In and Log Out works the same for him as well.

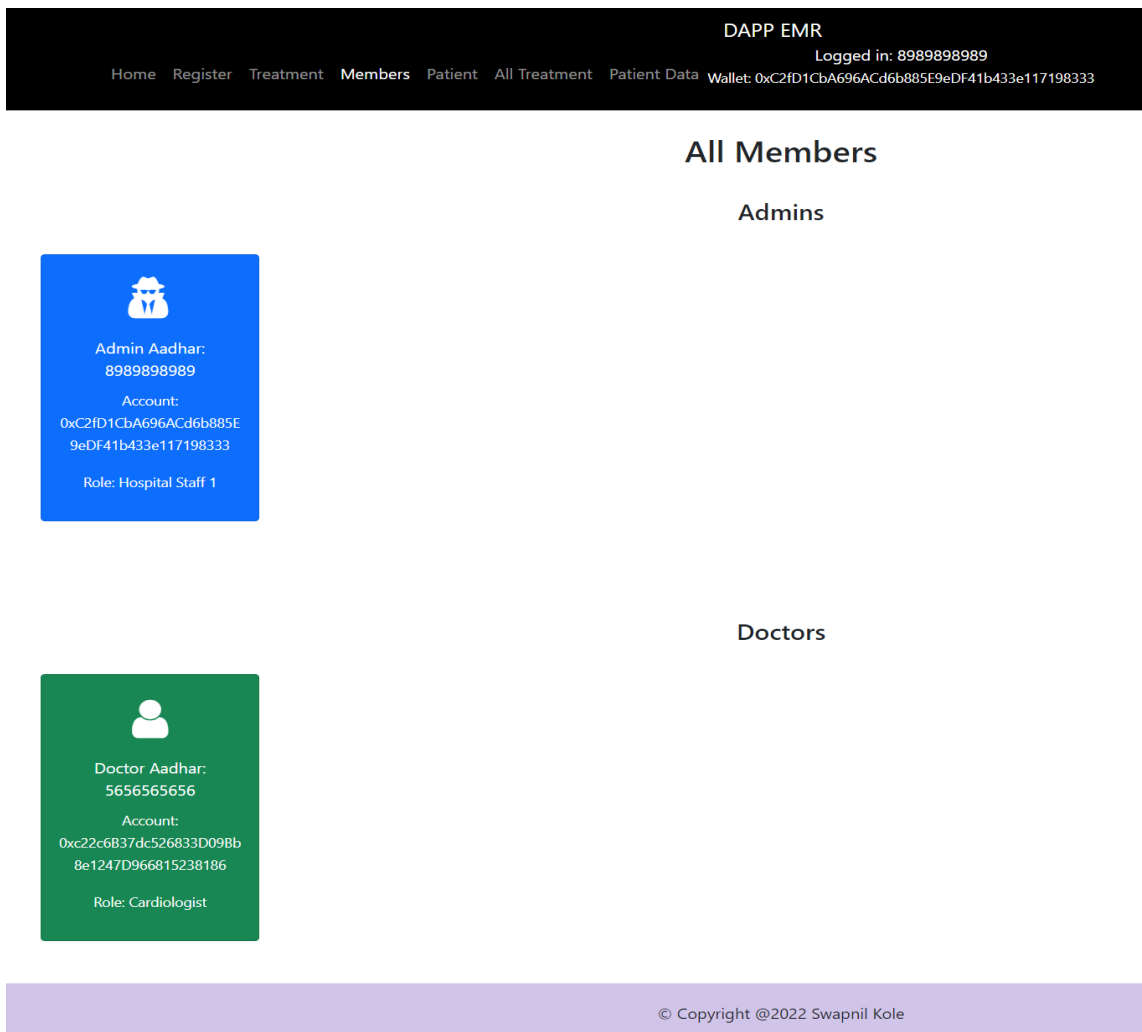


Fig 9: Details of All Members page

Here we have the member list and only the hospital staff can access it. They can see the details of all the hospital staff as in for now only the wallet address and aadhar no. but later the details can be increased also. In addition to this even the doctors' details namely aadhar number, wallet address, and role can be seen.

DAPP EMR

Logged in: 8989898989

me Register Treatment Members Patient All Treatment Patient Data Wallet: 0xC2fD1CbA696ACd6b885E9eDF41b433e117198333

### Add Patient

Patient Aadhar	1212121212
Weight	53000
Height	168
Gender	Male
Blood Type	O
Date of Birth	987558411
Location	Mumbai

Add Patient

© Copyright @2022 Swapnil Kole

Fig 10: Screenshot of Patient Registration page

This page is exclusively for patients' registration into the system for the first time and later on it can be updated and each time there is a new treatment. In this registration, the patient has to give his aadhar no., weight (in grams), height (in cms), gender, blood group, date of birth in epoch time, and location. After the hospital staff or the doctor enters this data it will go into the blockchain as a transaction. There is a validation for kind of extreme values for each field. If the value deviates from general values by a lot its going to throw an error statement. For example the Height cannot be more than 300 cms so we have the error handler on it which throws an error statement anytime somebody enters values exceeding the limit.

DAPP EMR

Logged in: 8989898989


me Register Treatment Members Patient All Treatment Patient Data Wallet: 0xC2fD1CbA696ACd6b885E9eDF41b433e117198333

Patient Details

Patient Aadhar1212121212

Get Data

Patient Details



Patient Aadhar : 1212121212

Height : 168

Weight : 53000

Bloodtype : O

Gender : Male

Location : Hyderabad

Treatments Undergone : 1,

© Copyright @2022 Swapnil Kole

Fig 11: Screenshot of Patient Details page

In this page, the hospital staff, doctor or the patient can retrieve the patient's data by putting his aadhar no. in the search box and clicking on "Get Data" and all the details will show in the below section. The patient's aadhar no., height, weight, bloodtype, gender and location is shown. In this section there is "Treatments Undergone" which will show all the treatments Id this patient has gone through.

DAPP EMR
Logged in: 8989898989
Wallet: 0xC2fD1CbA696ACd6b885E9eDF41b433e117198333

Home
Register
Treatment
Members
Patient
All Treatment
Patient Data

### Add Treatment

Patient Aadhar
1212121212
Add Treatment
0

### Add Doctor

Treatment Id
1
Doctor Aadhar
5656565656
Send Treatment

### Add Prescription and Report

Treatment Id
1
Prescription Upload
Choose File
images2.jpg
Add
Treatment Id
1
Report Upload
Choose File
No file chosen
Add

© Copyright @2022 Swapnil Kole

Fig 12: Add Treatment & Reports page

This is the page where hospital staff or doctors can add treatments. They should start by adding the patient's aadhar when he arrives at the hospital for some treatment. Once the add treatment is clicked a treatment is generated in the blockchain which has the treatment Id, the patient's aadhar no. and the logged in user's aadhar no. (hospital staff or doctor whoever did the transaction). Whenever this treatment is assigned to a doctor the "add doctor" form should be used in which the treatment id and doctor's aadhar no. should be added who is going to do the treatment and this data will go to the blockchain and also an event will be emitted in the blockchain to make this doctor addition immutable. Next during the whole process of this treatment any prescription or reports can be added just by adding the treatment Id and uploading the file for the same (any format) and then click on add. This file is first uploaded to Ipfs from where ipfs gives back a hash through which the file can be accessed. This hash is then sent to the blockchain to save up on space by keeping just hash rather than whole file.

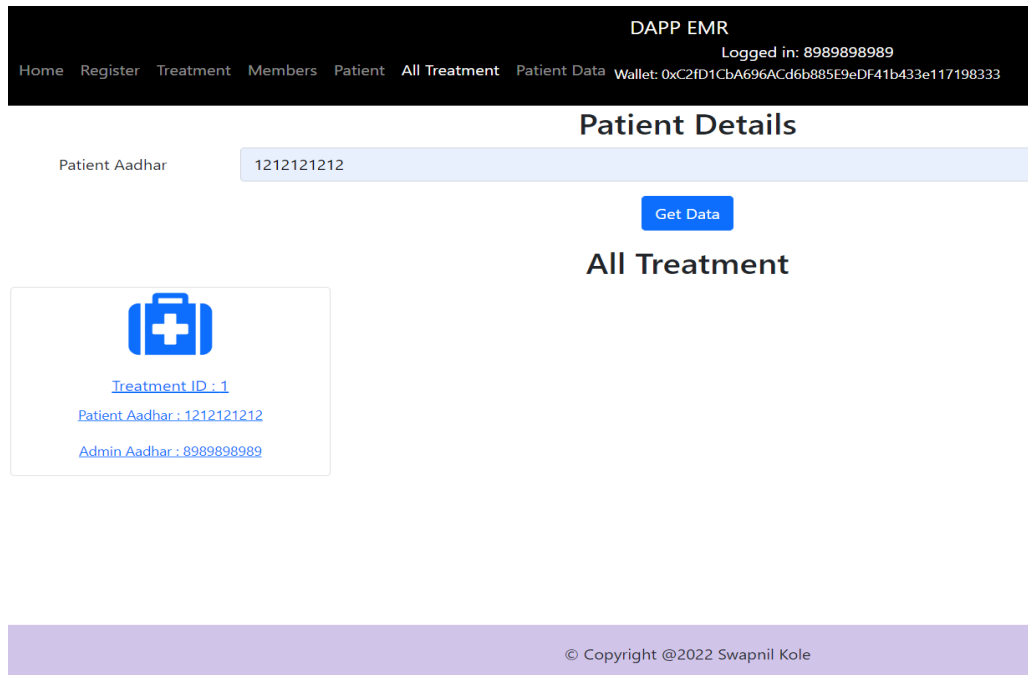


Fig 13: Treatment Details page

This page shows all the treatments in the system. It shows just basic data namely the treatment Id, Patient's aadhar and the admin's aadhar who added this treatment. There is a search bar in which when a patient's aadhar no. is put and searched for it will return only that particular patient's treatments. Every single treatment when clicked routes to a Treatment details page which is shown in the next image.

DAPP EMR

Logged in: 8989898989

Home Register **Treatment** Members Patient All Treatment Patient Data
Wallet: 0xC2fD1CbA696ACd6b85E9eDF41b433e117198333

## Treatment History

**Treatment ID** : 1

**Patient Aadhar** : 1212121212

**Admin Aadhar** : 8989898989

---

### Events

**Event: treatAdded**

Time: March 27th, 2022 at 10:45 PM

**Event: doctorAddedTreat**

Doctor: 5656565656

Time: March 27th, 2022 at 10:46 PM

**Event: PrescriptionAddedTreat**

Prescription:  
Qma2QiNRuvWeELkzwWWt9BRFwqGrXh  
QyP19h4omQ9DyzLi

Time: March 27th, 2022 at 10:49 PM

**Event: ReportAddedTreat**

Report:  
QmeAQWwVLbWK3qtCn4kVu4pJ3UadS  
GwLfpvbmFsQAXHjt

Time: March 27th, 2022 at 10:50 PM

© Copyright @2022 Swapnil Kole

**Fig 14: Treatment History page**

This is the Treatment History/Details page it firstly shows the treatment Id, Patient's aadhar and the admin's aadhar who added this treatment. Then in the events section it gives all the history of this treatment since when it was added and timestamp of each of them. In this particular example it shows when the treatment was added. It shows that a doctor was added to the treatment and his aadhar no. following a prescription and report was added and shows the time of it. The picture is a small version of the actual picture which can be viewed by clicking on this image and this image is getting retrieved from the ipfs by taking the hash from the blockchain. Also the hash is shown in the same card.



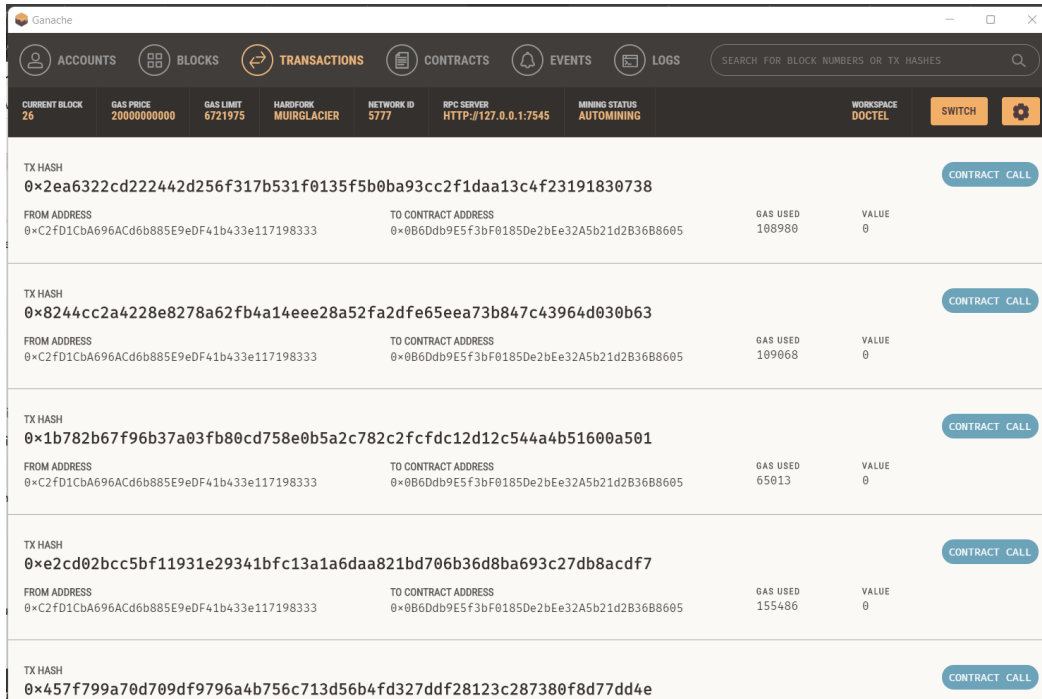


Fig 15: Ganache Application

This is Ganache application where I'm currently running a local blockchain and it functions exactly the same as the ethereum blockchain just with fake money and I'm using it for testing the application, seeing logs, having accounts and funds in them.

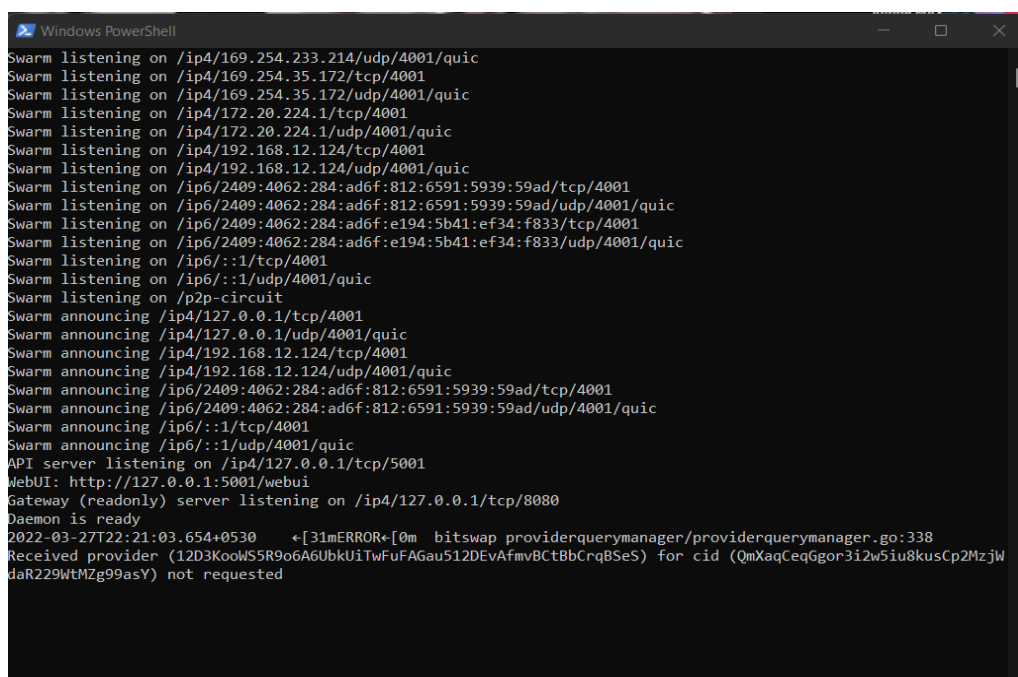


Fig 16: Terminal Page

This is my terminal which is running a node for the ipfs to get connected with the ipfs and send and receive data. It is running on 5001 port and without running this the ipfs files neither can be retrieved nor uploaded.

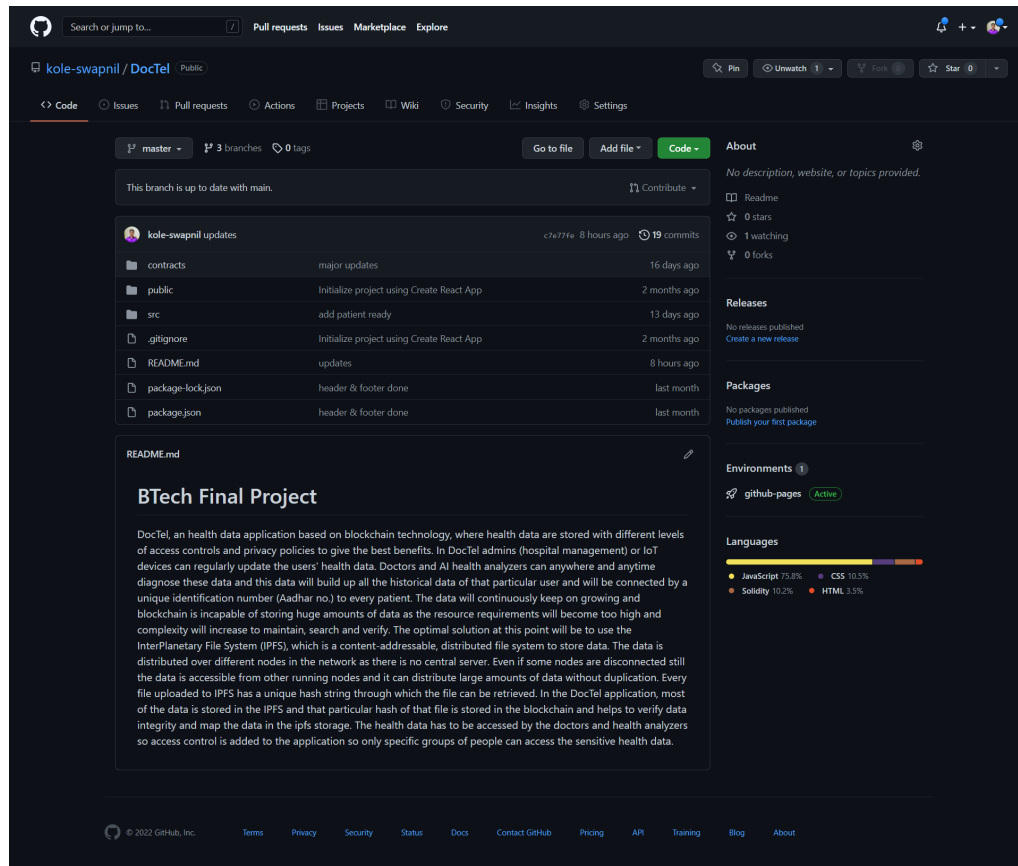


Fig 17: Github Repository

This screenshot is from my github repository which I'm using as a version control system and keeps my codes safe from getting deleted or modified.

Here is the link to my repository: <https://github.com/kole-swapnil/DocTel>

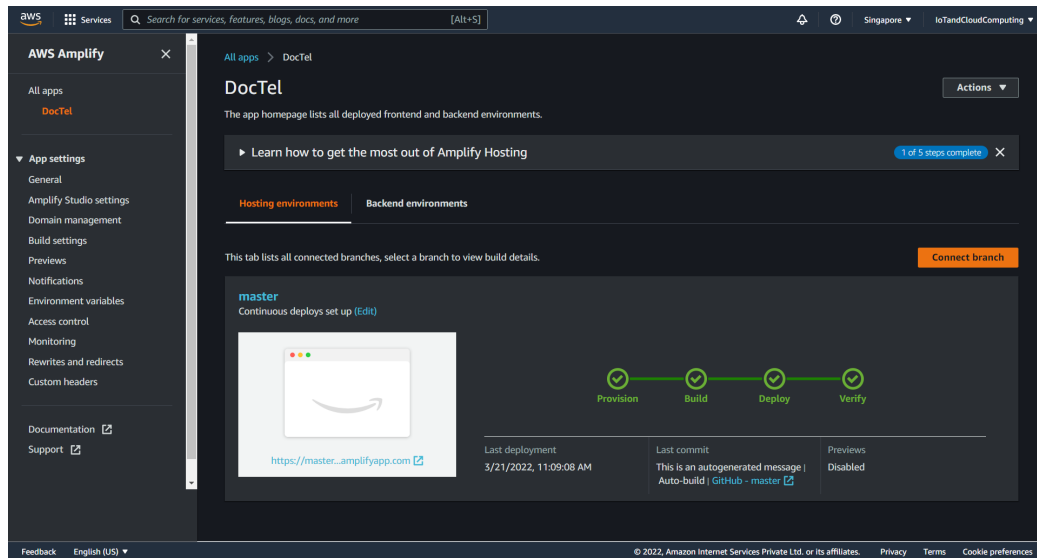


Fig 18: Amazon AWS Amplify

This screen is from Amazon AWS Amplify where I have hosted my website for this application and it helps in the whole CI/CD pipeline as everytime I push my code to github repository amplify will pull the changes and start with the deployment stages as provision, build, deploy and then verify. After these 4 steps, the website is live at a website from amplify having SSL certificate.

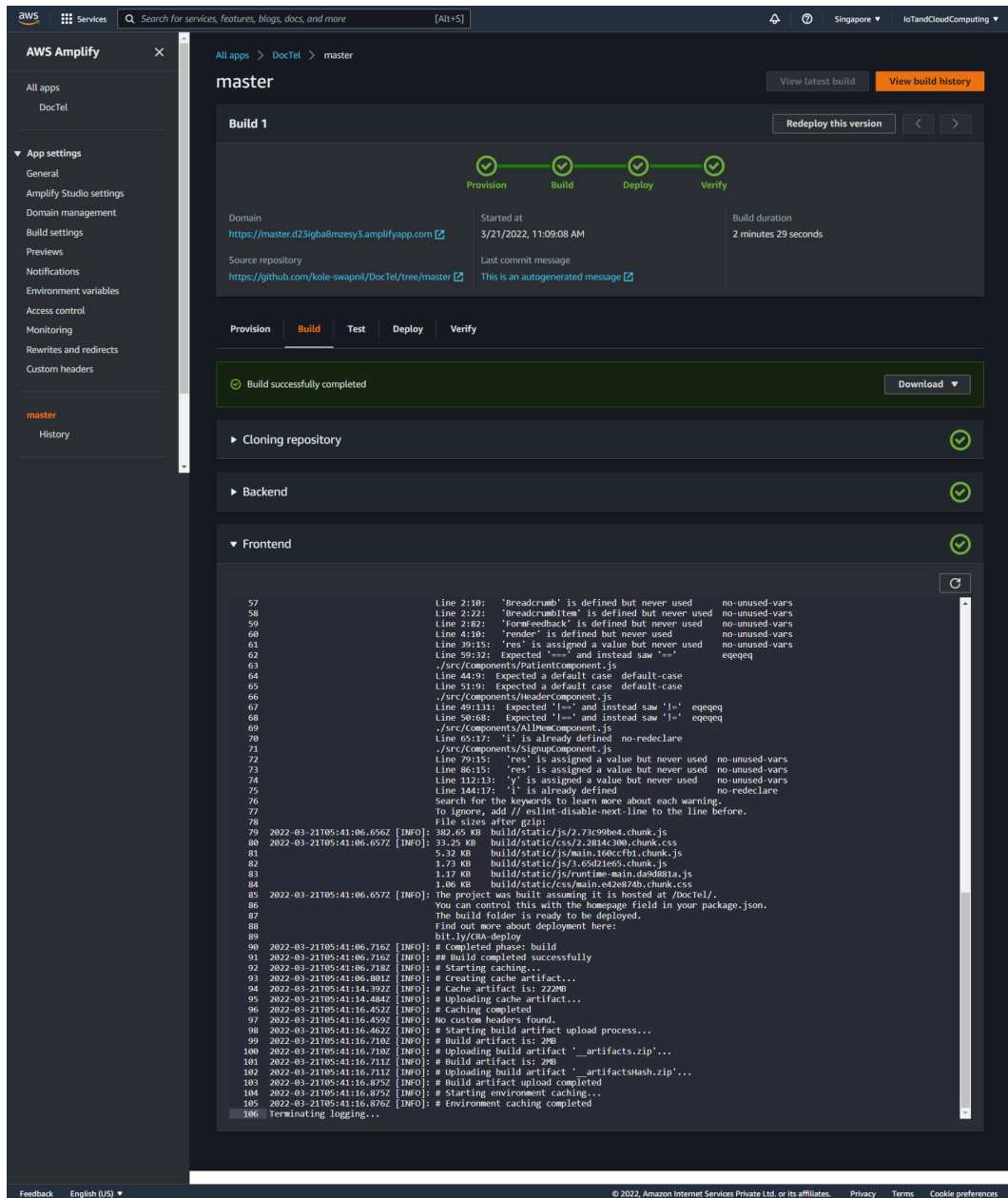


Fig 19: CI/CD pipeline build

A detailed view of each step in CI/CD pipeline is given here with logs of each step. The website at which my website is hosted is <https://master.doaswn5telp2q.amplifyapp.com/> Do not open this site as it needs metamask extension to work.

# Chapter 7

---

Result Discussion, Conclusion & Future Work

Result Discussion  
Conclusion  
Future Work

# Chapter 7

## Result Discussion, Conclusion & Future Work

### 6.1 Result Discussion

The application is already able to achieve all the objectives that were mentioned before making this proposal. The Medical records cannot be mutated, deleted, or tampered with anymore as the database is decentralized with the help of blockchain. Nobody at a later stage can show different results as once written on blockchain nothing can be changed but later on new reports can be added, as you might have seen in the application every operation is having a timestamp. Each health record is connected to a user's unique identification number or Aadhar no. and we can get a unified & decentralized database all across the country. Easily all the health records of a patient can be retrieved by searching by his aadhar no. and is way faster and more reliable for patients' moving from place to place. A lot of reliability as well as robustness is added to the application. Its rather simple, functional User interface makes it easy for all the users to like and use it.

### 6.2 Conclusion

I can conclude that this application after using the latest and the top technologies has a lot of potential and a large-scale implementation of this application is worth the efforts behind it. Also, the system once in production will be very reliable, efficient, and user-friendly. It drives today's medical records applications to all new levels and this application can have many more integrations so that other applications can be easily integrated into this application and they will become decentralized very easily. Decentralization is the new future and making applications decentralized is the first step

into it. Blockchain as an emerging technology will take everything into the decentralized world.

## 6.3 Future Work

A lot can be improved in the user interface (UI) and user experience (UX) to make it more user-friendly. A lot of applications (currently used in Healthcare) can be integrated or some major features can be added to make this application an all-in-one application for all healthcare-related tasks. The IoT part of the applications is also what will be incorporated next to take the application to a whole new dimension. New extensions will be added to the application to make it interoperable for diverse medical usage.

# Bibliography/References

- [1] Nakamoto, Satoshi “Bitcoin: A peer-to-peer electronic cash system”, Decentralized Business Review, Pages 21260, Year 2008
- [2] K. Ito, K. Tago, and Q. Jin, “i-blockchain: A blockchain-empowered individual-centric framework for privacy-preserved use of personal health data,” in 2018 9th International Conference on Information Technology in Medicine and Education (ITME). IEEE, 2018, pp. 829–833.
- [3] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, “Blockchain for secure ehds sharing of mobile cloud-based e-health systems,” IEEE access, vol. 7, pp. 66 792–66 806, 2019.
- [4] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, “Medblock: Efficient and secure medical data sharing via blockchain,” Journal of medical systems, vol. 42, no. 8, pp. 1–11, 2018.
- [5] G. S. Aujla and A. Jindal, “A decoupled blockchain approach for edge-envisioned iot-based healthcare monitoring,” IEEE Journal on Selected Areas in Communications, vol. 39, no. 2, pp. 491–499, 2020.
- [6] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, “A patient agent to manage blockchains for remote patient monitoring,” Stud Health Technol Inform, vol. 254, pp. 105–115, 2018.
- [7] A. Kumar, R. Krishnamurthi, A. Nayyar, K. Sharma, V. Grover, and E. Hossain, “A novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes,” IEEE Access, vol. 8, pp. 118 433–118 471, 2020.
- [8] X. Zheng, R. R. Mukkamala, R. Vatrappu, and J. Ordieres-Mere, “Blockchain-based personal health data sharing system using cloud storage,” in 2018 IEEE 20th international conference on e-health networking, applications and services (Healthcom). IEEE, 2018, pp. 1–6.
- [9] V. K. Chattu, A. Nanda, S. K. Chattu, S. M. Kadri, and A. W. Knight, “The emerging role of blockchain technology applications in routine disease surveillance systems to strengthen global health security,” Big Data and Cognitive Computing, vol. 3, no. 2, p. 25, 2019.



- [10] S. Wu and J. Du, "Electronic medical record security sharing model based on blockchain," in *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, 2019, pp. 13–17.
- [11] R. Jabbar, N. Fetais, M. Krichen, and K. Barkaoui, "Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity," in *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*. IEEE, 2020, pp. 310–317.
- [12] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," *Ieee Access*, vol. 6, pp. 38 437–38 450, 2018.
- [13] A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, "Medibchain: A blockchain based privacy preserving platform for healthcare data," in *International conference on security, privacy and anonymity in computation, communication and storage*. Springer, 2017, pp. 534–543.
- [14] H. Kaur, M. A. Alam, R. Jameel, A. K. Mourya, and V. Chang, "A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment," *Journal of medical systems*, vol. 42, no. 8, pp. 1–11, 2018.
- [15] B. Shen, J. Guo, and Y. Yang, "Medchain: Efficient healthcare data sharing via blockchain," *Applied sciences*, vol. 9, no. 6, p.1207, 2019.
- [16] N. Garg, M. Wazid, A. K. Das, D. P. Singh, J. J. Rodrigues, and Y. Park, "Bakmp-iomt: Design of blockchain enabled authenticated key management protocol for internet of medical things deployment," *IEEE Access*, vol. 8, pp. 95 956–95 977, 2020.
- [17] F. Jamil, S. Ahmad, N. Iqbal, and D.-H. Kim, "Towards a remote monitoring of patient vital signs based on iot-based blockchain integrity management platforms in smart hospitals," *Sensors*, vol. 20, no. 8, p. 2195, 2020.
- [18] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," *Journal of medical systems*, vol. 42, no. 7, pp. 1–7, 2018.

- [19] B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, "Healthblock: A secure blockchain-based healthcare data management system," *Computer Networks*, vol. 200, p. 108500, 2021. B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, "Healthblock: A secure blockchain-based healthcare data management system," *Computer Networks*, vol. 200, p. 108500, 2021.
- [20] G. Tripathi, M. Abdul Ahad, and S. Paiva, "Sms: A secure healthcare model for smart cities," *Electronics*, vol. 9, no. 7, p.1135, 2020.
- [21] M. M. Madine, A. A. Battah, I. Yaqoob, K. Salah, R. Jayaraman, Y. Al-Hammadi, S. Pesic, and S. Ellahham, "Blockchain for giving patients control over their medical records," *IEEE Access*, vol. 8, pp. 193 102–193 115, 2020.
- [22] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "Bbds: Blockchain-based data sharing for electronic medical records in cloud environments," *Information*, vol. 8, no. 2, p. 44, 2017.
- [23] Baran, Paul. "On distributed communications networks." *IEEE transactions on Communications Systems* 12.1 (1964): 1-9.
- [24] Kshemkalyani, Ajay D., and Mukesh Singhal. *Distributed computing: principles, algorithms, and systems*. Cambridge University Press, 2011.
- [25] Merkle, Ralph Charles. *Secrecy, authentication, and public key systems*. Stanford university, 1979.
- [26] Fan, Junfeng, Daniel V. Bailey, Lejla Batina, "Breaking elliptic curve cryptosystems using reconfigurable hardware." In *2010 International Conference on Field Programmable Logic and Applications*, pp. 133-138, 2010.