**CHAPTER 01**

**INTRODUCTION**

* 1. **OVERVIEW**

Smart Health Care Dapp is made to connect hospitals, Patient, Medicals, and pharma company. As in today’s world there are lot of misunderstandings between the doctors and patient and trust between them lacks. To develop trust between this entity smart health care Dapp will help. Whenever patient goes to the medicals to buy the medicines, he first think is the medicine provided by the medicals are good and not fake. Some medicals may keep fake medicines and expired medicines, these medicines may be provided to the patient. To avoid this, we can store all the medicines data on blockchain and track all process of medicines. And check if they came from trustworthy pharma company.

There are basically 4 clients included into this project such as Hospital, Medical, Pharma, and Patients. Our Decentralized Storage will have the detailed medical history of each patient. It will be stored with the help of blockchain. The data will be available to hospital as well as patients in the decrypted format for the future reference.

So, the medicals are directly linked with hospitals or doctor, and not directly with the patients, whatever the prescription would be there will be sent by doctors to medicals without any intervention of patients, they will just need to collect their meds and essentials as prescribed directly from medical. This will prevent unethical purchase of medicine. So, in this way no patients will directly go and collect any medicines from medicals and there would be no threat of providing allergic or any other medicines which doesn’t suit the Patient. Also, there will be no trust issues among the patients and medicals or pharma.

Hospitals will play a very crucial role here, our decentralized system will have the hospital name, doctor’s name, doctor’s degree. In DAO the system automatically verifies the user. To participate in blockchain, user must be verified, hence this information will be very important. We will keep record of medical’s sales and analyze the most sold or most used medicines. This will help us to keep track of market’s most valued medicines, so accordingly we it will be easy for us to make an order earlier based on its availability in the market.

A decentralized autonomous organization are organizations built according to rules coded as computer programs, often transparent, and controlled by one central government. Controlled by members of the organizations rather than influenced. Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets across corporate networks. Assets can be tangible (houses, cars, cash, land) and intangible (intellectual property, patents, copyrights, trademarks).Blockchain is a form of public ledger, a series (or chain) of blocks in which transaction details are recorded after proper authentication and verification by designated network participants.

**1.2 MOTIVATION**

1. To help people get access to their health data anywhere from the world.
2. To provide trust between hospitals and the patients due to fake certificates by some doctors.
3. To Provide trust between medicals and the patient due to fake medicines seller.
4. To help people access their data in the emergency due to some accidents.
5. To improve the data storage of the patient health history and make it more secure using blockchain.

**1.3 PROBLEM STATEMENT & OBJECTIVE**

Blockchain Based Patients data , Medicines data and doctors data storage has novel features of real time accessing of all the data and keeping watch on it which enables users like patient and the medicals to keep track of all the data been stored on the blockchain using secure hash and access the data using unique keys thus data like Pharma Company medicine making process and the important dates are been stored and patient data like health history and the current medicines required by the patient which can be seen by only medicals and the patient are been stored and accessed in the emergency thus this enables a trust worthy environment between Hospitals, Patient, Medicals and Pharma Company.

**Objective:**

1. To store data of patients for doctor more secure and effectively.
2. To access data anywhere in the world whenever needed.
3. To keep track of patient health issues
4. To keep track of medicines which were provided by doctor.

**1.4 PROJECT SCOPE & LIMITATIONS**

**Project Scope:**

1. **Secure and Private Data Sharing:** With a blockchain-based Dapp, healthcare providers can securely and privately share patient data across different organizations, ensuring data privacy and confidentiality. This could help reduce data breaches, which are a significant problem in the healthcare industry.
2. **Increased Efficiency:** By using a Dapp, healthcare providers can automate administrative tasks, reduce paperwork, and streamline processes, resulting in increased efficiency and improved patient care.
3. **Improved Patient Outcomes:** With secure and fast access to patient data, healthcare providers can make

more informed decisions and provide better care to patients, resulting in improved patient outcomes.

1. **Transparency:** Blockchain technology allows for transparent and immutable record-keeping, ensuring that

all stakeholders have access to accurate and up-to-date information.

1. **Tokenization:** A blockchain-based Dapp could use tokens to incentivize patients and healthcare providers to participate in the network. For example, patients could earn tokens for sharing their data, while healthcare providers could earn tokens for providing quality care.

**Limitations:**

1. **Limited Scalability:** Blockchain technology can be slow and limited in its scalability, which could be a significant limitation for a SMART healthcare Dapp. As the number of users and transactions increases, the blockchain could become congested, leading to slower transaction times and higher fees.
2. **Regulatory Challenges:** Healthcare is a heavily regulated industry, and implementing a blockchain-based Dapp could pose significant regulatory challenges. Compliance with HIPAA regulations and other data privacy laws would need to be carefully considered.
3. **Integration with Existing Systems:** Integrating a new blockchain-based Dapp with existing healthcare systems could be challenging, as many healthcare organizations use legacy systems that may not be compatible with blockchain technology.
4. **Limited Scalability:** Blockchain technology can be slow and limited in its scalability, which could be a significant limitation for a SMART healthcare Dapp. As the number of users and transactions increases, the blockchain could become congested, leading to slower transaction times and higher fees.

**1.5 METHODOLOGIES & PROBLEM SOLVING**

**1.** **Design thinking:** This methodology involves understanding the needs of the users and designing solutions that meet those needs. It involves empathizing with the patients, doctors, and healthcare providers to identify their main points and then ideating, prototyping, and testing solutions that solve those problems.  
  
**2.** **Agile methodology:** This methodology involves breaking down the project into smaller, manageable tasks.

**CHAPTER 02**

**LITERATURE SURVEY**

**[1]. Israa Abu-elezz, Asma Hassan, Anjanarani Nazeemudeen, Mowafa Househ, Alaa Abd alrazaq, The benefits and threats of blockchain technology in healthcare: A scoping review, International Journal of Medical Informatics, Volume 142,2020, 104246, ISSN 1386-5056**

In this paper the author summarizes about all the perspectives about the Blockchain in Healthcare domain. The objective of this paper is to categorize the benefits and threat of blockchain technology application in healthcare. It states that Blockchain is a viable technology that helps in data sharing and storing system owing to its decentralization, immutability, transparency, and traceability features. Here, in blockchain network it contains four elements like: Information, Hash of the current block, hash of the former block, and timestamp. Also, the structure for the storing of the data in blockchain has been described here. There is very little information about the threats and benefits of Blockchain technology in healthcare. The paper also states the importance about the security and authorization issues while saving the records of the patients. The main issue related to scalability of blockchain technology was related to the limited rate of processing transactions executed per second in the network, as reported. The paper mainly focused on patient related benefits and organizational benefits. organizational threats were mostly related to interoperability issues, lack of technical skill for integrating pharmaceutical supplies, installation and transaction costs.

**[2]. L. Soltanisehat, R. Alizadeh, H. Hao and K. - K. R. Choo, "Technical, Temporal, and Spatial Research Challenges and Opportunities in Blockchain-Based Healthcare: A Systematic Literature Review," in IEEE Transactions on Engineering Management.**

Discusses how Blockchain can be used to build a peer-to-peer, secure, and smart transaction system especially for the development of healthcare system. Currently the world trends have shifted from patient/health centred to eHealth centred. The Existing healthcare systems face challenges such as interoperability, delays in process and diagnosis, delays in sharing information, the high cost of operation and processes, time- consuming insurance processes and costs, privacy, security, data ownership, and control. Blockchain provides a robust and decentralized application which enables more security and control over the authorization. This paper aims to depict the technical, temporal, and spatial development of blockchain-based healthcare research by analysing recent progress in designing and implementing blockchainbased systems in various healthcare domains, comprehensive. This paper involves medical data management, interoperability, and consolidated healthcare, pharmaceutical supply chain (PSC), organ transplantation and blood donation, clinical trial and medical research, health insurance, and others. In fact, some of the identified categories share similar type of processes and applications of blockchain. Most of the application articles are focused on EHR and medical research/clinical trial domains.

The three popular consensus algorithms used by the developed applications. The Ethereum platform and Hyperledger is used for the implementation of the designed blockchain-based systems in most of the application articles. Currently, the major challenges faced by healthcare data management are security, interoperability of data, and incompatibility of EMRs.

**[3]. L. Ismail, H. Materwala and S. Zeadally, Lightweight Blockchain for Healthcare, in IEEE Access, vol. 7, pp. 149935-149951, 2019.**

The enormous potential for healthcare data management to deliver more precise and economical patient care has attracted a lot of attention in recent years. Single point of failure, data privacy, centralized data stewardship, system vulnerability, and traditional client-server and cloud-based healthcare data management systems are all problems. Blockchains replication mechanism, privacy, and security features have a bright future in the healthcare industry since they can address several problems with the health management system. However, the majority of current blockchain research in the healthcare industry has mostly concentrated on the permission-less Bitcoin network, which has issues including high energy consumption, constrained scalability, and slow transaction throughput. In order to meet the needs of the healthcare domain, a scalable, fault- tolerant, secure, traceable, and private blockchain is required. We suggest a lightweight blockchain architecture for managing healthcare data that, in comparison to the Bitcoin network, lowers computational and communication cost by grouping network users into clusters and keeping one copy of the ledger per cluster. Our architecture involves the use of canal, which enables private and secure communication among network participants. In addition, we suggest a way to prevent forking, which is a common occurrence in the Bitcoin networks. By examining various threats and assaults, we show how well our suggested architecture protects users’ privacy and security when compared to the Bitcoin network. We also go through how the threats identified are addressed by our suggested architecture. Our test results show that as the number of blocks rises, our suggested architecture generates 11 times less network bandwidth than the Bitcoin network. We update our ledger 1.13 times quicker. When the number of nodes is increased, our architecture exhibits a 67% improvement in ledger update speed and 10 times decrease in network traffic.

**[4]. B. Alamri, K. Crowley and I. Richardson, Blockchain-Based Identity Management Systems in Health IoT: A Systematic Review, in IEEE Access, vol. 10, pp. 59612-59629,2022**

Any information system, including healthcare information systems, needs Identity and Access Management (IAM) solutions. Due to the amount and sensitivity of health data, attackers target health IoT (HIoT) applications. IAM systems for HIoT must be created using strict guidelines and solid frameworks. A popular emerging technology for creating decentralized IAM solutions is blockchain (BC). Despite the current attention given to the integration of BC in HIoT for the purpose of presenting IAM solutions, BC is a developing technology that requires careful consideration before being used for IAM solutions in HIoT applications. In order to look into the security aspect of BC-based IAM systems in HIoT applications, a thorough literature analysis was done. This review includes 24 papers that met the criteria for inclusion and were found to be of high quality. In order to better understand the IAM system architecture, security requirements, and threats, we looked into BC-based solutions in HIoT applications. In HIoT, we outlined the key elements and technological advancements of conventional BC- based IAM systems as well as the layered architecture of these systems. The security threats and requirements were therefore summed up. Our thorough research reveals that BC-based IAM in HIoT

systems lacks a thorough security architecture, risk assessments, and security and functional performance evaluation criteria.

**[5]. S. Yongjoh, C. So-In, P. Kompunt, P. Muneesawang and R. I. Morien, "Development of an Internet-of-Healthcare System Using Blockchain," in IEEE Access, vol. 9, pp. 113017-113031, 2021**

In this paper the author summarizes about Internet-of-Healthcare System which is highly distributed special emulation of the Internet of Things technology. Here they gather patient’s medical data sourced from the participating hospitals are integrated with a decentralized storage system using blockchain technology to provide the highest level of storage and access security possible, overcoming the security and data administration problems that may occur at the local hospital level where the patient data is stored within the hospital’s central server, especially if that data is subjected to external threats. Here they describe difference between IoT and IoHCS (Internet-of-Health-Care- Systems) which is that IoT devices are addressed by an IP, and usually exchange a single interaction or single command or item of data whereas the IoHCS presents a canonical interface to the Internet by software agents, or web agents, which have an IP address, and exchange complex data. They have used blockchain as it has strong hold in security. In a blockchain, each block of data contains a hash of its previous block which can link all blocks together to form a chain of blocks in the order of their arrival in the blockchain. Any change to the data in a block will result in a different hash value being generated. In their NU medical Application, the staff can search by taking a photo of a patient/ citizen PID card or entering the patient PID directly and if the staff is permitted to search and access the patient information, they will be prompt with the alert for the staff to confirm. The staff needs to accept and confirm the privacy policy. The first page of the search result is the patient general information page and the staff can take a look for more medical information via the Medical Information menu button.

**[6]. S. S. Akash and M. S. Ferdous, "A Blockchain Based System for Healthcare Digital Twin," in IEEE Access, vol. 10, pp. 50523-50547, 2022.**

In this paper the author summarizes about Digital Twin which is emerging technology that replicates any physical phenomenon from a physical space to a digital space in congruence with the physical state. As there was also security and privacy concerns as healthcare data is very sensitive and can be used in malicious ways. They have decided to use blockchain technology to store data from Registration, Login, Health state query and also for sharing that data. The DT (Digital Twin) stands for the representation of the anatomy of a digital asset in a digital space which is the depiction of a physical phenomenon from a physical space. Here author also talks about Public Block Chain. A public blockchain allows anyone to

participate in creating and validating blocks as well as write data on the blockchain. A public blockchain has no restriction over nodes, for this reason it is also called a permissionless blockchain. Whereas, A private blockchain is permissioned and only a predefined set of entities can take part in the validation process. Such a blockchain has no concern of energy consumption and renders enough security. In this project they have used smart contracts. Smart contracts are computer programs that are deployed within

a blockchain platform and can be executed on distributed networks among distrusted entities. It translates real life contractual conditions into executable computer codes, integrates them with digital assets, and can run autonomously without any trusted authority.

**[7]. Xia, Qi, Emmanuel Boateng Sifah, Kwame Omono Asamoah, Jianbin Gao, Xiaojiang Du and Mohsen Guizani. “MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain.” IEEE Access 5 (2017): 14757-14767.**

In this paper they have given the name “MeDShare” to their proposed system. This system addresses the issue of medical data sharing among medical custodians in trust level environment. This system is based on blockchain provide auditing and control for shared medical data in cloud repository. They monitor entities that access data maliciously use from data custodian system. Data sharing, data transition all action is perform and recorded in tamper proof manner. They have design smart contract and access control mechanism to track the behavior of the system. By implementing this system cloud service provider and data guardians will be able to achieve data security and auditing while sharing of medical data in minimum risk. Whatever problem are arising while sharing data for that they have some cryptographic methods & provide some of the feasible solution to address the feature of immutability & decentralization. From this paper we conclude that they have design data sharing model between cloud service provider using blockchain. It uses smart contract and access control mechanism to trace behavior of the data as well as revoke the access of data. By implementing this system, they able to securely achieve data security among other cloud service provider without any risk on the data privacy.

**[8]. K. Azbeg, O. Ouchetto, S.J. Andaloussi, L. Fetjah, A Taxonomic Review of the Use of IoT and Blockchain in Healthcare Applications, IRBM, Volume 43, Issue 5, 2022, ISSN 1959-0318,**

This research paper is mainly focuses on categorizing the use cases of IoT and blockchain in the healthcare sector. And investigates the challenges associated with the adoption of the blockchain technology in healthcare IoT-based system and some of the existing solution. It also introduces some future directions. The survey of the use cases of IoT and blockchain in the healthcare sector will serve as a state for future researches. And it could also be help to revolutionize the healthcare sector by using other technologies such as artificial intelligence, big data & cloud computing. This system also represents the taxonomic review regarding the use of IoT devices and wearables created for healthcare & medical purpose is growing fast day by day. This device can be connected to the internet and able to collect health data, analyze it & share it with medical team. The paper is mainly highlights on different challenges facing the integration of blockchain in healthcare IoT-based system & some existing solutions.

**CHAPTER 03**

**SYSTEM REQUIREMENT**

**3.1 ASSUMPTIONS AND DEPENDENCIES**

1. Assumptions:
   * 1. The system must have enough computation power to work the application User should have all the software and library install to run this application.
2. Dependencies:
   * 1. The web project needs web3.js and MetaMask account to run.

**3.2 FUNCTIONAL REQUIREMENTS**

1. Functional Requirements mainly deal with something that the system should do. They specify the behavior or function of the system. Our system has a function that exclusively works towards storing data very securely using blockchain technology
2. The data provided by the user will be stored in DAO/Blockchain in encrypted format. The documents will be in photocopy. The input image must be well lit image with low exposure to yield the best possible results.

**3.3 EXTERNAL INTERFACE REQUIREMENTS**

**3.3.1 User Interfaces**

For User Interface we have used REACT which integrates well with Blockchain. The home screen will compromise of an option which says upload file image and then submit button. Once the file is submitted it will be stored in DAO/Blockchain. Once the file is submitted the final output screen will show the author image that was given as an input.

**3.3.2** **Hardware Requirements**

1. Processor - Intel I5 core
2. Speed - 3.20 GHz RAM - 8 GB (min)
3. Hard Disk - 400GB
4. Display Screen

**3.3.3 Software Interfaces**

For software interface we have used Visual Code. It supports all the libraries related to React.

**3.3.4 Communication Interfaces**

1. **Blockchain Network Interface:** This interface is used to connect the Dapp with the blockchain network. It allows the Dapp to access blockchain functionality, such as the ability to store and retrieve data securely.
2. **Smart Contract Interface:** Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. The Smart Contract Interface enables the Dapp to interact with smart contracts, which are used to automate certain processes, such as payment processing or insurance claims processing.
3. **Patient Interface:** This interface enables patients to interact with the Dapp, such as providing consent to share their medical data or viewing their medical records. The interface should be user-friendly and easy to use, even for patients who are not technically savvy.
4. **Doctor Interface:** This interface is used by doctors to access patient data, update patient records, and communicate with other providers like medicine. It should be designed to facilitate efficient and accurate communication between providers and support the delivery of high-quality care.

* 1. **NON -FUNCTIONAL REQUIREMENTS**

**3.4.1 Performance Requirement**

1. **Security:** Blockchain-based healthcare DApps must prioritize security. The blockchain technology itself offers an excellent level of security due to its decentralized nature, but developers should still implement additional security measures such as encryption, access control, and smart contracts.
2. **Privacy:** Healthcare DApps must prioritize the privacy of patient data. Developers should implement encryption, secure access control, and other privacy-enhancing technologies to protect patient data.
3. **Scalability:** Healthcare DApps must be scalable to handle a large number of users, transactions, and data. Developers should focus on optimizing the blockchain consensus protocol and transaction processing algorithms to ensure scalability.
4. **Speed:** Blockchain-based healthcare DApp must have a fast-processing time to provide real-time services. Developers should focus on reducing the time taken for transaction processing, network latency, and other factors that could impact the speed of the DApp.
5. **Interoperability:** Healthcare DApps must be interoperable to ensure seamless integration with other healthcare systems and technologies. Developers should focus on creating standardized interfaces and protocols for easy integration with other healthcare systems.

**3.4.2 Safety Requirements**

1. **Data security:** The safety of patient data is the most critical safety requirement. Blockchain technology can ensure data security by encrypting and decentralizing data storage. Additionally, it is necessary to implement strong access control mechanisms to protect data from unauthorized access.
2. **User privacy:** Privacy is a crucial safety requirement in the healthcare sector. Patient data must be kept confidential, and only authorized individuals should be granted access to it. Smart healthcare DApp must have privacy mechanisms built-in to protect users' sensitive information.

1. **Auditability:** It is necessary to have a mechanism to audit the smart healthcare DApp's transactions to maintain accountability and transparency. The blockchain technology's distributed ledger system enables auditing, making it easy to trace all transactions.
2. **Interoperability:** The smart healthcare DApp must be designed to interact with other systems seamlessly. This is particularly important in the healthcare industry where different systems need to exchange information to provide the best care.
3. **Scalability:** The smart healthcare DApp must be scalable to accommodate a growing number of users and healthcare providers. The blockchain technology's distributed ledger system makes it easy to scale the DApp by adding more nodes to the network.

**3.4.3 Security Requirements**

1. **Distributed ledger technology:** Distributed ledger technology is a core security requirement for smart healthcare DApp in blockchain. It involves the use of a distributed database that stores information across a network of nodes, making it resistant to tampering and hacking.
2. **Smart contract security:** Smart contract security is an essential security requirement for smart healthcare DApp in blockchain. Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. They can automate the execution of transactions without the need for intermediaries. Smart contracts should be audited and tested thoroughly to prevent any bugs or vulnerabilities.
3. **Encryption:** Encryption is a fundamental security requirement for smart healthcare DApp in blockchain. It involves converting sensitive data into an unreadable format that can only be decrypted with a secret key. Strong encryption algorithms should be used to secure data in transit and at rest.
4. **Access control:** Access control is a crucial security requirement for smart healthcare DApp in blockchain. It involves verifying the identity of users and granting them the appropriate level of access to the system. Access control mechanisms such as multi-factor authentication, role-based access control, and biometric authentication should be implemented.
5. **Secure communication protocols:** Secure communication protocols are a vital security requirement for smart healthcare DApp in blockchain. Communication between nodes in the network should be encrypted using secure communication protocols such as SSL/TLS to prevent eavesdropping or interception.
   * 1. **Software Quality Attributes**
6. The software is reliable as it can sustain under any given conditions. It consistently gives correct result.
7. It is maintainable in nature a new code can be easily added and integrated with the existing code.
8. It is modular in nature therefore correcting defects also becomes feasible and cost-effective.
9. It can be tested with ease and is also flexible with modifications and upgrades.

**3.5 SYSTEM REQUIREMENTS**

**3.5.1 Software Requirement:**

* 1. OS (Windows/Linux)
  2. 4Gb ram or above
  3. Python 3.0 or above
  4. React IDLE or any platform supporting React.
  5. Libraries to be installed:
  6. WEB3.js
  7. React Library
     1. **Hardware Requirement:**
     2. Processor - Intel I5 core
     3. Speed - 3.20 GHz RAM - 8 GB (min)
     4. Hard Disk - 400GB
     5. Display Screen

**3.6 ANALYSIS MODEL: SDLC MODEL**

The SDLC model that we have applied while working on this project is the incremental model.

1. **Requirement gathering & analysis:** In this phase, requirements are gathered from customers and checked by the analyst, to ensure if the requirements can be fulfilled or not. Analyst checks the need will achieve within budget or not.
2. **Design:** In the design phase, the design team designs different diagrams like Data Flow diagram, use case diagram, activity diagram, class diagram, state transition diagram, etc.
3. **Implementation:** In this phase, the requirements are coded using suitable language and transformed into computer programs which are called Software.
4. **Testing:** After completing the implementation phase, the software is tested using different test methods and testing tools. The methods like white box, black box, and gray box testing methods are used.
5. **Deployment:** After completing all the above phases, the software is deployed.
6. **Review:** In the review phase, after the software deployment, the behavior and validity of the developed product are checked. And if any error is found then, the SDLC process starts again from the first phase.
7. **Maintenance:** In this phase, after deployment of the software in the working environment there may raise a few bugs, or errors. Also, the customer may require new updates to the product. Maintenance involves debugging and new additional options.

Requirements

Design & development

Design & development

Design & development

Design & development

Design & development

Design & development

Implementation

Implementation

Implementation

**Figure 3.6: Incremental model**

As shown in above figure 3.6 the project follows the Incremental process model for early development of the project. As we know incremental model is an iterative process model that divides the software development into submodules helps to identify and correct the defect as early as possible.

**CHAPTER 04**

**SYSTEM DESIGN**

* 1. **SYSTEM ARCHITECTURE**

Hospital

Patient

Blockchain

Storage

Goes to

Pharma

Company

Medicals

Providee

Blockchain Storage

DAO

Take Medicine

DAO

**Figure 4.1: Block Diagram**

As shown in above figure 4.1 block diagram shows the system flow of smart healthcare dapp project. Namely it consist of four main modules like Hospital, patient, medicals and pharma company. System is developed in blockchain technology so it is completely decentralized means there is no central authority. And completely secure. Which is mainly useful to store the patient details securely.

* 1. **MATHEMATICAL MODEL**

**4.2.1 What Is a Merkle Tree?**

1. Merkle trees, also known as Binary hash trees, are a prevalent sort of [data structure](https://www.simplilearn.com/tutorials/data-structure-tutorial/what-is-data-structure) in computer science.
2. In [bitcoin](https://www.simplilearn.com/bitcoin-digital-currency-article) and other [cryptocurrencies](https://www.simplilearn.com/tutorials/blockchain-tutorial/what-is-cryptocurrency), they're used to encrypt blockchain data more efficiently and securely.
3. It's a mathematical data structure made up of hashes of various data blocks that summarize all the transactions in a block.
4. It also enables quick and secure content verification across big datasets and verifies the consistency and content of the data.

H( )

H( )

H( )

H( )

H( )

H( )

H( )

T

T

T

T

Mercle root

Non-leaf node

Leaf root

H( ) : Hash value

T : Transaction

### 

**Figure 4.2.1 Merkle Tree**

### 4.2.2 How Do Merkle Trees Work?

1. A Merkle tree is constructed from the leaf nodes level all the way up to the Merkle root level by grouping nodes in pairs and calculating the hash of each pair of nodes in that particular level. This hash value is propagated to the next level. This is a bottom-to-uptype of construction where the hash values are flowing from down to up direction.
2. Hence, by comparing the Merkle tree structure to a regular binary tree data structure, one can observe that Merkle trees are actually inverted down.

A

B

C

D

E

F

G

Top to Bottom

Binary Tree

Habcd=H(H(ab)+H(cd)+H(cd))

Hab=H(H(a)+H(b))

Hcd=H((c)+H(d))

H(a)

H(b)

H(c)

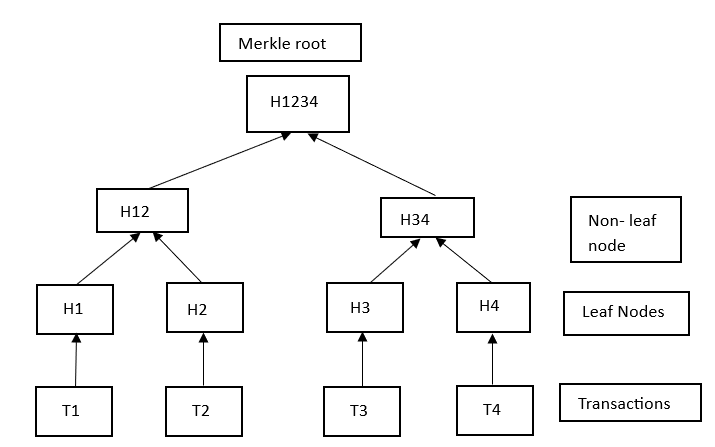
H(d)

Inverted(bottom to top)

Merkle Tree

**Figure 4.2.2 Binary tree direction vs Merkle tree direction**

**Example: Consider a block having 4 transactions- T1, T2, T3, T4. These four transactions have to be stored in the Merkle tree and this is done by the following steps-**



**Step 1:** The hash of each transaction is computed.

H1 = Hash(T1).

**Step 2:** The hashes computed are stored in leaf nodes of the Merkle tree.

**Step 3:** Now non-leaf nodes will be formed. In order to form these nodes, leaf nodes will be paired together from left to right, and the hash of these pairs will be calculated. Firstly hash of H1 and H2 will be computed to form H12. Similarly, H34 is computed. Values H12 and H34 are parent nodes of H1, H2, and H3, H4 respectively. These are non-leaf nodes.

H12 = Hash(H1 + H2)

H34 = Hash(H3 + H4)

**Step 4:** Finally H1234 is computed by pairing H12 and H34. H1234 is the only hash remaining. This means we have reached the root node and therefore H1234 is the Merkle root.

H1234 = Hash(H12 + H34)

* 1. **DATA FLOW DIAGRAM**
     1. **DFD level 0**

Smart Healthcare DAPP

Hospital

Pharma Company

Medicine

Patient

**Figure 4.3.1 DFD level 0**

As shown is above figure 4.3.1 DFD level 0 which is a data flow diagram of level 0 which shows us the basic overview of the whole system for analyzing purpose. Smart healthcare dapp consist of four modules like hospital, patient, medicine, pharma company. These modules are closely interlinked with each other to store the data securely.

* + 1. **DFD level 1**

Smart Healthcare DAPP

Hospital

Patient

Medicals

Pharma Company

Handle All Patients Data

Use Medical & Prescription Details

Handle all the details of medicine of particular patients

Handle Pharma Company details & medicine details

**Figure 4.3.2 DFD level 1**

As shown in above figure 4.3.2 DFD level 1 which is data flow diagram level 1 which shows us the details overview of the system than the level 0 diagram. Which shows the different modules present in the system and their particular operation of each single module.

* 1. **UML DIAGRAM**

**4.4.1 Activity Diagram**

Add Data

Patient

Medical

Hospital

DAO Part

Verify Medicine

See Patient Medicine

Add Data

Display Data

Mine Block And verify DAO

Patient Blockchain

DOA For Doctors

Medicine Details

Users

Features

Database

Security Layer

Pharma Company

Add Data

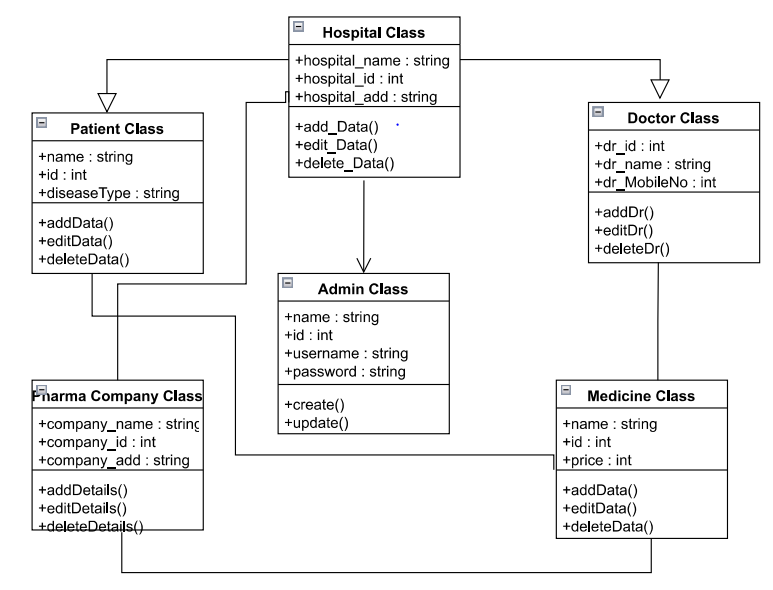
Verify data Medicine

Pharma Details

**Figure 4.4.1 Activity Diagram**

As shown in above figure 4.4.1 Activity diagram which represents a flow from one activity to another activity. In this figure shows the system structure of project from user interface to database, & it shows how system get flow from top to bottom and show the working of different modulus at particular layer.

* + 1. **Class Diagram**

**Figure 4.4.2 Class Diagram**

As shown is above figure 4.4.2 class diagram shows the relationship between different modules of the system. In this figure there are different classes are present like hospital, patient, pharma company, doctor. This class diagram shows the different attribute and operation of the class also the constraints imposed on the system.

* + 1. **State chart Diagram**

Admin

Hospital

Pharma Company

Doctor

Medicine

Patient

Start

Stop

**Figure 4.4.3 State chart Diagram**

As shown in above figure 4.4.3 State chart diagram shows the abstract description of the behavior of the system. As shown in above diagram different modules are there. they show the analytical behavior of the system.

**CHAPTER 05**

**PROJECT PLAN**

**5.1 PROJECT ESTIMATE**

We have made metric of some of the factors which will be directly involved in the project, called Project metric such as cost, time. Process metrics will be helpful to measure the quality of the product that is produced. These metrics can be analyzed to provide indicators for guide management and technical actions.

**5.1.1 Reconciled Estimate:**

|  |  |  |
| --- | --- | --- |
| Sr No | Hardware/Software | Quantity |
| 1. | Test Network Ether, web3.js , React js | 1 |
| 2. | Windows 10 OS | 1 |

**5.1.2 Project Resources**

1. **Project Manager:** A project manager is responsible for overseeing the entire project, ensuring that it is delivered on time, within budget, and meets the quality standards. The project manager should have experience in managing software development projects and knowledge of blockchain technology.
2. **Blockchain Developer:** A blockchain developer is responsible for developing and implementing the blockchain technology, such as creating smart contracts and integrating them into the system. The developer should have experience in blockchain development, cryptography, and smart contract programming.
3. **Front-end Developer:** A front-end developer is responsible for developing the user interface and user experience of the DApp. The developer should have experience in HTML, CSS, JavaScript, and front-end frameworks such as React or Angular.
4. **Back-end Developer:** A back-end developer is responsible for developing the server-side of the DApp. The developer should have experience in programming languages such as Java, Python, or Node.js, and knowledge of server-side frameworks such as Express or Spring.
5. **Quality Assurance Engineer:** A quality assurance engineer is responsible for testing the DApp for functionality, security, and performance. The engineer should have experience in software testing, knowledge of testing frameworks such as Selenium or Appium, and knowledge of security testing techniques.
6. **Security Engineer:** A security engineer is responsible for ensuring the security of the DApp, such as implementing encryption, access control, and secure communication protocols. The engineer should have experience in cybersecurity, cryptography, and knowledge of security frameworks such as OWASP.
7. **Technical Writer:** A technical writer is responsible for creating the documentation for the DApp, such as user manuals, developer guides, and API documentation. The writer should have experience in technical writing and knowledge of the DApp and blockchain technology.

**5.2 RISK MANAGEMENT**

**5.2.1 Risk Identification**

1. **Data Privacy and Security Risks:** One of the most significant risks associated with implementing a blockchain-based healthcare Dapp is the potential for data privacy and security breaches. Healthcare data is highly sensitive, and any unauthorized access or disclosure could have serious consequences. The Dapp should be designed with robust security protocols, such as multi-factor authentication and encryption, to prevent unauthorized access and protect patient data.
2. **Smart Contract Risks:** Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. While they offer many benefits, smart contracts also introduce new risks, such as bugs, errors, or vulnerabilities in the code. These risks can potentially compromise the integrity of the Dapp, so it is essential to thoroughly test smart contracts before deploying them to the blockchain network.
3. **Blockchain Network Risks:** Blockchain networks are decentralized, which means that they are not controlled by a single entity. While this provides many benefits, it also introduces new risks, such as network congestion, transaction delays, or malicious attacks. These risks can potentially impact the functionality and security of the Dapp, so it is important to choose a reliable and secure blockchain network and implement appropriate measures to manage network risks.
4. **Adoption Risks:** Finally, a SMART healthcare Dapp based on blockchain may face adoption risks, as healthcare providers and patients may be resistant to change or unfamiliar with blockchain technology. Adequate training and education will be required to ensure that all stakeholders are comfortable using the Dapp and understand its benefits.

**5.2.2 Risk Analysis**

1. **Blockchain Network Risks:** Blockchain networks are decentralized, which means that they are not controlled by a single entity. While this provides many benefits, it also introduces new risks, such as network congestion, transaction delays, or malicious attacks. These risks can potentially impact the functionality and security of the Dapp, so it is important to choose a reliable and secure blockchain network and implement appropriate measures to manage network risks.
2. **Smart Contract Risks:** Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. While they offer many benefits, smart contracts also introduce new risks, such as bugs, errors, or vulnerabilities in the code. These risks can potentially compromise the integrity of the Dapp, so it is essential to thoroughly test smart contracts before deploying them to the blockchain network.
3. **Data Privacy and Security Risks:** One of the most significant risks associated with implementing a blockchain-based healthcare Dapp is the potential for data privacy and security breaches. Healthcare data is highly sensitive, and any unauthorized access or disclosure could have serious consequences. The Dapp should be designed with robust security protocols, such as multi-factor authentication and encryption, to prevent unauthorized access and protect patient data.
4. **Adoption Risks:** Finally, a SMART healthcare Dapp based on blockchain may face adoption risks, as healthcare providers and patients may be resistant to change or unfamiliar with blockchain technology. Adequate training and education will be required to ensure that all stakeholders are comfortable using the Dapp and understand its benefits.

**5.2.3 Overview of Risk Mitigation, Monitoring, Management**

1. **Risk Mitigation:** To mitigate risks, organizations should take proactive measures to address potential risks before they can become an issue. This may include implementing robust security protocols, conducting regular audits, and designing the Dapp to comply with relevant regulations. It is also important to design the Dapp to be easily upgradable, enabling quick fixes to any issues that arise.
2. **Risk Monitoring:** Risk monitoring involves regularly monitoring the Dapp for any potential risks or vulnerabilities. This may include conducting regular security audits, monitoring network performance, and tracking compliance with relevant regulations. Any identified risks or issues should be promptly addressed to minimize their impact.
3. **Risk Management:** Risk management involves establishing processes to manage risks as they arise. This may include incident response plans, disaster recovery plans, and business continuity plans. It is important to ensure that all stakeholders are aware of these plans and know what to do in the event of a security incident or other risk.

**5.3 PROJECT SCHEDULE**

**5.3.1 Project Task Set**

Major Tasks in the Project stages are:

Task 1: Requirement Analysis (Base Paper Explanation).

Task 2: Project Specification (Paperwork).

Task 3: Technology Study and Design.

Task 4: Coding and Implementation (Module Development).

**5.3.2 Task Network**

Individual tasks and subtasks have interdependencies based on their sequence. A task network is a graphic representation of the task flow for a project. Project tasks and their dependencies are noted.

**5.3.3 Timeline Chart**

|  |  |  |
| --- | --- | --- |
| **Schedule** |  | **Project Activity** |
| July | 1st week | Formation of Project Group |
| 2nd week | Project Topic Selection |
| 3rd week | Synopsis Submission |
| August | 1st week | Presentation on Project Ideas |
| 2nd week | Submission of Literature Survey |
| 3rd week | Feasibility Assessment |
| September | 1st week | Mid Sem Presentation |
| 2nd week | Mathematical model finalization |
| 4th week | End Sem Presentation |
| October | 1st week | Report Preparation and Submission |
| December | 4th week | 1st Module presentation |
| January | 1st week | Discussion about further strategy of  developing Prototype |
| 2nd week | 2nd Module Implementation followed by presentation |
| February | 3rd week | Design test cases for module |
| 4th week | Developing User Interface |
| March | 2nd week | Integration all modules including interactive GUI |

**Table 5.2.3 Timeline**

**5.4 TEAM ORGANIZATION**

**5.4.1 Team Structure**

**Project Guide Name:** Prof. P. R. Patil

**Group Members:** Sneha Patil

Sakshi S. Patil

Sakshi R. Patil

Rhushabh Pethkar

**5.4.2 Management Reporting & Communication**

1. **Establish a communication plan:** Develop communication plan that outlines how team members will communicate with each other, how often communication will occur, and what channels will be used for communication. This plan should also include guidelines for sharing updates, feedback, and progress reports.
2. **Schedule regular meetings:** Schedule regular team meetings to discuss progress, resolve issues, and provide updates. These meetings can be conducted in person or virtually, depending on the location of team members.
3. **Establish clear reporting lines:** Define reporting lines to ensure that team members know who to report to and how to escalate issues. This will help prevent confusion and ensure that issues are resolved quickly.
4. **Develop progress reports:** Develop progress reports that summarize the status of the project and highlight any issues or challenges. These reports can be shared with guides and used to track progress against key milestones.
5. **Share updates with project guide:** Share regular updates with project guide, including designing, development of the project. It will help to overcome the challenges in the project.

**CHAPTER 06**

**PROJECT IMPLEMENTATION**

**6.1 OVERVIEW OF PROJECT MODULES**

1. **Module Hospital:** Hospitals must submit request to our system for being the part of DAO.After Verification Hospitals will be able to add patient data on the blockchain network.Hospitals must buy the tokens which are created on ERC20. Using Token hospitals can access the data and store.
2. **Module Patient:** Once patient data is stored on the blockchain, patient can access the data from the web application. To access the data patient will have to provide they private key. Only using the private key, the data can be access. Patient data like all medical history will be accessed and stored.
3. **Module Medicals**: Medicals will be able to access the pharma company data and check all the process and required data of medicine if they are trustworthy or not. Medicals can verify before adding them to stock. Medicals will be able to see the patient required medicines and can provide the medicines as per that.
4. **Module Pharma Company**: Pharma company will be able to store the data of their company and also the medicines made by them. Before being the part of system pharma companies have to be the part of DAO system.

**6.2 TOOLS & TECHNOLOGIES USED**

1. **Blockchain Platforms:** Blockchain platforms like Ethereum, Hyperledger, and Corda are used to develop the underlying blockchain infrastructure that powers the smart healthcare DApp. These platforms provide a secure and decentralized framework for managing transactions, data storage, and access control.
2. **Smart Contracts:** Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. Smart contracts are used to automate various processes in the smart healthcare DApp, such as patient record management, prescription management, and medical billing.
3. **Web Development Frameworks:** Web development frameworks like React, Angular, and Vue.js are used to develop the front-end of the smart healthcare DApp. These frameworks provide a fast and efficient way to build user interfaces and create responsive web applications.
4. **Security Tools:** Security tools like Metamask, Solidity, and Truffle are used to ensure the security and integrity of the smart healthcare DApp. These tools provide secure ways to manage user authentication, data encryption, and code verification.
5. **Backend Technologies:** Backend technologies like Node.js, react are used to develop the server-side of the smart healthcare DApp. These technologies provide a scalable and efficient way to manage data storage, handle user authentication, and manage API requests.

**6.3 ALGORITHM DETAILS**

**1 Module Hospital**

**Step 1** - Hospitals must submit request to our system for being the part of DAO.

**Step 2** - After Verification Hospitals will be able to add patient data on the blockchain network.

**Step 3** - Hospitals must buy the tokens which are created on ERC20.

**Step 4** - Using Token hospitals can access the data and store.

**2 Module Patient**

**Step 1** - Once patient data is stored on the blockchain, patient can access the data from the web application.

**Step 2** - To access the data patient will have to provide they private key.

**Step 3** - Only using the private key, the data can be access.

**Step 4** - Patient data like all medical history will be accessed and stored.

**3 Module Medicals**

**Step 1** Medicals will be able to access the pharma company data and check all the process and required data of medicine if they are trustworthy or not.

**Step 2** Medicals can verify before adding them to stock.

**Step 3** Medicals will be able to see the patient required medicines and can provide the medicines as per that.

**4 Module Pharma Company**

**Step 1** - Pharma company will be able to store the data of their company and also the medicines made by them.

**Step 2 -** Before being the part of system pharma companies have to be the part of DAO system.

**CHAPTER 07**

**SOFTWARE TESTING**

**7.1 TYPES OF TESTING**

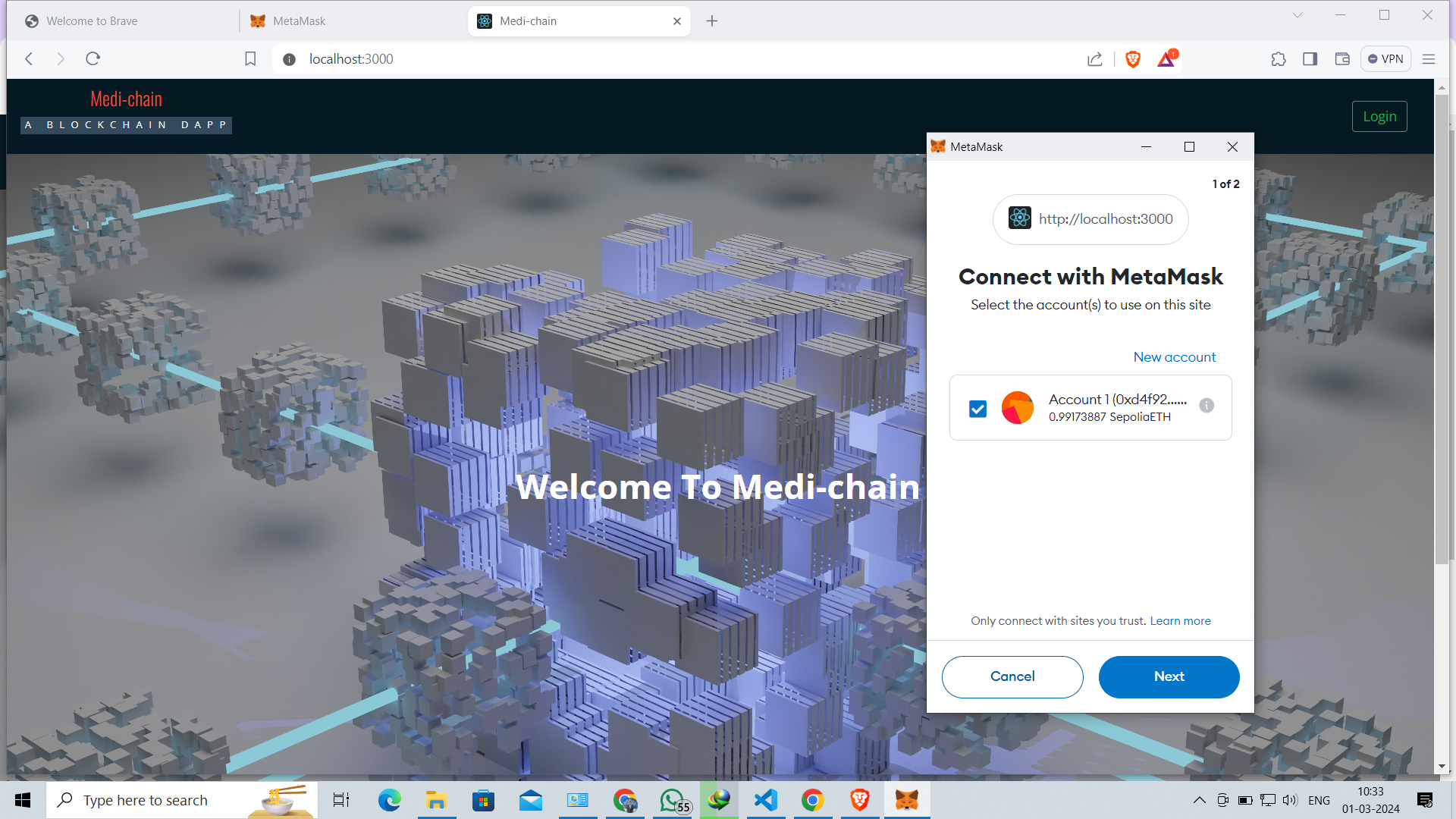
* + 1. **Unit Testing:** This type of testing is used to test individual functions or modules of the DApp. It helps in ensuring that each component of the DApp works as expected.
    2. **Integration Testing:** This type of testing is used to test the interaction between different components of the DApp. It helps in ensuring that the different components work together seamlessly.
    3. **Performance Testing:** This type of testing is used to test the performance of the DApp under different loads and stresses. It helps in ensuring that the DApp can handle the expected number of users and transactions.
    4. **Security Testing:** This type of testing is used to test the security of the DApp. It helps in identifying and fixing any vulnerabilities or weaknesses that could be exploited by attackers.
    5. **User Acceptance Testing:** This type of testing is used to test the DApp's functionality from a user's perspective. It helps in ensuring that the DApp meets the user's expectations and requirements.
  1. **TEST CASES & TEST RESULTS**

1. **User Registration Test Case:**
   1. Test the user registration process to ensure that users can successfully register and log in to the DApp.
   2. Test the validation of user inputs such as email, password, and username.
   3. Test the generation of a unique user ID for each registered user.
2. **Patient Record Test Case:**
3. Test the creation of a new patient record and ensure that all required fields are filled out.
4. Test the validation of patient inputs such as name, birthdate, and medical history.
5. Test the ability to view, edit, and delete patient records.
6. **Blockchain Integration Test Case:**
7. Test the integration of the DApp with the blockchain network.
8. Test the ability to read and write data to the blockchain.
9. Test the security measures implemented to protect the data on the blockchain.
10. **Smart Contract Test Case:**
11. Test the smart contract used in the DApp to ensure that it executes as intended.
12. Test the verification of digital signatures for transactions.
13. Test the handling of exceptions and errors that may occur during contract execution
14. **Security Test Cases:**
15. Test the security measures implemented to protect user data and prevent unauthorized access.
16. Test the validation of user inputs to prevent injection attacks and other types of vulnerabilities.
17. Test the ability to recover data in the event of a security breach.
18. **Performance Test Case**
19. Test the DApp's ability to handle a high volume of users and transactions
20. Test the response time of the DApp for different types of requests
21. Test the scalability of the DApp as the number of users and transactions increases.

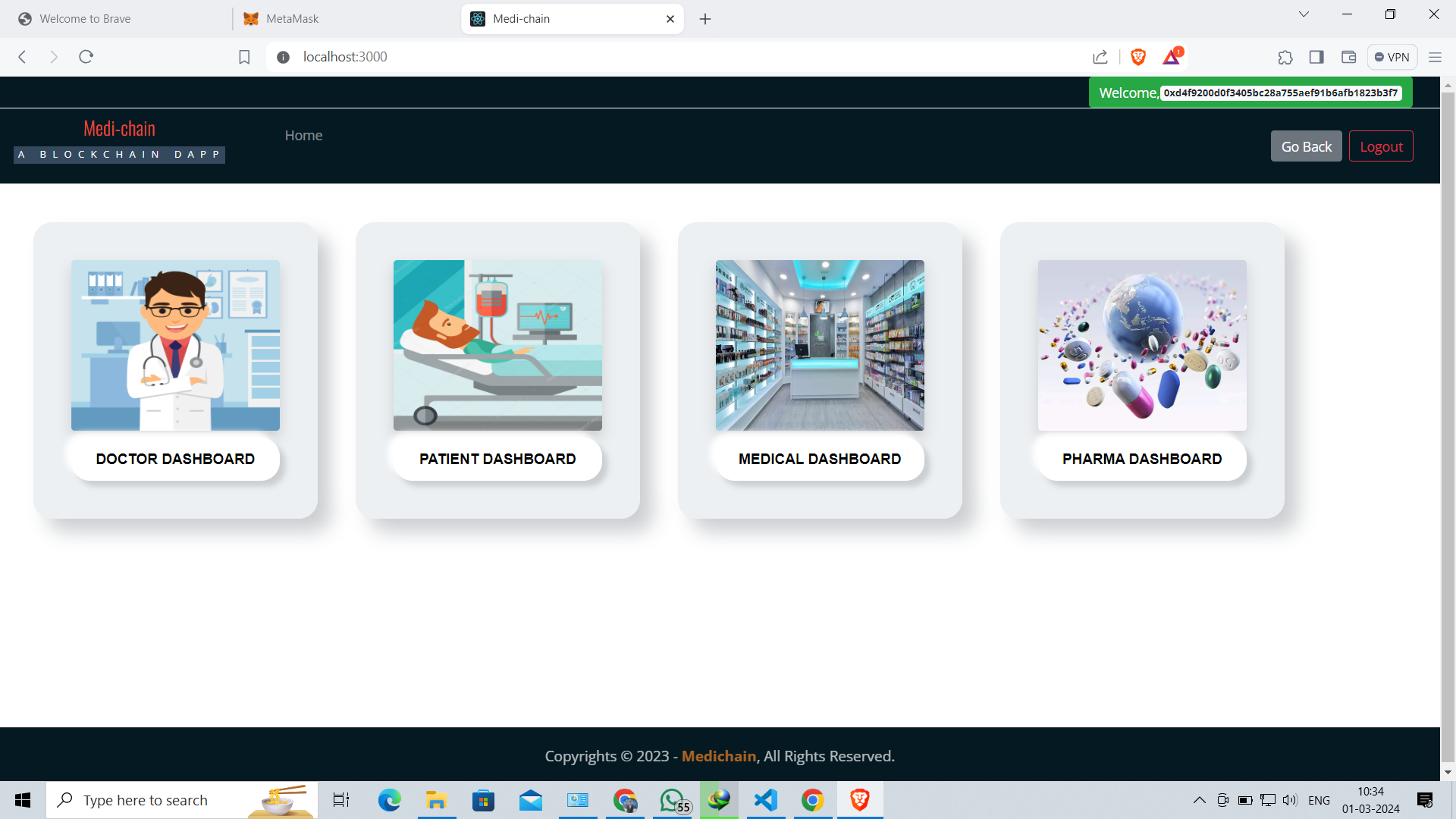
**Test cases**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Test Case Objectives** | **Steps** | **Input** | **Expected Result** | **Actual Result** | **Status** |
| **TC\_1** | **MetaMask Availability** | Click on extension button in your browser and check for MetaMask extension | Click on extension icon in top right corner | MetaMask should be available to connect | MetaMask Available to connect | Pass |
| **TC\_2** | Goerli Test Network in MetaMask | Enable test network option in MetaMask settings.  Click on Network option beside profile and select Goerli test network | Select goerli network from given option | Selected goerli network | Selected goerli network | Pass |
| **TC\_3** | Login using MetaMask credentials | Click on login button | Enter MetaMask ID/Password | Get logged in into Smart Health Chain DApp | Got logged in into Smart Health Chain DApp | Pass |
| **TC\_4** | Check working of Doctor Dashboard Button | Click on Doctor Dashboard Button | Click on Doctor Dashboard Button | Doctor dashboard home page should open | Doctor dashboard home page opened | Pass |
| **TC\_5** | Check working of Doctor Dashboard, “Add yourself and get verified” | Click on Add yourself and get verified | Click on Add yourself and get verified | Doctor information add panel should open | Doctor information add panel opened | Pass |
| **TC\_6** | Check functionality of save button Doctor information add panel | After filling form click on save button in green color | Click on save button | Profile should be created | Profile created | Pass |
| **TC\_7** | Check functionality of clear button Doctor information add panel | After filling form click on clear button in red color | Click on clear button | Form should be cleared | Form cleared | Pass |
| **TC\_8** | Click on home button to check functionality of home button on Doctor information add panel page | Click on Home button | Click on Home button | Home must be page loaded | Home page loaded | Pass |
| **TC\_9** | Check working of View Patient Details Button | Click on View Patient Details Button | Click on View Patient Details Button | View Patient Details Button page should open | View Patient Details Button home page opened | Pass |
| **TC\_10** | Enter Patient ID in Field | Enter Patient ID in Field | Click on search button | Should Display Patient Data | Displayed Patient Data | Pass |
| **TC\_11** | Check working of Clear Button of Patient Information Search Panel | Enter Patient ID in field | Click on clear button | Should clear data from text field | Cleared data from text field | Pass |
| **TC\_12** | Check working of Medical Dashboard Button | Click on Medical Dashboard Button | Click on Medical Dashboard Button | Medical Dashboard home page should open | Medical Dashboard home page opened | Pass |
| **TC\_13** | Check working of Medical Dashboard, “Add yourself and get verified” | Click on Add yourself and get verified | Click on Add yourself and get verified | Medical information add panel should open | Medical information add panel opened | Pass |
| **TC\_14** | Check functionality of save button Medical Information add panel | After filling form click on save button in green color | Click on save button | Profile should be created | Profile created | Pass |
| **TC\_15** | Check working of Pharma Dashboard Button | Click on Pharma Dashboard Button | Click on Pharma Dashboard Button | Pharma Dashboard home page should open | Pharma Dashboard home page opened | Pass |
| **TC\_16** | Check working of Add Medicine and get verified Button | After filling form click on save button in green color | Click on save button | Profile should be created | Profile created | Pass |
| **TC\_17** | Check working of Clear Button of Pharma(Medicine) Information Add Panel | Enter Patient ID in field | Click on clear button | Should clear data from text field | Cleared data from text field | Pass |
| **TC\_18** | Check working of View Verification Medicine Status | Enter Medicine batch ID in Field | Click on search button | Should Display Medicine Batch ID | Displayed Medicine Batch Data | Pass |
| **TC\_19** | Check working of Clear Button of Pharma(Medicine) Information Search Panel | Enter Medicine ID in field | Click on clear button | Should clear data from text field | Cleared data from text field | Pass |
| **TC\_20** | Check working of Logout Button | Click on logout button | Click on logout button | Should logout from site | Open Home page for login | Pass |

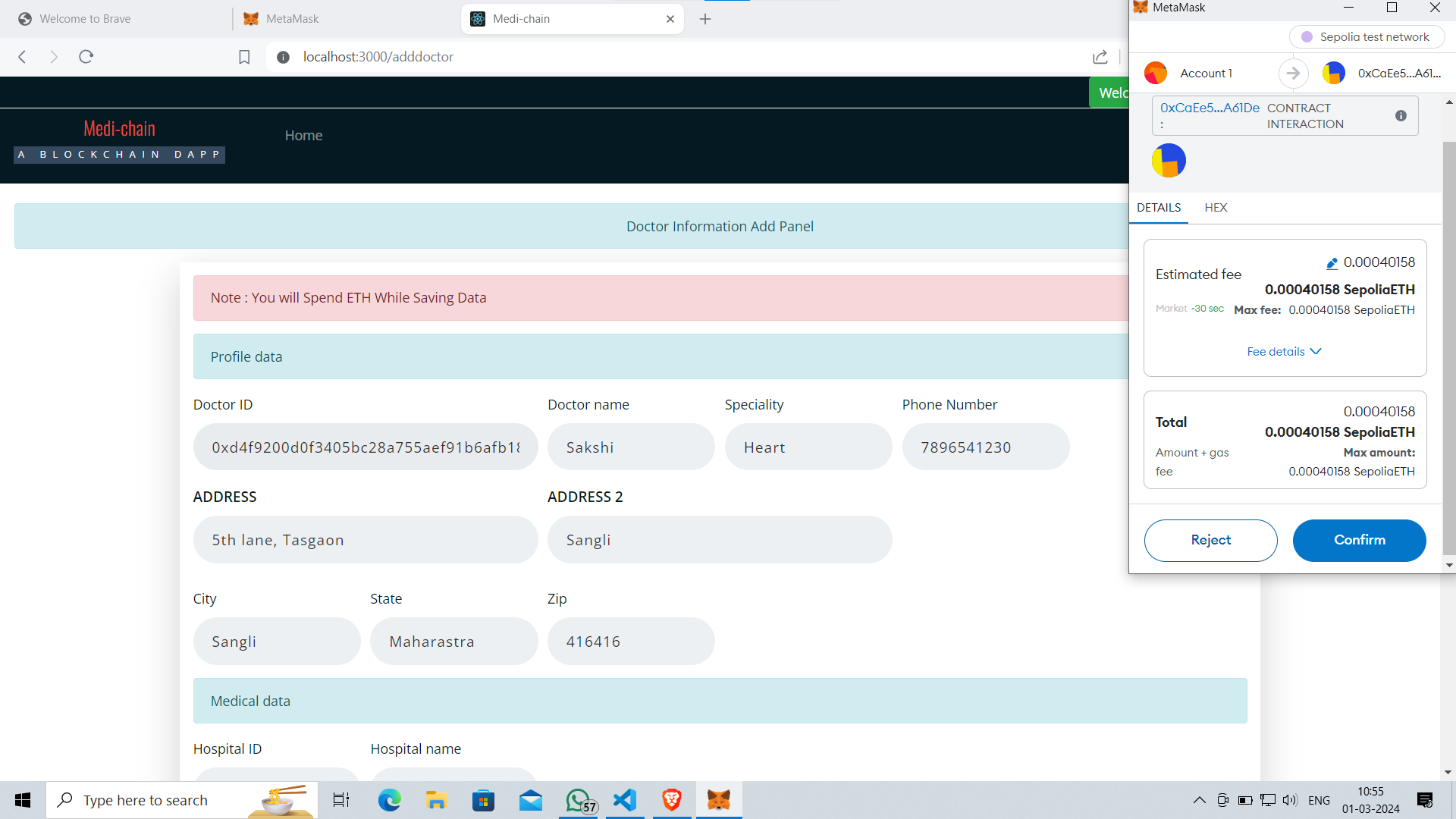
**CHAPTER 08**

**RESULTS: **

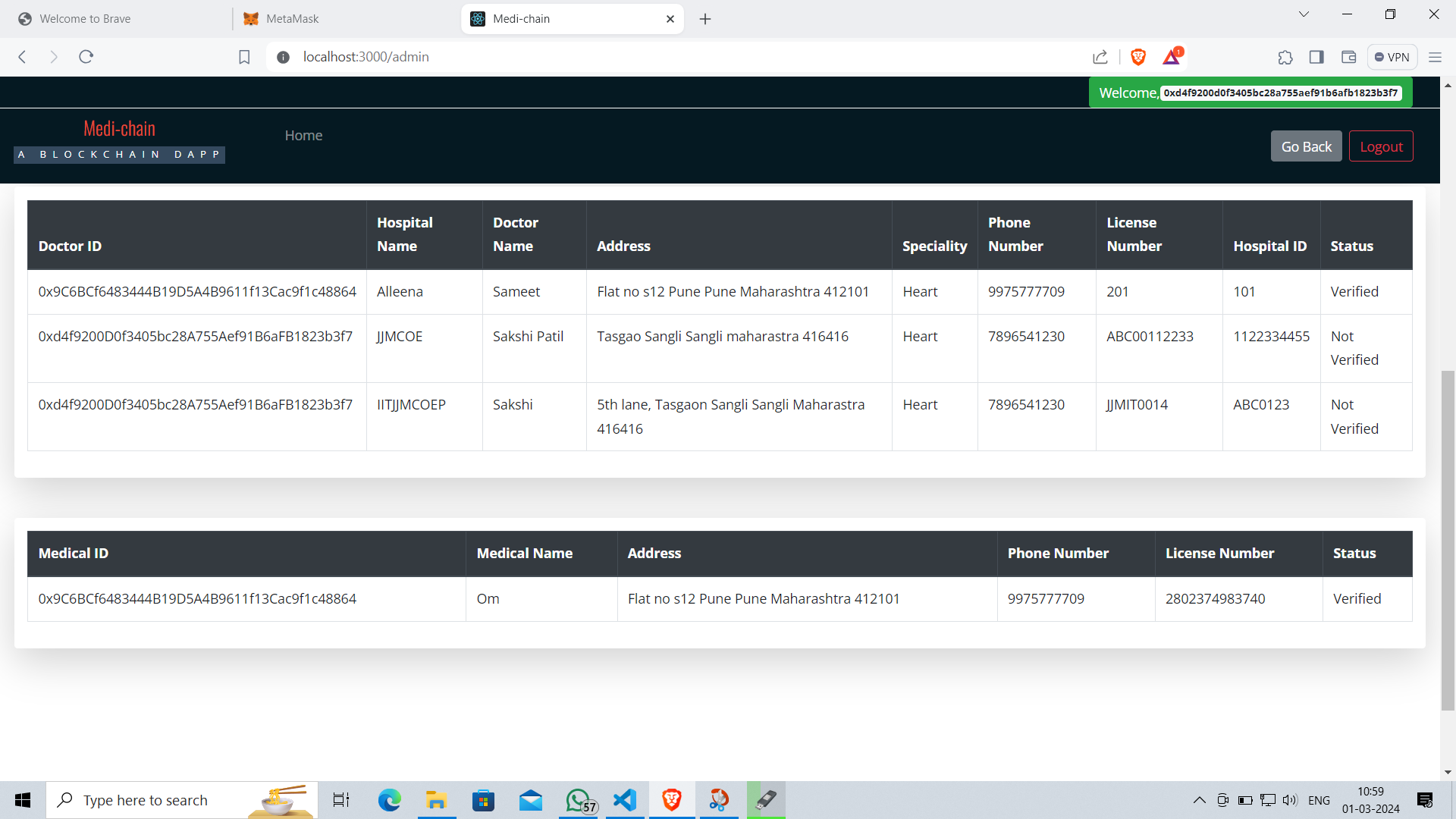
**Fig.01 user interface**

****

**Fig.02 Dashboard**

****

**Fig.03 Adding Doctors**

****

**Fig.04 Admin Panel**

**CHAPTER 09**

**CONCLUSION**

Healthcare data management has been gaining increasing attention in the last few years as it can provide more accurate, efficient, and cost-effective patient care. Blockchain technology has strong potential to improve the management of medical data because it can address issues such as single point of failure, data stewardship, system vulnerability, distributed information, and high security and privacy risks prevailing in the existing client-server and cloud-based approaches. However, most of the recent research efforts aimed at implementing blockchain in the healthcare domain have focused on the Bitcoin network. However, as we have mentioned previously, the Bitcoin network suffers from high energy consumption, low transaction throughput, limited scalability, and privacy and security threats. Consequently, there is a need for a more scalable and efficient blockchain architecture. In this paper, we have proposed a fast way blockchain architecture for healthcare data management that has low computational, and communication overhead as compared to the Bitcoin network. We replaced the energy consuming mining consensus protocol of the Bitcoin network with a scalable and an energy-efficient consensus protocol.

**9.2 FUTURE WORK**

The Overall technique can be improved to get better results as the existing one is not up to the mark. Very high computational power and Advance security will be required for the proposed model restricting its use in real time.

**9.3 APPLICATIONS**

1. Can be used in Hospitals.
2. Can be used in Medicals.
3. Can be used by patients for verifying and storing their medical data.
4. Can be used for storing medicines whole data.

**APPENDIX A**

This problem statement is solved in Exponential time using the relevant mathematical model of Blockchain and DAO.

**APPENDIX B**

**Details of Paper Publications:**

**International Journal for Research in Applied Science and Engineering Technology (IJRASET).**

**Status:** Published

**Proof:** Paper ID- IJRASET56530

**Name of Conference:**

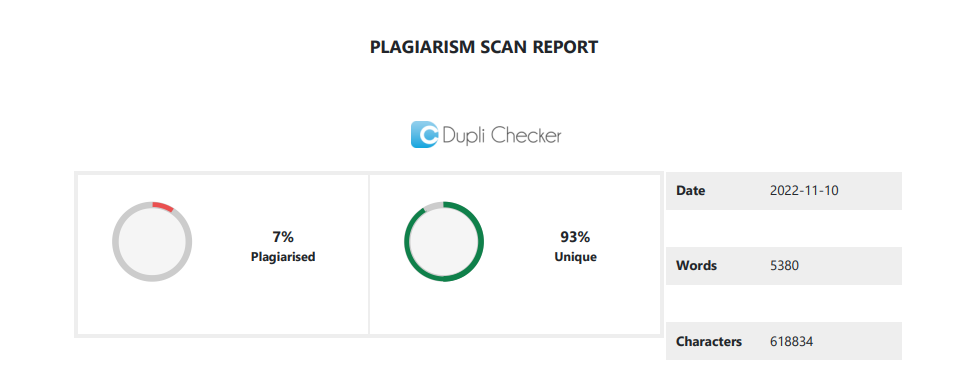
**International Journal Of Scientific Research in Engineering and Management (IJSREM).**

**Status:** Published

**Proof:** Paper ID- IJSREM31576

**APPENDIX C**

Plagiarism report



**REFERENCES**

[1].Israa Abu-elezz, Asma Hassan, Anjanarani Nazeemudeen, Mowafa Househ, Alaa Abd alrazaq,

The benefits and threats of blockchain technology in healthcare: A scoping review,

International Journal of Medical Informatics, Volume 142,2020, 104246, ISSN 1386-5056

[2].: L. Soltanisehat, R. Alizadeh, H. Hao and K. -

K. R. Choo, "Technical, Temporal, and Spatial Research Challenges and Opportunities in Blockchain-Based Healthcare: A Systematic Literature Review," in IEEE Transactions on Engineering Management.

[3]. L. Ismail, H. Materwala and S. Zeadally, &quot;Lightweight Blockchain for

Healthcare,&quot; in IEEE Access, vol. 7, pp. 149935-149951, 2019,

[4].B. Alamri, K. Crowley and I. Richardson, &quot;Blockchain-Based Identity Management Systems in

Health IoT: A Systematic Review, &quot; in IEEE Access, vol. 10, pp. 59612-59629, 2022

[5].S. Yongjoh, C. So-In, P. Kompunt, P. Muneesawang and R. I. Morien, "Development of an Internet-of-Healthcare System Using Blockchain," in IEEE Access, vol. 9, pp. 113017-113031, 2021

[6].S. S. Akash and M. S. Ferdous, "A Blockchain Based System for Healthcare Digital Twin," in IEEE Access, vol. 10, pp. 50523-50547, 2022

[7].Xia, Qi, Emmanuel Boateng Sifah, Kwame Omono Asamoah, Jianbin Gao, Xiaojiang Du and Mohsen Guizani. “MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain.” IEEE Access 5 (2017): 14757-14767.

[8].K. Azbeg, O. Ouchetto, S.J. Andaloussi, L. Fetjah,A Taxonomic Review of the Use of IoT and Blockchain in Healthcare Applications, IRBM, Volume 43, Issue 5, 2022, ISSN 1959-0318.