CHAPTER 1

INTRODUCTION

1.1 Introduction

Domain Introduction

Blockchain technology is an advanced database mechanism that allows transparent information sharing within a business network. A blockchain database stores data in blocks that are linked together in a chain. The data is chronologically consistent because you cannot delete or modify the chain without consensus from the network. As a result, you can use blockchain technology to create an unalterable or immutable ledger for tracking orders, payments, accounts, and other transactions. The system has built-in mechanisms that prevent unauthorized transaction entries and create consistency in the shared view of these transactions.

Features of blockchain technology

- Decentralization

  Decentralization in blockchain refers to transferring control and decision making from a centralized entity (individual, organization, or group) to a distributed network. Decentralized blockchain networks use transparency to reduce the need for trust among participants. These networks also deter participants from exerting authority or control over one another in ways that degrade the functionality of the network.

- Immutability

  Immutability means something cannot be changed or altered. No participant can tamper with a transaction once someone has recorded it to the shared ledger. If a transaction record includes an error, you must add a new transaction to reverse the mistake, and both transactions are visible to the network.

- Consensus

  A blockchain system establishes rules about participant consent for recording transactions. You can record new transactions only when the majority of participants in the network gives their consent.

Why is blockchain important

Traditional database technologies present several challenges for recording financial transactions. For instance, consider the sale of a property. Once the money is exchanged, ownership of the property is transferred to the buyer. Individually, both the buyer and the seller can record the monetary transactions, but neither source can be trusted. The seller can easily claim they have not received the money even though they have, and the buyer can equally argue that they have paid the money even if they haven't.

To avoid potential legal issues, a trusted third party has to supervise and validate transactions. The presence of this central authority not only complicates the transaction but also creates a single point of vulnerability. If the central database was compromised, both parties could suffer.

Blockchain mitigates such issues by creating a decentralized, tamper-proof system to record transactions. In the property transaction scenario, blockchain creates one ledger each for the buyer and the seller. All transactions must be approved by both parties and are automatically updated in both of their ledgers in real time. Any corruption in historical transactions will corrupt the entire ledger. These properties of blockchain technology have led to its use in various sectors, including the creation of digital currency like Bitcoin.

How does blockchain work

While underlying blockchain mechanisms are complex, we give a brief overview in the following steps. Blockchain software can automate most of these steps:

1.Record the transaction

A blockchain transaction shows the movement of physical or digital assets from one party to another in the blockchain network, it is recorded as a data block.

2. Gain consensus

Most participants on the distributed blockchain network must agree that the recorded transaction is valid. Depending on the type of network, rules of agreement can vary but are typically established at the start of the network.

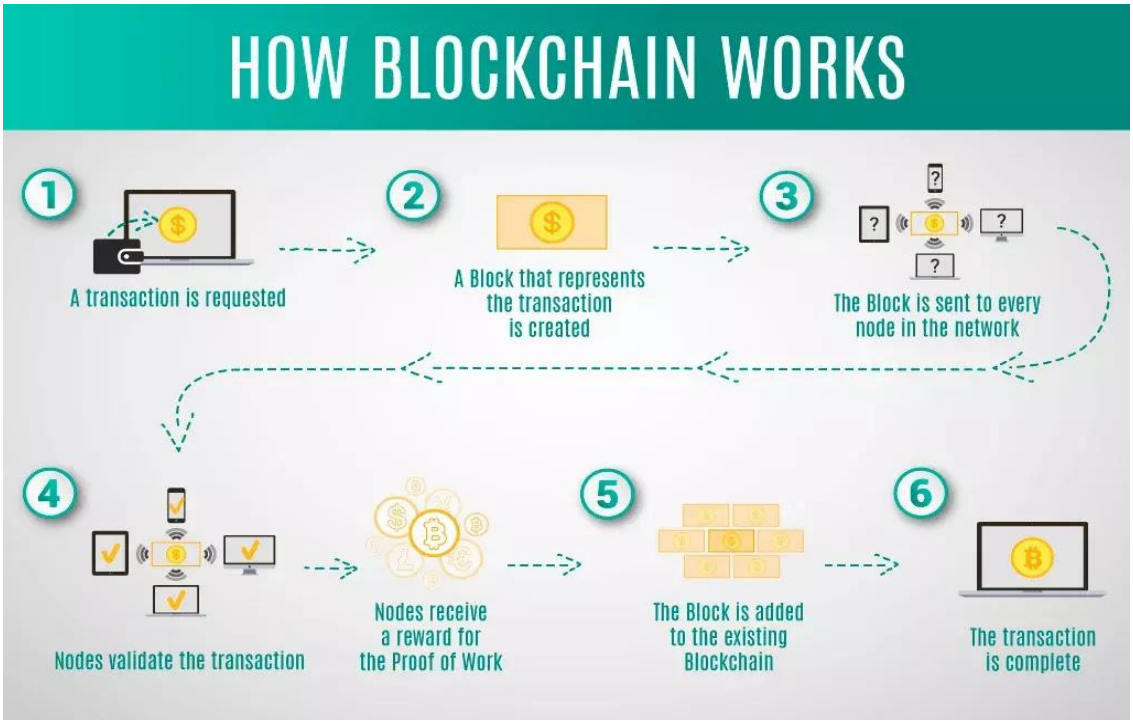

Figure : working of blockchain

3. Link the blocks

Once the participants have reached a consensus, transactions on the blockchain are written into blocks equivalent to the pages of a ledger book. Along with the transactions, a cryptographic hash is also appended to the new block. The hash acts as a chain that links the blocks together. If the contents of the block are intentionally or unintentionally modified, the hash value changes, providing a way to detect data tampering. Thus, the blocks and chains link securely, and you cannot edit them. Each additional block strengthens the verification of the previous block and therefore the entire blockchain. This is like stacking wooden blocks to make a tower.

4. Share the ledger

The system distributes the latest copy of the central ledger to all participants.

Blockchain architecture has the following main components

1.A distributed ledger

A distributed ledger is the shared database in the blockchain network that stores the transactions, such as a shared file that everyone in the team can edit. In most shared text editors, anyone with editing rights can delete the entire file. However, distributed ledger technologies have strict rules about who can edit and how to edit. You cannot delete entries once they have been recorded.

2.Smart contracts

Companies use smart contracts to self-manage business contracts without the need for an assisting third party. They are programs stored on the blockchain system that run automatically when predetermined conditions are met. They run if-then checks so that transactions can be completed confidently. For example, a logistics company can have a smart contract that automatically makes payment once goods have arrived at the port.

3.Public key cryptography

Public key cryptography is a security feature to uniquely identify participants in the blockchain network. This mechanism generates two sets of keys for network members. One key is a public key that is common to everyone in the network. The other is a private key that is unique to every member. The private and public keys work together to unlock the data in the ledger.

Project Introduction

The recent advent in technology is affecting all parts of human life and is changing the way we use and perceive things previously. Just like the changes technology has offered in various other sectors of life, it is also finding new ways for improvement in healthcare sector. The main benefits that advancement in technology is offering are to improve security, user experience and other aspects of healthcare sector. An electronic health record (EHR) is a technology that allows you to keep track of your health information. It keeps computerized records of several healthcare organizations. Records are exchanged via enterprise-wide data systems as well as other networking technologies and exchanges. Patients nowadays expect immediate access to their health information. However, the health sector comes with immediate access to data, and there are worries about the privacy and security of medical records of patients. As a result, a blockchain-based solution can assist in resolving this issue. The blockchain has the potential to

beat the conventional centralized system, which suffers from a severe lack of accessibility. The blockchain-based system that helps the patient's data be managed and secured into a single record held by the patient. The proposed system uses this platform to store patients" data and execute functions in a decentralized system using blockchain smart contracts. Transactions are communicated through the smart contract once it has been launched, providing security and privacy features. Furthermore, the transaction's desired alterations can be verified and transmitted to the entire distributed network. There is also a crypto currency wallet (Metamask) that holds a centrally controlled, private information system in which records can be quickly accessed and secured by authorities. Doctors and patients can access the system through the wallet. Moreover, all the data of the doctor and patient will be secured and managed through this system. A blockchain is a decentralized network that uses peer-to-peer (p2p) technology to track all transactions. It lacks a centralized authority or a single point of contact. Rather, it is a group of nodes that keep the system functioning. Each transaction is extremely safe because of the network's nodes. Encryption provides an additional level of security to the connection. The digital record is duplicated at every node in the system. Each node must verify the authenticity of a transaction before adding it back. A number of blocks make up a digital ledger. Each block gives a detailed report of each transaction. Education, manufacturing, and the healthcare industry are just a few of the domains where blockchain has piqued interest. It contributes to the health sector in a variety of ways because it is a distributed and decentralized technology. The Ethereum blockchain is powered by ETH, Ethereum native crypto currency. Ethereum is a decentralized blockchain technology that creates a peer-to-peer network for securely executing and verifying a smart contract code. It allows developers to build new sorts of ETH-based tokens that are used to power decentralized apps (Dapps) via smart contracts. Participants can transact with one another without lying on a trusted central authority. A smart contract differs from blockchain technology in that it is a computer mechanism that operates automatically when specific circumstances are met. From a blockchain viewpoint, it brings logic to the blockchain.

1.2 Related work

Blockchain-Based Electronic Medical Record Model

In recent years, blockchain technology has experienced rapid development and is characterized by its decentralized nature, data immutability, and transparency. It was first proposed by Nakamoto in 2008 and initially applied in the context of Bitcoin. Blockchain technology can be seen as a distributed database that enables reliable and secure data storage within the system, eliminating the need for third-party cloud storage and addressing potential data security issues associated with cloud storage. Building upon these distinctive features, researchers have begun exploring the application of blockchain technology in the medical field. Azaria et al. introduced MedRec, an electronic medical record model based on blockchain technology, which enhances the security of data transmission. However, this model still relies on centralized cloud servers, making it susceptible to data leakage and malicious tampering. Liang et al. proposed a secure data transfer scheme using Fabric blockchain, which improves data transfer security and reduces communication overhead. Zhang and Poslad put forth a fine-grained access control-based secure storage model for electronic medical records, enabling granular access control by authorizing different queries. This blockchain-based approach effectively addresses data requests without revealing unauthorized personal information. However, it increases the computational consumption of querying electronic medical records, resulting in inefficiencies for the entire system. Nevertheless, the calculation of tokens is susceptible to attacks or tampering. Sun et al. ensured the security of the storage platform by suggesting decentralized storage of encrypted electronic medical data in IPFS. Only the hash address returned from IPFS is uploaded to the blockchain. Li et al. proposed a transaction record-centric system and utilized game theory to introduce a new token economic system, aiming to optimize the process of sharing electronic medical records and achieve a Nash equilibrium point. Liu et al. combined searchable encryption with federated blockchain to achieve efficient and reliable multikey word searches. However, there is still a presence of cloud servers in the system architecture. However, the transaction record-centric approach makes the system inefficient and prone to congestion. Jayabalan and Jeyanthi addressed the system overhead by adopting a patient-centric model and utilizing IPFS. However, handing over the entire system network maintenance to the patient is challenging to implement in reality, and centralized access control remains an issue. Kaur et al. proposed a blockchain-based approach for EMR storage and sharing by utilizing IPFS as an off-chain storage and encrypting the patient-related records while encrypting and decrypting them using the CP-ABE algorithm. However, it still suffers from a high system overhead and centralization of the access control. Alrebdi et al. proposed a

blockchain-based scheme for secure storage and access to EMRs through a combination of IPFS and cloud storage to achieve search and verification of encrypted files. Still, the scheme does not achieve better access control, while the existence of cloud storage leads to system vulnerability to attacks. Ramesh et al. proposed blockchain-based tamper-proof EMR storage access in cloud environment. Still, the third-party reviewer in the scheme is susceptible to attacks due to the lack of a distributed architecture, which leads to the review process of a single point of failure. Mohammed et al. proposed a blockchain-based distributed EMR system, which achieves secure storage of EMR data through biological signalling and light-weighted encryption, but did not design a corresponding access control policy.

Smart Contract-Based Access Control Technology

The concept of smart contracts traces its origins back to the paper by Szabo, which introduced the idea of using computer code and cryptographic techniques to automate contract execution and ensure the immutability and nonrepudiation of their execution. With the advancement of blockchain technology, smart contracts have gained widespread adoption and implementation. They are designed as code or programs embedded within the blockchain that can autonomously execute and update its state. The emergence of smart contract platforms like Ethereum has propelled the development of smart contract technology. Ethereum introduced Solidity, a Turing-complete language for smart contracts, and provided developers with tools and environments to create and deploy smart contracts. Building upon these features, researchers have explored the use of smart contracts for access control. For instance, Cruz et al. implemented a role-based access control mechanism using smart contract technology, enabling cross-organizational role usage. Zhang et al. proposed a framework for IoT environments by introducing multiple access control contracts to achieve enhanced access control. In access control, Wang et al. utilized smart contract technology to implement access control and revocation within the Internet of Things (IoT) environment using a single contract. However, they did not tackle the security vulnerabilities of a lone access control node. Maesa et al. introduced a decentralized and dynamic access control approach based on policies, allowing for complex access control policies based on user or environmental properties. These studies highlight the potential of smart contract technology in implementing robust and flexible access control mechanisms within various domains.

1.3 Problem definition

After reviewing all the papers, it has been noticed that there is a lack of blockchain design and application in the healthcare sector, because they are not user-friendly and have no particular website that is merged with blockchain technology. However, the novelty of our system is that it improves the efficiency of the healthcare sector. It is also a less time- consuming method of healthcare than traditional healthcare because patients may receive services while still at home.

1.4 Objectives

The objectives of implementing EHRs using blockchain technology:

1. To develop a system to provide enhanced Data Security and Privacy.
2. To develop a system to facilitate Interoperability and Data Exchange.
3. Patient Empowerment and Ownership.
4. Auditable and Transparent Recordkeeping.
5. Data Integrity and Trustworthiness.

1.5 Scope

A blockchain, in which records are maintained in a linked sequence of blocks, has made it feasible to create and deploy new programs based on a distributed and decentralized ideology rather than traditional cloud-based apps. The present smart contract will be extended to improve the lookup and provide the advanced features required by an EHR administration system. Future development could most likely aim at providing a real-time video conference communication feature. In this COVID-19 outbreak, it is highly recommended. Another possibility is that the payment module will eventually be integrated into the existing architecture.

This can be accomplished via a decentralized architecture based on blockchain technology, in which a patient pays for a specialist's consultation with a credit or debit card. In the event of verification, the NID number can be included. With the introduction of Ganache, we now have the opportunity to experiment with a similar technique utilizing a private blockchain. It will involve enhancing lookup and supporting the extra capabilities required by an EHR management solution. In addition, there will be a comparison of present and future methodologies.

1.6 Existing system

The fact that notion behind usage of EHR systems in the hospitals or healthcare was to improve the quality of health care, these systems faced certain problems and didn't meet the expectations associated with them. A study was conducted in Finland to find the experiences of nursing staff with the EHR, it was concluded that EHR systems faced the problems related to them being unreliable and having a poor state of user- friendliness.

- The existing healthcare system is insecure among several medical services because of data availability delays and the danger of data theft. Hospital records can be archived without the patient's knowledge. Due to several challenges, such as security and accessibility of data, there has been no exploration or experimentation in the healthcare industry.
- Existing technology's restrictions must be recognized, and future study requirements must be evaluated.
- Existing e-healthcare platforms, on the other hand, are not properly established and stable and, hence, lack the level of privacy, authenticity, identity, and user confidence that are required for universal use.

The EHR system also faces some other problems in existing system which are as follows

A. Interoperability

It is the way for different information systems to exchange information between them. The information should be exchangeable and must be usable for further purposes. An important aspect of EHR systems is its Health Information Exchange (HIE) or in general data sharing aspect. With a number of EHR systems being deployed in various hospitals they have a varying level of terminologies, technical and functional capabilities which makes it to have no universally defined standard. Moreover, at technical level the medical records being exchanged should be interpretable, and that interpreted piece of information could be further used.

B. Information asymmetry

Today the greatest problem in healthcare sector defined by the critics is information asymmetry which refers to one party having better access to information than the other party. In

case of EHR systems, or in general healthcare sector is suffering from this problem as doctors or hospitals have access to the patient's records, thus making it central. If a patient wants to access his medical records, he would have to follow a long and tedious process to access them. The information is centralized to only a single healthcare organization and its control is only provided to the hospitals or organizations.

C. Data breaches

Data breaches in healthcare sector also calls for the need of a better platform. A study was done for analyzing the data breaches in EHR systems and it depicted that 173 million data entries have been compromised in these systems since October 2009. Another study conducted by Argawet al., explains that hospitals have become a target of cyber-attacks and an increasing trend has been witnessed by the researchers while conducting this study that a lot of research work has been done in this domain. Moreover, many EHR systems are not designed to fulfill the needs and requirements of the patients and face the issues related to inefficiency and poor adaptation of these systems. The literature also suggests that use of EHRs have introduced negative consequences to information processing. These problems make it reasonable to find a platform that would be helpful in transforming healthcare sector to be patient-centered, i.e., Blockchain. A platform which is secure, transparent and it also provides data integrity to the medical records of the patients. The paper proposes a framework that creates such a decentralized platform that would store patient's medical records and give access of those records to providers or concerned individuals, i.e., patient. We also intend to solve the scalability problem of blockchain, as it is not in the design of blockchain to store huge volumes of data on it. So, we would use off-chain scaling method that makes use of the underlying medium to solve the scalability problem by storing the data on that medium. Moreover, our proposed work is intending to solve the above mentioned information asymmetry and data breaches problem faced by the EHR system.

1.6 Proposed system

The novelty of our system is that it improves the efficiency of the healthcare sector. It is also a less time-consuming method of healthcare than traditional healthcare because patients may receive services while still at home. This section formally describes the preliminaries used in

proposed framework. It describes the software platform used for development of this framework and its advantages. Ethereum and IPFS being the most prominent and important for implementation of this framework are also discussed in the following section.

A. Ethereum

Ethereum is a distributed blockchain network that uses the idea of blockchain that was previously used in the popular crypto currency Bitcoin. Ethereum was formally introduced in year 2015 and the idea behind Ethereum was to create a trustless smart contract platform that would be open-source and would also hold the feature of programmable blockchain.

This technology also shares the peer-to-peer networking that makes it distributed. This platform also makes use of its own crypto currency known as Ethers. This crypto currency can be used for sharing it between accounts connected on Ethereum blockchain. Ethereum also provides the programmers a language in which they can customize their own blockchain, this language is known as Solidity. It was developed for smart contracts that are the main feature of Ethereum.

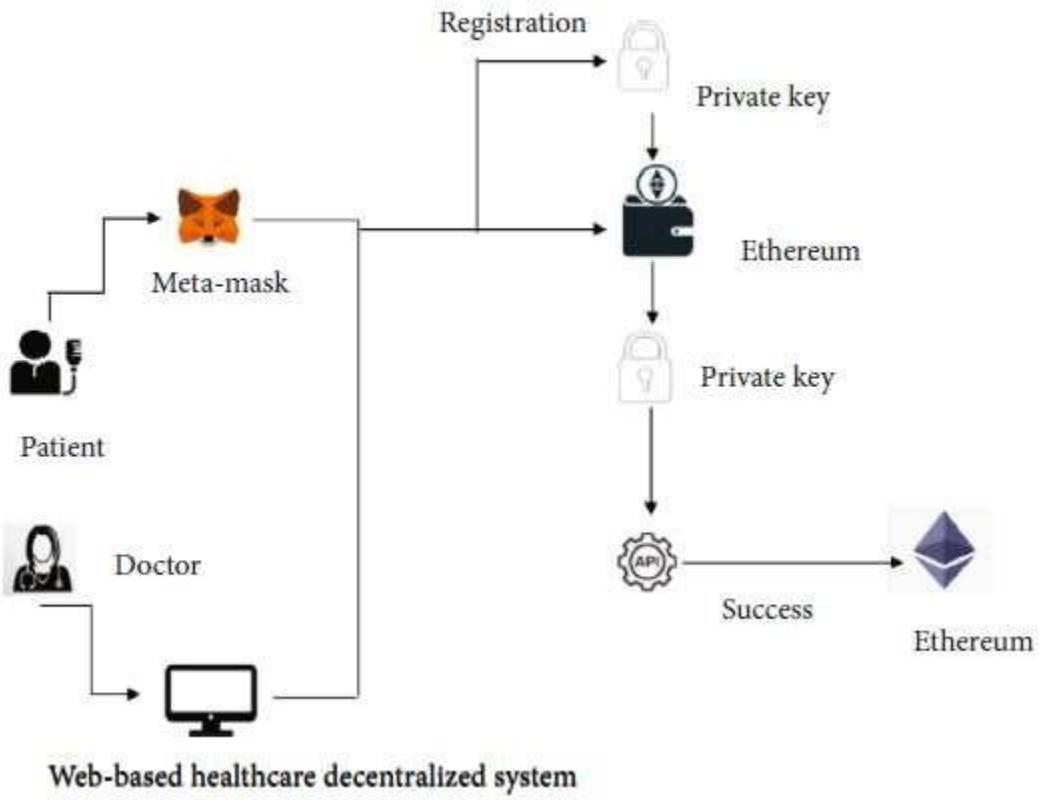

Figure 6: The protocol layout of the HER system

B. Information transaction

In Ethereum, transaction is the way external entity would interact with Ethereum. It can be used by external user to update the state of the record or information stored on the Ethereum blockchain network.

An Ethereum transaction contains following elements:

- From–messages under, having a 20-bytes address.
- To–message recipient, also having a 20-bytes address.
- Value-the fund amount transferred from sender to recipient.

C. Smart contracts

Smart contracts are known as the piece of code that is used to perform any task on the blockchain. This piece of code is executed when the users send the transactions. They run on the blockchain directly thus making themselves secure from any kind of tampering and alterations. Smart contract commonly use solidity language and they can be used to program any kind of operation that a programmer wants to do on the blockchain.

D. Interplanetary file system (ipfs)

IPFS is a protocol that uses peer-to-peer network for data storage. It provides secure data storage as data stored on IPFS is protected from any alteration. It uses a cryptographic identifier that protects the data from alteration as any attempt to make change on the data stored on IPFS could only be done by changing the identifier. All the data files stored on IPFS contains a hash value that is generated cryptographically. It is unique and is used for identification of stored data file on the IPFS.

1.7 Outline

The rest of the thesis is organized as below:

In Chapter 2, we discussed literature review of related works towards Secure electronic health records sharing using blockchain.

In Chapter 3, the terminologies, UI design in detail.

In Chapter 4, we discussed the methodology. Hypothesis validation, experiments and

subjective and technical analysis details with the participants who used the application.

In Chapter 5, we discussed the results of our experimentation.

Finally, Chapter 6 concludes the study and future work is discussed.

CHAPTER 2

LITERATURE SURVEY

2.1 Survey

[1] Blockchain technology was designed by Nakamoto the basic idea was to have a cryptographically secured and a decentralized currency that would be helpful for financial transactions. Eventually, this idea of blockchain was being used in various other fields of life; healthcare sector also being one of them intends to use it. A number of researchers have carried out the research on this area, these research works focus on the fact that whether the idea of using blockchain for healthcare sector is feasible or not. They also identify the advantages, threats, problems or challenges associated by the usage of this technology. Some researchers also discussed the challenges that would be faced while actually implementing this on a larger scale.

[2] Gordon and Catalini conducted a study that focused on the methods by which blockchain technology would facilitate the healthcare sector. They identified, that healthcare sector is controlled by hospitals, pharmaceutical companies and other involved third parties. They specified data sharing as the key reason why blockchain should be used in healthcare. This study also identified four factors or approaches due to which healthcare sector need to transform for usage of blockchain technology. These include way for dealing of digital access rights, data availability, and faster access to clinical records and patient identity. It also discusses the on-chain and off chain storage of data. The study also included the challenges or barriers faced by usage of blockchain technology these were huge volume of clinical records, security and privacy, patient engagement.

[3] Eberhardt and Tai conducted a study to understand possible approaches to solve the scalability problem of blockchain and also to identify such projects that intend to solve this problem. They need blockchain as composition of various computational and economical concepts based on peer-to-peer system. The aim of this study was to which data should be stored on-chain and what could be stored off chain. This study present patterns for off-chain storage of data and also includes the basic ideas and implementation framework of these patterns. The authors explain on-chain data is any data that is stored on the blockchain by performing

transactions on it. While off-chain data storage is to place data elsewhere on any other storage medium but not on-chain and it also would not include any transactions.

[4] Vuji£i¢ et al. presented an overview of blockchain technology, bitcoin and Ethereum. The authors de ne that information technology landscape is constantly changing and blockchain technology is benefiting the information systems. They explained bitcoin as a peer-to-peer distributed network used for performing bitcoin transactions. They also denied that proof-of-work consensus algorithm along with the mining of blockchain concept. The authors emphasize on the fact that scalability is a severe problem faced by blockchain and that certain solutions are proposed for solution of scalability problem these include SegWit and Lightning, Bitcoin Cash and Bitcoin Gold. The paper also explained Ethereum and its dependencies and it also differentiates Ethereum blockchain from bitcoin's blockchain.

[5] Wang et al. conducted a study that focused on smart contracts and its application in blockchain technology. They are introduced the smart contracts, their working framework, operating systems and other important concepts attached with them. The authors also discuss that how could smart contracts be used for the new concept of parallel blockchains. They identify that reason of using smart contracts in blockchain is due to the decentralization that is offered through the programming language code written in them. After introducing the basics of smart contract, the author explained the various layers of blockchain that combine together to keep system functioning. These layers are data, network, consensus, incentive, contract, and application layer. The paper not only discusses the architecture and framework followed by smart contracts but it also gives an insight on its applications and challenges.

[6] Kuo et al. conducted a review that discussed several applications of blockchain in biomedical and healthcare sector. The author identied that using blockchains for this domain offers many advantages and some of these are decentralization, persistence of clinical or medical records, data pedigree, and continuous accessibility to data and lastly secure information being accessible to biomedical or healthcare stakeholders. The limitations of blockchain technology were identified to be, confidentiality, speed, scalability and threat of malicious attack, i.e., 51% attack. The authors identified these limitations to be critical for healthcare or biomedical sector as they are being used to store sensitive medical or clinical records. The solution to these problems were presented by authors to store sensitive medical data off chain, encryption of data to ensure confidentiality, and lastly to use VPNs (Virtual Private Networks) to ensure safety from

malicious attacks.

[7] Sahoo and Baruah proposed a scalable framework of blockchain using Hadoop database. In order to solve the scalability problem of blockchain, they proposed to use the scalability provided by the underlying Hadoop database along with the decentralization provided by the blockchain technology. They used the method to store blocks on the Hadoop database, the blockchain on top of this framework includes all of the needed dependencies of blockchain but the blocks are stored on Hadoop database to improve scalability of the blockchain technology. To tackle the scalability problem of blockchain platform this study offers to use Hadoop database system, along with SHA3-256 for hashing used for transactions and blocks. The programming language used for this architecture was Java.

[8] Zhang et al. proposed a scalable solution to the blockchain for clinical records. The basic aim of this study was to design such an architecture that complies with the office of National Coordinator for Health Information Technology (ONC) requirements. This study identified the barriers that this technology faces mainly include concerns related to privacy, security of blockchain, and scalability problems related to huge volume of datasets being transmitted on this platform, and lastly there is no universal standard enforced for data being exchanged on blockchain. This study also include a demonstration of a decentralized application (DAPP) based on the design formulated on the ONC requirements as mentioned before. They also included the lessons learnt and how can FHIR chain be improved.

[9] Kim et al. proposed a system for management of medical questionnaires and the aim of this system is data sharing through blockchain technology. The authors explain that selection of data storage and sharing of medical question this data for further medical and clinical research purposes. They emphasized that it would be helpful for developing diagnosis system, resolving terminologies being used in EHR systems and security issues associated with these systems was also areas on due to which authors selected blockchain technology for their proposed framework. This study contains two main functions, i.e., to create, store the data gathered by questionnaires and to share that data. Another benefit proposed by the system is the validation of the questionnaire being submitted in the system. The questionnaires that are added on this system arrest validated to be correct specified format and then are parsed to differentiate the personal data and specific data related to question are results. This would ensure that data could be shared for future research purposes.

[10] ihuan Chen, Zhixiong Tan, Wei Fang "Blockchain-Based Implementation for Financial Product Management" IEEE 2018.In the above project, they have proposed the platform for financial product management which is based on blockchain. It forms a constructed architecture of network for management of financial product information which own information transparency and secured environment for information sharing. The management platform in this project uses Hyper Ledger Fabric as underlying architecture concluded the fundamental financial product operations such as routine maintenance of product, multiple function of data inquiry and financial product tractability. At last, considering the financial product management characteristics, a follow-up for improving the weakness of Hyper Ledger has been put forward.

[11] V. Arun, Aditya Dutta, Sourav Rajeev, Rohan Varghese Mathew "E-Voting using a Decentralized Ethereum Application" IJEAT, 2019.As the technology progress day by day its impact is only positive. One of such evolution is blockchain. It can revolutionize the voting process since it has decentralized nature and immutability. Voting in most of the place is a cloudy process and it is common to corruption. By introducing the concept of blockchain in voting process, a potential protocol can be created which makes the voting process open, fair and verifiable by anyone. Moreover, the paper illuminates the potential of the ledger using a case study. It also aims to highlight the advantage and disadvantage of using the architecture of blockchain as a application in the voting process.

[12] Mohamed Amine Ferrag, Makhlouf Derdour, Mithun Mukherjee "Blockchain Technologies for the Internet of Things: Research Issues and Challenges" IEEE 2019.This paper presents a complete survey on existing technology of blockchain protocol for IOT networks. The paper starts with introduction of blockchain and explains the existing survey that is associated with the blockchain concept. Then an overview of application domain of blockchain in IOT is provided. Moreover, the five main classification of blockchain in IOT is also provided briefly.

[13] Xing Liu "A Small Java Application for Learning Blockchain" IEEE 2018.This paper preface Chain Tutor, a Java application for learning the concepts of blockchain technology. Even though the concept of blockchain is widely known and its application are found in various areas such as health care, etc some of its concepts are not known for beginners. Text based tutorials

can be difficult to follow. Even the pictures of block chain can also be lost in such documented tutorials. With the help of the Java application introduced in the paper, user can implement the concept of blockchain technology via GUI. They can also view how the mining works and how each blocks are added to the blockchain.

[14] Andrei Cirstea, Nicu Bizon, Cosmin Stirbu "Blockchain Technology Applied in Health" ECAI, 2018.This paper provides a small introduction of blockchain concepts and then brief on its medical applications. The purpose of this application is to make the medical field more efficient. This technology has the ability to transform medical and any other field for decentralization. This can bring a change to the world via secure and efficient way. The main idea of the paper is to show the exceptional potential of this technology and how it changes all ways of receiving, securing and transmitting the information.

[15] M. Drozdova, S. Rusnak, P. Segec, J. Uramova, M. Moravcik, "Contribution to cloud computing security architecture", ICETA 2017 Cloud computing has changed complex system's software support from server oriented to service oriented. By this change a wide range of demands in design and delivery of services has been emerged. All the users are relocating their application software to remote servers due to cloud flexibility. This should be able to provide relevant information service and storage for client data by ensuring availability of data, integrity and privacy. This may also cause data stealing and data breach of the data stored in cloud. The paper identifies the threats and provides solutions to the challenges using the existing solutions.

2.2 Conclusion

The literature survey on secure electronic health record (EHR) sharing using blockchain technology highlights the potential and challenges of integrating blockchain into healthcare systems. Blockchain's decentralized and immutable nature addresses several critical issues in EHR management, such as data security, privacy, interoperability, and patient control over personal health information.

CHAPTER 3

SYSTEM SPECIFICATIONS

3.1 Introduction

Introducing a system for secure electronic health record (EHR) sharing using blockchain involves outlining the technical specifications and components that ensure privacy, security, interoperability, and efficiency.

3.2 Technology used

The technologies include for the development of electronic health record system are listed below with a detailed explanation.

1.Ethereum blockchain

Ethereum is a decentralized blockchain platform that establishes a peer-to-peer network that securely executes and verifies application code, called smart contracts. Smart contracts allow participants to transact with each other without a trusted central authority. Transaction records are immutable, verifiable, and securely distributed across the network, giving participants full ownership and visibility into transaction data. Transactions are sent from and received by user-created Ethereum accounts. A sender must sign transactions and spend Ether, Ethereum's native cryptocurrency, as a cost of processing transactions on the network.

Benefits of building on Ethereum

Ethereum offers an extremely flexible platform on which to build decentralized applications using the native Solidity scripting language and Ethereum Virtual Machine. Decentralized application developers who deploy smart contracts on Ethereum benefit from the rich ecosystem of developer tooling and established best practices that have come with the maturity of the protocol. This maturity also extends into the quality of user-experience for the average user of Ethereum applications, with wallets like MetaMask, Argent, Rainbow and more offering simple interfaces through which to interact with the Ethereum blockchain and smart contracts deployed there. Ethereum’s large user base encourages developers to deploy their applications on the network, which further reinforces Ethereum as the primary home for decentralized applications like DeFi and NFTs. In the future, the backwards-

compatible Ethereum 2.0 protocol, currently under development, will provide a more scalable network on which to build decentralized applications that require higher transaction throughput.

Advantages of Ethereum

Decentralisation

The Ethereum network operates in a decentralised method across nodes located globally. This means no single entity or central authority controls the platform, making it resistant to censorship, manipulation, or single points of failure. Decentralisation enhances security and fosters trust among users, ensuring that transactions and data are recorded transparently and immutably on the blockchain.

Transparency and security

All transactions and Smart Contracts executed on Ethereum are recorded on a public ledger, providing unparalleled openness. This transparency lowers the chance of fraud and corruption, as anyone can verify the authenticity of transactions. Moreover, Ethereum's security features, such as cryptographic encryption and decentralised consensus mechanisms, make it highly resistant to attacks.

Flexibility and customization

Ethereum's flexibility allows developers to create various decentralised applications and tokens to suit different use cases. Ethereum's programming language, Solidity, supports Turing-complete Smart Contracts, enabling the creation of complex and customisable applications. This adaptability has led to the emergence of various innovative projects, including Decentralised Finance (DeFi) platforms, Non-Fungible Token (NFT) marketplaces, and more.

Ethereum's growing ecosystem

Ethereum has fostered a thriving and rapidly expanding ecosystem. Its open-source nature has encouraged collaboration and innovation, resulting in many projects, protocols, and initiatives built on the platform. Ethereum-based tokens and DApps have gained widespread adoption, attracting users and investors. The network effect generated by this growing ecosystem reinforces Ethereum's position as a leader in the blockchain space.

Interoperability and standards

Ethereum's adoption of common standards like ERC-20 (for fungible tokens) and ERC-721 (for non-fungible permits) has contributed significantly to the interoperability of blockchain assets. These standards have become widely accepted, facilitating the creation and exchange of tickets across different DApps and platforms. This has streamlined the development and integration of blockchain-based solutions.

Community and developer support

Ethereum boasts a large and active community of developers, enthusiasts, and stakeholders deeply committed to its growth and improvement. This strong community support results in continuous development, research, and upgrades to address issues and enhance the platform's capabilities.

Ethereum 2.0 transition

Ethereum is actively addressing its scalability and energy consumption issues with Ethereum 2.0. This multi-phase upgrade involves transitioning from a Proof-of-Work (PoW) to a more energy-efficient Proof-of-Stake (PoS) consensus mechanism. It also includes shard chains to improve scalability. Once

fully implemented, Ethereum 2.0 is expected to enhance the platform's performance and sustainability significantly.

Economic incentives

Ethereum's native cryptocurrency, Ether (ETH), is a fuel for executing Smart Contracts and a store of value. This financial incentive system encourages participants to secure the network, validate transactions, and develop DApps, creating a self-sustaining ecosystem.

2.Ganache

It is a local Ethereum blockchain for the rapid creation of decentralized programs. Ganache can be used to deploy, develop, and test in a predictable and secure environment throughout the development cycle. It works both ways as a desktop program and as a command-line tool (Ethereum).

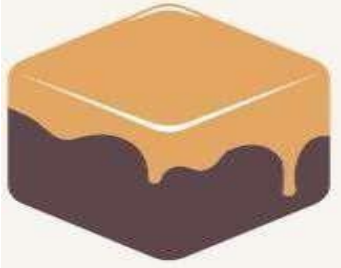

Figure : Ganache icon

3.MetaMask: It is an entry point that allows you to view the decentralized web of the future in your browser right now. It allows you to execute Ethereum decentralized applications without having to run a full Ethereum node in your browser.

Figure3: Metamask icon

4.Ethereum node: This could be a node in ETH wallets from the local system. Metamask is an in-browser extension that allows you to operate from Ethereum accounts and can be used to integrate Ethereum with the website. Metamask is a browser-based Ethereum wallet that connects the browser to a Web3 provider class. A Web3 provider is a data structure that provides a link to Ethereum nodes that are publicly available.

Figure 4: Ethereum icon

5.Truffle: It is a strong Ethereum Virtual Machine development environment that uses blockchains, as well as an asset pipeline and a test framework for the same. It has some features, such as computation, implementation, and maintenance of smart contracts, as well as binary dependency management. It also has an environment for testing smart contracts that is fully automated and a deployment and migration framework that can be scripted and expanded. It can create direct communication with the contract and a pipeline with tight integration. The truffle environment is used to run programs.

Figure5: Truffle icon

6.VS Code: Microsoft's Visual Studio Code is an editor for Windows, Linux, and macOS.

Troubleshooting, Git management, GitHub, syntax underlining, smart code completion, samples, and bug fixes are all available.

7.Languages: The front-end design of our website has been created using HTML (Hypertext Markup Language), CSS (Cascading Style Sheets), and React.js. The server and back-end of the website are controlled using the Solidity programming language and Node.js. There are two tools, Truffle and Ganache, which are used for generating local Ethereum blockchains to build the system. The Ethereum virtual interface, Metamask (as a wallet), Truffle (as an IDE), Yarn (command-line interface), Ganache (account creation), and Local Web3 (web interface) are used to establish the blockchain and access or use the system.

8.Web3: Verification of transactions should be done in the chain in order to interact with the modules in the chain. To generate and verify a transaction, a participant in the network of another offline framework must relay it to the peer-to- peer (p2p) connection, which is an actual network. It also includes a library collection that makes it easier for Ethereum nodes and in-chain components to communicate. It is utilized on the server side for Node.js.

3.3 Software Requirements

Operating system:

Frontend: HTML (Hypertext Markup Language), CSS (Cascading Style Sheets), and React.js

Backend: Solidity and Node.js

Blockchain Platform: Ethereum

Text Editor: Visual studio Code

3.4 Hardware Requirements

RAM: 8GB

SSD: 256GB

Processor: 8-core CPU with 4 performance cores and 4 efficiency cores

GPU: 7-core and 8-core GPU

CHAPTER 4

SYSTEM DESIGN AND IMPLEMENTATION

4.1 System Architecture

Block diagram of the project

Illustrate the block diagram. Our proposed design has four major components a user application, a blockchain handshake protocol, a cloud, and a public blockchain network. The system is a virtual representation that serves two purposes. For starters, it provides users with access to application interfaces. Doctors and system administrators are two types of users in our system. Each user has a distinct function. As a result, the user application delivers different user interfaces depending on the user role. Second, based on the data entered by the user, the user application creates an initial transaction. For the purpose of confirmation, the transaction is submitted to the blockchain handshake protocol. Finally, a user interface establishes the relationship between users and the blockchain handshake protocol.

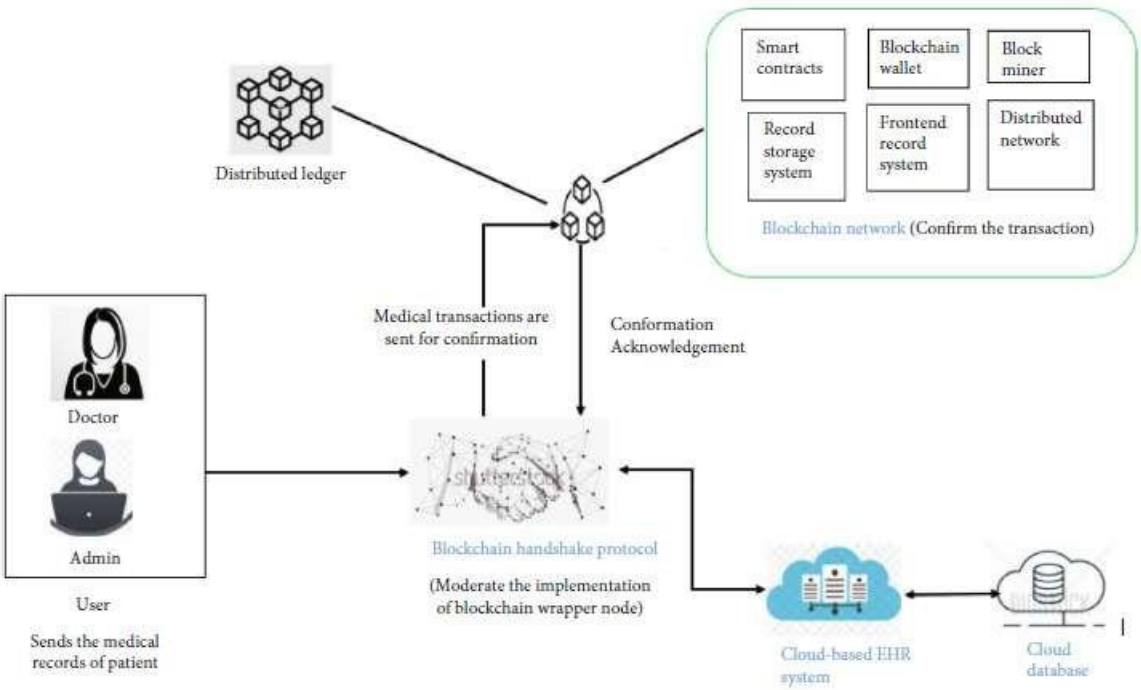

Figure 1: Block diagram of the blockchain-based HER system.

The proposed architecture's fundamental component is the blockchain handshake (BH) protocol. This component connects the database server, the blockchain network, and the cloud-based health record system, which acts as a wrap- per. This proposed architecture makes use of the Ethereum blockchain network.

Use Case Diagram of Proposed System.

This applications use-case has three key entities: an administrator, a patient, and a doctor. Now, inputting profile details, which is a unique feature that grants access to all three organizations, is also included in the list of actions. The patient has access to three out of ten operations, while the doctor has access to three out of ten operations. Only the administrator has access to all ten actions, allowing them to examine and monitor all the information. The only operation that can change block data once it has been retrieved is writing the record of the patient, which can only be done by the doctor. The use case diagram is shown in Figure

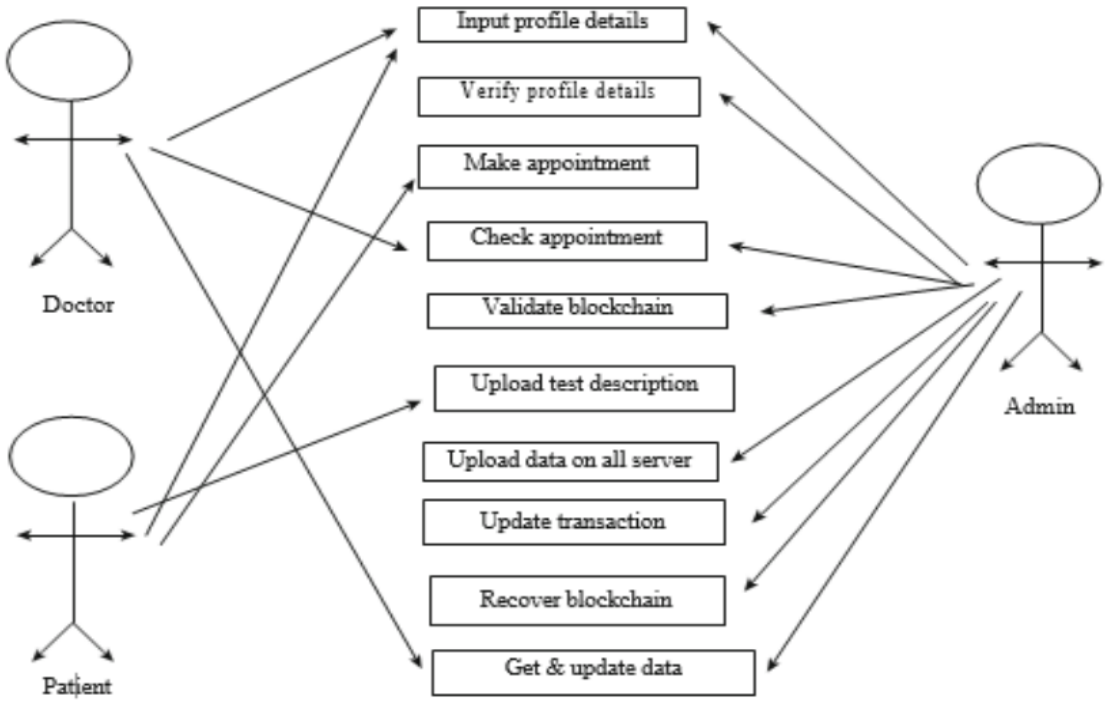

Figure: Use case of proposed system

Flowchart of Proposed System

The process of creating a medical record the system's first doctor will produce a medical record. After that, the doctor records each patient's examination results. The metadata transaction for that medical record will be processed. A portion of data called transaction metadata is appended to a transaction after it has been processed. Regardless of whether a transaction is successful or not, all transactions that are recorded in a ledger have metadata. The transaction information provides a detailed description of the transaction's conclusion. Following that, the medical file will be uploaded to the IPFS network. IPFS (Interplanetary File System) is a document system that allows transactions to be completed with minimal resources and time. We acquire a content address after a file is uploaded to the IPFS network. The Ethereum transaction is the next stage. Ganache is required for Ethereum transactions since it provides addresses and private keys. The addresses are kept on file, and the transactions are visible to all. To carry out a transaction, the private keys are utilized to unlock these addresses. The Ethereum Virtual Machine (EVM) is used to process Ethereum transactions. The EVM is primarily used to conduct smart contract interactions, in which all nodes must agree that the transaction occurred every time someone interacts with the contract. After that, the EVM executes an immediate post contract in accordance with the transaction rules. Figure shows Ethereum retains a record of all previous transactions and the blockchain's history, which is kept and confirmed through consent. Ethereum's node operators, on the other hand, keep track of all smart contract interactions that take place on the Ethereum network. In this situation, the miner will be turned into a bot that will process transactions automatically whenever a transaction is received.

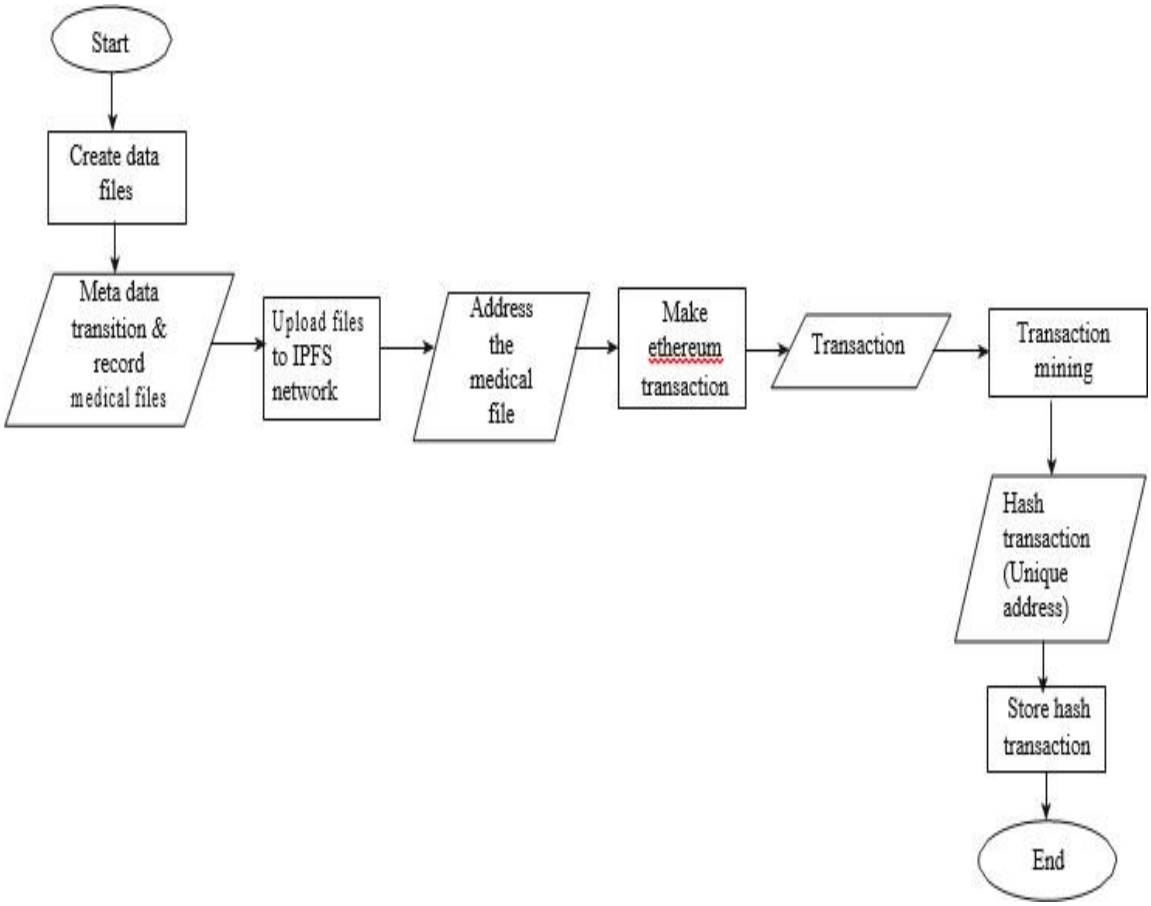

Figure 9: Flowchart of explaining the process of creating a medical record

Process of Doctor Dash board

With the appropriate information and a transaction ID, a doctor can finish the registration. The dashboard will only be accessible to the doctor; otherwise, access will be blocked. In addition to the admin's responsibility of viewing appointments, the doctor performs five procedures on the dash board. On the doctor's dashboard, a doctor may see his own personal information. Doctors can update personal information such as their name, age, phone number, current address, and photo, as well as their educational qualifications if necessary. The doc-tor can evaluate a patient's past medical records and personal information for future therapy. He can add extra data to the patient's dashboard if he thinks it is essential.

A doctor can change a patient's record the same way admin can. To avoid misunderstandings, the doctor can also delete any sort of record, including those that are several years old, from the patient's dashboard. The most recent data is more accurate. Shown in Figure

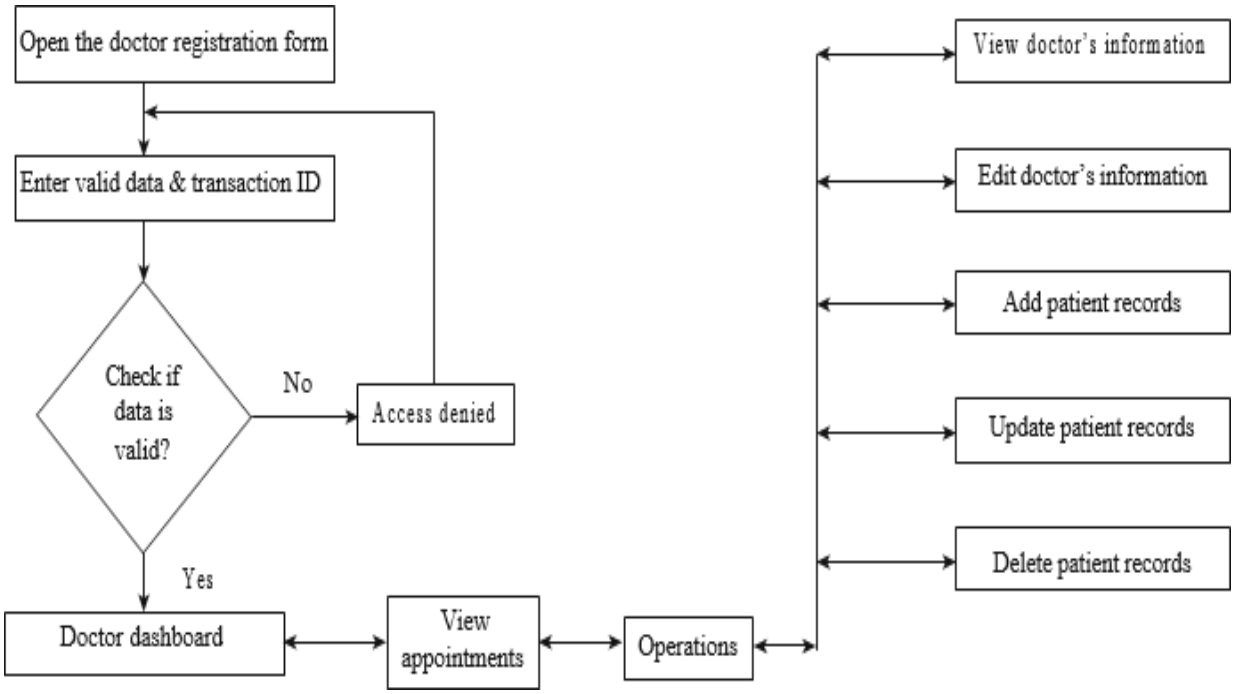

Figure 10: process of doctor dashboard

Process of Patient Dashboard

Depicts the method of constructing a patient dashboard. With the proper information and a transaction ID, a patient can finish the registration. A patient can only view the dashboard if they have a registered ID and valid information. Otherwise, the patient's access will be refused, and he or she will be required to input the right password. In addition to booking appointments, the patient performs three procedures on the dashboard. Two of them are the ability to view extensive information and medical records. Only after successful registration can patients read their personal information. Patients can also access their medical records, which have been supplied by their doctor. Patients can make changes to their personal information, such as their name, age, phone number, current address, and photo, if required. Shown in the below figure.

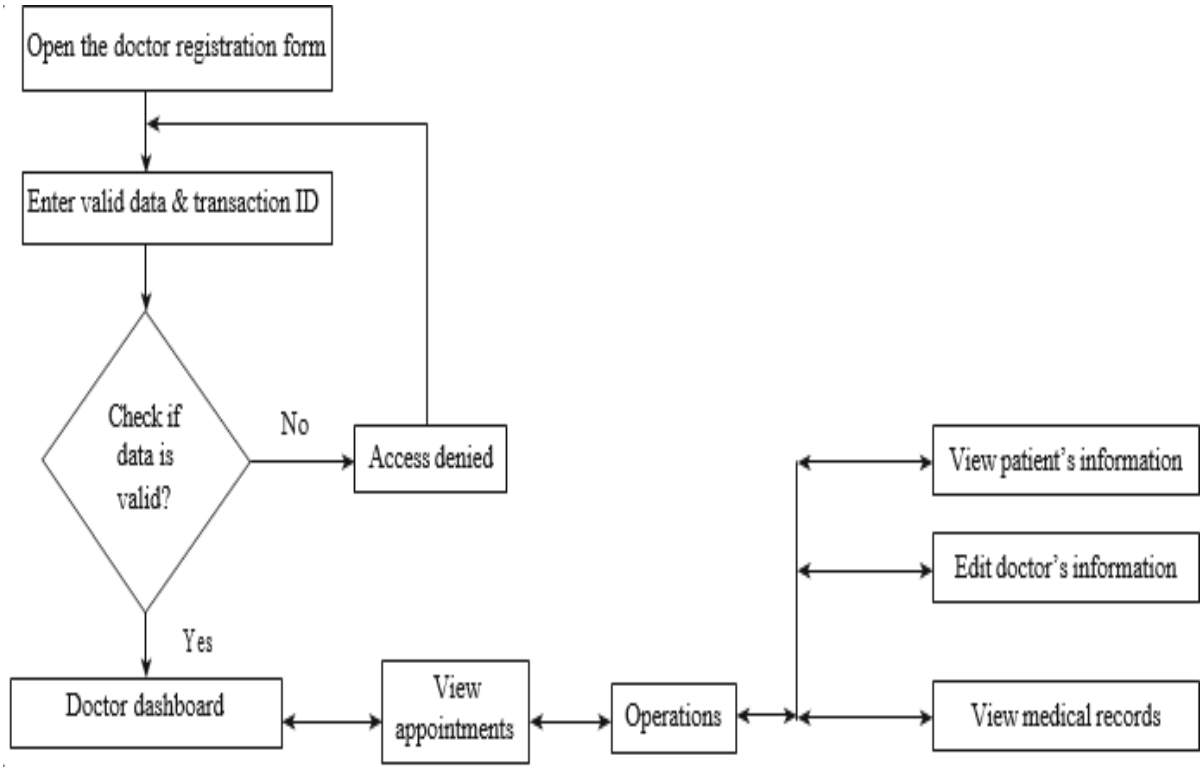

Figure 11: process of patient dashboard

4.2 System design

System design is the most important and vital part of any framework as it is used for the development of the system from its theory. This section includes the modules, architecture and various elements that are combined together to form the whole system's framework. As defined earlier the purpose behind this proposed framework is to create such a decentralized system that is temper-proof, secure and confidential blockchain-based system for electronic health records. As visible in below figure 2, the proposed framework or system has three entities or modules. These modules when combined together would keep our system working. These entities or modules have further concepts that need to be understood they are explained as follows. The proposed framework consists of users that could be patients, doctors, administration and nursing staff. They were given granular access as they should have varying level of authority on the system.

1)USER LAYER

A user of a system is defined as an individual who makes effective use of the system and its resources. A user has various roles and features on the system, making him identifiable on the system. The users of this system could be patients, doctors and administrative staff etc. The main task of these users would be to interact with the system and perform basic tasks such as create, read, update and delete the medical records. The users using this system would be accessing the system's functionality by a browser which in technical terms we refer as DApp browser, as it is containing the GUI (Graphical User Interface) of the DApp, i.e., our proposed system framework. The GUI contains all the functions that could be accessed by a particular user. The user according to the assigned role could use this GUI for interacting with the other layer of the system, i.e., blockchain layer.

2) BLOCKCHAIN LAYER The next layer on the system is the blockchain layer; this layer contains the code or mechanism for interaction of user with the DApp which is functioning on the blockchain. This layer contains three elements inside it. They are: • Blockchain Assets: In Ethereum blockchain, transaction is the process by which external user can update the state of the record or information stored on the Ethereum blockchain network. These transactions are treated as assets by the Ethereum blockchain as they are piece of information that user can send to another user or to simply store it for using it later.

• Governance Rules: Blockchain technology in general follows some consensus rules for its transactions to be done and computed. For this purpose, it needs some consensus algorithms to keep the blockchain temper-proof and secure. Ethereum blockchain uses Proof of Work (PoW) consensus algorithm, the reason behind using it is also for ensuring that governance of blockchain is maintained in a trusted manner which is through consent from all the trusted nodes attached to the blockchain network.

• Network: Ethereum blockchain uses the peer-to-peer network. In this network all the nodes are connected as peers with no node acting as the central node controlling all the functions of the network. The reason behind using this network was because the idea was to create a distributed platform not a centralized. So, using a network where all the connected nodes have equal status and right was the best choice this technology could have done.

TRANSACTION

The system includes following transactions:

• Add records would create patient's medical records in the DApp. It contains the fields of

ID, name, co-morbid, blood group, and IPFS hash. The patient's basic medical records is stored along with the IPFS hash that contains the file uploaded containing the lab results or other medical records of patient.

• Update records would update the medical records of patient. This can only change the basic information of the patient not the IPFS hash. IPFS hash is non-updateable to ensure security of records.

• View records would let the user view the medical records of a patient stored in DApp. The view records function is used both by doctors and patients. The patient can view his records by the system authenticating that patient views only his own medical records. For this purpose system uses the public account address of the patient to ensure that only the relevant medical records is shown to the patient.

• Delete records would make the user be able to delete record of any patient. The user here would be the doctors they are given this right to delete any patient's record stored on the blockchain.

• Grant access for each of the above-mentioned transactions, certain user would need to have access to them, i.e., only the doctor or nursing staff can make changes in the records of the patient or add them. So, add and update records would only be accessible to these entities. Moreover, patient can view his medical records but won‟t be given the access to add or update them.

3) SMART CONTRACTS

As explained earlier, smart contracts are an important part of DApps as they are used for performing basic operations. Following contracts are included in this framework:

• Patient Records

• Roles

These contracts are used for giving access to the users on the DApp and performing CRUD operations on the records of patient.

The Patient Records smart contract is made purely for implementing the functionality of the proposed framework. It performs the CRUD operations along with the defining roles for access of these functions. The second contract mentioned above, i.e., Roles is a predefined smart contract by the Open Zeppelin smart contract library. This library contains several smart contracts performing various functionalities that could be used for creating your own smart

contracts. The reason behind using this library was to make use of the benefits it provides, i.e., tested and community reviewed code. The Roles smart contract belongs to the Asset library, which is a sub-library of the Open Zeppelin library. The asset library contains various other contracts for defining the access rules but roles library provide a granular role definition mechanism which was the main reason behind selection of this smart contract.

CHAPTER 5

RESULT AND DISCUSSION

The process of getting access to the proposed system is discussed in this section. This system is built with Truffle and Ganache, two easy-to-use tools for creating local Ethereum blockchains. The server and back-end of the system have been controlled using the Solidity language and Node.js. To create a blockchain and access the system, the Ethereum virtual interface, Metamask (as a wallet), Truffle (as an IDE), Yarn (command-line interface), Ganache (account creation), and Local Web3 (web interface) are used.

A. Step-by-Step Process of the System (Front-End Part).

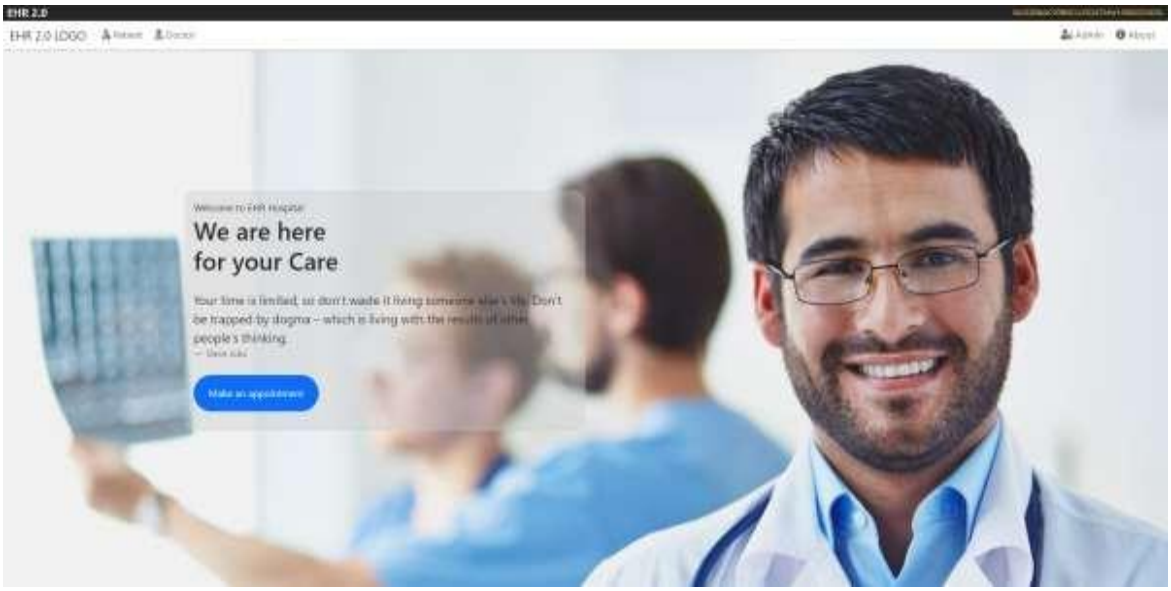

Figure 7: Homepage of the proposed system.

Homepage: Figure illustrates the homepage of the system. To access this homepage, a user needs to create an account. After that, users can access this system through the homepage. There are three portals on this homepage. The system administrator is one, while the patient and doctor are the other users. In addition to the admin, doctor, and patient portals, this website features an appointment bar and a Chabot on the top page. Furthermore, doctors, patients, and admin need a unique account to get access to this homepage.

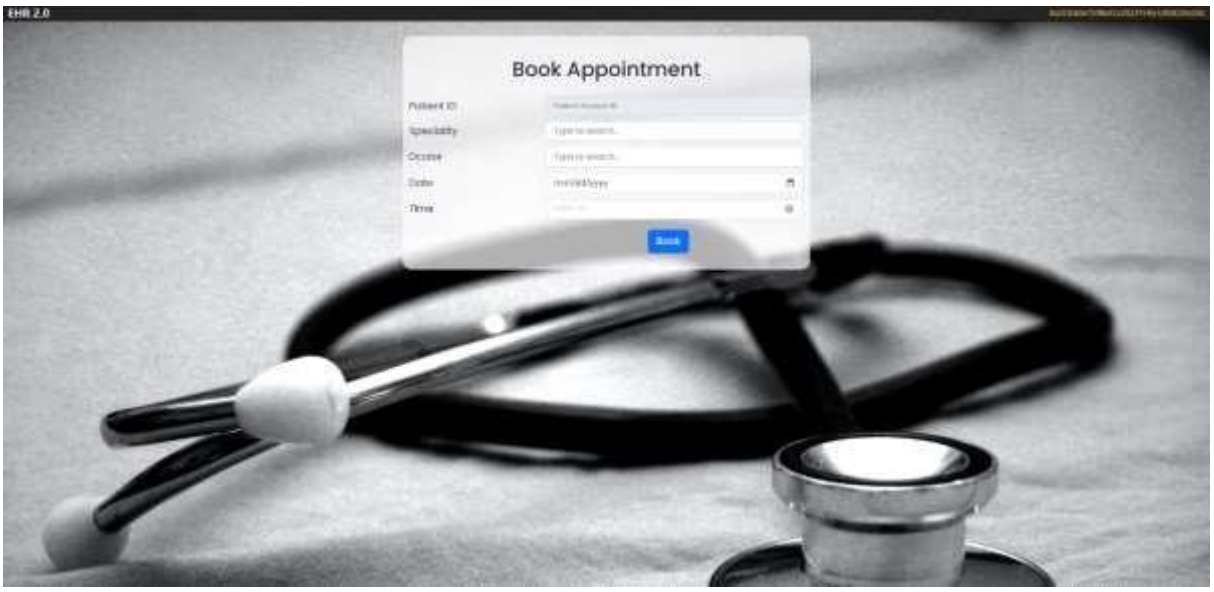

Figure 8: Appointment created with the Doctor

Above figure shows the appointment-making bar. This bar is used for making time slots to visit the hospital, and users can ask for the next appointment or visit the time slot of a doctor through this bar.

Figure 9: Admin panel.

Admin Panel: This system's admin interface is seen in Figure. Admin can add doctors and view doctor's details in the system, as well as delete current users, using the admin interface i.e. doctors. The administrator has their own unchangeable and inaccessible account in this system, which has the authority to create and delete users For the sake of authenticity and security, no one else has access to this. Appointments and notify doctors about their patient list. He can also plan the appointment based on the number of patients. He can also provide information about appointments and other responses to the questions and appointments.

Figure 10: Add doctor

Add Doctor: Figure shows the process of adding a doctor. Figure shows the doctor registration module where you need to fill in the details of a doctor such as name; date of birth; email ID; mobile number; doctor ID, which is an account address from Ganache Ethereum; city; state; and specialty. Figure shows the confirmation message from Metamask that is used as a smart contract. Through Meta-Mask, all the information about the doctor will

be stored, and the system will get the confirmation message for authentication. But, if a user uses the wrong information or the same account address, the system will show an access denied message. Finally, this smart contract ensures the security of the doctor's data.

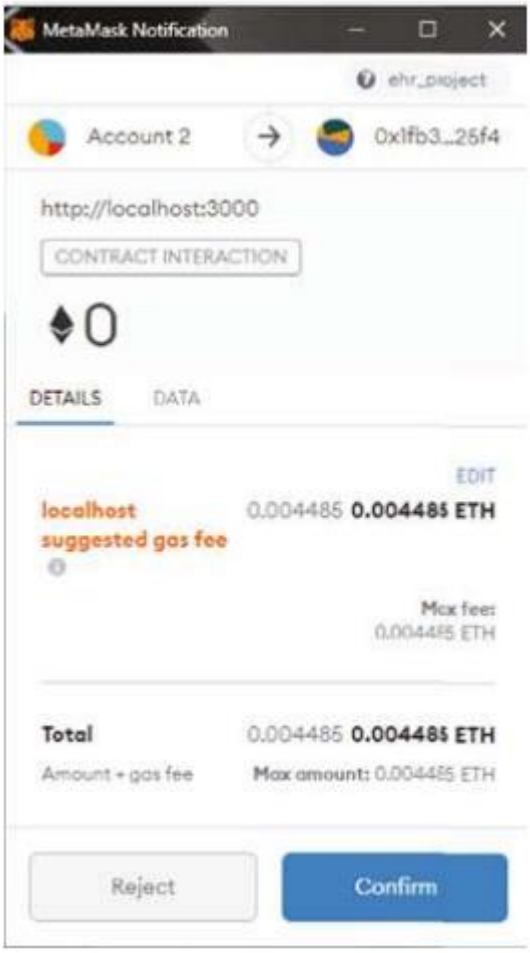

Figure: confirmation message from the smart contract (Metamask)

Add Patient

Figure 16 describes the method of adding a patient. Figure 16(a) depicts the patient registration module, which requires you to input patient information such as names, email addresses, phone numbers, and patient IDs, which is a Ganache Ethereum account address. After filling up all of the spaces with the required information, the user must click the "Add Doctor" button to store the data, then move on to the next process. The confirmation message from MetaMask, which is employed as a smart contract, is shown in Figure 16(b). All of the patient's information will be saved using MetaMask, and the system will get a confirmation message for authentication.

To save all of the data, the MetaMask notification displays the Ethereum currency rate in detail on the screen. It stores all of the data in the Ethereum currency format. The system will display an access forbidden message if a user enters incorrect information or the same account address. Finally, the security of the patient's data is ensured by this smart contract

FigurE11: Patient registration form

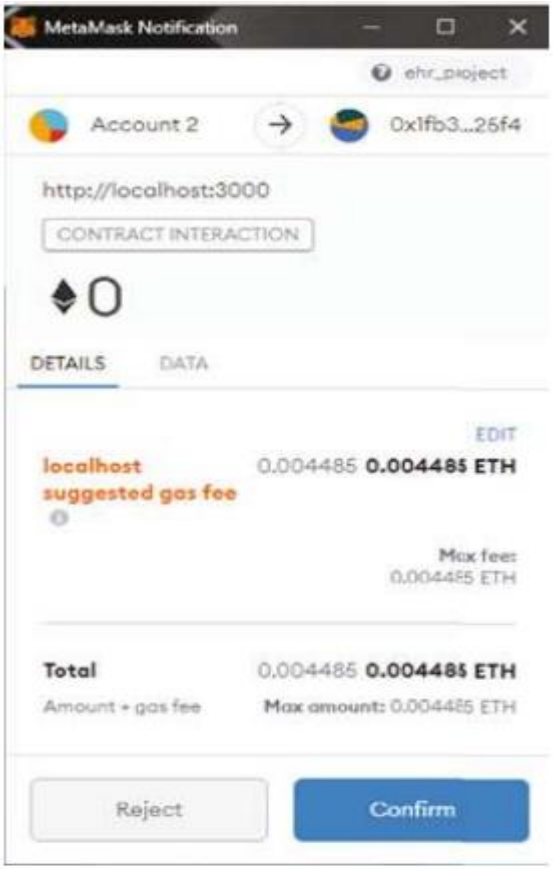

Figure: confirmation message from smart contract (MetaMask)

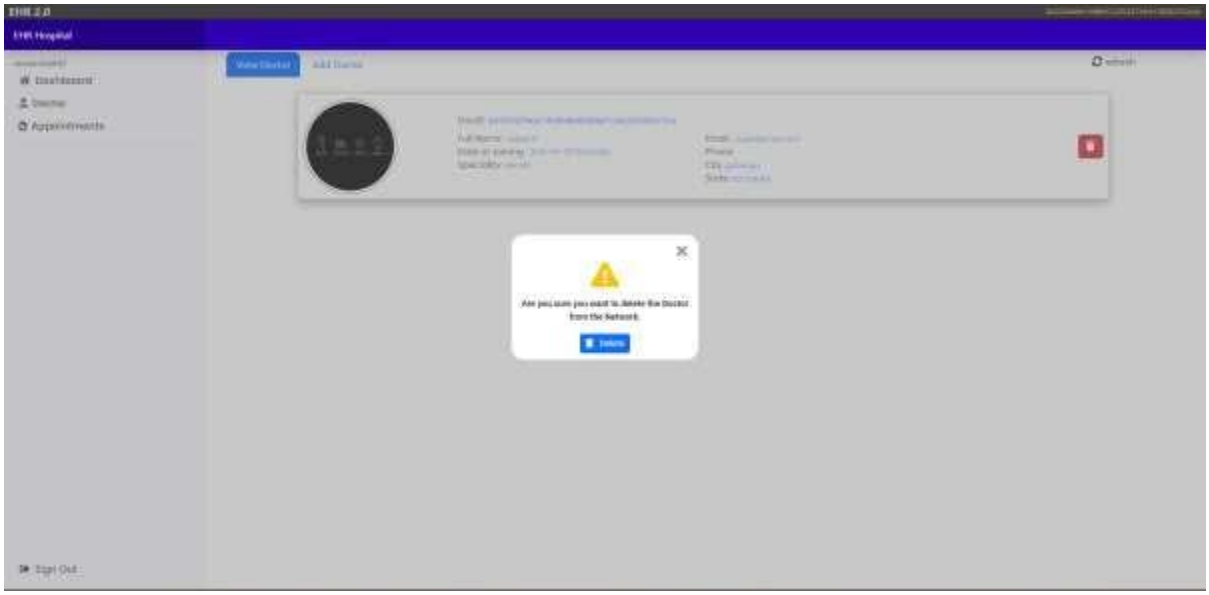

Figure 12: User deletion by admin

Figure 13: Patient's Panel

Patient's Panel. Figure shows the patient's panel. A patient can view and modify their personal information on the patient's panel if any changes have occurred. Patients can now see their medical records that physicians have uploaded. A patient can examine a doctor's comprehensive prescription but cannot make any adjustments for any sort of offence.

CHAPTER 7

CONCLUSION

The standard medical record-keeping method is inefficient, and it necessitates a tremendous amount of storage space to retain the results of all medical tests for all patients. The data in prior systems was unstructured, making it impossible to transmit information. Because of the massive volume of data produced by the healthcare industry, we need to start thinking about improving efficiency of data management methods without risking the data's security and privacy. Because of the confidentiality data, there will be additional changes. This change brings many issues that need to be addressed, and blockchain successfully addresses the fundamental issues.

This system allows the patient to grant and withdraw any record-specific authorization to the authorities with a single tap. This automation has been made much easier to deploy due to Ethereum and smart contracts. The suggested wallet serves as a bridge for providing secure and convenient access to the blockchain, as well as hassle-free secret key maintenance. It can also act as a link for patients who are uncertain about migrating their information to electronic health records (EHRs). The system's cryptographic encryption methods, which are difficult and impossible to crack, will offer security and dependability. It has been determined that this system has achieved the majority of the project's objectives, namely, authentication data exchange of medical reports utilizing blockchain security, and it is expected that the project's implementation will meet the users" needs. As a result, the authentication, data exchange, and security of medical reports have already been completed successfully utilizing blockchain. The system also deals with the problems caused by direct disease transmission in hospitals, like the COVID-19 situation, mainly through physical copies of medical records and the increased risk associated with additional human chain contamination.

REFERENCES

[1] S. Nakamoto, Bitcoin APeer-to-PeerElectrnicCashSystem.2008, pp.1-9.

[2] W. J. Gordon and C. Catalini, :Blockchain technology for healthcare: Facilitating the transitiontopatient-driveninteroperability,Comput.Struct.Biotechnol.J., vol.16, pp. 224230, Jan.2018.

[3] J. Eberhardt and S. Tai, ``On or off the blockchain? Insights on off chaining computation and data," in Proc. Eur. Conf. Service-Oriented Cloud Compute, Oct. 2014, pp. 11-45.

[4] D. Vuji£i¢, D. Jagodi¢, and S. Randi¢, ``Blockchain technology, bitcoin, and Ethereum: A brief overview," in Proc. 17th Int. Symp. INFOTEH- JAHORINA (INFOTEH), Mar. 2018, pp. 1-6.

[5] S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin, and F.-Y. Wang, ``An overview of smart contract: Architecture, applications, and future trends," in Proc. IEEE Intell. Vehicles Symp. (IV), Jun. 2018, pp. 108-113.

[6] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, ``Blockchain distributed ledger technologies for biomedical and health care applications," J. Amer. Med. Inform. Assoc., vol. 24, no. 6, pp. 1211 1220, 2017.

[7] M. S. Sahoo and P. K. Baruah, ``HB chain DB A scalable blockchain framework on Hadoop ecosystem," in Supercomputing Frontiers. 2018, pp. 18-29.

[8] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosen bloom, ``FHIRChain: Applying blockchain to securely and saleably share clinical data," Compute. Struct. Biotechnol. J., vol. 16, pp. 267 278, Jul. 2018.

[9] M. G. Kim, A. R. Lee, H. J. Kwon, J. W. Kim, and I. K. Kim, ``Sharing medical questionnaires based on blockchain," Proc. IEEE Int. Conf. Bioinf. Biomed. (BIBM), Dec. 2018, pp. 2767 2769.

[10] “Electronic Healthcare Data Record Security Using Blockchain and Smart Contract” Farjana Khanam Nishi, Mahi zebin Shams-E-Mofiz, Mohammad Moni rujjaman Khan, Abdul majeed Alsufyani, Sami Bourouis, Punit Gupta, and Dinesh Kumar Saini, Journal of Sensors, Volume 2022, Article ID 7299185, 22 pages, https://doi.org/10.1155/2022/7299185

[11] "Patient Data Management Using Blockchain" Bharath H*, Rahul N, Shylash S, Vinny Pious, International Journal of Scientific and Research Publications, Volume 10, Issue 7, July 2020 ISSN 2250-3153.

[12] "Using Blockchain for Electronic Health Records" AYESHA SHAHNAZ 1 , USMAN QAMAR1 , AND AYESHA KHALID 2 , (Member, IEEE)

[13] L. Academy, "Consensus protocols," 2019, https://lisk.io/academy/ blockchain-basics/how-does-blockchain-work/consensus- protocols.

[14] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology-a systematic review," Plos One, vol. 11, no. 10, 2016.

[15] P. A. Laplante, M. Kassab, N. L. Laplante, and J. M. Voas, "Building caring healthcare systems in the Internet of Things," Systems Journal, vol. 12, no. 3, pp. 3030–3037, 2018.

[16] Gharat, P. Aher, P. Chaudhari, and B. Alte, "A framework for secure storage and sharing of electronic health records using blockchain technology," ITM Web of Conferences, vol. 40, article 03037, 2021.

[17] R. Sreeraj, A. Singh, and V. Anbarasu, "Preserving EMR records using blockchain," Annals of Romanian Society for cell Biology, vol. 25, no. 6, pp. 5344–5350, 2021.

[18] R. Harika and B. Thirumal Rao, "Survey on smart healthcare using blockchain," Journal of Critical Reviews, vol. 7, no. 14, pp. 615–621, 2020.

[19] G. Rathee, A. Sharma, H. Saini, R. Kumar, and R. Iqbal, "A hybrid framework for multimedia data processing in IoThealthcare using blockchain technology," Multimedia Tools and Applications, vol. 79, no. 15-16, pp. 9711–9733, 2020.