PROJECT REPORT

BLOKCHAIN TECHNOLOGY FOR ELECTRONIC HEALTH RECORDS

Date	22 October 2023
Team ID	NM2023TMID05954
Project Name	BLOKCHAIN TECHNOLOGY FOR ELECTRONIC HEALTH RECORDS

TEAM MEMBERS

M.MOHAMED EJAS	**812420104052**
I.IMTHIYAS HUG	**812420104034**
M.ABDUL RAHMAN	**812420104005**
S.GUHAN	**812420104029**

Source Code

GitHub & Project Demo Link

ABSTRACT:

Blockchain have been an interesting research area for a long time and the benefits it provides have been used by a number of various industries.
Similarly, the healthcare sector stands to benefit immensely from the blockchain technology due to security, privacy, confidentiality and decentralization.
Nevertheless, the Electronic Health Record (EHR) systems face problems regarding data security, integrity and management.
In this paper, we discuss how the blockchain technology can be used to transform the EHR systems and could be a solution of these issues.
We present a framework that could be used for the implementation of blockchain technology in healthcare sector for EHR.
The aim of our proposed framework is firstly to implement blockchain technology for EHR and secondly to provide secure storage of electronic records by defining granular access rules for the users of the proposed framework.
Moreover, this framework also discusses the scalability problem faced by the blockchain technology in general via use of off-chain storage of the records.
This framework provides the EHR system with the benefits of having a scalable, secure and integral blockchain-based solution.

INTRODUCTION

Project Overview:

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. These benefits were offered by Electronic Health Record (EHR) and Electronic Medical Record (EMR) systems. However, they still face some issues regarding the security of medical records, user ownership of data, data integrity etc. The solution to these issues could be the use of a novel technology, i.e., Blockchain. This technology offers to provide a secure, temper-proof platform for storing medical records and other healthcare related information.

Before the advent of modern technology, healthcare sector used paper based system to store the medical records, i.e., using handwritten mechanism. This paper-based medical record system was inefficient, insecure, unorganized and was not temper-proof. It also faced the issue of data- duplication and redundancy as all the institutions that patient visited had various copies of patient's medical records.

The healthcare sector faced a trend shift towards EHR systems that were designed to combine paper-based and electronic medical records (EMR). These systems were used to store clinical notes and laboratory results in its multiple components [1]. They were proposed to enhance the safety aspect of the patients by preventing errors and increasing information access [2]. The goal of EHR systems was to solve the problems faced by the paper-based healthcare records and to provide an efficient system that would transform the state of healthcare sector [3].

The EHR systems have been implemented in a number of hospitals around the world due the benefits it provides, mainly the improvement in security and its cost-effectiveness. They are considered a vital part of healthcare sector as it provides much functionality to the healthcare [4]. These functionalities are electronic storage of medical records, patients' appointment management, billing and accounts, and lab tests. They are available in many of the EHR system being used in the healthcare sector. The basic focus is to provide secure, temper-proof, and shareable medical records across different platforms. Despite the fact that notion behind usage of EHR systems in the hospitals or healthcare was to improve the quality of healthcare, these systems faced certain problems and didn't meet the expectations associated with them [3]. 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 [5]. The EHR system also faces some other problems 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 [6]. Moreover, at technical level the medical records being exchanged should be interpretable, and that interpreted piece of information could be further used [6].

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 [7] 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 Argaw et al. [8], 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 [9]– [11].

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 [12]. The literature also suggests that use of EHRs have introduced negative consequences to information processing [2]. 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.

This 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.

This paper is organized as follows the section II of this paper summarizes the basics of blockchain technology and its dependencies; section III narrates the related work done in this domain. The section IV explains the design and architecture of the proposed framework and section V explains the performance of this framework. The last section provides the conclusion and references.

Purpose:

The primary purpose of this project is to explore and evaluate the potential integration of blockchain technology in Electronic Health Records (EHRs) and its impact on the healthcare industry. Specifically, the project aims to achieve the following objectives:

1. Enhance Data Security: Assess how blockchain can enhance the security and privacy of patient health records by implementing robust encryption, access control, and tamper-proof mechanisms.

2. Improve Interoperability: Investigate the role of blockchain in promoting seamless data sharing and interoperability among different healthcare providers and institutions, facilitating better patient care coordination.

3. Maintain Data Integrity: Analyze how blockchain can ensure the integrity and accuracy of EHRs, reducing the risk of data inconsistencies, errors, or fraudulent activities.

4. Empower Consent Management: Explore blockchain-based solutions for efficient and transparent consent management, enabling patients to have greater control over who accesses their medical records.

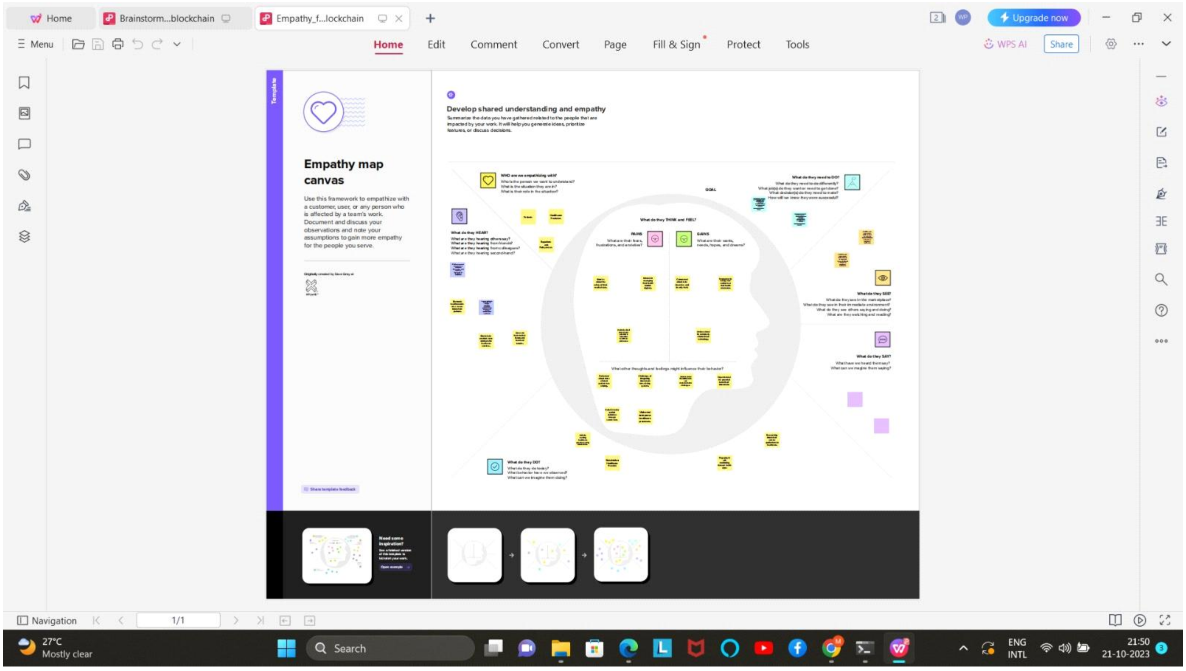
5. Inform Healthcare Decision-Makers: Provide valuable insights and recommendations based on the project's findings to healthcare organizations, policymakers, and stakeholders in the healthcare sector. This information will

assist in making informed decisions regarding the adoption of blockchain technology in EHR systems.

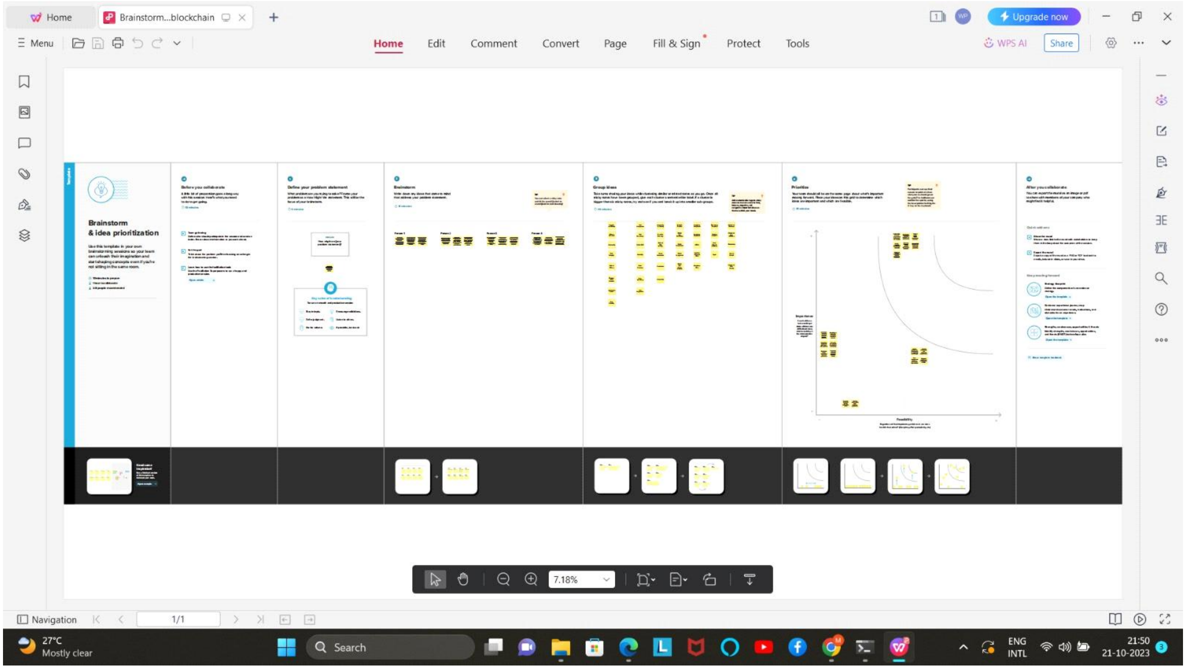
The overarching purpose of this project is to contribute to the ongoing discourse on the utilization of blockchain in healthcare. By addressing these objectives, we aim to advance the understanding of blockchain's potential in improving the security, privacy, and interoperability of Electronic Health Records, ultimately benefiting both healthcare providers and patients.

IDEATION & PROPOSED SOLUTION

Empathy Map Canvas



Ideation & Brainstorming



REQUIREMENT ANALYSIS

Functional requirement:

1. User Authentication and Authorization:

   - Users (healthcare professionals, patients, administrators) must have secure and role-based access to the system.

   - Role-specific permissions should be defined, allowing different levels of access.

2. Electronic Health Record (EHR) Creation and Management:

   - Users should be able to create, access, update, and manage EHRs.

   - EHRs must support structured data entry for patient information, medical history, diagnosis, and treatment plans.

3. Data Encryption and Security:

- All patient data within the EHRs must be encrypted to ensure confidentiality.
- Implement encryption protocols and mechanisms to secure data at rest and during transmission.

4. Interoperability:
   - Enable seamless data exchange among different healthcare providers and EHR systems.
   - Support standardized healthcare data formats (e.g., HL7) for interoperability.

5. Data Integrity and Immutability:
   - Implement blockchain technology to ensure that EHRs are tamper-proof and immutable.
   - Any changes or access to records should be transparently recorded and audited.

6. Consent Management:
   - Implement a user-friendly system for patients to grant or revoke consent for data access.
   - Use smart contracts to automate consent management and access control.

7. Search and Retrieval:
   - Enable efficient search and retrieval of patient records based on various criteria.
   - Provide advanced search capabilities, such as by date, diagnosis, or treatment.

8. Notifications and Alerts:
   - Send automated notifications and alerts to healthcare professionals for updates or critical patient information.
   - Allow customization of notification preferences.

9. Reporting and Analytics:

- Generate reports and analytics on patient health trends, outcomes, and system usage.
- Provide customizable reporting tools for healthcare administrators.

10. Audit Trail:
- Maintain a detailed audit trail for all actions related to EHRs.
- Ensure traceability of every transaction within the system.

Non-Functional Requirements:

1. Scalability:
- The system must be scalable to handle a growing number of EHRs and users.
- It should accommodate increased data storage and processing requirements.

2. Performance:
- Ensure fast response times for user interactions, data retrieval, and updates.
- Implement load balancing and performance optimization techniques.

3. Reliability and Availability:
- The system must be highly reliable, with minimal downtime.
- Implement redundancy and failover mechanisms for continuous availability.

4. Security and Compliance:
- Adhere to healthcare data security standards (e.g., HIPAA) and other relevant regulations.
- Regular security audits and updates to protect against data breaches.

5. Usability and User Experience:
- Design an intuitive user interface that is user-friendly for healthcare professionals and patients.
- Ensure accessibility for users with disabilities.

6. Data Backup and Recovery:
   - Implement regular data backup procedures to prevent data loss.
   - Enable efficient data recovery mechanisms in case of system failures.

7. Data Privacy and Confidentiality:
   - Ensure strict data privacy and confidentiality measures.
   - Protect against unauthorized access to sensitive patient information.

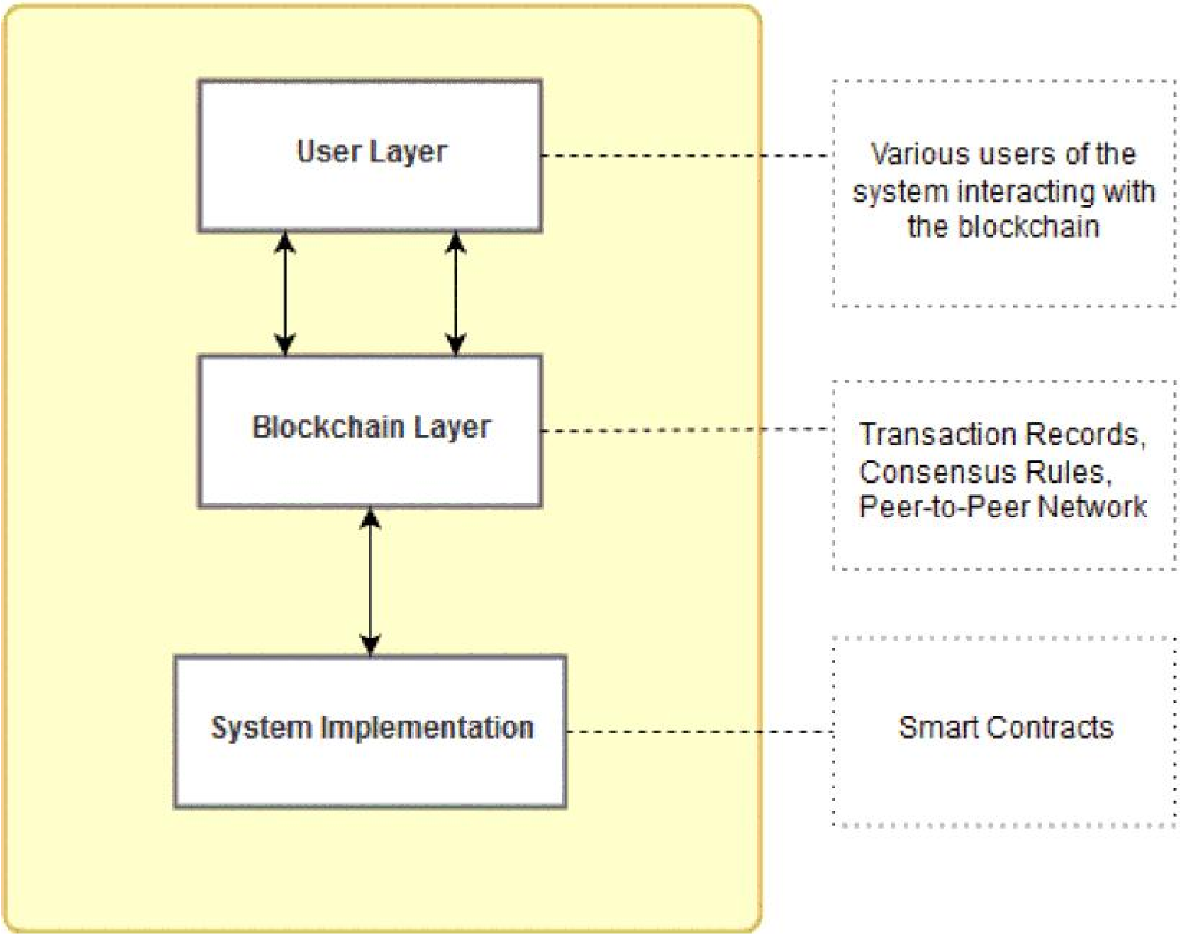
8. Documentation and Training:
   - Provide comprehensive system documentation for users and administrators.
   - Offer training programs for users to effectively utilize the EHR system.

9. Integration Capabilities:
   - Support integration with existing healthcare IT systems, such as laboratory systems and billing software.
   - Ensure compatibility with a wide range of healthcare applications and devices.

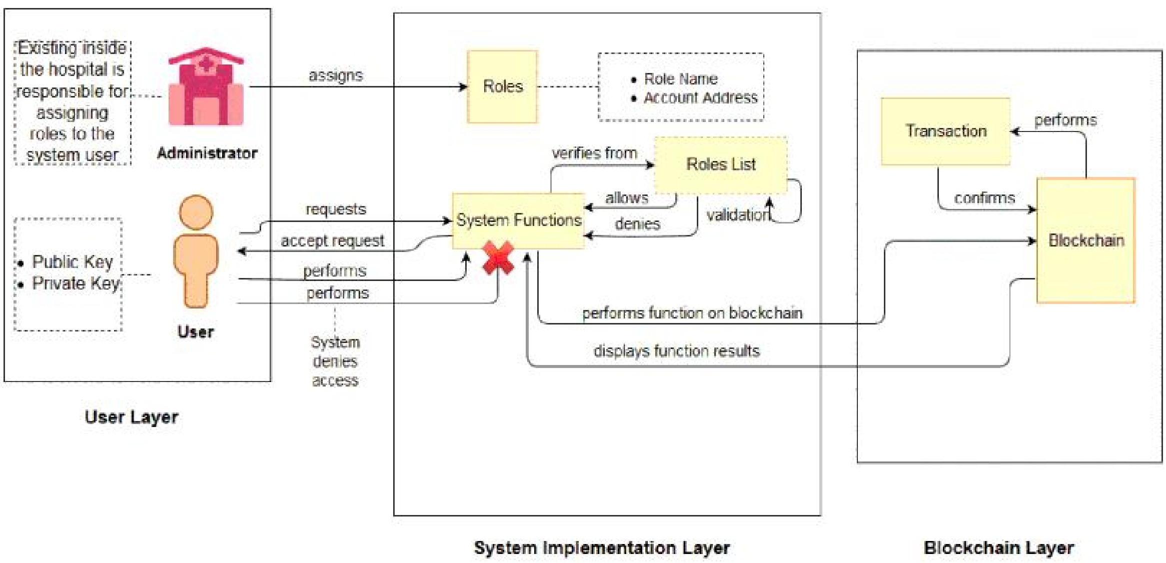
10. Cost-effectiveness:
   - Optimize resource utilization to ensure cost-effectiveness in system maintenance and operation.
   - Provide a clear cost-benefit analysis for stakeholders.

PROJECT DESIGN

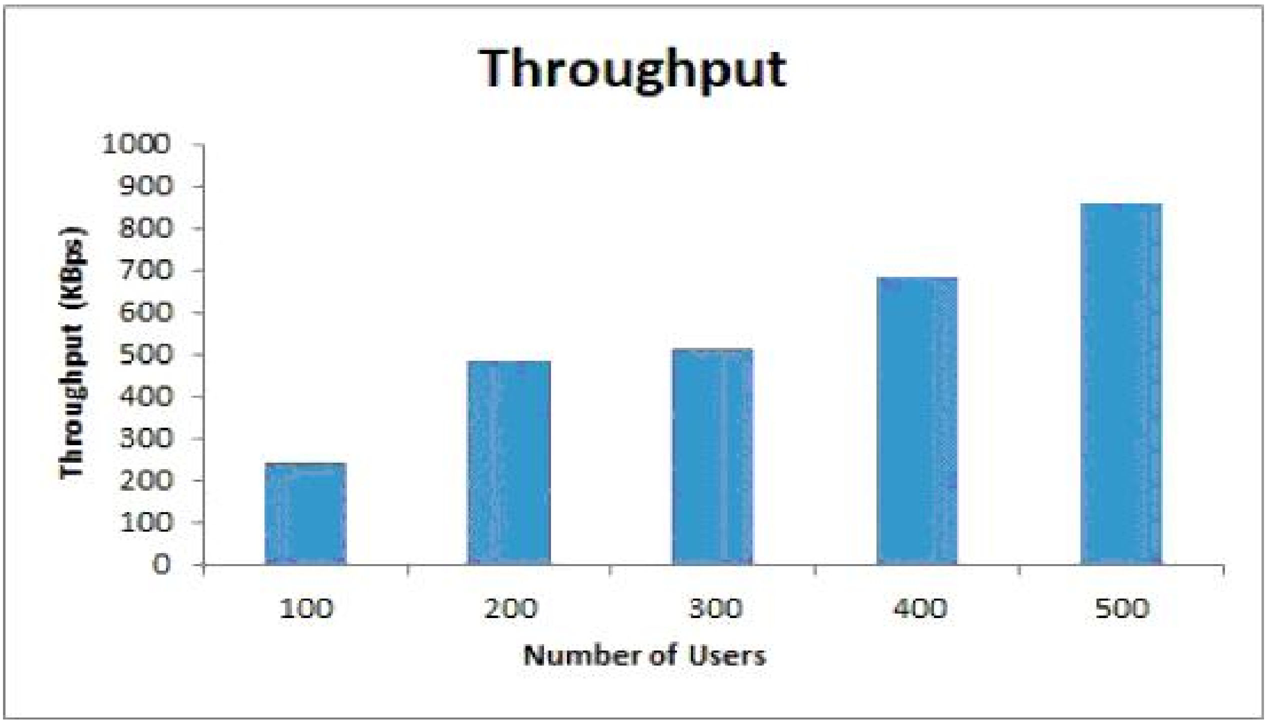
Data Flow Diagrams



1. System design of proposed framework

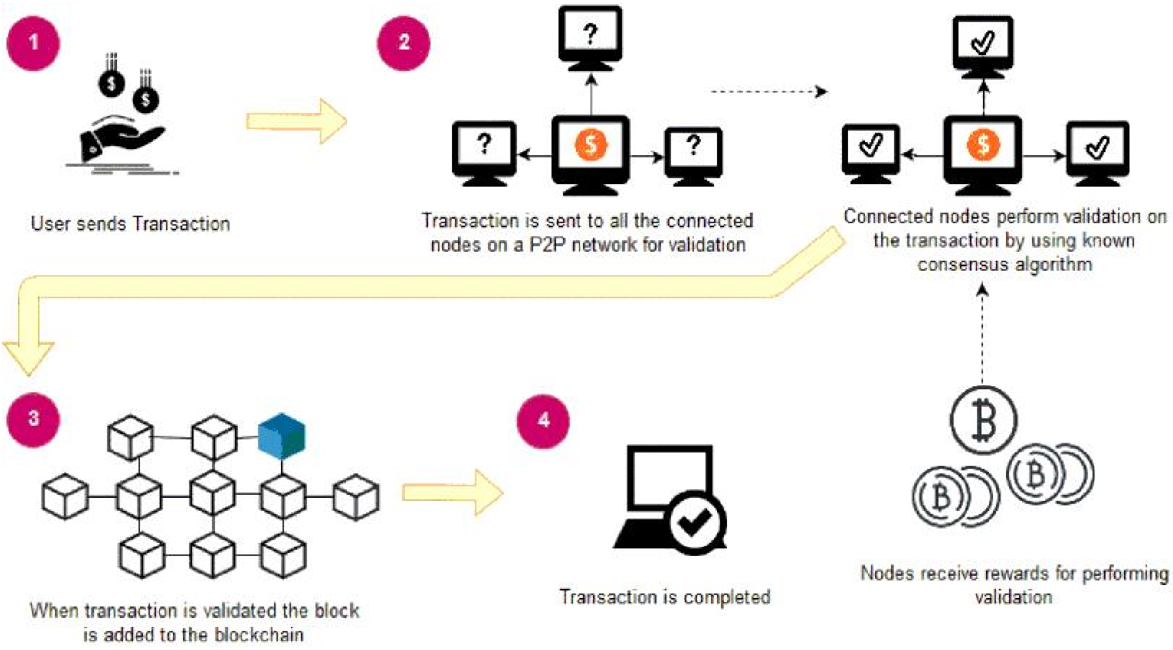


2. User interaction with DApp



3. Throughput of the proposed framework

Solution Architecture



An overview of blockchain architecture

BLOCKCHAIN TECHNOLOGY AND ITS DEPENDENCIES

Architecture:

To understand the blockchain architecture let us use the following figure 1 that explains the whole process of a transaction being send from a user on the blockchain network.

A new transaction being sent by a user on the blockchain network suggests that a new block is created. A block in the blockchain is used for keeping transactions in them and these blocks are distributed to all of the connected nodes in the network. That transaction placed inside a block is broadcasted to all of the nodes in the network. All the nodes in the network have a copy of the complete blockchain that helps them in verification process. When a block containing the user transaction is broadcasted to all of the connected nodes, they verify that the block is not tampered by any means. If this verification results in success then the nodes add that block in their own copy of blockchain.

This whole process of the block being added on the blockchain is done by the nodes reaching upon a consensus where they decide which blocks are valid to be added on the blockchain and which are not. This validation is performed by the connected nodes using some known algorithms to verify the transaction and to ensure that sender is an authenticated part of the network. When a node succeeds in performing the validation that node is rewarded with crypto-currency. This process of validating the transaction is known as mining and the node performing this validation is known as miner.

After validation is done that block is added to the blockchain.

After the whole process of validation is performed the transaction is completed.

Some basic concepts of blockchain technology can be understood in the following descriptions.

Block & Algorithm

Block:

As explained earlier blockchain are formed together by a number of blocks connected together in a peer-to-peer network thus making a decentralized application. The header of these blocks contains hashes of previous blocks in them. A block contains three things in it which are data, hash of current block and hash of previous block. The data could be anything as it depends on the type of blockchain. As in case of bitcoin, the data consists of coins that are actually electronic cash [13]. The hash that is stored in these blocks contains a SHA-256 cryptographic algorithm which is used for unique identification of a block on the chain.

Consensus Algorithm:

Each block that is added on the chain would need to follow some consensus rules for it to be added on the blockchain. For this purpose blockchain technology uses consensus algorithms. The most common consensus algorithm used is Proof of Work (PoW) algorithm and it was used by Nakamoto [13], in bitcoin network. The basic working of this algorithm is that there are number of nodes or participants on a blockchain network so when a transaction is requested to be added on the network by any participating node it needs to be calculated. This process is called mining and the nodes that are performing these calculations are miners .

Algorithm 1 Smart Contract for Patient Records
Assign Roles:

function Define Roles (New Role, New Account)

add new role and account in

roles mapping

end function

Add Data:

function Add Patient Record (contains variables to add data)

if (msg.sender == doctor) then

add data to particular patient's record

else Abort session

end if

end function

Retrieve Data:

functionView Patient Record (patient id)

if (msg.sender == doctor || patient) then

if (patient id) == true then

retrieve data from specified patient (id) return (patient record) to the account that requested the retrieve operation

else Abort session

end if

end if

end function

Update Data:

function Update Patient Record (contains variables to update data)

if (msg.sender == doctor) then

if(id == patient id && name == patient name) then

update data to particular patient’s record

return success

else return fail

end if

else Abort session

end if

end function

Delete Data:

function Delete Patient Record (patient id)

```
if (msg.sender == doctor) then

if (id == patient id) then

delete particular patient’s record

return success

else return fail

end if

else Abort session

end if

end function
```

Challenges Faced by Blockchain Technology

1) Scalability and Storage Capacity

Storage of data on the blockchain causes two main problems, i.e., confidentiality and scalability. The data on the blockchain is visible to everyone that is present on the chain this makes the data vulnerable which is not a desired outcome for a decentralized platform. The data stored on the blockchain would contain patient medical history, records, lab results, X-rays reports, MRI results and many other reports, all of this voluminous data is to be stored on the blockchain that would highly affect the storage capacity of blockchain.

2) Lack of Social Skills

The way the blockchain technology works is understandable by very few people. This technology is still in its initial phases and is constantly evolving. Moreover, the shift from trusted EHR systems to the blockchain technology would take time as hospitals, or any other healthcare institutes need to completely shift their systems to blockchain.

3) Lack of Universally Defined Standards

As this technology is still in the initial phases and is constantly evolving so there is no defined standard for it. Due to this the implementation of this technology in healthcare sector would also take more time and effort. As it would require certified standards from international authorities that overlook the standardization process of any technology. These universal standards would benefit in deciding upon the data size, data format and type of data that could be stored on the blockchain. Moreover, the adaptation of this technology would become easier due to the defined standards, as they could be easily enforced in the organizations.

CODING & SOLUTIONING

Features 1

1) Decentralization

With blockchain the information is distributed across the network rather than at one central point. This also makes the control of information to be distributed and handled by consensus reached upon by shared input from the nodes connected on the network. The data that was before concentrated at one central point is now handled by many trusted entities.

2) Data Transparency

Achieving data transparency in any technology is to have a trust based relationship between entities. The data or record at stake should be secured and temper proof. Any data being stored on the blockchain is not concentrated at one place and is not controlled by one node but is instead distributed across the network. The ownership of data is now shared and this makes it to be transparent and secure from any third party intervention.

3) Security and Privacy

Blockchain technology uses cryptographic functions to provide security to the nodes connected on its network. It uses SHA-256 cryptographic algorithm on the hashes that are stored on the blocks. SHA stands for Secure Hashing Algorithm, these hashes provide security to the blockchain as data integrity is ensured by them. Cryptographic hashes are strong one way functions that generate checksum for digital data that cannot be used for data extraction. This makes blockchain as such a decentralized platform made secure by the cryptographic approaches which makes it to be a good option for privacy protection of certain applications.

Features 2

Blockchain technology was designed by Nakamoto [13], 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.

A. Theoretical/Analytical Blockchain-Based Research

Gordon and Catalini [14], 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 blockchains should be used in healthcare. This study also identified four factors or approaches due to which healthcare sector needs 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.

Eberhardt and Tai [20], 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 define blockchain as composition of various computational and economical concepts based on peer-to-peer system. The aim of this study was to find which data should be stored on-chain and what could be stored off-chain. This study presented five 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.

Vujičić et al. [21], presented an overview of blockchain technology, bitcoin and Ethereum. The authors define 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 defined 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 bitcoins' blockchain.

Wang et al. [22], conducted a study that focused on smart contracts and its application in blockchain technology. They first introduce 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. The paper also discusses an important future trend of parallel blockchain that intends to create such blockchain that can optimize two different but important modules.

Kuo et al. [23], conducted a review that discussed several applications of blockchain in biomedical and healthcare sector. The authors identified 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.

B. Prototype/Implementation Blockchain-Based Research

Sahoo and Baruah [24], 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. This study, was helpful in understanding that blockchain can be used with other platforms that are scalable to improve or solve the scalability of this platform.

Zhang et al. [25], 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.

Kim et al. [26] 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 questionnaire is to use 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 a reason 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 are first validated to be correct specified format and then are parsed to differentiate the personal data and specific data related to questionnaire results. This would ensure that data could be shared for future research purposes. The authors also address the scenario when a third party requests to access this questionnaire data, this would need the patients' permission that is asked by the doctor to let third party view that data.

DataBase Schema

Entities and Their Attributes:

1. Patients:
   - Patient ID (Primary Key)
   - First Name
   - Last Name
   - Date of Birth
   - Contact Information

2. Healthcare Providers:
   - Provider ID (Primary Key)
   - Name
   - Specialization
   - Contact Information

3. User Accounts:
   - User ID (Primary Key)
   - Username
   - Password (hashed)

- Role (Patient, Healthcare Provider, Administrator)

4. Electronic Health Records (EHRs):
   - Record ID (Primary Key)
   - Patient ID (Foreign Key)
   - Provider ID (Foreign Key)
   - Date of Entry
   - Diagnosis
   - Treatment Plan
   - Lab Results
   - Medication History
   - Notes

5. Access Control:
   - Access Control ID (Primary Key)
   - Patient ID (Foreign Key)
   - Provider ID (Foreign Key)
   - Consent Granted (Boolean)
   - Consent Expiry Date
   - Timestamp of Consent

6. Blockchain Transactions:
   - Transaction ID (Primary Key)
   - Record ID (Foreign Key)
   - Transaction Type (Create, Read, Update, Delete)
   - Timestamp
   - Digital Signature

Table Relationships:

- Each patient is associated with multiple EHR records.
- Each healthcare provider can be associated with multiple EHR records.
- Users are linked to either patients or healthcare providers through their role.
- Access Control defines the permissions for accessing specific EHR records.
- Blockchain Transactions record all actions related to EHRs, including creation, updates, and access requests.

PERFORMANCE & TESTING

In this section we evaluate the performance of the proposed framework. By assessing the performance we can mitigate the risks associated with this novel technology that is understandable by very few individuals.

Experimental Setup

For testing performance of the proposed framework we have conducted experiments by using the following configurations:

Intel Core i7-6498DU CPU @ 2.50GHz 2.60 GHz processor

And 8.00 GB of memory with Windows 64-bit OS (version 10)

We developed our proposed framework by using the Solidity which is programming language of Ethereum. JavaScript and Python are encapsulated in the Solidity language which is provided by the Ethereum to write code in smart contracts.

Data Collection for Performance Evaluation

This section explains what kind of data is used for evaluation of performance of the proposed framework. This section also discusses the metrics that are used to explain the results of this performance evaluation being conducted.

1) Transaction Data

To evaluate the performance of the proposed framework following transaction data with its details are used.

Transaction Deployment Time (tx1)

It is defined as the time when transaction gets deployed. In Ethereum, a smart contract is deployed using the transaction so this deployment time refers to that time.

Transaction Completion Time (tx2)

It is defined as the time when the transaction is completed and confirmed by the blockchain which in this case is Ethereum.

2) Evaluation Metrics

The metrics used for evaluation include the execution time, latency and throughput of the proposed framework. These are explained briefly as follows:

Execution Timeis defined as time duration (in seconds) between the transaction confirmation and its execution in the blockchain network. Mathematically, it is (max (tx2) - min (tx1)).

Throughputrefers to the amount of data that could be transferred from one location to another in a unit amount of time.

Latencyis known as the delay that occurs when a system component is waiting for another component of the system to respond to an action. In terms of time it could be referred as the difference of deployment and completion time of transaction.

Results

1) Performance Assesment

In order to understand how our proposed framework would perform in real-case scenario of various users performing different functions on the framework we conducted performance evaluation using Apache JMeter version 5.1.1 and Apache Version 2.00. Apache JMeter is a desktop performance testing tool which is used for analysis and testing of applications.

a: Average Execution Time

The execution time increases with the number of transactions being increased. These transactions are performed for the various functions that are included in the smart contract whose algorithm is defined in Section V. When there is only one user using the system the functions Assign Roles, Add Patient Recordsand View Patient Records would take 18.29 sec, 1 min 48 sec and 50 sec respectively for these functions to be executed. This time would increase when 100 users are using the system simultaneously.

b: Throughput

Algorithm 1 explains various functions that are included in the smart contract of the proposed framework. By using JMeter we simulated number of users from 100 users to 500 users (with period of 10 to 35), who are using the system and performing its various functions. In JMeter the throughput is represented in Data/time i.e. KB/sec units. While conducting the experiments we simulated the number of users as specified above and evaluated the performance of the system. These simulations are run on the proposed framework and at the end throughput is analyzed.

c: Average Latency

Latency as defined earlier is the delay or difference in time when one system component sends a request and a response is generated by any other system component. The difference between these two actions is defined as latency. Here we have evaluated the average latency of the proposed framework by using JMeter. While evaluating the latency of the proposed framework we simulated the number of users by JMeter. In JMeter latency is measured in terms of milliseconds.

2) Performance Evaluation (Transaction)

Every transaction on Ethereum contains a data payload field. Data payload is included in that transaction which is meant to invoke smart contract functions. This data payload is in the hex-serialized format and has bytes associated with it. Here we would discuss two functions from Algorithm 1 in order to understand the data payload included in the transactions being generated.

Data payload is the optional field of a transaction which is only used when there is some form of interaction with contract functions. It has two important parts,

- Function Selector
- Function Arguments

The function selector are first 4 bytes of Keccak-256 hash, it is used for identification of the smart contract function which is being invoked. The function arguments include various static and dynamic element types which have different rules for encoding them in payload.

3) Comparison of Proposed Framework With Related Work

We also discuss some parameters that are present in our framework and are used for comparison with the related work in this domain. While ensuring the presence of these parameters in the framework it is also considered that it would not compromise the security and privacy of the system. For this both security and privacy are discussed in each of the parameters discusses below.

A. Scalability

Scalability in simpler terms refers to the ability of an information system to perform it functions well in such situations when the storage volume of the system increases or decreases. In case of blockchain technology scalability is an issue that needs some permanent solution. As data size or volume is increasing on the blockchain. Our proposed system used the off-chain storage mechanism as the patient's data stored on the blockchain contains the basic information of patient along with the IPFS hash, i.e., the off-chain scaling solution used in our proposed system framework. This solves the scalability issue mentioned as now huge volume of patient medical record is not stored on the blockchain. As, the data size being stored on the blockchain has now decreased the transactions could also be performed faster. As mentioned earlier, IPFS uses cryptographic hash which is stored in the decentralized manner using peer-to-peer network. This also ensures that while solving the scalability problem the security of the framework is not compromised.

B. Content-Addressable Storage

Content-addressable storage refers to the off-chain storage mechanism of IPFS used in the proposed framework [20]. The sensitive record of patient is stored on the IPFS, which ensures that a hash of the stored record is generated. That hash is now stored in the blockchain and is accessed when needed by the doctors and patients. The IPFS generates the cryptographically secure hash which ensures the security of the data being stored on it. And this also ensures security in our proposed framework.

C. Integrity

Integrity of a system is measured by the trustfulness of that system and also that system storing that information is temper-proof and reliable. This blockchain-based system ensures that it does not compromise this feature. The information stored in this system is intact and is not changed by any unauthorized channel. Moreover, information is available to only the associated parties that are doctors and patients. The users of the system and any third party do not have the right to make any changes in the smart contract as they are not having any access to it. This is done by using the access rules which ensure that the private data or medical records of patients are not accessible and remain temper-proof. Moreover, using IPFS for storage of records also ensures the security of the medical records of the patients.

D. Access Control

Using the Role-based access mechanism, this framework makes sure that every entity of the system is assigned a role. Any third party who is not authorized to have access to the system would not be able to access the system. This system provides a two core security as firstly blockchain technology in itself is secure and uses certain protocols and mechanism to keep itself secure from third-part intrusions. And secondly our system uses the Role-based access that also only allows the users having defined roles to have access to the system and its functions. So, our system would not only ensure security of patient records but would also make sure the access control of entities associated with it. This parameter also ensures that the security of the patient's personal medical data is not compromised and the access is provided to only the authorized users of the system.

E. Information Confidentiality

The patient medical records stored on the blockchain should be secured from any third party access to ensure the confidentiality of the patients' record. The patient’s data include the important information of patient such as the patient medical history, blood group, records, lab results, X-rays reports, MRI results and many other related results and reports. All of this information is critical not only to patients but also to the hospital. Smart contracts are a really helpful element in this system as they ensure transparency, precision and trust on the transactions being performed. The record being stored and accessed in the system are only accessible by the trusted parties. Any untrusted third party trying to access the system is denied access by the system. With the information being kept as confidential from third party access the framework would ensure that it would the aspect of privacy as well.

ADVANTAGES & DISADVANTAGES

Advantages

1. Enhanced Data Security: Implementing blockchain in Electronic Health Records (EHRs) significantly improves data security by encrypting and decentralizing patient information. This reduces the risk of data breaches and unauthorized access.

2. Improved Patient Privacy: Blockchain-based EHRs empower patients to have more control over their data, granting or revoking access as needed. This enhances patient privacy and gives individuals more ownership of their health information.

3. Interoperability: The project facilitates seamless data sharing among healthcare providers, leading to better coordination of care. Blockchain's interoperability features reduce data fragmentation and improve the quality of patient care.

4. Data Integrity: Blockchain ensures the integrity of EHRs by creating immutable records. This reduces the chances of data inconsistencies or tampering, enhancing the reliability of medical information.

5. Efficient Consent Management: Smart contracts and transparent consent mechanisms make it easier for patients to manage who can access their records. This streamlines consent management and boosts patient engagement.

6. Transparency and Auditability: The transparent nature of blockchain technology allows for detailed audit trails of all actions related to EHRs. This transparency fosters trust and accountability.

7. Reduced Costs: Over time, blockchain can reduce costs related to data breaches, data reconciliation, and administrative overhead. It can lead to cost savings for healthcare organizations.

Disadvantages

1. Implementation Challenges: Integrating blockchain into existing EHR systems can be complex and costly. Healthcare organizations may face resistance to change and may struggle with the technical aspects of implementation.

2. Scalability: Managing large volumes of healthcare data on a blockchain network can be challenging. Ensuring scalability while maintaining data security is a significant concern.

3. Regulatory Compliance: Healthcare is heavily regulated, and ensuring that blockchain-based EHRs comply with all relevant laws and standards can be a complex and ongoing process.

4. Initial Investment: Implementing blockchain technology requires a significant initial investment in infrastructure, training, and development. Smaller healthcare organizations may find this cost-prohibitive.

5. User Adoption: Healthcare professionals may need time to adapt to new EHR systems based on blockchain technology. Training and change management efforts are required for successful user adoption.

6. Technological Maturity: Blockchain technology is evolving, and the healthcare industry may need to wait for it to mature further before achieving its full potential.

7. Data Recovery: In cases of lost private keys or other technical issues, recovering patient data from a blockchain can be challenging, if not impossible.

8. Energy Consumption: Some blockchain implementations, especially proof-of-work systems, can have high energy consumption, which may not align with environmental sustainability goals.

CONCLUSION

The integration of blockchain technology into Electronic Health Records (EHRs) presents a promising avenue for improving the healthcare industry. This project has highlighted several advantages, including enhanced data security, improved patient privacy, better interoperability, data integrity, efficient consent management, transparency, and potential cost savings.

However, challenges such as implementation complexity, scalability, regulatory compliance, initial investment, and user adoption must be addressed. The success of blockchain in EHRs will depend on the willingness of healthcare organizations to adapt and invest in this transformative technology.

As blockchain technology continues to mature and gain acceptance, it holds the potential to revolutionize the management of EHRs and healthcare data. Further research and development in this field are essential to realize the full benefits of blockchain in healthcare. It is crucial to work collaboratively with healthcare professionals, policymakers, and technology experts to refine and implement blockchain solutions effectively.

FUTURE SCOPE

The future of blockchain in Electronic Health Records is promising and offers several avenues for further exploration:

1. Advanced Security Measures: Research and development can focus on creating more advanced security measures to safeguard patient data, such as zero-knowledge proofs and enhanced encryption techniques.

2. Interoperability Standards: The development of standardized protocols for healthcare data interoperability on blockchain networks will be pivotal in achieving seamless data exchange between different providers.

3. Cross-Border Healthcare: Blockchain can facilitate secure cross-border healthcare data exchange, allowing patients and providers to access medical information across international boundaries.

4. Integration with Emerging Technologies: Combining blockchain with other emerging technologies like artificial intelligence and the Internet of Things can lead to more advanced diagnostics and patient care.

5. Regulatory Frameworks: The establishment of comprehensive regulatory frameworks and industry standards is crucial for the widespread adoption of blockchain in healthcare.

6. Blockchain-based Health Identity: Creating decentralized health identity systems can empower patients to own and control their medical information, further enhancing privacy and security.

7. Research and Clinical Trials: Blockchain can streamline data management in medical research and clinical trials, offering transparency and traceability for research data.

8. Education and Training: Investing in education and training programs for healthcare professionals is essential to ensure they can effectively use blockchain-based EHR systems.

9. Reduced Environmental Impact: Exploring eco-friendly consensus mechanisms to reduce the energy consumption associated with blockchain networks.

The future scope of blockchain in Electronic Health Records is expansive, with potential benefits for healthcare organizations, providers, and patients. As the technology matures and solutions become more tailored to the healthcare sector's unique needs, blockchain is poised to drive efficiency, security, and transparency in healthcare data management, ultimately improving patient outcomes and the overall quality of care.

APPENDIX

Source Code:

```
import React, { useState } from "react";
import { Button, Container, Row, Col } from 'react-bootstrap';
import '../../node_modules/bootstrap/dist/css/bootstrap.min.css';
import { contract } from "./connector";

function Home() {
 const [Id, setId] = useState("");
 const [name, setName] = useState("");
 const [pAddr, setpAddr] = useState("");
 const [disease, setdisease] = useState("");
 const [contact, setContact] = useState("");
 const [recordId, setrecordId] = useState("");
 const [newOwner, setNewOwner] = useState("");
 const [recordIdData, setrecordIdData] = useState("");
 const [Data, setData] = useState("");
  const [Wallet, setWallet] = useState("");



 const handleId = (e) => {
  setId(e.target.value)
 }

 const handleName = (e) => {
  setName(e.target.value)
 }

 const handlePatientAddress = (e) => {
```

```
 setpAddr(e.target.value)
}

const handleDisease = (e) => {
 setdisease(e.target.value)
}

const handleContact = (e) => {
 setContact(e.target.value)
}

const handleCreateRecord = async() => {
 try {
  let tx = await contract.createRecord(Id, name, pAddr, disease, contact)
  let wait = await tx.wait()
  alert(wait)
  console.log(wait.transactionHash);
 } catch (error) {
  alert(error)
 }
}

const handleRecordId = (e) => {
 setrecordId(e.target.value)
}

const handleNewOwner = (e) => {
 setNewOwner(e.target.value)
}

const handleTransferRecord = async () => {
```

```
 try {
  let tx = await contract.transferRecord(recordId.toString(),newOwner)
  let wait = await tx.wait()
  alert(wait.transactionHash)
  console.log(wait);
 } catch (error) {
  alert(error)
 }
}

const handleRecordDataId = (e) => {
 setrecordIdData(e.target.value)
}

const handleRecordData =async () => {
 try {
 let tx = await contract.getRecordData(recordIdData)
 let arr = []
 tx.map(e => arr.push(e))
   setData(arr)
 // alert(tx)
 console.log(tx);

 } catch (error) {
  alert(error)
 }
}

 const handleWallet = async () => {
   if (!window.ethereum) {
     return alert('please install metamask');
```

```
    }

    const addr = await window.ethereum.request({
      method: 'eth_requestAccounts',
    });

    setWallet(addr[0])

  }

 return (
  <div>
   <h1 style={{ marginTop: "30px", marginBottom: "80px" }}>Health Records
Using Blockchain</h1>
     {!Wallet ?

       <Button onClick={handleWallet} style={{ marginTop: "30px",
marginBottom: "50px" }}>Connect Wallet </Button>
       :
       <p style={{ width: "250px", height: "50px", margin: "auto", marginBottom:
"50px", border: '2px solid #2096f3' }}>{Wallet.slice(0, 6)}....{Wallet.slice(-
6)}</p>
     }
     <Container style={{ margin:"Auto" }}>
       <Row >
     <Col>
      <div>

       <input style={{ marginTop: "10px", borderRadius: "5px" }}
onChange={handleId} type="number" placeholder="Enter Record Id"
value={Id} /> <br />
```

```
      <input style={{ marginTop: "10px", borderRadius: "5px" }}
onChange={handleName} type="string" placeholder="Enter name"
value={name} /> <br />

      <input style={{ marginTop: "10px", borderRadius: "5px" }}
onChange={handlePatientAddress} type="string" placeholder="Enter patient
Address" value={pAddr} /><br />

      <input style={{ marginTop: "10px", borderRadius: "5px" }}
onChange={handleDisease} type="string" placeholder="Enter disease"
value={disease} /><br />

      <input style={{ marginTop: "10px", borderRadius: "5px" }}
onChange={handleContact} type="string" placeholder="Enter contact Info"
value={contact} /><br />

      <Button onClick={handleCreateRecord} style={{ marginTop: "10px" }}
variant="primary">Create Record</Button>
     </div>
    </Col>
    <Col>
      <div>
      <input style={{ marginTop: "10px", borderRadius: "5px" }}
onChange={handleRecordId} type="number" placeholder="Enter new record
Id" value={recordId} /><br />
      <input style={{ marginTop: "10px", borderRadius: "5px" }}
onChange={handleNewOwner} type="string" placeholder="Enter new owner
metamask address" value={newOwner} /><br />
      <Button onClick={handleTransferRecord} style={{ marginTop: "10px" }}
variant="primary">Transfer Record</Button>

      </div>
    </Col>
   </Row>
    <Col>
```

```
    <Row style={{marginTop:"100px"}}>

    <input style={{ marginTop: "10px", borderRadius: "5px" }}
onChange={handleRecordDataId} type="string" placeholder="Enter Id"
value={recordIdData} /><br />



    <Button onClick={handleRecordData} style={{ marginTop: "10px" }}
variant="primary">Get Record Data</Button>
     {Data? Data?.map(e => {
     return <p>
       {e.toString()}
     </p>
     }
     ) : <p></p>}
    </Row>
   </Col>
  </Container>

 </div>
 )
}

export default Home;
```

GitHub & Project Demo Link

https://github.com/Imthiyazulhaque/naan-mudhalvan-project.git

https://drive.google.com/drive/folders/1dSmw5rtSOlAJ61Jfnl_8pBu3kaSKT98q?usp=drive_link