DRUG TRACEABILITY

PROJECT REPORT

SUBMITTED BY   **TEAM ID: NM2023TMID00389**

DHARUN D   - 9635201140316   MENTOR: Dr.M.SIVA PRAKASH

KIBIN KUMAR K   - 963520114322   SPOC   : Dr.BHARADWAJ

ABISH X L   - 963520114701

ALWINS LEEM A   - 963520114009

SUJIN G   - 963520114327

In the partial fulfilment of the requirements for the award of a degree of

BACHELOR OF ENGINEERING

IN

MECHANICAL ENGINEERING

STELLA MARY'S COLLEGE OF ENGINEERING

ARUTHENGANVILAI, KALLUKATTI JUNCTION

AZHIKKAL (PO), KANYAKUMARI- 629202

2023-2024(odd)

Project Report

BLOCK CHAIN TECHNOLOGY FOR ELECTRONIC HEALTH RECORDS

Date	04.11.2023
Team ID	NM2023TMID00389
Project Name	Blockchain Technology For Electronic Health Records

Contents :

1. INTRODUCTION

 A blockchain is a decentralized network that uses peer-topeer (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's native cryptocurrency. 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 relying 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. Smart contracts are identity contracts that include a peer-to-peer agreement's terms of service. It is a collection of code and data discovered at a specific position on the Ethereum blockchain. Smart contracts are used in our suggested approach to transfer records, grant access to medical care experts to see client records, or restrict access to medical care employees. In the healthcare industry, there are various obstacles, such as keeping track of the huge volumes of data created by hospitals. Patient information will be highly secure with the implementation of smart contracts in medical associations. It will limit the number of data leaks caused by hackers. They also offer a new architecture and discuss the benefits, problems, and future trends of combining all three. When compared to standard techniques, their suggested architecture beats them in terms of the average packet delivery ratio, average latency, and average energy savings,addressed a blockchain-based certificate concept for more authentication. It uses the blockchain's integrity, so the serial numbers of certificates are saved on the blockchain rather than on the original certificates. The design incorporates alpha-blending of unique impressions to prevent further counterfeiting. Agbo performed an analysis of the current blockchain development in the healthcare industry. According to their findings, blockchain

could be a feasible solution for a range of healthcare applications such as medicine management, biological research, and electronic health record administration. Sharma suggested a cyber-physical system for e-healthcare data transmission services that is both energy and service-level agreement (SLA) efficient. Through developments in the ad hoc on-demand distance vector (AODV) protocol, the suggested phenomena will be upgraded to assure security by identifying and deleting unwanted devices/nodes participating throughout the communication process. The framework targets two security concerns that have a significant impact on network services: grey and black holes. Pariselvam and Swarnamukhi discussed the issues and various protective strategies for securing the privacy of health information in the cloud. A new cloud-based strategy for protecting patient information based on difficulties and varying security has been proposed. This approach provides for the encryption of strong and secure indicators using separate cryptographic keys, as well as the merging of protected data from many sources in the cloud without the content being known.

PROJECT REVIEW

A project review for an Electronic Health Record (EHR) system utilizing blockchain technology reveals a promising and innovative approach to healthcare data management. The integration of blockchain in EHR systems has the potential to enhance data security, privacy, and interoperability. Blockchain's decentralized nature ensures that patient records are tamper-proof and transparent, reducing the risk of unauthorized access or data breaches. Moreover, smart contracts can be employed to automate processes like consent management and data sharing, streamlining administrative tasks. Despite these advantages, challenges such as scalability and regulatory compliance need to be carefully addressed. In conclusion, the project's use of blockchain in EHR demonstrates a commendable effort to revolutionize healthcare data management, but it must navigate these challenges to fully realize its potential. Title: Enhancing Electronic Health Records (EHR) with Blockchain Technology: A Comprehensive Project Review. In recent years, electronic health records (EHR) have emerged as a transformative tool in healthcare, promising improved patient care, streamlined administrative processes, and better data accessibility. However, despite their potential benefits, EHR systems are not without their challenges, such as data security, interoperability, and patient data control. This project review explores the integration of blockchain technology into EHR systems as a means to address these challenges and enhance the overall

effectiveness of electronic health records. Electronic health records (EHR) have gained prominence due to their ability to digitize patient data, making it easier to access and share health information among healthcare providers. However, these systems often suffer from data fragmentation, privacy concerns, and limited interoperability. This necessitates a closer examination of the potential role of blockchain technology in addressing these issues. Blockchain is a distributed ledger technology known for its security, transparency, and immutability. These characteristics make it a compelling choice for healthcare applications, including EHR systems. The ability to secure health data, maintain data integrity, and enable patients to have greater control over their records are some of the key aspects that make blockchain an attractive option. One of the primary benefits of integrating blockchain into EHR is enhanced data security. Blockchain uses cryptographic techniques to secure data, ensuring that patient records are tamper-proof. This aspect is particularly crucial in healthcare, where the privacy and confidentiality of patient information are paramount.

PURPOSE

The purpose of using blockchain technology in Electronic Health Records (EHR) is to revolutionize and enhance the healthcare industry's data management, security, interoperability, and patient-centric care. Blockchain, as a decentralized and immutable ledger, offers several critical advantages for EHR systems: Data Security and Integrity, Blockchain ensures the security and integrity of patient health records by employing cryptographic techniques to create a tamper-proof ledger. This safeguards sensitive health information against unauthorized access, fraud, and data breaches, which have been significant concerns in traditional EHR systems. Patient Control and Consent, Blockchain can enable patients to have greater control over their health data. Through smart contracts and consent mechanisms, patients can grant or revoke access to their records, promoting transparency and patient empowerment in healthcare decision-making. Interoperability, Blockchain can facilitate the seamless sharing of health records across different healthcare providers and institutions. The decentralized nature of blockchain allows for standardized data exchange protocols and ensures that data is consistent and up-to-date, promoting better coordination of care and reducing duplication of tests and treatments. Reduced Administrative Overheads, By automating various administrative processes, such as billing and insurance claims, blockchain can reduce the administrative costs associated with

managing EHR systems. This, in turn, can lead to more cost-effective healthcare services. Immutable Audit Trail, Every transaction on the blockchain is recorded in a transparent and immutable manner. This feature is particularly valuable in EHR, as it allows for a comprehensive audit trail of all interactions with patient data, which can be crucial for regulatory compliance and resolving disputes. Research and Analytics, The use of blockchain in EHR can facilitate research by securely and efficiently providing access to large datasets for medical research and clinical trials. Data analytics can be performed with the assurance of data quality and patient privacy. Streamlined Insurance and Billing, Blockchain can simplify the insurance and billing processes in healthcare by reducing fraud and errors. Smart contracts can automate claims processing and payments, making the system more efficient and reducing the administrative burden on healthcare providers. Disaster Recovery and Redundancy, Blockchain's distributed nature ensures that healthcare data is redundantly stored across multiple nodes. This redundancy enhances data resilience, making it less vulnerable to data loss due to natural disasters or technical failures. Compliance and Regulation, Blockchain can help EHR systems comply with increasingly stringent healthcare regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States. The transparent and secure nature of blockchain can simplify the auditing and reporting processes required for compliance. In summary, the integration of blockchain technology into Electronic Health Records serves the overarching goal of improving the quality, security, and accessibility of healthcare data. It empowers patients, enhances data integrity, reduces administrative overhead, fosters interoperability, and opens new avenues for research and innovation in the healthcare industry, ultimately aiming to deliver better, more efficient, and patient-centric healthcare services.

2. LITERATURE SURVEY

EXISTING PROBLEM

Electronic Health Records (EHR) have revolutionized healthcare by digitizing patient information, improving data accessibility, and streamlining healthcare processes. However, despite their many advantages, EHR systems are not without their challenges, and the integration of blockchain technology holds the potential to address some of the existing problems in this domain. One of the significant issues with EHR systems are,

Data security and privacy: EHRs store highly sensitive patient data, and breaches can have severe consequences. Traditional EHR systems rely on centralized databases, making them susceptible to cyberattacks and unauthorized access. Blockchain technology, known for its decentralized and immutable ledger, can enhance data security by providing a secure and transparent way to record and verify access to patient information. This ensures that patient records are tamper-proof and accessible only to authorized parties.

Data interoperability: Healthcare providers often use different EHR platforms that may not easily communicate with one another. This lack of interoperability can result in fragmented patient records, which can hinder efficient care coordination and result in medical errors. Blockchain can establish a standardized protocol for data exchange and interoperability, allowing healthcare providers to share patient information seamlessly and securely across different EHR systems.

Data integrity and authenticity: These are vital in healthcare, as incorrect or fraudulent data can lead to misdiagnoses and improper treatments. Blockchain's immutable ledger ensures data integrity by creating an audit trail of all changes made to patient records. This transparent and traceable system can help maintain the accuracy and authenticity of EHRs.

Patient consent and data control: Thses are critical issues in EHR systems. Patients often have limited control over who accesses their data and for what purposes. Blockchain technology can enable patients to have more granular control over their health data, granting permissions for specific data access, and tracking who has viewed their records. This not only enhances patient privacy but also empowers individuals to have a say in how their data is used.

Insurance fraud and overbilling: Blockchain can address this issue by creating smart contracts that automatically validate and process insurance claims, reducing the potential for fraud and ensuring that healthcare providers are accurately reimbursed. In conclusion, while EHR systems have transformed healthcare by digitizing patient records, they face several challenges related to data security, interoperability, data integrity, patient consent, and fraud prevention. Blockchain technology holds the promise of mitigating these problems by providing a secure and transparent platform for managing electronic health records. By leveraging the decentralized, tamper-proof, and interoperable nature of blockchain, the healthcare industry can enhance the overall quality of care and patient trust while reducing inefficiencies and errors. However, the successful integration of blockchain into EHR

systems will require careful planning, collaboration, and regulatory adaptation to maximize its benefits and address the existing problems in healthcare data management.

Problem Statement Definition

Data security and privacy: Data security and privacy are of paramount importance when it comes to Electronic Health Records (EHR), and blockchain technology has emerged as a promising solution to address these critical concerns. EHR contains sensitive and confidential information about patients' medical histories, diagnoses, treatments, and personal details, making it a prime target for cyberattacks and breaches. Blockchain, with its decentralized and immutable ledger, offers a robust mechanism to safeguard EHR data. In a blockchain-based EHR system, patient records are stored in a distributed network of nodes, ensuring that no single entity has complete control over the data. Each transaction or update to the EHR is recorded in a new block, and these blocks are linked together in a chronological chain. Once a block is added, it becomes nearly impossible to alter or delete the information within it, ensuring data integrity. This immutability and transparency make it extremely challenging for unauthorized individuals to tamper with or access patient records without proper authorization.

Data interoperability: Data interoperability for Electronic Health Records (EHR) has long been a critical challenge in healthcare systems worldwide. The adoption of blockchain technology has emerged as a promising solution to address this issue. Blockchain, with its decentralized and immutable ledger, can revolutionize the way health information is stored, accessed, and shared. In the context of EHR, blockchain ensures data integrity and security by creating a tamper-resistant ledger that records every transaction or modification made to a patient's health record. This not only prevents unauthorized access but also establishes an auditable trail, fostering trust among patients, healthcare providers, and other stakeholders. Moreover, blockchain's decentralized nature eliminates the need for a central authority, reducing the risk of a single point of failure. The use of smart contracts in blockchain technology further enhances data interoperability. These self-executing contracts enable automatic and standardized data exchanges between different EHR systems, overcoming the compatibility issues that have traditionally hindered seamless information sharing among

healthcare providers. Patients can also maintain greater control over their health data, granting or revoking access to specific parties while adhering to privacy regulations like HIPAA in the United States or GDPR in Europe.

Data integrity and authenticity: Ensuring data integrity and authenticity in Electronic Health Records (EHR) is of paramount importance for the healthcare industry, patients, and practitioners alike. Blockchain technology has emerged as a powerful solution to address these critical concerns. Blockchain, essentially a distributed ledger, provides a transparent and tamper-proof system for recording and sharing EHR data. Each transaction, such as a new patient record entry or a change to an existing record, is recorded in a "block" that is linked to the previous one, creating a chain of information. This decentralized structure ensures that data cannot be altered or deleted without consensus from the network, making it highly resistant to data tampering or fraud. Data integrity is maintained through cryptographic hashes, which serve as digital fingerprints for each block. Any modification to a record would require recalculating the hash for that block and all subsequent blocks, which is practically impossible to do without detection. This cryptographic verification guarantees that once data is recorded on the blockchain, it remains unchanged and trustworthy. Data authenticity is established through a consensus mechanism within the blockchain network. In a permissioned blockchain used for EHR, only authorized entities like healthcare providers, patients, and relevant authorities have the ability to validate and add new blocks. This not only prevents unauthorized access but also verifies the legitimacy of data inputs, ensuring that records come from credible sources.

Patient consent and data control: In the context of Electronic Health Records (EHR) management, patient consent and data control are crucial elements, and blockchain technology plays a pivotal role in enhancing these aspects. Patient consent is the cornerstone of ethical healthcare data management. It empowers individuals to make informed decisions about how their medical information is used and shared. Blockchain, with its decentralized and immutable ledger, offers a robust framework for recording and managing patient consent. When a patient provides consent, it can be securely recorded on the blockchain, creating a tamper-proof and auditable record of their authorization. This ensures that patients have greater control over their data, and healthcare providers can only access and share information when explicitly authorized by the patient. Moreover, blockchain's decentralized nature reduces the risk of unauthorized access or data breaches. Patient data is distributed across a network of nodes, making it significantly harder for any single entity to compromise

the system. Access to EHRs can be granted based on predefined smart contracts, which can be executed when the patient's consent is validated. This not only enhances data security but also streamlines data management and sharing processes, reducing administrative overhead. In addition, blockchain technology empowers patients to have real-time visibility into who is accessing their data and for what purposes. This transparency fosters trust between patients and healthcare providers, as individuals can monitor their data's usage and revoke access if they deem it necessary. Furthermore, the immutability of blockchain ensures that once data is recorded, it cannot be altered or deleted without the patient's consent, providing a robust audit trail for data control.

Insurance fraud and overbilling: Insurance fraud and overbilling in the context of Electronic Health Records (EHR) have become significant concerns in the healthcare industry. The adoption of blockchain technology has emerged as a potential solution to combat these issues. By integrating blockchain into EHR systems, healthcare providers can create a tamper-proof and transparent ledger of patient information and medical billing data. This technology ensures that all data entries are time-stamped and cryptographically secured, making it extremely difficult for any unauthorized alterations or fraudulent activities to occur. One of the primary benefits of blockchain in EHR is its ability to maintain data integrity. Patient records, treatment histories, and billing information are securely recorded, and any changes made are visible to authorized parties in real-time, reducing the likelihood of fraudulent alterations. This transparency is particularly useful in preventing overbilling, as all charges can be verified against the documented services provided. Furthermore, blockchain technology allows for the creation of smart contracts, which can automate the billing process and reduce the risk of human error or intentional manipulation. These contracts can be programmed to automatically calculate and process charges based on the services rendered, ensuring accurate billing practices.

3. IDEATION & PROPOSED SOLUTION

Empathy Map Canvas

Empathy Map Canvas: An empathy map is a simple, easy-to-digest visual that captures knowledge about a user's behaviours and attitudes. It is a useful tool to helps teams better understand their users. Creating an effective solution requires understanding the true problem and the person who is experiencing it. The exercise of creating the map helps participants consider things from the user's perspective along with his or her goals and challenges.

Empathy Map : Blockchain Technology For Electronic Health Records

Says 💬	Thinks 🤔	Feels 🙁	Needs 🙏	Does 👥
What are some key phrases or quotes that the user might say?	What might be going through the user's mind?	What emotions might the user be experiencing?	What are the user's underlying needs or desires?	What actions or behaviors might the user exhibit?
I'm concerned about the privacy of my health records.	Will my sensitive health information be safe on the blockchain?	Anxiety about the potential exposure of personal health data.	Greater control over their own health records.	Researching blockchain technology and its applications in healthcare.
I want to have control over who can access my medical information.	How can blockchain technology improve the efficiency of accessing medical records?	Frustration with the complexity of managing medical records.	Assurance of privacy and security of sensitive health information.	Seeking healthcare providers that utilize blockchain for electronic health records.
I find it difficult to trust the security of electronic health records.	Can I trust the accuracy and integrity of the information stored on the blockchain?	Hopeful for improved privacy and security measures.	Simplified and efficient access to medical history.	Expressing concerns about privacy and security to healthcare providers.
I wish I could easily share my medical history with healthcare providers.	Will blockchain eliminate the need for paper-based medical records?	Excited about the potential for seamless sharing of health information.	Trust in the integrity and accuracy of electronic health records.	Advocating for the adoption of blockchain technology in healthcare systems.

Ideation & Brainstorming

Brainstorming provides a free and open environment that encourages everyone within a team to participate in the creative thinking process that leads to problem solving. Prioritizing volume over value, out-of-the-box ideas are welcome and built upon, and all participants are encouraged to collaborate, helping each other develop a rich amount of creative solutions.

Brainstorm & idea prioritization

Use this template in your own brainstorming sessions so your team can unleash their imagination and start shaping concepts even if you're not sitting in the same room.

- 10 minutes to prepare
- 1 hour to collaborate
- 2-8 people recommended

Before you collaborate

A little bit of preparation goes a long way with this session. Here's what you need to do to get going.

🕐 10 minutes

A **Team gathering**
Define who should participate in the session and send an invite. Share relevant information or pre-work ahead.

B **Set the goal**
Think about the problem you'll be focusing on solving in the brainstorming session.

C **Learn how to use the facilitation tools**
Use the Facilitation Superpowers to run a happy and productive session.

Open article →

Define your problem statement

What problem are you trying to solve? Frame your problem as a How Might We statement. This will be the focus of your brainstorm.

🕐 5 minutes

PROBLEM

Many users and doctors prefer paper records. They prefer to keep the medical records in a file system. Some medicine shops are not 100% paperless. Most medicine shops use prescriptions to keep records of their medicines. Patients also keep the paper works for their handy purpose. So adapting to a total paperless blockchain network is a challenging task.

Key rules of brainstorming
To run a smooth and productive session

- Stay in topic.
- Defer judgment.
- Go for volume.
- Encourage wild ideas.
- Listen to others.
- If possible, be visual.

2

Brainstorm

Write down any ideas that come to mind that address your problem statement.

⏱ 10 minutes

NARESH KUMAR.N.P

Doctors should use small blockchains in order to get habituated to the latest technology.

Publishing or sharing documents online is the most obvious and cheapest option to go paperless.

SANJAY KUMAR.S

They should try to use minimum papers. For X-ray plates and other surgery-related documents, they can use paper.

for prescriptions and other file records, the health sector should adopt blockchains as it is easy to store.

LIVINGSTON.I

Offer training and resources to help individuals and organizations understand the benefits of paperless methods and how to use them effectively.

Develop user-friendly, intuitive software and tools that make the transition to paperless methods easier for people of all tech-skill levels.

ASWIN.N

Implement robust data security measures to alleviate concerns about privacy and data breaches.

This could include encryption, secure cloud storage, and access controls.

ARUL.S

Highlight the cost-saving benefits of going paperless, including reduced paper, ink, and storage costs.

Consider offering incentives or subsidies for adopting paperless methods

3

Group ideas

Take turns sharing your ideas while clustering similar or related notes as you go. Once all sticky notes have been grouped, give each cluster a sentence-like label. If a cluster is bigger than six sticky notes, try and see if you and break it up into smaller sub-groups.

⏱ 20 minutes

Emphasize the positive environmental impact of reducing paper usage and going green to gain public and corporate support.

Share examples of successful paperless transitions in similar industries to inspire others to follow suit.

Develop programs to enhance digital literacy, particularly for older or less tech-savvy individuals.

Continually update and improve digital systems to make them more efficient and user-friendly

Encourage collaboration between organizations, businesses, and government agencies to collectively work towards paperless goals.
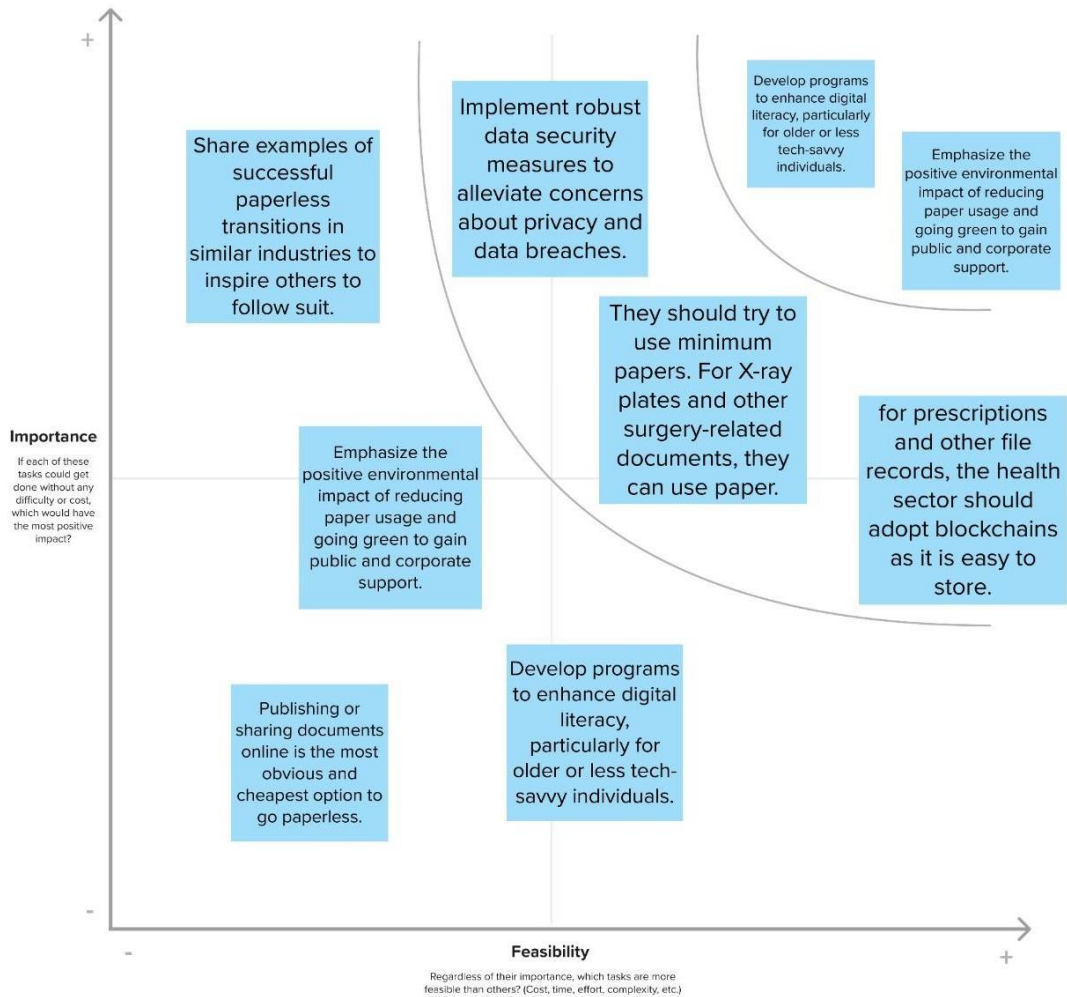
(4)

Prioritize

Your team should all be on the same page about what's important moving forward. Place your ideas on this grid to determine which ideas are important and which are feasible.

⏱ **20 minutes**

Importance

If each of these tasks could get done without any difficulty or cost, which would have the most positive impact?

Share examples of successful paperless transitions in similar industries to inspire others to follow suit.

Implement robust data security measures to alleviate concerns about privacy and data breaches.

Develop programs to enhance digital literacy, particularly for older or less tech-savvy individuals.

Emphasize the positive environmental impact of reducing paper usage and going green to gain public and corporate support.

They should try to use minimum papers. For X-ray plates and other surgery-related documents, they can use paper.

for prescriptions and other file records, the health sector should adopt blockchains as it is easy to store.

Emphasize the positive environmental impact of reducing paper usage and going green to gain public and corporate support.

Publishing or sharing documents online is the most obvious and cheapest option to go paperless.

Develop programs to enhance digital literacy, particularly for older or less tech-savvy individuals.

Feasibility

Regardless of their importance, which tasks are more feasible than others? (Cost, time, effort, complexity, etc.)

4. REQUIREMENT ANALYSIS

Functional requirement

Functional requirements for an Electronic Health Record (EHR) system utilizing blockchain technology are essential to ensure the security, transparency, and efficiency of healthcare data management. Firstly, the system must enable secure and immutable record-keeping through blockchain, guaranteeing the integrity and traceability of patient information. This entails the ability to create, update, and access patient records while maintaining a tamper-proof audit trail. Secondly, the EHR system should support robust user authentication and access control mechanisms to safeguard patient privacy. It must allow for role-based access, ensuring that only authorized personnel can view and modify specific parts of a patient's record. Access logs and permissions management are critical aspects to consider. Furthermore, interoperability is crucial for EHR systems. It should facilitate data exchange between healthcare providers, laboratories, pharmacies, and other stakeholders. This requires adherence to standardized data formats and protocols, promoting seamless communication and data sharing, thereby improving the quality of care. Data encryption and encryption key management are paramount for maintaining the confidentiality of patient records. The system must employ strong encryption methods to protect data both in transit and at rest. The secure storage and management of encryption keys are equally important to prevent unauthorized access. In terms of scalability, the EHR system should be designed to handle a growing volume of healthcare data and transactions without compromising performance. This requires efficient data storage, retrieval, and processing mechanisms, as well as the ability to accommodate the ever-expanding healthcare ecosystem. Audit and compliance functionalities are integral to ensure adherence to healthcare regulations. The system should generate comprehensive audit reports, supporting compliance with data protection laws, healthcare standards, and other relevant regulatory requirements. Additionally, it should allow for easy data rectification and erasure in line with data privacy regulations. User-friendly interfaces and mobile accessibility are crucial to enhance usability for healthcare professionals and patients. The EHR system should offer intuitive interfaces, support mobile access, and provide a seamless user experience to encourage adoption and facilitate efficient healthcare delivery. Finally, disaster recovery and backup capabilities are vital. The EHR system must have robust backup mechanisms and disaster recovery plans to prevent data loss in the event of hardware failures, natural disasters, or cyber attacks. In summary, functional requirements for an EHR system using blockchain should encompass security, privacy, interoperability,

scalability, compliance, usability, and data resilience, all of which are fundamental to the successful adoption and operation of blockchain technology in healthcare data management.

Non-Functional requirements

Non-functional requirements for an Electronic Health Record (EHR) system using blockchain technology are paramount to ensure the system's performance, security, and reliability in a healthcare environment. First and foremost, scalability is essential to accommodate the ever-growing volume of medical records and transactions. The system must be able to handle a high number of concurrent users, support a large number of data entries, and ensure efficient data retrieval. Security is another critical non-functional requirement. The EHR system should employ robust encryption and authentication mechanisms to safeguard sensitive patient data from unauthorized access or tampering. Compliance with healthcare regulations like HIPAA is imperative to ensure patient confidentiality and data integrity. Availability and reliability are essential to ensure continuous access to patient records. The system should have minimal downtime, and data should be redundantly stored to prevent data loss. Additionally, disaster recovery and backup mechanisms should be in place to mitigate the impact of unforeseen events. Performance requirements demand low latency for data retrieval and transaction processing. Users expect a responsive system, and therefore, network bandwidth, data processing speed, and query performance should be optimized. Consistency and data integrity are also crucial to prevent inconsistencies in patient records and ensure the trustworthiness of the blockchain ledger. Interoperability is vital for seamless data exchange between different healthcare providers and systems. The EHR system should adhere to standards like HL7 and FHIR to facilitate data sharing while maintaining data integrity through the blockchain. Usability is another significant non-functional requirement. The user interface should be intuitive, and training requirements for healthcare professionals using the system should be minimal. Accessibility features should also be considered to cater to a diverse user base, including those with disabilities. Lastly, compliance with legal and regulatory requirements, both in th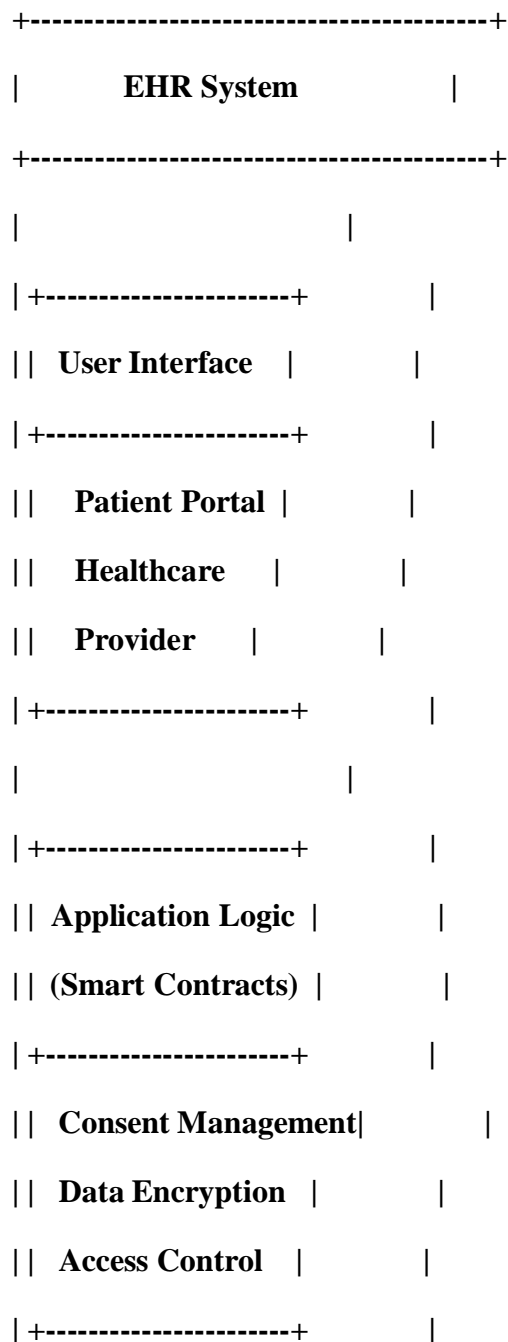e healthcare and blockchain sectors, is non-negotiable. This includes data retention policies, audit trails, and the ability to demonstrate compliance with applicable laws and regulations. In conclusion, non-functional requirements for an EHR system utilizing blockchain technology are integral to its success in the healthcare industry. They encompass scalability, security, availability, performance, interoperability, usability, and compliance, all of which must be meticulously addressed to deliver a system that enhances patient care, data security, and overall healthcare operations.
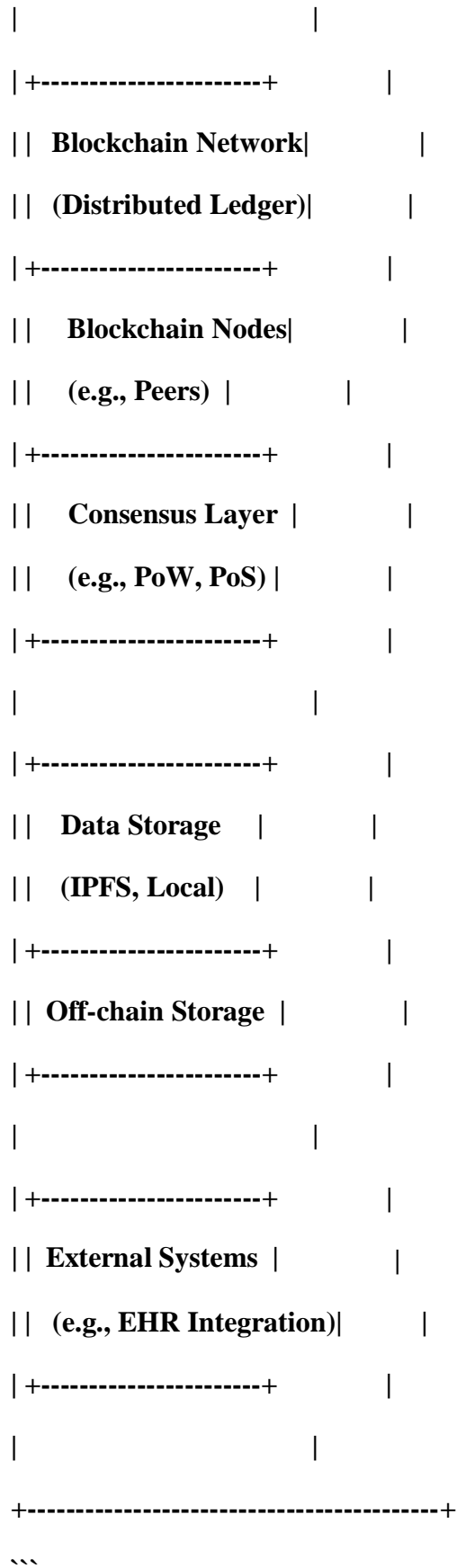
5. PROJECT DESIGN

Architectural Diagram

Designing an architecture diagram for an Electronic Health Record (EHR) system using blockchain technology can be a complex task, as it involves several components and layers. Here's a simplified high-level architecture diagram to give you an overview:

```
+----------------------------------------+
|            EHR System                  |
+----------------------------------------+
|                        |
| +---------------------+           |
| |   User Interface    |           |
| +---------------------+           |
| |   Patient Portal    |           |
| |   Healthcare        |           |
| |   Provider          |           |
| +---------------------+           |
|                        |
| +---------------------+           |
| |  Application Logic  |           |
| |  (Smart Contracts)  |           |
| +---------------------+           |
| |  Consent Management |           |
| |  Data Encryption    |           |
| |  Access Control     |           |
| +---------------------+           |
```

```
|                        |
|+---------------------+           |
||  Blockchain Network|           |
||  (Distributed Ledger)|           |
|+---------------------+           |
||   Blockchain Nodes|           |
||   (e.g., Peers)  |           |
|+---------------------+           |
||   Consensus Layer |           |
||   (e.g., PoW, PoS) |           |
|+---------------------+           |
|                        |
|+---------------------+           |
||   Data Storage    |           |
||   (IPFS, Local)    |           |
|+---------------------+           |
||  Off-chain Storage |           |
|+---------------------+           |
|                        |
|+---------------------+           |
||  External Systems  |           |
||  (e.g., EHR Integration)|           |
|+---------------------+           |
|                        |
+-------------------------------------+
```

Explanation of components:

User Interface: This is the front-end of the EHR system, accessible to users, including patients and healthcare providers. It can consist of patient and healthcare provider portals. **Application Logic (Smart Contracts):** This layer manages the core functionality of the EHR system. It includes smart contracts for handling patient consent, data encryption, access control, and other business rules. **Blockchain Network (Distributed Ledger):** This is the underlying blockchain infrastructure. It consists of a distributed ledger where EHR data is stored in a tamper-proof and decentralized manner. The network comprises multiple blockchain nodes (peers) distributed across the network. **Consensus Layer:** This layer ensures agreement among network nodes about the state of the blockchain. It could use various consensus mechanisms like Proof of Work (PoW) or Proof of Stake (PoS). **Data Storage:** EHR data is stored on the blockchain and may use off-chain storage solutions like the InterPlanetary File System (IPFS) or local databases for scalability and performance reasons. **External Systems**: This part integrates the EHR system with external healthcare systems or EHR systems to ensure interoperability and data exchange. The key features of this architecture are security, privacy, and data integrity, which are ensured by the blockchain technology. Smart contracts manage patient consent, data encryption, and access control, enhancing the privacy and security of patient records. Data is stored in a distributed and immutable ledger, reducing the risk of data tampering and unauthorized access. Please note that this is a simplified architecture, and real-world implementations can vary greatly depending on the specific requirements, regulatory constraints, and the choice of blockchain technology (e.g., Ethereum, Hyperledger Fabric) and consensus mechanisms. Furthermore, the architecture must adhere to healthcare data security standards and regulations, such as HIPAA (in the United States) or GDPR (in the European Union).
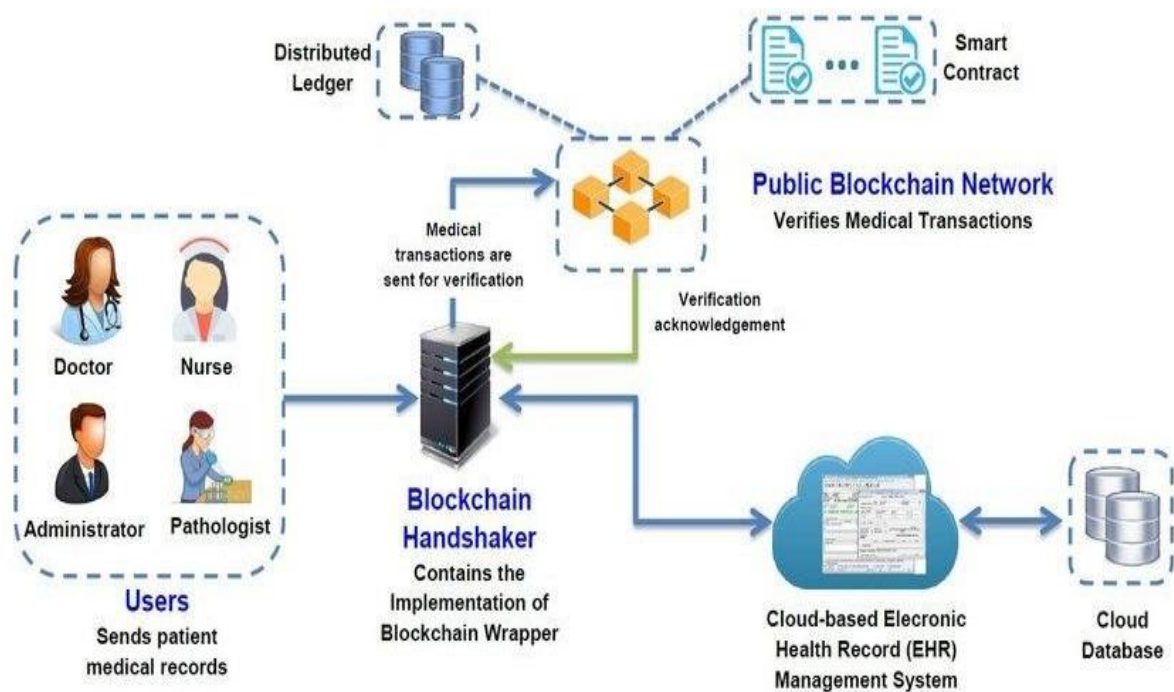
Designing an Electronic Health Record (EHR) system using blockchain technology requires a deep understanding of both healthcare data management and blockchain technology. Blockchain can provide several benefits in the healthcare sector, such as data security, interoperability, and patient control. Here's an outline of the architecture for an EHR system using blockchain:

Network Structure:

Permissioned Blockchain, Use a permissioned blockchain, which allows only authorized participants, such as healthcare providers, patients, and regulatory bodies, to access and validate transactions.

Blockchain Components:

Nodes:

EHR Nodes: These nodes store and manage electronic health records.

Consensus Nodes: Responsible for reaching consensus on transactions. Use a consensus mechanism like Practical Byzantine Fault Tolerance (PBFT) or Proof of Authority (PoA) to ensure data integrity.

Patient Nodes, Patients should have their nodes to control access to their health records.

Smart Contracts, Develop smart contracts to define the rules for accessing and updating health records, consent management, and data sharing.

Blockchain Protocol Choose a suitable blockchain protocol such as Ethereum, Hyperledger Fabric, or a custom solution, depending on the specific requirements of your EHR system.

Data Structure:

Health Records:

Store patient data, including medical history, diagnoses, treatment plans, prescriptions, and lab results. Use appropriate data standards like HL7 FHIR for interoperability.

- Encrypt sensitive patient data to ensure privacy.

- Consent Records.

- Record patient consent for data sharing.

- Implement granular consent mechanisms to specify who can access what parts of the EHR.

-Timestamps and Provenance: Include timestamps for every transaction and maintain a record of data provenance to track changes and maintain data integrity.

Access Control and Identity Management:

- Use a robust identity management system to authenticate users and ensure that only authorized individuals can access EHR data.

- Implement multi-factor authentication for added security.

- Patients should have control over who can access their data and can revoke access at any time.

Interoperability:

- Implement standards like HL7 FHIR to ensure interoperability with other healthcare systems.

- Use middleware solutions to convert and route data between legacy systems and the blockchain.

Privacy and Security:

 - Implement encryption and data masking techniques to protect patient data.

   - Regularly audit and monitor the blockchain for unauthorized access and suspicious activities.

Consent Management:

   - Create a user-friendly interface for patients to manage their consent preferences.

   - Implement smart contracts to enforce consent rules.

Data Sharing:

- Allow authorized entities to request access to specific EHR data through smart contracts.

   - Ensure that data sharing complies with applicable laws and regulations, such as HIPAA in the United States.

Audit Trails and Compliance:

   - Maintain detailed audit trails of all EHR transactions.

   - Ensure compliance with data protection regulations, such as GDPR or HIPAA.

Scalability and Performance:

 - Address scalability challenges through proper blockchain protocol selection and optimization.

    - Consider off-chain storage solutions for large data sets.

Disaster Recovery: Implement robust disaster recovery and backup mechanisms to ensure data availability in case of system failures.

User Training and Support: Train healthcare providers, administrators, and patients on how to use the blockchain-based EHR system effectively.

Regulatory Compliance: Ensure that the EHR system complies with relevant healthcare regulations and standards. Remember that implementing a blockchain-based EHR system is a complex endeavor that requires collaboration between healthcare providers, technologists, and legal experts to ensure the system is secure, compliant, and user-friendly. Additionally, the architecture may need to be adapted to specific regulatory requirements in your jurisdiction.

6. PROJECT PLANNING & SCHEDULING

Technical Architecture:

Before the introduction of smart contacts on the blockchain, the main discussions on Electronic Health Record (EHR) Management focused on whether to use cloud infrastructures or local centralized systems for storing and sharing EHRs. These centralized systems implied that each hospital and healthcare company would have to keep data on premises in locally managed structures and databases.

A blockchain is a data structure where the records are stored in a linked sequence of blocks. This sequence forms a distributed ledger, which means it is replicated in multiple machines, called nodes, that communicate with one another. The nodes form a peer-to-peer network where every update to the ledger must be accepted by the network using a consensus protocol. The consensus protocol assures that everybody has the same view on the status of the system.

After the design and implementation of a basic EHRs management system and the execution of a set of test cases, it will be possible to discuss the benefits and trade-offs that the system entails. The discussion will focus on the performance of a permissioned blockchain for EHRs management. Normal and disaster scenarios will be compared using the following indicators to get important insights on how a crisis affects the operations of a blockchain network:

• Success rate: the number of successes and failures of a batch of requests. It is important to limit the number of failures caused by a surge of requests during an emergency;

• Transaction commit and read latency: this refers to the time it takes for the blockchain-based system to process an access request to an EHR in a disaster situation. It is important as timeliness in getting health data, especially in emergencies, is critical.

• Transaction commit and state read throughput (TPS): this refers to the number of requests that can be managed by the system at the same time. Being able to access and modify a growing number or request is essential to enable everybody to interact with the system;

• Resource consumption (CPU, Memory and network IO): it is necessary to take these parameters into account as they affect all the other indicators.
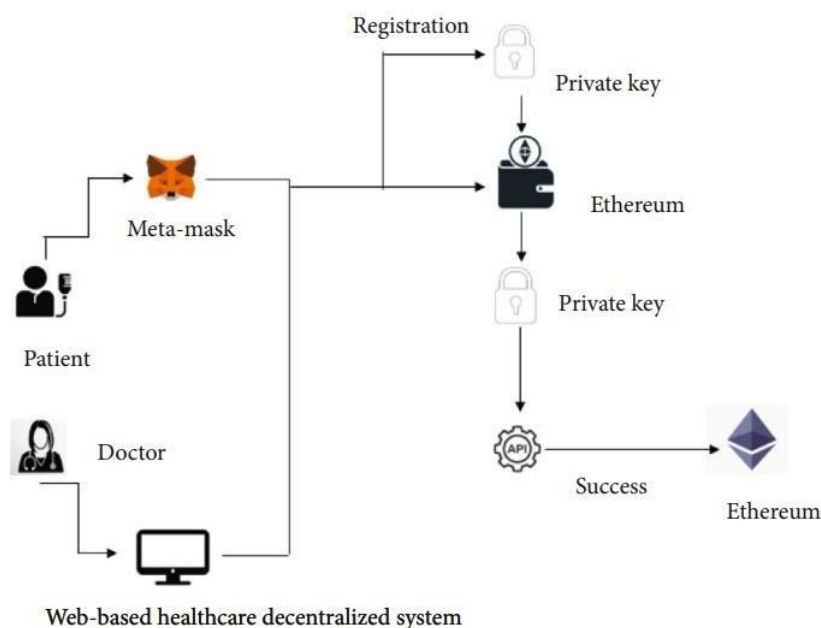
**Sprint Planning & Estimation:**

Block Diagram illustrates 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. 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 wrapper. This proposed architecture makes use of the Ethereum blockchain network. A distributed ledger that connects blockchain nodes is known as the public blockchain network. Blockchain nodes are miners who are in charge of updating the blockchain based on the decision method. Alternatively, blockchain nodes accept transactions and use the network's smart contracts to authenticate them.

**Block diagram of the blockchain-based EHR system**
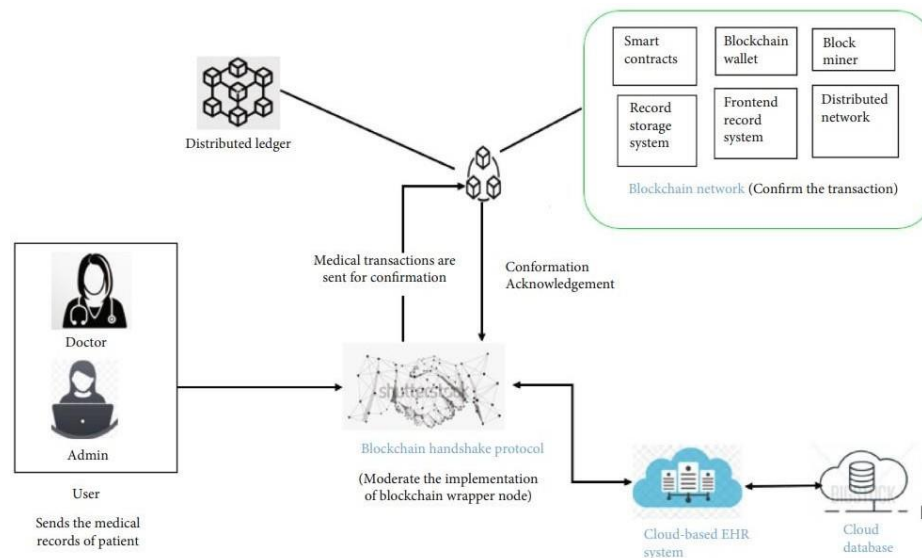
Use case diagram of the EHR system
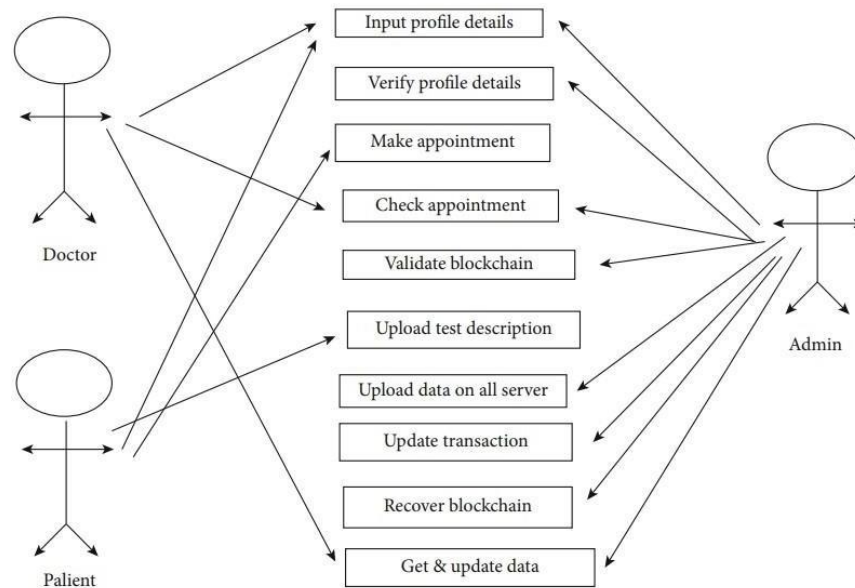
Sprint Delivery Schedule:

Flowchart of the Proposed System shows 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.
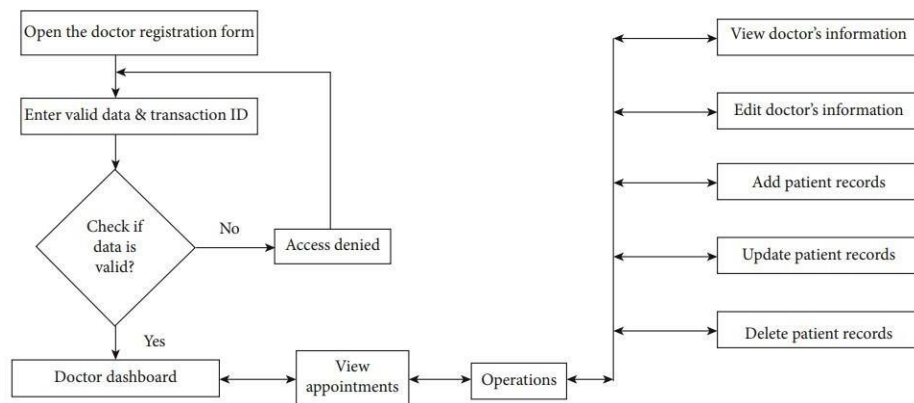
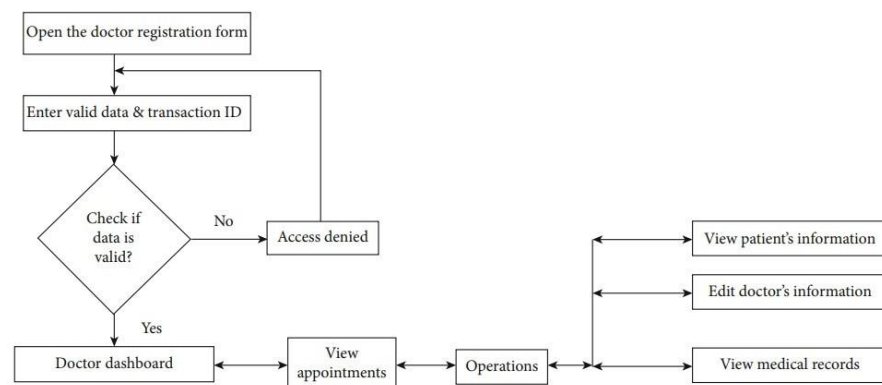**Flowchart of explaining the process of creating a medical record:**
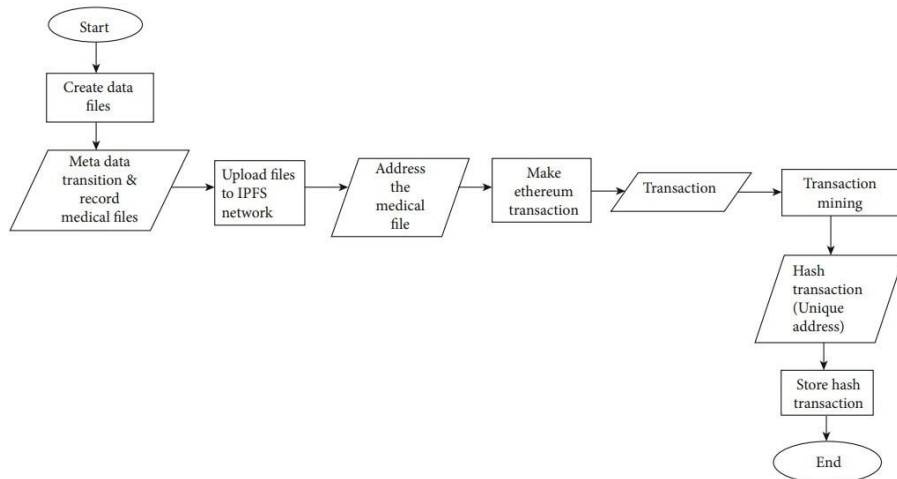
Flowchart of the admin dashboar
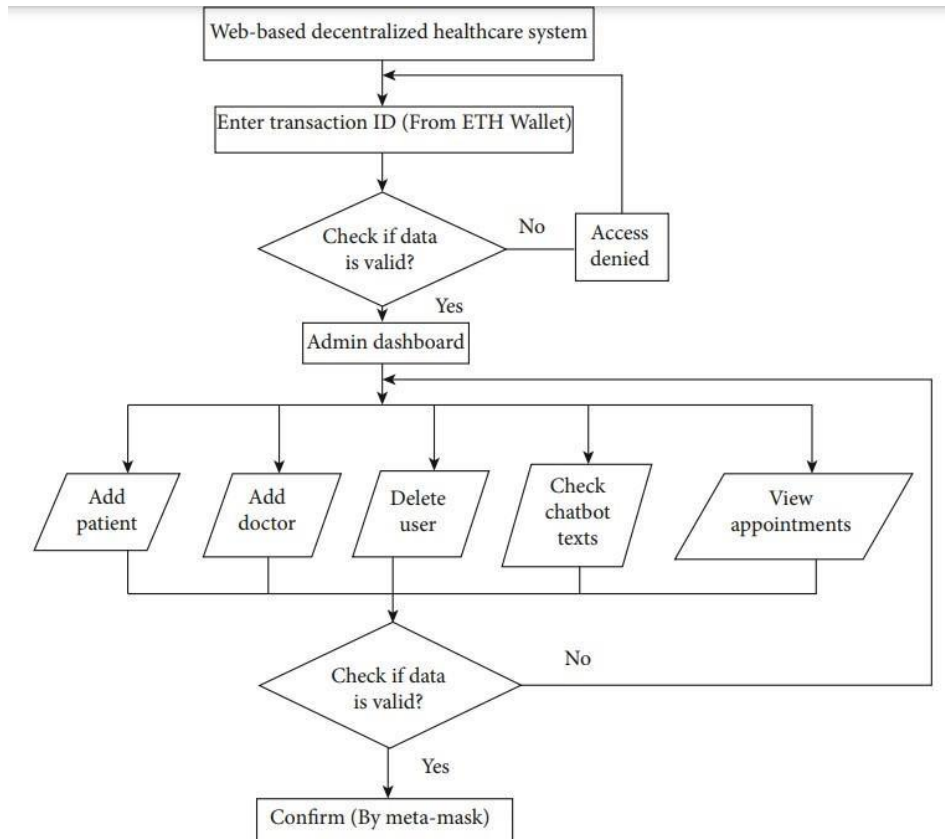
Flowchart of the doctor dashboard

Flowchart of the patient dashboard

7. CODING & SOLUTIONING

FEATURE CODE 1 :

```solidity
// SPDX-License-Identifier: MIT

pragma solidity ^0.8.0;

contract HealthRecords
{
    struct PatientRecord
    {
        String Name;
        address patientAddress;
```

```solidity
        string dieses;

        string contactInfo;

    }

        mapping(uint256 => PatientRecord) public records;

        event RecordCreated(uint256 indexed recordId, address indexed patientAddress);

        event RecordTransferred

(

        uint256 indexed recordId,

         address indexed from,

         address indexed to

    );

 modifier onlyOwner(uint256 recordId)

{

    require(msg.sender == records[recordId].patientAddress,"Only contract owner can call
this");

        _;

    }

function createRecord

(

        uint256 recordId,

        string memory name, address _patientAddress, string memory _diseases, string
        memory _contactInfo

    )

 external {

         records[recordId].Name = name;

        records[recordId].patientAddress = _patientAddress;

        records[recordId].dieses = _diseases;

        records[recordId].contactInfo = _contactInfo;
```

```solidity
        emit RecordCreated(recordId, _patientAddress);

     }

     function transferRecord(uint256 recordId, address newOwner) external
onlyOwner(recordId)

     {

      //require(records[recordId].patientAddress == newOwner, "New Owner should have
different Address");

      require(records[recordId].patientAddress == msg.sender, "Only record owner can
transfer");

     records[recordId].patientAddress = newOwner;

     emit RecordTransferred(recordId, records[recordId].patientAddress, newOwner)

     }

     function getRecordData

     (

      uint256 recordId

     )

     external view returns (string memory, address, string memory,string memory) {

     return (records[recordId].Name,

     records[recordId].patientAddress,

     records[recordId].dieses,

     records[recordId].contactInfo);

      }

      function getRecordOwner(uint256 recordId) external view returns (address)

      {

    return records[recordId].patientAddress;

      }

}
```

FEATURE CODE 2

```javascript
const { ethers } = require("ethers");


const abi = [
 {
  "anonymous": false,
  "inputs": [
   {
    "indexed": true,
    "internalType": "uint256",
    "name": "recordId",
    "type": "uint256"
   },
   {
    "indexed": true,
    "internalType": "address",
    "name": "patientAddress",
    "type": "address"
   }
  ],
  "name": "RecordCreated",
  "type": "event"
 },
 {
  "anonymous": false,
  "inputs": [
   {
```

```json
      "indexed": true,
      "internalType": "uint256",
      "name": "recordId",
      "type": "uint256"
    },
    {
      "indexed": true,
      "internalType": "address",
      "name": "from",
      "type": "address"
    },
    {
      "indexed": true,
      "internalType": "address",
      "name": "to",
      "type": "address"
    }
  ],
  "name": "RecordTransferred",
  "type": "event"
},
{
  "inputs": [
    {
      "internalType": "uint256",
      "name": "recordId",
      "type": "uint256"
```

```
    },
    {
     "internalType": "string",
     "name": "name",
     "type": "string"
    },
    {
     "internalType": "address",
     "name": "_patientAddress",
     "type": "address"
    },
    {
     "internalType": "string",
     "name": "_diseases",
     "type": "string"
    },
    {
     "internalType": "string",
     "name": "_contactInfo",
     "type": "string"
    }
   ],
   "name": "createRecord",
   "outputs": [],
   "stateMutability": "nonpayable",
   "type": "function"
  },
```

```json
{
  "inputs": [
    {
      "internalType": "uint256",
      "name": "recordId",
      "type": "uint256"
    }
  ],
  "name": "getRecordData",
  "outputs": [
    {
      "internalType": "string",
      "name": "",
      "type": "string"
    },
    {
      "internalType": "address",
      "name": "",
      "type": "address"
    },
    {
      "internalType": "string",
      "name": "",
      "type": "string"
    },
    {
      "internalType": "string",
```

```json
      "name": "",
      "type": "string"
     }
    ],
    "stateMutability": "view",
    "type": "function"
   },
   {
    "inputs": [
     {
      "internalType": "uint256",
      "name": "recordId",
      "type": "uint256"
     }
    ],
    "name": "getRecordOwner",
    "outputs": [
     {
      "internalType": "address",
      "name": "",
      "type": "address"
     }
    ],
    "stateMutability": "view",
    "type": "function"
   },
   {
```

"inputs": [

 {

 "internalType": "uint256",

 "name": "",

 "type": "uint256"

 }

],

"name": "records",

"outputs": [

 {

 "internalType": "string",

 "name": "Name",

 "type": "string"

 },

 {

 "internalType": "address",

 "name": "patientAddress",

 "type": "address"

 },

 {

 "internalType": "string",

 "name": "dieses",

 "type": "string"

 },

 {

 "internalType": "string",

 "name": "contactInfo",

```
      "type": "string"
     }
    ],
    "stateMutability": "view",
    "type": "function"
   },
   {
    "inputs": [
     {
      "internalType": "uint256",
      "name": "recordId",
      "type": "uint256"
     },
     {
      "internalType": "address",
      "name": "newOwner",
      "type": "address"
     }
    ],
    "name": "transferRecord",
    "outputs": [],
    "stateMutability": "nonpayable",
    "type": "function"
   }
  ]

  if (!window.ethereum) {
```

```
alert('Meta Mask Not Found')

window.open("https://metamask.io/download/")

}
```

```
export const provider = new ethers.providers.Web3Provider(window.ethereum);

export const signer = provider.getSigner();

export const address = "0x8837a10cf07813729bCEB5381A6D435E986240d4"

export const contract = new ethers.Contract(address, abi, signer)
```

8. PERFORMANCE TESTING

Performance testing for an Electronic Health Record (EHR) system that uses blockchain technology is crucial to ensure the system's reliability, scalability, and responsiveness. Here are the steps and considerations for conducting performance testing for an EHR system utilizing blockchain:

Define Performance Objectives:

   Start by identifying specific performance objectives, such as response times, transaction throughput, and system availability. Understand what is considered acceptable performance in your context**.**

Identify Key Scenarios:

   Determine the most critical use cases for your EHR system. These may include patient record creation, retrieval, and updates, as well as access to medical history, billing, and prescription processes.

Test Environment Setup:

   Create a test environment that closely mirrors the production environment, including the same hardware, network configurations, and blockchain infrastructure. This ensures that test results are representative of real-world conditions.

Test Data Preparation:

Use realistic and diverse data sets, including patient records, medical histories, and transactions, to simulate actual usage scenarios.

Performance Testing Types:

Conduct various types of performance tests, including**:**

a. Load Testing: Assess the system's performance under expected load levels.

b. Stress Testing: Determine how the system behaves under extreme conditions to identify its breaking point.

c. **Volume Testing**: Evaluate system performance with a high volume of data.

d. **Scalability Testing**: Assess the system's ability to scale horizontally or vertically when additional resources are added.

e. Latency Testing: Measure network and blockchain transaction latencies.

f. Security Testing: Assess the system's ability to maintain data privacy and security under high loads.

Blockchain Network Testing:

Blockchain-specific performance metrics include the transaction confirmation time, block creation time, and the number of transactions processed per second. These metrics are important for the EHR system's blockchain component.

Monitoring Tools:

Implement monitoring tools to collect data during testing. These tools should capture key performance metrics, such as CPU usage, memory consumption, network latency, and blockchain-related statistics**.**

Test Execution:

Execute the defined test scenarios, gradually increasing the load to evaluate system behavior at different load levels.

Analyze Results:

Carefully analyze the test results to identify bottlenecks, performance degradation points, and areas that need optimization. Pay close attention to blockchain-specific metrics.

Tuning and Optimization:

Based on the test results, fine-tune the EHR system and blockchain components. This may involve optimizing smart contracts, configuring blockchain nodes, or adjusting system parameters.

Repeat Testing:

Conduct iterative performance testing to ensure that the system performs well across various scenarios and after optimizations.

PERFORMANCE METRICS

EHR (Electronic Health Records) systems using blockchain technology can offer various benefits, including enhanced security, data integrity, and interoperability. When assessing the performance of such systems, it's essential to consider several key performance metrics:

Data Integrity: Ensure that data stored in the EHR system remains accurate and unaltered. Metrics to assess data integrity may include the frequency and scale of data audits and comparisons with traditional EHR systems.

Security: Measure the system's ability to prevent unauthorized access and data breaches. Key security metrics include the number of attempted breaches, successful attacks, and the time it takes to detect and respond to security incidents.

Consensus Mechanism: Evaluate the blockchain's consensus mechanism (e.g., Proof of Work, Proof of Stake) for its efficiency, scalability, and energy consumption. Monitor the time it takes for transactions to be validated and added to the blockchain.

Interoperability: Assess the EHR system's ability to exchange data with other healthcare providers, organizations, and systems. Metrics may include the number of successful data exchanges, compliance with healthcare data standards (e.g., HL7, FHIR), and the ease of integrating with other systems.

Scalability: Measure the system's ability to handle an increasing number of EHR records and transactions. Track the performance as the system's load grows, monitoring factors such as transaction processing times and resource utilization.

Transaction Throughput: Calculate the number of transactions (e.g., patient records updates, access requests) the blockchain can process per unit of time. This metric is crucial for assessing the system's ability to handle high volumes of data.

Latency: Determine the time it takes for data to be recorded on the blockchain and subsequently retrieved. Low latency is essential for timely access to patient information.

Cost-Efficiency: Evaluate the total cost of ownership, including hardware, software, energy consumption, and maintenance. Compare the costs of blockchain-based EHR systems with traditional EHR solutions.

User Experience: Collect feedback from healthcare providers and patients to gauge their satisfaction with the system's usability, performance, and reliability. Metrics may include user satisfaction scores and response times for user queries.

Data Privacy and Compliance: Ensure that the system complies with healthcare data privacy regulations, such as HIPAA (in the United States) or GDPR (in the European Union). Monitor the number of data access requests, data breaches, and compliance violations.

Redundancy and Disaster Recovery: Assess the system's resilience to hardware failures and disasters. Measure the time and success rate of data recovery in case of failures.

Smart Contract Performance: If the EHR system uses smart contracts for automating certain processes, monitor the execution time and efficiency of these contracts.

Audit Trail: Ensure that the blockchain maintains a comprehensive and tamper-evident audit trail. Monitor the completeness and accessibility of the audit logs.

Regulatory Compliance: Ensure that the system complies with local and international regulations governing healthcare and blockchain technology.

Blockchain Network Health: Monitor the overall health and performance of the blockchain network, including factors like block propagation time, block size, and network congestion.

Energy Consumption: Track the environmental impact of the blockchain network, including energy consumption and carbon footprint.

To effectively assess the performance of an EHR system using blockchain, it's essential to establish baseline values for these metrics and regularly review them to identify areas for improvement and optimization. Additionally, consider involving healthcare professionals, IT experts, and regulatory authorities in the evaluation process to ensure that the system meets the needs of all stakeholders while maintaining data security and privacy.
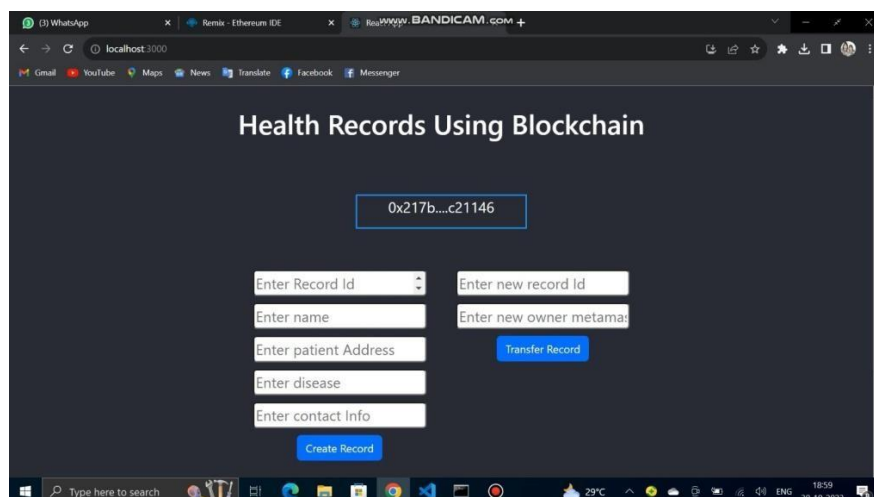
9. RESULTS

The results of Electronic Health Care system using Block Chain are attached below.

Output Screenshots

Local Host IP address : http://localhost:3000/

Screenshot of output

10. Advantages and Disadvantages

Electronic Health Records (EHR) using blockchain technology offer several advantages and disadvantages:

Advantages of EHR using Blockchain:

Data Security: Blockchain's decentralized and encrypted nature enhances the security and privacy of patient data. Each block of data is linked to the previous one using cryptographic hashes, making it difficult for unauthorized users to tamper with or access sensitive information.

Data Integrity: Blockchain ensures data integrity by creating an immutable ledger of all transactions. This prevents unauthorized alterations or deletions of patient records, which is crucial for maintaining accurate medical histories.

Interoperability: Blockchain can facilitate data exchange and interoperability between different healthcare providers and systems. This can lead to better coordination of care and a more holistic view of a patient's medical history.

Patient Control: Patients can have more control over their health data. They can grant permission for specific entities to access their records and maintain greater transparency about who has accessed their information.

Reduced Fraud: The transparency and security of blockchain can help reduce healthcare fraud. It can prevent the creation of duplicate records or the unauthorized access of medical information, ultimately saving costs for healthcare providers.

Streamlined Processes: Blockchain can simplify administrative and billing processes by securely and transparently recording transactions. This can lead to reduced administrative overhead and improved efficiency in healthcare operations.

Disadvantages of EHR using Blockchain:

Complex Implementation: Integrating blockchain into existing healthcare systems can be complex and costly. Healthcare organizations need to invest in new infrastructure and adapt their processes to accommodate blockchain technology.

Scalability: Blockchain networks can become slow and expensive to operate as the number of transactions and participants increases. Scaling blockchain for the healthcare sector while maintaining performance can be challenging.

Regulatory Challenges: The regulatory environment surrounding healthcare data is complex and varies from region to region. Blockchain may not always align perfectly with existing regulations, creating legal and compliance issues.

Data Recovery: While blockchain ensures data immutability, it can also make data recovery difficult if an error occurs. If incorrect data is added to the blockchain, it can be challenging to rectify without a consensus from all participants.

User Experience: Using blockchain for EHRs may require patients and healthcare professionals to navigate new systems and interfaces, potentially causing initial usability challenges.

Privacy Concerns: While blockchain can enhance data privacy, it can also raise concerns about total data transparency. Striking a balance between transparency and privacy is crucial.

In conclusion, EHRs using blockchain have the potential to significantly improve data security and integrity in healthcare. However, the technology is still evolving, and healthcare organizations must carefully consider the advantages and disadvantages when deciding whether to adopt blockchain for EHR management.

11. CONCLUSION

Implementing Electronic Health Records (EHR) using blockchain technology holds significant promise for the healthcare industry. While this conclusion may vary based on specific use cases and the maturity of blockchain technology, there are several key points to consider. Data Security and Integrity, Blockchain provides a decentralized and immutable ledger for storing health records. This ensures that patient data is secure, tamper-proof, and accessible only to authorized personnel, reducing the risk of data breaches and unauthorized access. Interoperability, Blockchain can facilitate interoperability between different healthcare systems and EHR platforms. Patients and healthcare providers can access and update records securely, regardless of the EHR system they use. This improves continuity of care and reduces duplication of efforts. Patient Control, Blockchain enables patients to have

greater control over their health data. They can grant and revoke access to their records, increasing transparency and trust in the healthcare system. Data Accuracy, By reducing the risk of errors and fraud, blockchain can improve the accuracy of health records. This can lead to better diagnosis, treatment, and overall patient care. Streamlined Processes, Smart contracts can automate various administrative and billing processes, reducing paperwork, costs, and the potential for errors. This can improve the efficiency of healthcare operations. Data Availability, Blockchain ensures that health records are available 24/7, regardless of the healthcare provider's operating hours. In emergencies, this can be critical for making informed medical decisions. Research and Analytics, Healthcare organizations and researchers can access large datasets for analysis, leading to improved insights into public health, medical research, and treatment outcomes. Patient data can be anonymized while still being accessible for research. Challenges and Considerations, It's important to recognize that blockchain implementation in healthcare faces challenges related to scalability, regulation, and data privacy. These must be carefully addressed to ensure successful deployment. In conclusion, implementing EHR using blockchain can greatly enhance the security, interoperability, and transparency of health records. It empowers patients and streamlines healthcare processes. However, successful implementation requires a well-thought-out strategy, collaboration between stakeholders, and adherence to regulatory requirements. As blockchain technology continues to evolve, it holds the potential to revolutionize the way healthcare data is managed, ultimately improving patient care and outcomes.

12. FUTURE SCOPE

The use of blockchain technology in Electronic Health Records (EHR) has the potential to revolutionize healthcare data management and security. Here are some future scope and possibilities for EHR using blockchain technology:

Data Security and Privacy: Blockchain can enhance the security and privacy of patient health data. EHRs on a blockchain are more resistant to unauthorized access and breaches due to their decentralized and immutable nature. Patients can have more control over who can access their data.

Interoperability: Blockchain can improve data interoperability, allowing different healthcare providers and systems to securely access and share patient data. This can lead to better-coordinated care and fewer medical errors.

Consent Management: Smart contracts on a blockchain can facilitate granular control over data access, allowing patients to specify who can access their records, for what purposes, and for how long. This ensures that data is only used with explicit patient consent.

Data Accuracy: Immutable records on a blockchain can reduce the risk of data errors and duplication, leading to more accurate and reliable health records.

Research and Analytics: Researchers and healthcare organizations can access de-identified patient data on the blockchain for research purposes, while maintaining patient privacy and consent.

Telemedicine and Remote Monitoring: Blockchain can support secure data sharing for telemedicine consultations and remote patient monitoring, enabling healthcare providers to access real-time, secure patient data.

Supply Chain Management: Blockchain can be used to track the supply chain of pharmaceuticals and medical devices, ensuring authenticity and reducing the risk of counterfeit products.

Credentialing and Licensing: Healthcare professionals' qualifications, licenses, and credentials can be stored and verified on a blockchain, making the verification process more efficient.

Billing and Claims Processing: Blockchain can streamline the billing and claims processing in healthcare, reducing administrative overhead and potential for fraud.

Global Health Data Exchange: Blockchain can facilitate cross-border health data exchange, allowing for secure and efficient sharing of health records across countries, which can be particularly useful for travelers and expatriates.

Disaster Response and Public Health: In emergency situations, blockchain can help ensure quick access to critical patient data, such as allergies and pre-existing conditions, even if the patient is unable to provide this information.

Compliance and Auditing: Blockchain's transparent and auditable nature can help with compliance in the healthcare industry, ensuring that organizations adhere to regulations and standards.

Patient Empowerment: With control over their data and the ability to grant or revoke access, patients are empowered to have a more active role in managing their health information.

Integration with AI and IoT: Combining blockchain with artificial intelligence and the Internet of Things (IoT) can lead to more advanced healthcare solutions, such as predictive analytics and personalized medicine**.**

Healthcare Innovation: Blockchain can encourage innovation in healthcare through secure data sharing, leading to the development of new applications and services.

It's important to note that while the potential for blockchain in EHR is significant, there are also challenges and considerations, including regulatory compliance, scalability, and interoperability with existing systems. The successful adoption of blockchain in EHR will depend on collaboration between healthcare providers, technology companies, and regulatory bodies to establish industry standards and best practices.

13. APPENDIX SOURCR CODE, GITHUB & PROJECT DEMO LINK

Source code 1 :

```solidity
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;
contract HealthRecords
{
        struct PatientRecord
  {
        String Name;
         address patientAddress;
```

```solidity
        string dieses;

        string contactInfo;

    }

        mapping(uint256 => PatientRecord) public records;

        event RecordCreated(uint256 indexed recordId, address indexed patientAddress);

        event RecordTransferred

(

        uint256 indexed recordId,

         address indexed from,

         address indexed to

    );

 modifier onlyOwner(uint256 recordId)

{

    require(msg.sender == records[recordId].patientAddress,"Only contract owner can call
this");

        _;

    }

function createRecord

(

        uint256 recordId,

        string memory name, address _patientAddress, string memory _diseases, string
        memory _contactInfo

    )

 external {

         records[recordId].Name = name;

        records[recordId].patientAddress = _patientAddress;

        records[recordId].dieses = _diseases;

        records[recordId].contactInfo = _contactInfo;
```

```solidity
        emit RecordCreated(recordId, _patientAddress);

    }

    function transferRecord(uint256 recordId, address newOwner) external
onlyOwner(recordId)

    {

    //require(records[recordId].patientAddress == newOwner, "New Owner should have
different Address");

     require(records[recordId].patientAddress == msg.sender, "Only record owner can
transfer");

    records[recordId].patientAddress = newOwner;

    emit RecordTransferred(recordId, records[recordId].patientAddress, newOwner)

    }

    function getRecordData

    (

     uint256 recordId

    )

    external view returns (string memory, address, string memory,string memory) {

    return (records[recordId].Name,

    records[recordId].patientAddress,

    records[recordId].dieses,

    records[recordId].contactInfo);

    }

     function getRecordOwner(uint256 recordId) external view returns (address)

    {

   return records[recordId].patientAddress;

    }

}
```

Source code 2 :

```javascript
const { ethers } = require("ethers");

const abi = [
 {
  "anonymous": false,
  "inputs": [
   {
    "indexed": true,
    "internalType": "uint256",
    "name": "recordId",
    "type": "uint256"
   },
   {
    "indexed": true,
    "internalType": "address",
    "name": "patientAddress",
    "type": "address"
   }
  ],
  "name": "RecordCreated",
  "type": "event"
 },
 {
  "anonymous": false,
  "inputs": [
   {
    "indexed": true,
```

```json
      "internalType": "uint256",

      "name": "recordId",

      "type": "uint256"

     },

     {

      "indexed": true,

      "internalType": "address",

      "name": "from",

      "type": "address"

     },

     {

      "indexed": true,

      "internalType": "address",

      "name": "to",

      "type": "address"

     }

    ],

    "name": "RecordTransferred",

    "type": "event"

   },

   {

    "inputs": [

     {

      "internalType": "uint256",

      "name": "recordId",

      "type": "uint256"

     },
```

```json
    {
     "internalType": "string",
     "name": "name",
     "type": "string"
    },
    {
     "internalType": "address",
     "name": "_patientAddress",
     "type": "address"
    },
    {
     "internalType": "string",
     "name": "_diseases",
     "type": "string"
    },
    {
     "internalType": "string",
     "name": "_contactInfo",
     "type": "string"
    }
   ],
   "name": "createRecord",
   "outputs": [],
   "stateMutability": "nonpayable",
   "type": "function"
  },
  {
```

"inputs": [

 {

  "internalType": "uint256",

  "name": "recordId",

  "type": "uint256"

 }

],

"name": "getRecordData",

"outputs": [

 {

  "internalType": "string",

  "name": "",

  "type": "string"

 },

 {

  "internalType": "address",

  "name": "",

  "type": "address"

 },

 {

  "internalType": "string",

  "name": "",

  "type": "string"

 },

 {

  "internalType": "string",

  "name": "",

```json
      "type": "string"
     }
    ],
    "stateMutability": "view",
    "type": "function"
   },
   {
    "inputs": [
     {
      "internalType": "uint256",
      "name": "recordId",
      "type": "uint256"
     }
    ],
    "name": "getRecordOwner",
    "outputs": [
     {
      "internalType": "address",
      "name": "",
      "type": "address"
     }
    ],
    "stateMutability": "view",
    "type": "function"
   },
   {
    "inputs": [
```

```
      {
        "internalType": "uint256",
        "name": "",
        "type": "uint256"
      }
    ],
    "name": "records",
    "outputs": [
      {
        "internalType": "string",
        "name": "Name",
        "type": "string"
      },
      {
        "internalType": "address",
        "name": "patientAddress",
        "type": "address"
      },
      {
        "internalType": "string",
        "name": "dieses",
        "type": "string"
      },
      {
        "internalType": "string",
        "name": "contactInfo",
        "type": "string"
      }
```

```
      }
    ],
   "stateMutability": "view",
   "type": "function"
  },
  {
   "inputs": [
    {
     "internalType": "uint256",
     "name": "recordId",
     "type": "uint256"
    },
    {
     "internalType": "address",
     "name": "newOwner",
     "type": "address"
    }
   ],
   "name": "transferRecord",
   "outputs": [],
   "stateMutability": "nonpayable",
   "type": "function"
  }
]

if (!window.ethereum) {
 alert('Meta Mask Not Found')
```

```
  window.open("https://metamask.io/download/")

}
```

```
export const provider = new ethers.providers.Web3Provider(window.ethereum);

export const signer = provider.getSigner();

export const address = "0x8837a10cf07813729bCEB5381A6D435E986240d4"

export const contract = new ethers.Contract(address, abi, signer)
```

GITHUB LINK :

https://github.com/Aswin21092002/Blockchain-Technology-For-Electronic-Health-Records

PROJECT DEMO LINK :

https://youtu.be/cNsyMfDFRks?feature=shared