Blockchain Technology for Electronic Health Records

Team ID: NM2023TMID11607

TEAM LEADER:

ANANTHI K (Reg No.: 511520106001)

TEAM MEMBER 1:

MOHANRAJ P (Reg No.: 511520106006)

TEAM MEMBER 2:

KARTHIKA S (Reg No.: 511520106004)

TEAM MEMBER 3:

ARULKUMAR K (Reg No.: 511520106002)

TABLE OF CONTENT

1.INTRODUCTION

1.1 Project Overview

A blockchain is a decentralized network that uses peer-to-peer (p2p) technology to track all transactions. It lacks a centralized authority or a single point of contact. Rather, it is a group of nodes that keep the system functioning. Each transaction is extremely safe because of the network's nodes. Encryption provides an additional level of security to the connection. The digital record is duplicated at every node in the system. Each node must verify the authenticity of a transaction before adding it back. A number of blocks make up a digital ledger. Each block gives a detailed report of each transaction. Education, manufacturing, and the healthcare industry are just a few of the domains where blockchain has piqued interest. It contributes to the health sector in a variety of ways because it is a distributed and decentralized technology. The Ethereum blockchain is powered by ETH, Ethereum'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. Decentralization, security, privacy, and resilience through cryptographic algorithms are all elements of blockchain that have the potential to tackle the present difficulties in the healthcare industry.

1.2 Purpose

Implementing blockchain in Electronic Health Records (EHR) projects serves several critical purposes:

1. Security and Privacy: Blockchain's decentralized and immutable nature ensures the security and privacy of patient data. It allows for secure, tamper-proof storage and controlled access to sensitive medical information.

2.Data Integrity: It ensures the integrity of health records by maintaining a transparent, unchangeable ledger of transactions, reducing the risk of data manipulation or errors.

3.Interoperability: Blockchain can facilitate data exchange between different healthcare providers and systems, improving interoperability, which is often a challenge in healthcare.

4.Patient Empowerment: It enables patients to have greater control over their health data, granting them access rights and permission controls. Patients can share their information securely and maintain ownership of their data.

5.Streamlined Processes: Smart contracts and automation within blockchain technology can streamline administrative tasks, payment processing, and authorization procedures, reducing bureaucracy and enhancing efficiency in healthcare operations.

6.Research and Development: Blockchain can facilitate anonymized data sharing for research purposes while ensuring patient privacy, potentially accelerating medical research and innovation.

7.Fraud Reduction: The decentralized and transparent nature of blockchain reduces the risk of fraudulent activities within healthcare systems.

Overall, the implementation of blockchain technology in Electronic Health Records projects aims to improve data security, streamline processes, and empower patients, while also fostering collaboration and innovation in the healthcare industry.

2.LITERATURE SURVEY

2.1 Existing problem

One of the existing problems with implementing blockchain technology for electronic health records (EHR) revolves around:

1.Interoperability and Standards:

Lack of standardized protocols and interoperability between various EHR systems and healthcare providers can hinder the effective implementation of blockchain. Healthcare systems often use different data formats and structures, making seamless integration and sharing of patient data challenging.

2.Scalability and Performance:

Blockchain technology, especially public blockchains, can face scalability issues when handling a vast amount of healthcare data. The processing and storage requirements for EHR across a blockchain might result in slower transaction speeds and increased costs.

3.Data Privacy and Security Concerns:

While blockchain offers enhanced security through its decentralized and immutable nature, ensuring patient data privacy, especially sensitive health information, is complex. Balancing transparency and data privacy within a public ledger is a significant challenge.

4.Regulatory Compliance:

Healthcare systems must adhere to strict regulatory standards such as HIPAA (Health Insurance Portability and Accountability Act) or GDPR (General Data Protection Regulation). Integrating blockchain while maintaining compliance with these regulations and ensuring the right to be forgotten or data erasure is challenging.

5.User Adoption and Usability:

Implementing blockchain technology in healthcare requires healthcare professionals to understand and trust the system. User adoption may be slow due to the complexity of the technology and a lack of training and understanding among medical personnel.

6.Cost and Infrastructure:

Introducing blockchain into existing healthcare infrastructure might involve significant costs and the need for technological upgrades. Additionally, the maintenance and ongoing costs related to blockchain integration could be substantial for healthcare providers. Addressing these challenges is crucial for the successful implementation of blockchain technology in electronic health records, as it has the potential to revolutionize the healthcare industry by providing secure, interoperable, and transparent patient data management. However, overcoming these hurdles is necessary to fully realize the benefits of this innovative technology in the healthcare sector.

2.2 Reference

[1] A. Bakhtawar, R. J. Abdul, C. Chinmay, N. Jamel, R. Saira, and R. Muhammad, "Blockchain and ANFIS empowered IoMT application for privacy preserved contact tracing in COVID-19 pandemic," Personal and Ubiquitous Computing, vol.1-17,2021.

[2] C. Chakraborty, Mobile health (M-Health) for tele-wound monitoring. In: Mobile Health Applications for Quality Healthcare Delivery, IGI Global, Hershey, PA, USA,pp.98–116, 2019.

[3] C. Chinmay, B. Gupta, and S. K. Ghosh, "A review on tele-medicine-based WBAN framework for patient monitoring," Int. Journal of Telemedicine and eHealth, Mary Ann Libert inc.vol. 19, no. 8, pp. 619–626, 2013.

[4] Y. Shelke and C. Chakraborty, "Augmented reality and virtual reality transforming spinal imaging landscape: a feasibility study," IEEE Computer Graphics and Applications, vol. 41, no. 3, pp. 124–138, 2021.

[5] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pp. 1–5, Montreal, QC, Canada, October 2017.

[6] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "Continuous patient monitoring with a patient centric agent: a block Architecture," IEEE Access, vol. 6, Article ID 32700, 2018.

[7] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: privacypreserving framework for access control and interoperability of electronic health records using blockchain technology," Sustainable Cities and Society, vol. 39, pp. 283–297, 2018.

[8] L. Ismail, H. Hameed, M. Alshamsi, and M. Alhammadi, "Towards a blockchain deployment at UAE university: per-formance evaluation and blockchain taxonomy," in Pro-ceedings of the 2019 International Conference on Blockchain Technology, pp. 30–38, Honolulu, HI, USA, July 2019.

[9] A. Juneja and M. Marefat, “Leveraging blockchain for retraining deep learning architecture in patient-specific ar-rhythmia classification,” in Proceedings of the 2018 IEEE EMBS International Conference on Biomedical & Health In-formatics (BHI), pp. 393–397, Las Vegas, NV, USA, March 2018.

[10] E. W. Jamoon, N. Yang, and E. Hing, “Adoption of certified electronic health record systems and electronic information sharing in physician offices,” NCHS Data Brief, vol. 236, 2016.

[11] E. Kim, S. M. Rubinstein, K. T. Nead, A. P. Wojcieszynski, P. E. Gabriel, and J. L. Warner, “evolving use of electronic health records (EHR) for research,” Seminars in Radiation Oncology, vol. 29, no. 4, pp. 354–361, 2019.

[12] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, “Healthcare blockchain system using smart contracts for secure automated remote patient monitoring,” Journal of Medical Systems, vol. 42, no. 130, 2018.

[13] J. L. Fernandez-Alem ´ an, I. C. Senior, P. ´ A. O. Lozoya, and ´A. Toval, “Security and privacy in electronic health records: a systematic literature review,” Journal of Biomedical Infor-matics, vol. 46, no. 3, pp. 541–562, 2013.

[14] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, “MedBlock: efficient and secure medical data sharing via blockchain,”Journal of Medical Systems, vol. 42, no. 8, p. 136, 2018.

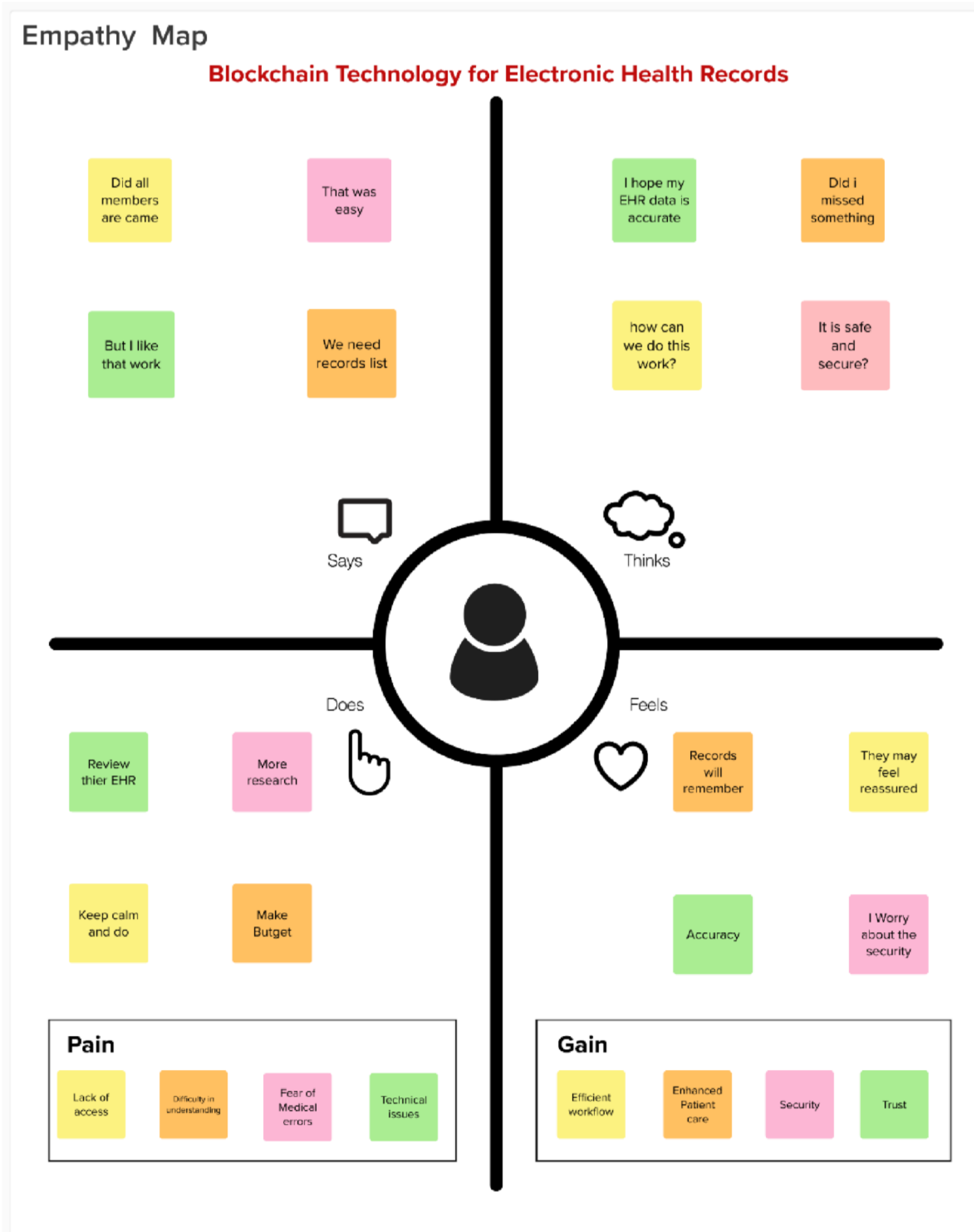
2.3 Problem Statement Definition

The problem is to enhance the security, integrity, and accessibility of electronic health records (EHR) while maintaining patient privacy and data accuracy. Traditional EHR systems are vulnerable to data breaches, lack transparency, and face challenges in interoperability between different healthcare providers. Thus, the goal is to implement a blockchain-based system to address these issues and revolutionize the management of electronic health records.

The project aims to explore, develop, and implement a blockchain-based system for managing electronic health records. It involves designing a secure, decentralized, and transparent platform that ensures the privacy and integrity of patient data. The system will focus on creating a distributed ledger for EHR, enabling secure data sharing among healthcare providers while maintaining regulatory compliance and safeguarding patient confidentiality. Key components include the creation of smart contracts, encryption methodologies, user access controls, and interoperability standards to ensure efficient and secure data management across the healthcare ecosystem. The project's success will be evaluated based on its ability to provide a secure, transparent, and interoperable solution for managing electronic health records.

3.IDEATION & PROPOSED SOLUTION

3.1 Empathy map Canvas



3.2 Ideation & Brainstorming

Step-1: Team Gathering, Collaboration and Select the problem Statement

Step-2: Brainstorm, Idea Listing and Grouping

2

Brainstorm

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

10 minutes

TIP

You can select a sticky note and hit the pencil [switch to sketch] icon to start drawing!

BALASUBRAMANIAN S

Create a patient-centric EHR system

ensuring the privacy and security

To Securely manage and share patient data for medical research and clinical trials

YOGAMURUGAN K

Enable seamless data sharing among healthcare institutions

facilitate better care coordination and reduce duplication of tests and treatments

Develop a blockchain-based system for tracking prescription medications

SANKAR MAHARAJA B

Patients,pharmacies and doctors could all have access to this ledger

Build an interoperable EHR platform

Patients can consent to share their data, and researchers can access it with proper authorization

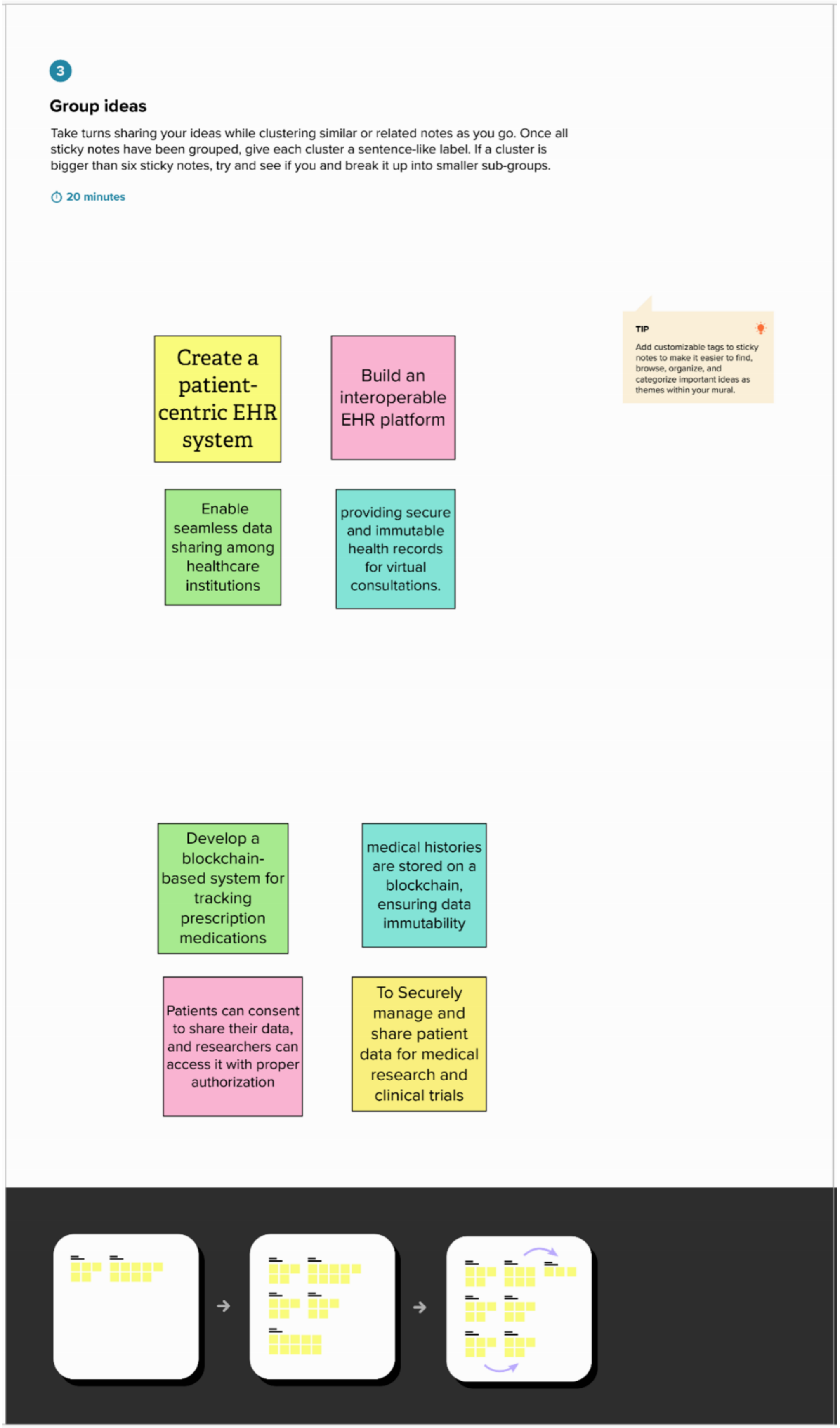
KALIARASAN K

medical histories are stored on a blockchain, ensuring data immutability

Develop smart contracts that automatically process insurance claims based on predetermined criteria

providing secure and immutable health records for virtual consultations.

Step-3: Idea Prioritization

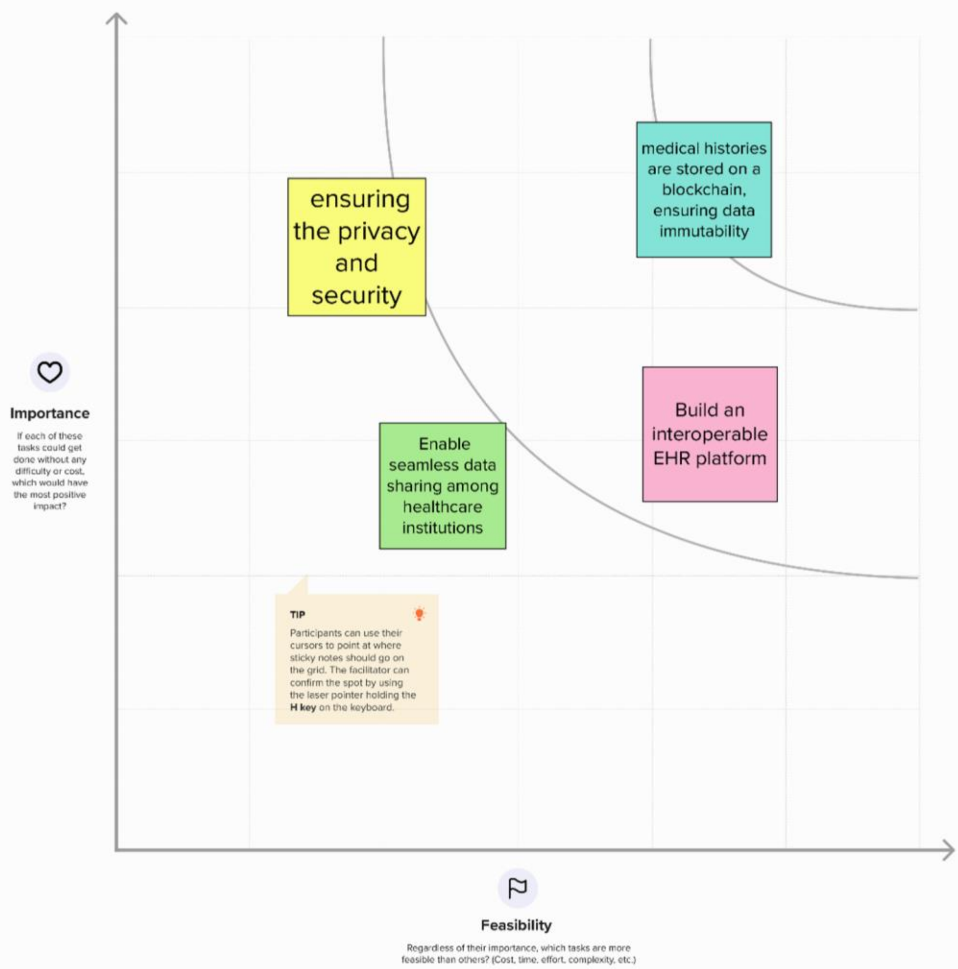


4

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



4.REQUIREMENT ANALYSIS

4.1 Functional Requirements:

Following are the functional requirements of the proposed solution.

FR No.	Functional Requirement (Epic)	Sub Requirement (Story / Sub-Task)
FR-1	Data Privacy and Security	Blockchain should offer robust encryption and access control mechanisms to protect sensitive health data from unauthorized access.
FR-2	Data Immutability	Records on the blockchain should be tamper-proof, ensuring that once data is added, it cannot be altered or deleted.
FR-3	Smart Contracts	Utilize smart contracts to automate processes, such as insurance claims, appointments, and consent management.
FR-4	Data Recovery	Implement mechanisms for data recovery and backup to prevent data loss in case of system failures.
FR-5	Emergency Access	Plan for emergency access to EHRs during critical situations, while still maintaining privacy and security.
FR-6	Data Purging	Define policies and mechanisms for removing outdated or irrelevant data to ensure data integrity and minimize storage costs.

4.2 Non-Functional requirements

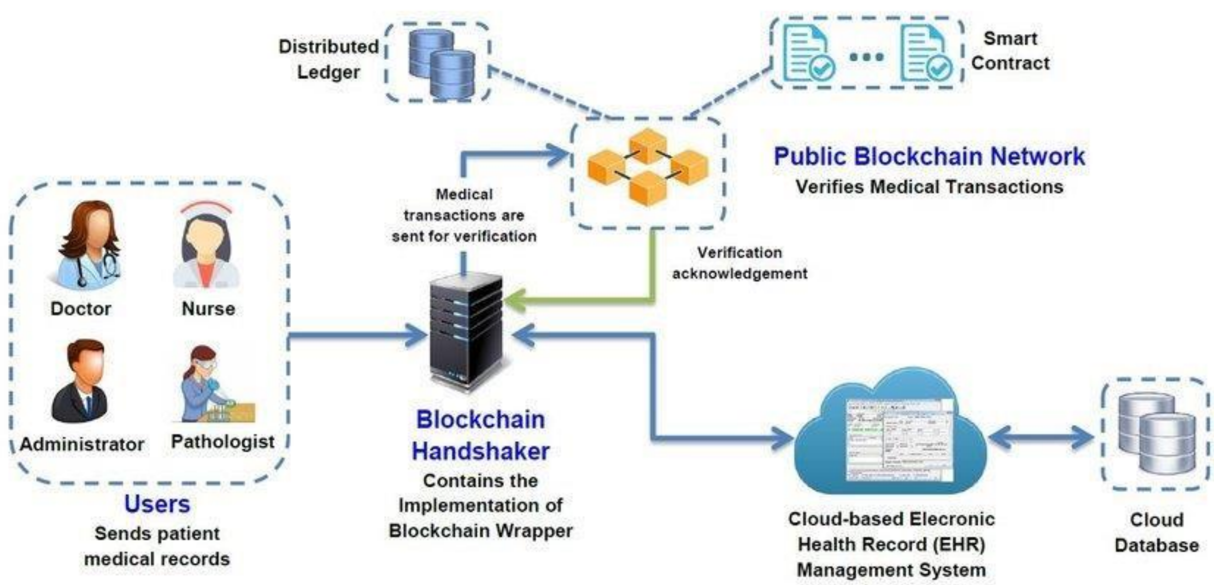
Following are the non-functional requirements of the proposed solution.

FR No.	Non-Functional Requirement	Description
NFR-1	Performance	Ensure that the system performs efficiently, with low latency, to provide timely access to EHR data.

NFR-2	Scalability	The system should be able to scale horizontally and vertically to accommodate a growing number of EHRs and users.
NFR-3	Disaster Recovery	Develop a disaster recovery plan to ensure the system's continuity in the event of natural disasters or other catastrophic events.
NFR-4	Resource Utilization	Efficiently manage hardware resources, such as CPU, memory, and storage, to avoid bottlenecks and performance degradation.
NFR-5	Security and Compliance	Adhere to industry-specific security standards and regulatory compliance (e.g., HIPAA, GDPR) to protect patient data.

5.PROJECT DESIGN

5.1 Data Flow Diagrams & User Stories



User stories

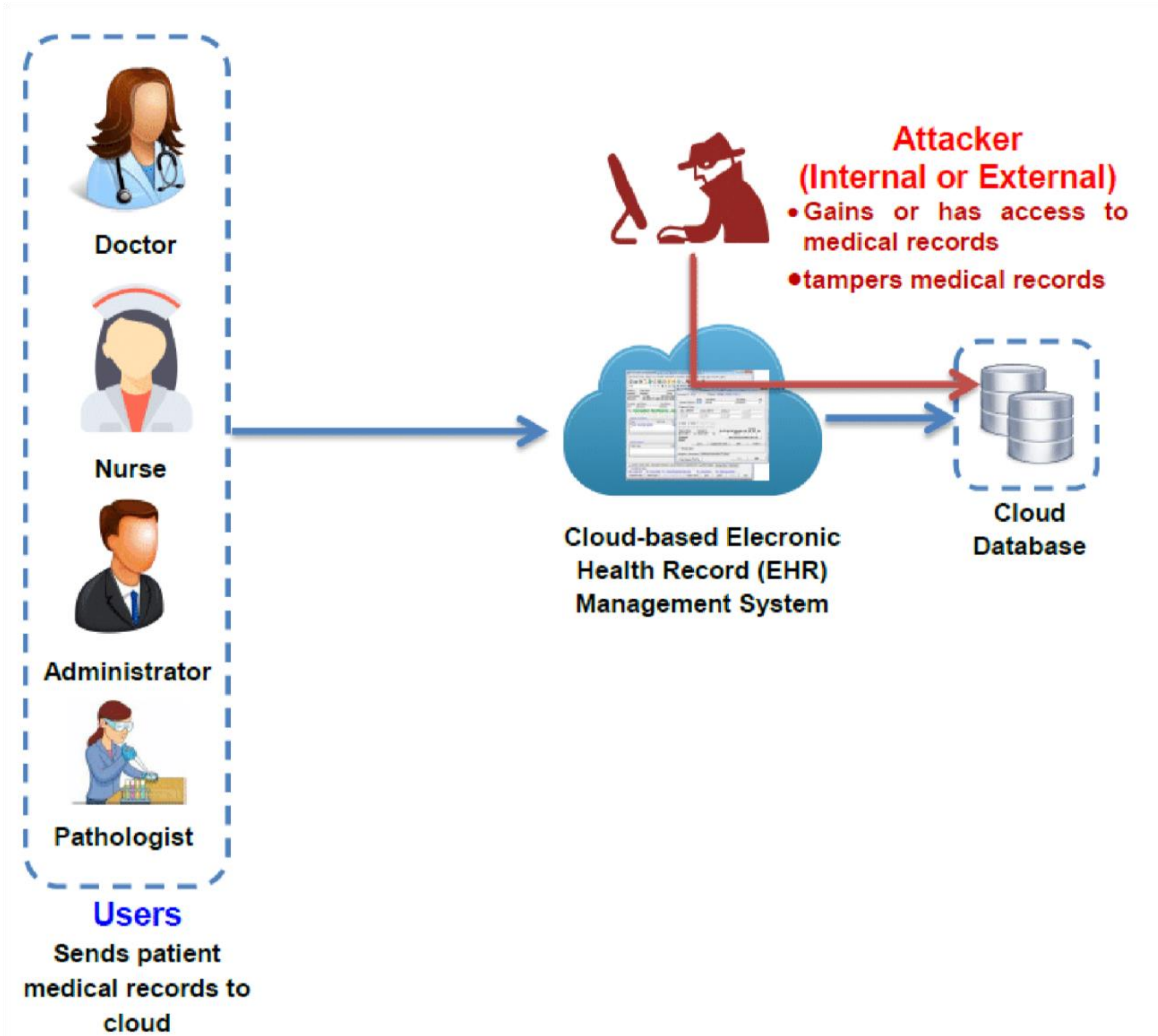
User type	**Functional requirements**	**User story no.**	**User story/ task**	**Acceptance Criteria**
Health care Provider	E-prescriptions, Audit Trail, Provide a secure messaging feature for communication between healthcare providers for discussing patient care.	USN-1	As a healthcare provider working in a busy urban hospital, I need a secure and efficient way to access and manage electronic health records (EHRs) for my patients to provide high-quality care. I require a modern and efficient electronic health record (EHR) system to streamline patient care and ensure that I can deliver the best medical services possible.	The EHR system should offer a user-friendly login experience, allowing me to access it securely with a username and password or other secure authentication methods.
Government Health Departments	Data Collection and Aggregation, Real-time Data Updates, Disease Surveillance, Data Analysis and Reporting	USN-2	As a public health official working in a government health department, I need a robust and secure blockchain-based electronic health record (EHR) system to monitor and safeguard public health effectively.	The EHR system should provide secure access for authorized public health officials using role-based authentication.I require the capability to collect, aggregate, and standardize health data from various sources, including hospitals, clinics, and laboratories.

Block chain Developers and Experts	Design and develop the overall architecture of the blockchain system,Data Encryption, Security Auditing, Blockchain	USN-3	blockchain developer and expert with a passion for healthcare technology, I aim to create and maintain a secure and innovative blockchainbased electronic health record (EHR) system that empowers healthcare providers, safeguards patient data, and	The system should support data backup and recovery to prevent data loss during system failures or data corruption.I need access to a reliable and efficient development
	Platform Upkeep		enhances the quality of healthcare services.	environment with the necessary tools and resources to create and maintain the blockchain-based EHR system
Patient Advocacy Group	Develop tools and processes to help patients easily manage their consent preferences for data sharing and access by healthcare providers and researchers. Data Transparency, Security and Privacy Oversight.	USN-4	As a member of a patient advocacy group committed to safeguarding patient rights and privacy, I aim to leverage a blockchain-based electronic health record (EHR) system to advocate for transparent data practices, empower patients, and ensure that their healthcare data remains secure and confidential.	I need secure and auditable access to the blockchain-based EHR system to monitor patient data usage, consent management, and data security.

Medical Students and Trainees	Access to resources related to patient safety, quality improvement, and adverse event reporting.Compliance with Educational Regulations, Feedback and Evaluation.	USN-5	As a medical student or trainee aspiring to become a proficient healthcare provider, I need access to a blockchain-based electronic health record (EHR) system to support my education, enhance my clinical skills, and ensure the highest standard of patient care.	I need access to deidentified patient data for educational purposes, which should be presented in an organized and comprehensible format.The system must allow me to efficiently navigate through patient records, including diagnoses, treatment plans, medication histories, and medical images.
Patients' Legal Representatives	Collaborate with legal authorities and systems to streamline the authorization and verification process for legal representatives, Data Portability, Educational Resources	USN-6	As a legal representative advocating for the healthcare rights and interests of patients, I require a secure and efficient blockchain-based electronic health record (EHR) system to ensure that patients' data is accessible, up-to-date, and their rights are upheld.	The EHR system should offer secure authentication for legal representatives, ensuring authorized access to patients' health records.
Health Insurance companie	Fraud Detection and Prevention Tools and algorithms for detecting and preventing insurance fraud by analyzing claims data.Claims Processing, Payment Management	USN-7	As a health insurance company dedicated to providing comprehensive and efficient coverage, I require a secure and innovative blockchain-based electronic health record (EHR) system to streamline our operations, ensure data accuracy, and enhance the quality of healthcare services for our policyholders.	Access to patient EHR data for claims verification should be available, with clear visibility into patient histories.Data backup and recovery mechanisms should be in place to prevent data loss in case of system failures or data corruption.

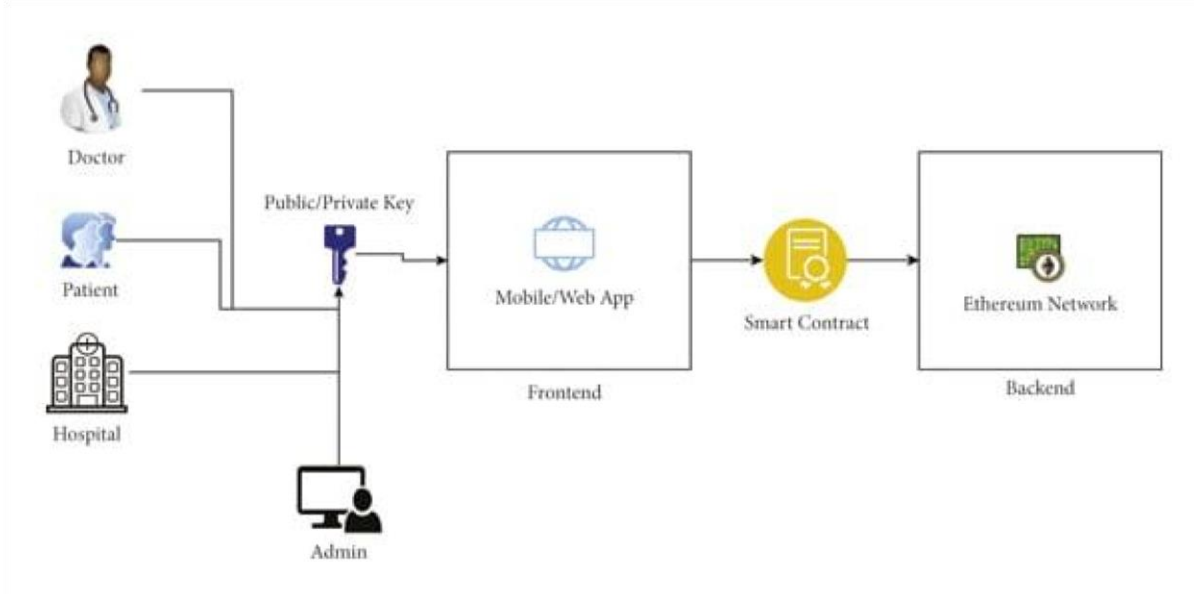
Regulators and Auditor	Data Privacy Assessment, "Integration with Regulatory Systems", Compliance Monitoring, Data Verification and Audit	USN-8	As a regulatory authority or auditor responsible for overseeing and ensuring compliance within the healthcare industry, I require access to a secure and transparent blockchain-based electronic health record (EHR) system to effectively monitor, audit, and verify data practices, safeguard patient privacy, and uphold regulatory standards.	I need access to comprehensive audit trails and data access history for monitoring and evaluating actions taken within the blockchain system. Tools for data verification and audit are essential to assess data integrity, authenticity, and compliance with regulatory standards and guidelines.

5.2 Solution Architecture



6.PROJECT PLANNING & SCHEDULING

6.1 Technical Architecture



Outline of Full System

Figure 1 shows the EHR architecture of the proposed system in this paper. The primary users in the blockchain architecture are a doctor, a patient, and a hospital. Furthermore, in the blockchain ecosystem, everyone will have a unique power due to the system's own private keys. Doctors, patients, and hospitals may also have limited access to some functionalities. Using his or her private key, the doctor will gain access to the web app (Frontend). By using his own private key, the patient communicates with the doctor. Both parties will share medical information via a web app (Frontend). Patients must use a smart contract to transact after receiving the service. As a backend support, we are deploying the Ethereum network. Below, the roles of every character in this figure are described:

(1) Doctor: doctors can access the system by using a private key, which will be given by the patient's unique key.

(2) Patient: patients will provide private key to doctors. Patients can share personal data through our portal.

(3) Hospital: hospital admin can look into the process but not details. They can maintain the flawless communications system.

(4) Website: the website is under frontend programming. It connects with the backend through smart contracts.

(5) Smart contracts: It is the main bone of our system. Every change in a block will have a log in it.

(6) Ethereum network: for backend processing, we used the Ethereum network.

6.2 Sprint Planning & Estimation

Sprint Planning:

1. Initiation & Research: Understand existing EHR systems, regulatory requirements, and blockchain technology's potential in healthcare.

2. Requirements Gathering: Identify key features, user stories, and functionalities required for the blockchain-based EHR system.

3. Design & Architecture: Develop the system's architecture, focusing on data structure, consensus mechanism, encryption, and smart contract integration.

4. Prototype Development: Build a basic blockchain-based EHR system to demonstrate core functionalities and test feasibility.

5. Security Implementation: Implement encryption, access controls, and smart contract logic to ensure data security and privacy.

6. Interoperability Integration: Develop protocols and standards for interoperability among various healthcare providers and systems.

7. Testing & Debugging: Conduct thorough testing, including stress testing, security audits, and user acceptance testing.

8. Documentation & Training: Prepare user manuals, guidelines, and training materials for stakeholders.

Estimation:

Initiation & Research: 1 week

Requirements Gathering: 2 weeks

Design & Architecture: 2 weeks

Prototype Development: 3 weeks

Security Implementation: 2 weeks

Interoperability Integration: 2 weeks

Testing & Debugging: 2 weeks

Documentation & Training: 1 week

This estimation totals approximately 15 weeks, allowing for potential adjustments based on the complexity and unforeseen challenges during the development phase. Each sprint is focused on completing specific tasks and achieving measurable progress toward the goal of a functional blockchain-based EHR system.

6.3 Sprint Delivery Schedule

1. Sprint 1 (2 weeks):

   - Initiation & Research

   - Establish project scope and goals

   - Gather initial information on existing EHR systems and regulatory landscape

2. Sprint 2 (2 weeks):

   - Requirements Gathering

   - Define user stories and key functionalities for the blockchain-based EHR system

3. Sprint 3 (2 weeks):

   - Design & Architecture

   - Develop the system architecture, focusing on blockchain integration and data structure

4. Sprint 4 (3 weeks):

   - Prototype Development

   - Build a basic version of the blockchain-based EHR system to showcase core functionalities

5. Sprint 5 (2 weeks):

   - Security Implementation

   - Implement encryption, access controls, and smart contract logic for data security

6. *Sprint 6 (2 weeks):
   - Interoperability Integration

   - Develop protocols and standards for interoperability among healthcare providers

7. *Sprint 7 (2 weeks):

- Testing & Debugging

- Conduct comprehensive testing, including security audits and user acceptance testing

8. *Sprint 8 (1 week):

- Documentation & Training

- Prepare user manuals, guidelines, and training materials for stakeholders

This sprint schedule spans over 16 weeks, allowing for comprehensive development, testing, and documentation phases. Each sprint's delivery includes a tangible output or a completed phase of the project, ensuring incremental progress and the achievement of defined objectives at the end of each cycle.

7.CODING & SOLUTIONING

7.1 Feature 1

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;


contract HealthRecords {


        struct PatientRecord {
        string Name; address
                patientAddress;
        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;




}    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;
    }
}
```

7.2 Feature 2

```
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,
  "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"
} ,
{
"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": "",

"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 =

"0x0a6FaBfee08271049Fb6E3e9231C4F9175126918" export const contract =

new ethers.Contract(address, abi, signer)
```

8. PERFORMANCE TESTING

8.1 Performance Metrics

For a Blockchain Technology in Electronic Health Records project, performance metrics can be diverse and cover various aspects of the system. Here are some essential performance metrics to consider:

1. Transaction Throughput: Measure the number of transactions the blockchain network can process per second. Higher throughput is essential for a scalable EHR system.

2. Latency: Assess the time taken for a transaction to be recorded and confirmed on the blockchain. Lower latency ensures quick data accessibility.

3. Data Storage Efficiency: Monitor the efficiency of data storage on the blockchain to ensure it’s not only secure but also optimized for space.

4. Security Measures: Track the number of attempted breaches, successful security incidents, and the effectiveness of encryption methods employed to safeguard patient data.

5. Interoperability Index: Measure the level of compatibility and data exchange capability between different healthcare providers and systems using the blockchain.

6. Consensus Algorithm Performance: Evaluate the energy efficiency and speed of the chosen consensus mechanism, like proof of work (PoW), proof of stake (PoS), or other consensus models.

7. Smart Contract Execution Speed: Assess the time taken for smart contracts to execute within the system.

8. User Adoption & Satisfaction: Monitor user feedback and adoption rates to gauge how well the system is accepted and utilized by healthcare providers and patients.

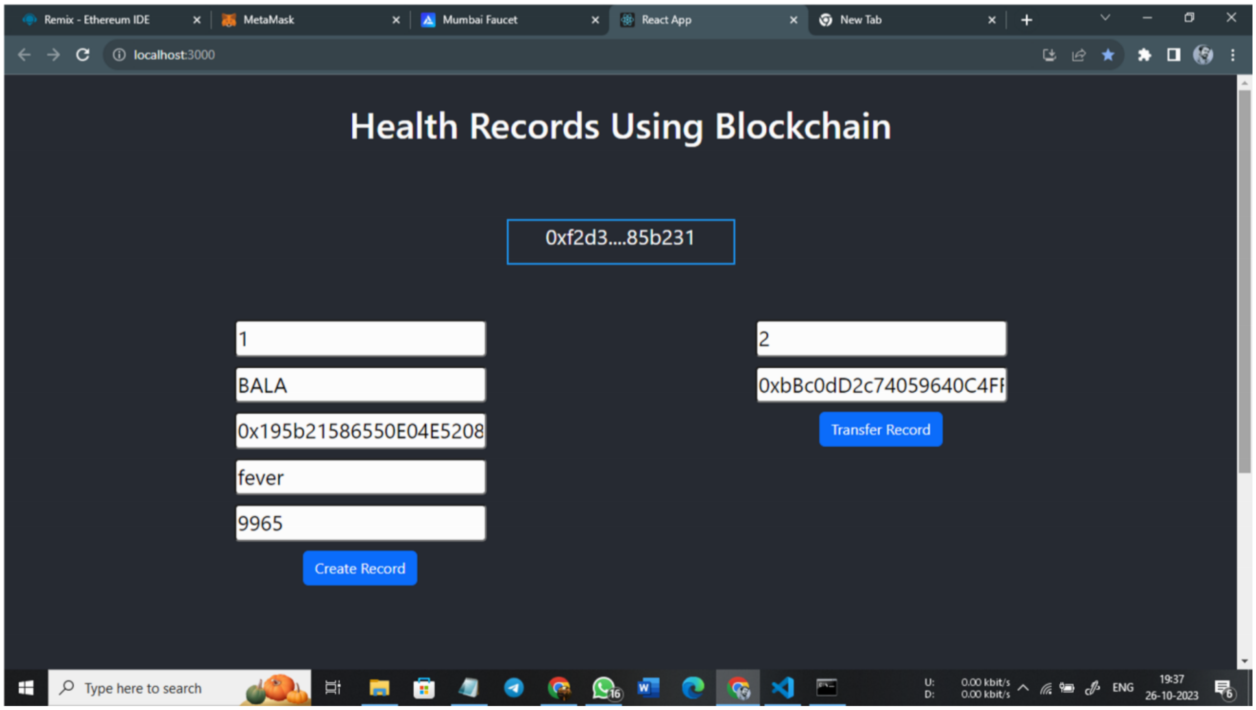
9. Compliance Adherence: Ensure the system complies with healthcare regulations and standards, measuring the level of adherence to various regulatory requirements.

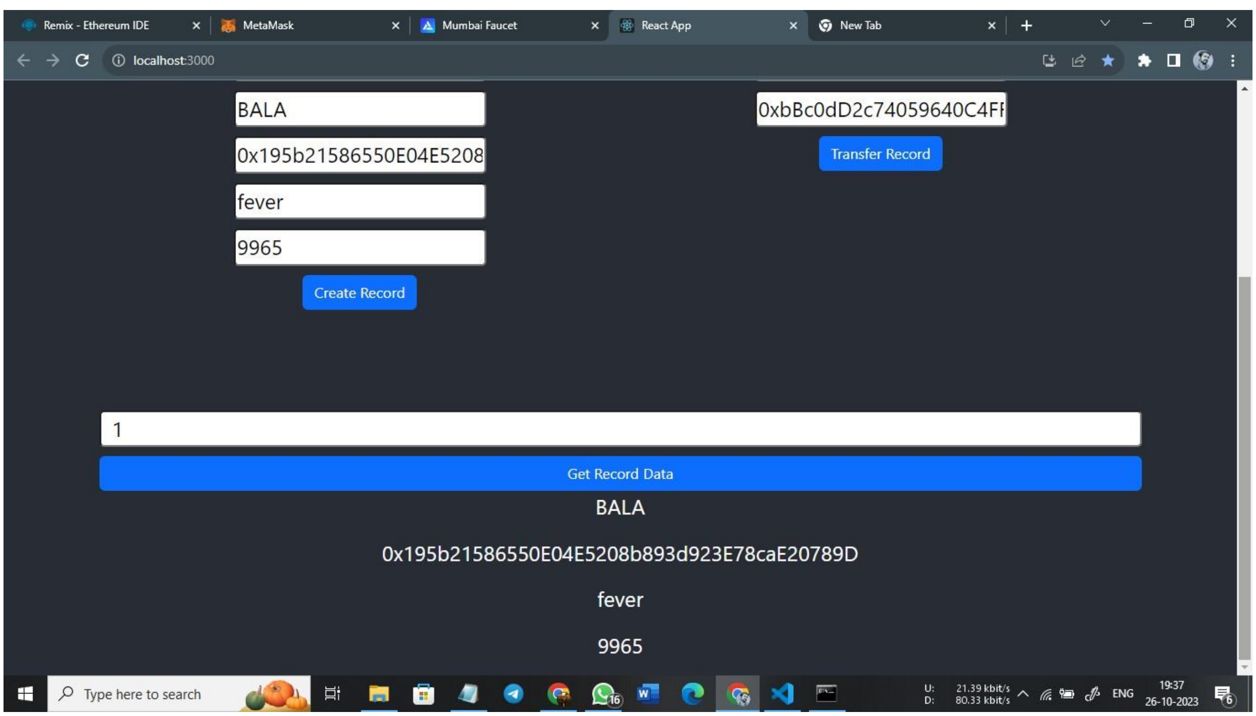
10. Fault Tolerance & Resilience: Evaluate the system’s ability to continue functioning and maintaining data integrity in the face of node failures or network disruptions.

These metrics collectively ensure the performance, security, scalability, and user satisfaction of the blockchain-based EHR system, offering a comprehensive view of its effectiveness in the healthcare ecosystem.

9.RESULTS

9.1 Output Screenshots





10. ADVANTAGES & DISADVANTAGES

Advantages:

1. Security and Data Integrity:

- Blockchain ensures that EHR data is tamper-proof and cannot be altered or deleted without proper authorization, enhancing data integrity.
- Robust encryption and access controls protect EHRs, making it challenging for unauthorized users to access sensitive information.

2. Privacy and Consent Management:

- Patients can have more control over their EHR data and grant consent for sharing with healthcare providers or researchers.
- Blockchain-based EHRs can maintain a transparent and auditable record of consent.

3. Interoperability:

- Blockchain can facilitate seamless data exchange among different healthcare providers and systems, improving interoperability.
- Standardized data formats and coding systems ensure uniformity and compatibility.

4. Reduced Data Redundancy:

- Patients' records can be updated in real-time, reducing duplicate data entry and redundancy across multiple healthcare providers.

5. Access Control:

- Fine-grained access control mechanisms enable healthcare professionals to access only the relevant parts of a patient's EHR, protecting privacy.

Disadvantage

Implementing blockchain technology for electronic health records (EHRs) comes with certain disadvantages and challenges, including:

1. Scalability Issues:

- Many public blockchain platforms struggle with scalability, leading to slower transaction processing and higher costs as the network grows.
- Scaling on a blockchain while maintaining data integrity can be complex and costly.

2. Interoperability Challenges:

- Integrating blockchain-based EHR systems with existing healthcare infrastructure and legacy EHR systems can be complicated and may require significant development efforts.
- Lack of uniform standards for blockchain interoperability can hinder data exchange between different systems.

3. Complexity and Cost:

- Developing and maintaining a blockchain-based EHR system can be complex and expensive, particularly in terms of infrastructure, skilled personnel, and ongoing maintenance.

4. Energy Consumption:

- Some blockchain consensus mechanisms, like Proof of Work (PoW), are energy-intensive, contributing to environmental concerns and increased operating costs.

5. Privacy Concerns:

- While blockchain can enhance data security, the transparency of the ledger means that all data, including sensitive information, is visible to authorized participants, potentially raising privacy concerns.
- It may be challenging to strike the right balance between data privacy and transparency.

6. Lost Private Keys:

- If a patient loses their private key, it can result in permanent loss of access to their EHR data, which can be problematic for continuity of care.

11. CONCLUSION

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

This automation has been made much easier to deploy due to Ethereum and smart contracts. The suggested wallet serves as a bridge for providing secure and convenient access to the blockchain, as well as hassle-free secret key maintenance. It can also act as a link for patients who are uncertain about migrating their information to electronic health records (EHRs). The system's cryptographic encryption methods. As a result, the authentication, data exchange, and security of medical reports have already been completed successfully utilizing blockchain. The system also deals with the problems caused by direct disease transmission in hospitals, like the ongoing COVID-19 situation, mainly through physical copies of medical records and the increased risk associated with additional human chain contamination.

12.FUTURE SCOPE

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

Another possibility is that the payment module will eventually be integrated into the existing architecture. This can be accomplished via a decentralized architecture based on blockchain technology, in which a patient pays for a specialist’s consultation with a credit or debit card. In the event of verification, the NID number can be included.

With the introduction of Ganache, we now have the opportunity to experiment with a similar technique utilizing a private blockchain. It will involve enhancing lookup and supporting the extra capabilities required by an EHR management solution. In addition, there will be a comparison of present and future methodologies.

13. APPENDIX

Source Code

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;


contract HealthRecords {


        struct PatientRecord {
        string  Name;  address
                patientAddress;
        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;

} 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;
    }
}
```

GitHub & Project Demo Link

Githublink: https://github.com/MohanRaj147/NAANMUDHALVAN---NM2023TMID11607/tree/main

Project Demo Link: https://youtu.be/TVpuNzHoKFE?si=JJ6dNRPvtKDKGDrW