A PROJECT REPORT ON

EHR MANAGEMENT USING BLOCKCHAIN

SUBMITTED TO THE SAVITRIBAI PHULE PUNE UNIVERSITY, PUNE

IN THE PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE AWARD OF THE DEGREE

OF

BACHELOR OF ENGINEERING

(COMPUTER ENGINEERING)

SUBMITTED BY

Sneha Joshi	63
Atharva Sajgure	62
Vedant Patil	08
Swapnil Singh	09

UNDER THE GUIDNACE OF

PROF. MOHAMMAD SHARIQUE

DEPARTMENT OF COMPUTER ENGINEERING

Sandip Institute of Technology and Research Centre, Nashik

Nashik-422213

SAVITRIBAI PHULE PUNE UNIVERSITY

2022 -2023

SANDIP FOUNDATION

CERTIFICATE

This is to certify that the project report entitles

"EHR MANAGEMENT USING BLOCKCHAIN"

Submitted by

Sneha Joshi	63
Atharva Sajgure	62
Vedant Patil	08
Swapnil Singh	09

is a bonafide student of this institute and the work has been carried out by him/her under the supervision of **Guide Name** and it is approved for the partial fulfillment of the requirement of Savitribai Phule Pune University, for the award of the degree of **Bachelor of Engineering** (Computer Engineering).

Prof. Mohammad Sharique
Guide
Department of Computer Engineering

Dr. Amol Potgantwar
Head
Department of Computer Engineering

Dr. M. M. Patil
Principal

DEPARTMENT OF COMPUTER ENGINEERING

Sandip Institute of Technology and Research Centre, Nashik

Nashik-422213

SAVITRIBAI PHULE PUNE UNIVERSITY

2022 -2023

ACKNOWLEDGEMENT

It gives us great pleasure in presenting the preliminary project report on “EHR sytem using blockchain ”.

Firstly, we would like to express our indebtedness appreciation to our internal Guide Prof. Mohammad Sharique . His constant guidance and advice played very important Role in making the execution of the report. He always gave us his suggestions, that were crucial in making this report as flawless as possible.

We would like to express our gratitude towards Prof. Dr. Amol Potgantwar Head of Computer Engineering Department, SITRC For his kind co-operation and encouragement which helped us during the completion of this report.

Sneha Joshi

Atharva Sajgure

Vedant Patil

Swapnil Singh

ABSTRACT

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

Keywords: Blockchain, health records, electronic health records, decentralization, and scalability.

TABLE OF CONTENTS

LIST OF ABBREVATIONS

ABBREVIATION	ILLUSTRATION
EHR	Electornic Health Record
EVM	Ethereum Virtual Machine
IPFS	Interplanetary File System

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION

The objective of this project is to provide the application which is user friendly and cost effective. The major advantage of this project is security. A securable system is more important to be reliable. Electronic Health Records (EHRs) provide a convenient health record storage service, which promotes traditional patient medical records on paper to be electronically accessible on the web. This system was designed to allow patients to possess the control of generating, managing and sharing EHRs with family, friends, healthcare providers and other authorized data consumers. Moreover, provided that the healthcare researcher and providers of such service access these EHRs across-the aboard, the transition program of healthcare solution is expected to be achieved. However, in the current situation, patients scatter their EHRs across the different areas. During life events, causing the EHRs to move from one service provider database to another. Therefore, the patient may lose control of the existing healthcare data, while the service provider usually maintains the primary stewardship. Patient access permissions to EHRs are very limited, and patients are typically unable to easily share these data with researchers or providers.

Blockchain is a decentralized database whose data block is connected chronologically. In the healthcare industry, there are many different parties who need to collaboratively manage personal EHRs blockchain (in a model of consortium blockchain), such as medical specialists, hospitals, insurance departments, etc. Electronic Record Systems are proprietary that is centralized by design. This means that, there's a single supplier that controls the code base, database and the system outputs and supplies the monitoring tools at the same time. It is difficult for centralized systems to gain trust from patients, doctors and hospital management. Open source, independently verifiable systems solves this issue. The cryptographic property in the blockchain networks guarantees the patients' privacy. Data integrity and incorruptibility protect medical data from being tampered. The blockchain can be viewed as a distributed database, which stores data in each network nodes to avoid the halting problem. It thus provides higher stability, consistency and attack-resistance. The problem of distributed denial-ofservice attacks (DDOS) in the conventional centralized framework can be solved by the blockchain technique. Deployment of blockchain in the medical record system not only provides the reliable service but also speeds up the medical

record exchange. Owing to decentralization, the ownership of the medical record is returned to the patients, allowing them to manage the medical record directly and take care of their own health.

MOTIVATION

Even after such an advancement in technology, storage, verification, synchronization and sharing of medical records have always been a challenge difficult to address. When healthcare providers and researchers need to access and share healthcare data, they are under strict policy and technological constraints, which means a substantial amount of time and resources must be spent on conducting permission review and data verification. In most cases, the databases of each hospital are independently managed; each platform has its own set of standards and there is a lack of motivation and incentive for sharing data between different healthcare organizations. Patients have no control over their own medical data. They are unaware of what their medical records contain and who is able to access their data.

With recent rapid development in blockchain technology, it is proposed that records such as diagnosis, prescriptions, and payments can be stored and managed securely using blockchain. The technology can be used to give the patients ability to manage their own medical data. Patients would have the power to decide who can access their data and for what duration. Any change in the data would reflect in the blockchain permanently making storing of data secure.

PROBLEM DEFINITION

- The current solution in healthcare for storing and sharing medical records is electronic healthcare record which is highly sensitive.
- The majority of EHR data sharing is still done through mail because shortage of trustable and reliable health data sharing mechanism. This leads to significant delays in patient's treatment and many other reasons
- For patients the decision to participate in a clinical trial is a complex decision and often requires weighing the pros and cons of potential medical benefits vs. the unidentified risks of side effects. One solution could be that the patient becomes owner of their data to find the correct and efficient cure.
- Different hospitals and health facilities have different systems. Hence, Integration and interoperability issues are the consequences.
- Blockchain has a decentralized system providing a cryptographic guarantee of data integrity, security, privacy, smart contracts for data access.
- A part of literature on EHRs management addresses these problems by proposing centralized frameworks and systems for sharing EHRs on cloud infrastructures. Although these frameworks brought solutions to many of the challenges listed above, they still suffered from limitations especially as related to transparency, data ownership, and privacy.
- Natural disasters introduce new challenges as the healthcare sector should be prepared and able to respond to the crisis promptly. This is one of the arguments that demonstrate how decentralizing the management of EHRs and replicating and distributing the information can assure better performance and availability in disaster situations, compared to centralized models.

LITERATURE SURVEY

Authors in [2] presented the MedRec system, a decentralized medical record management system based on blockchain technology. There are three types of Ethereum smart contracts to associate patients' medical data to allow third-party users to access the data. Yang et al. [3] further presented an attribute-based authentication mechanism on the MedRec system to enable the secure sharing of medical data. A high-level blockchain-based framework was designed in [4], where an identity-based authentication and key agreement protocol is applied to achieve user membership authentication. They also developed the MedShare [5] system to provide data provenance and control in cloud repositories among hospitals. Liang et al. [6] used the hyperledger fabric membership service and channel formation scheme to guarantee data privacy in a blockchain network for medical data sharing. The mobile application was also implemented to collect data from wearable devices for storage and sharing with healthcare providers. Patientory [7] is a peerto-peer medical record data storage network. The software framework in [7] was presented to address the authentication, authorization, access control, data encryption interoperability enhancement and token management.

Authors in [8] proposed the MedChain system, where the timed-based smart contracts can interact with the various demands of health providers, patients and third parties. An incentive mechanism in [8] was also presented to leverage the degree of health providers about their efforts on maintaining medical records. In [9], an attribute-based signature scheme with multiple authorities was designed. There are multiple authorities without a centralized one to generate and deliver public/private keys of the patient, avoiding the escrow problem. Liu et al. [10] presented a healthcare insurance anti-fraud system based on blockchain. A hybrid architecture to facilitate access control of medical data was developed in [11]. A blockchain is used to manage identity and access control and acts as a tamperproof log of access events. Hasavari et al. [12] introduced a combination of secure file transfer methods and blockchain techniques as a solution to record patient's emergency medical data such that ambulance crews can access and use it to provide high quality pre-hospital care.

SOFTWARE REQUIREMENTS SEPCIFICATION

INTRODUCTION

Project Scope:

Electronic Medical Record (EMR) systems. However, hospital still face some issues regarding the security of medical records, user ownership of data, data integrity etc. The solution to these issues could be the use of a novel technology, i.e., Blockchain.

User classes and characteristics:

Applications has mainly three types of users, admin, patients and doctors. Users login to the application by connecting their MetaMask wallet to the application.

1. **Admin –** Admin can register a user as a patient or a doctor. MetaMask wallet address of user is used to identify the identity.
2. **Patient –** A patient is the owner of his data, patient can grant and revoke permissions from doctors and other health organizations like hospitals, research labs, medical insurer, etc.
3. **Doctor –** A doctor can add, edit, view or delete the medical records of patients who have given access to their medical records.

Assumptions and dependencies:

Assumptions-

There is a finite cyclic group G with prime order q, and $a,b,c,n \in Z*q$ are picked out randomly. The difficult problems bellows underlying the security of this scheme.

Definition 1 (Discrete Logarithm (DL) Problem):

Given two elements $P,Q \in G$, find an integer n to satisfy the equation $Q=nP$.

Definition 2 (Computational Bilinear Diffie-Hellman (CBDH) Problem):

Given random elements $\{A=aP,B=bP,C=cP\} \in G3$ and the bilinear pairing map $e^{\wedge}:G \times G \rightarrow GT$, it is computing the value $e^{\wedge}(P,P)abc$.

The CBDH assumption asserts that there exists no probabilistic polynomial-time algorithm B to successfully solve the CBDH problem, i.e., for any positive number $\varepsilon>0$, the equation $Pr[B(A,B,C)=e^{\wedge}(g,g)abc]<\varepsilon$ holds.

FUNCTIONAL REQUIREMENTS

System Feature 1

- The web application is user friendly.
- It provides an easy interface to user.
- The accessibility or response time of the application should be fast

System Feature 2

The EHR app inputs the info into the scheduling systems in order to keep it updated about the most recent appointments.

EXTERNAL INTERFACE REQUIREMENTS

1. **User Interfaces –** User interface needs to be user-friendly and responsive, usable on android device, desktop and laptop.
2. **Software Interfaces**
    a. User must have MetaMask web-extension installed on their browser.
    b. MetaMask is an extension for accessing Ethereum enabled distributed applications, or "Dapps" in your browser!
    c. User need to login using their MetaMask wallet address

NON-FUNCTION REQUIREMENTS

Performance Requirements

We evaluate the performance of TP-EHR in terms of communication and computational overhead. We conduct the experiments on a computer with Window 10 system, an Inner Core 2 i5 CPU, and 8 GB DDR 3 of RAM. We utilize C language and MIRACL Library to implement TP-EHR. The security level is selected to be 80 bits.

Safety Requirements

- *Decentralization*: Compared with the centralized mode, blockchain no longer needs to rely on the semi-trusted third party.

- *Security*: It is resilient to single point of failure and insider attacks in the blockchain-based decentralized system.
- *Pseudonymity*: Each node is bound with a public pseudonymous address to protect its real identity.
- *Immutability*: It is computationally hard to delete or modify any record of any block included in the blockchain by one-way cryptographic hash function.
- *Autonomy*: Patients hold the rights of their own data and share their data flexibly by the settings of special items in the smart contract.
- *Incentive mechanism*: Incentive mechanism of blockchain can stimulate the cooperation and sharing of competitive institutions to promote the development of medical services and research.
- *Auditability*: It is easy to keep trace of any operation since any historical transaction is recorded in the blockchain.

Security Requirements:

1: EHR confidentiality.

The cloud storage and server should not gain any knowledge from the outsourced EHR on their premises. Apart from that, suppose an adversary breaches the cloud storage and obtains the EHR, the adversary should not be able to read or carry out a known ciphertext attack to obtain any knowledge from the EHR.

In the BHMV scheme, symmetric encryption is used to encrypt all the EHRs before outsourcing them to third-party online storage. The EHRs are encrypted with a user-defined secret key using a 256-bit Advanced Encryption Standard Cipher-Block Chaining (AES-CBC) encryption algorithm. As a result, the adversary cannot decrypt and read the EHR ciphertext without the EHR owner's symmetric key. Additionally, the initialisation vector used for encryption can hide the ciphertext pattern by adding the random factor to each block of the cipher. Therefore, encrypting an identical block of plaintext will not result in the identical ciphertext that may reveal the ciphertext pattern to the adversary.

Notice that the entries of the bitmap index are computed with a different secret key. The separate keys prevent any similarities between the encrypted keyword matrix and the EHR ciphertext. The document identifiers in the bitmap index are created from the file hash values, preventing leaking any information about the document. The search of the encrypted keyword is done in the blockchain—a separate network from the database where the EHR ciphertext is stored. As a result, the cloud service provider would not gain any information between the search token and search result. Finally, the underlying communication channel is assumed to have additional protection in place under the protocol level, such as SSL/TLS. This will prevent adversaries from obtaining any link between the searches and the search results from different sessions, even if they were aware (e.g., revoked users) of the past searched keyword and search results. As a result, the BHMV scheme should be secure against adaptively chosen keyword attacks. Under the circumstances, the confidentiality of the outsourced EHR is safeguarded against the adversary.

2: Two-side verifiability.

Consider an intermediate party intersects and modifies the search token T or the search result R transmitted from the user-side or the server-side. The man-in-the-middle adversary tampers with the message and signs a new Elliptic Curve Digital Signature Algorithm (ECDSA) digital signature based on the hash value of the modified message. Upon receiving the modified message, the digital signature will fail the verification test and the message will be discarded.

In the EHR searching phase, the search request from the user and the search result from the server are needed to be verified and authenticated with an ECDSA signature. If the signer's ECDSA public key is not present in the access list on the blockchain, the recovered ECDSA signature will automatically fail the verification process. Moreover, if the hash function H_{ECDSA} used is collision-resistant, the adversary is unable to forge an ECDSA digital signature under a chosen message attack. Therefore, the adversary cannot carry out a man-in-the-middle attack for spoofing as a legitimate user due to the two-side verifiability.

3: Storage immutability.

BHMV provides a durable medium for storing the EHR safely even in the outsourced environment. Assuming an adversary gains access and tries to modify the EHR on the Interplanetary File System (IPFS) storage, the malicious modification attempt of the EHR can be easily identified and prevented. The EHR index used for searching is also tamper-proof from any malicious party who tries to breach the search result accuracy by tampering with the EHR index.

Given the hash function H_{IPFS} used by IPFS storage, any minor modification in the EHR will result in an extensively new hash value. By comparing the modified EHR hash value to the original EHR hash value stored on the Ethereum blockchain, the attempt of EHR modification can be easily identified. In addition, the hash function used is collision-resistant, in which it is infeasible for the adversary to compute the same hash value with the modified EHR'.
Given $EHR \neq EHR'$, it is computationally infeasible to find $H(EHR) = H(EHR')$. Since the index of the EHR is stored on the distributed ledger of the Ethereum blockchain, the index storage is inherently supporting tamper-proof and non-repudiation properties from the characteristics of the blockchain storage. Consequently, the data storage of the EHR and its corresponding index satisfies the storage immutability property.

SYSTEM REQUIREMENTS

Database Requirements –

- Firebase
- NoSQL database

Software Requirements –

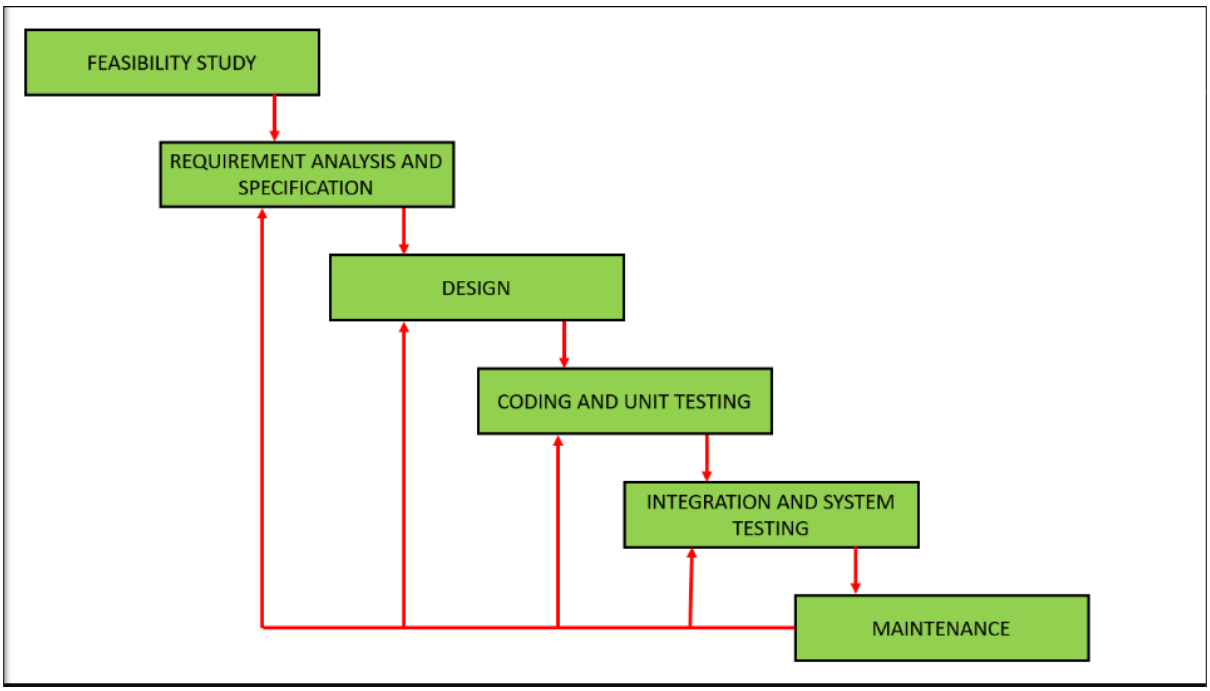
- Operating System: Windows 10 (64bit) or above / Linux / Mac OS
- Languages:
    - Solidity
    - TypeScript
    - HTML
    - CSS
    - SASS
    - Javascript
- Angular JS
- Node JS
- Ganache
- Metamask chrome
- Json
- Git, Github
- Truffle
- VS code
- Npm

Hardware Requirements –

- Ram: 2GB or above
- Hard Disk: 1GB or above
- Processor: 64bit, single-core, 2.5GHz minimum per core speed

ANALYSIS MODELS: SDLC MODEL TO BE APPLIED

The project uses iterative waterfall model for development. Iterative waterfall model is a modified version of classical waterfall model, it is made by incorporating the necessary changes to classical waterfall model to make it usable in practical software development projects.



The key difference between iterative and classical waterfall model is the feedback paths that iterative model provides. These feedback paths allow correcting error committed in some previous phase. It reduces the effort and time required to correct the errors.

Feasibility study: The feasibility study is based on needs of the project, where it evaluated whether the project can be done or not, based on aspects like, legal, technical, operation feasibility, economic, schedule.

Requirement analysis and specification: In this phase, requirements are gathered from customers and check by an analyst whether requirements will fulfil or not.

Design: In the design phase, team design the software by the different diagrams like Data Flow diagram, activity diagram, class diagram, state transition diagram, etc.

Coding and Unit testing: In the implementation, requirements are written in the coding language and transformed into computer programmes which are called Software.

Integration and System testing: After completing the coding phase, software testing starts using different test methods. There are many test methods, but the most common are white box, black box, and grey box test methods.

Maintenance: In the maintenance phase, after deployment of the software in the working environment there may be some bugs, some errors or new updates are required. Maintenance involves debugging and new addition options.

The iterative model is suitable for development of this project because –

- Requirements of software are well understood in the initial stage and there is hardly any possibility of change in requirements.
- Software need not to be delivered immediately, so the software can be completely built and delivered after the completion of last phase of SDLC.

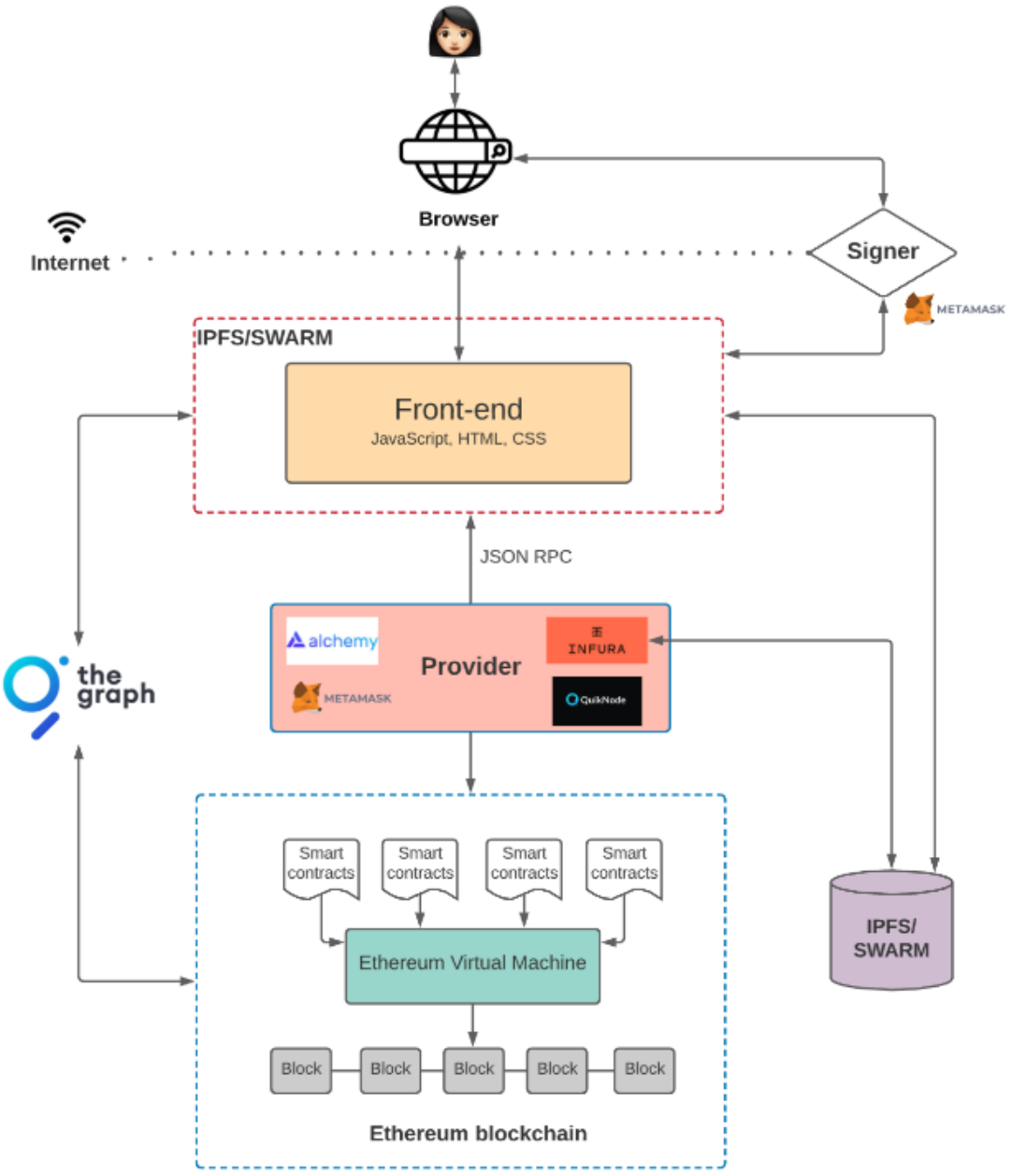
There is no requirement of parallel development, development phases can be executed sequentially.

SYSTEM IMPLEMENTATION PLAN

Task	**Start date**	**End date**
Preliminary survey		
Define the problem		
Literature survey		
Project statement		
Deciding blockchain platform		
Finalizing Techstack		
Designing Architecture		
Creating and testing smart contracts		
Building APIs		
Creating User Interface		
Deployment		
Testing		

SYSTEM DESIGN

SYSTEM ARCHITECTURE



Ethereum – The Ethereum blockchain is often touted as a "world computer". That's because it's a globally accessible, deterministic state machine maintained by a peer-to-peer network of nodes. State changes on this state machine are governed by the rules of consensus that the peers in the network follow.

Smart contract – A smart contract is a program that runs on the Ethereum blockchain and defines the logic behind the state changes happening on the blockchain.

Ethereum Virtual Machine (EVM) – EVM is responsible for execution of smart contracts and processes the state changes that happen on this globally accessible state machine.

Provider – The nodes on the blockchain that we connect to interact with the blockchain are called providers. Every provider implements JSON-RPC (remote procedure call) protocol that defines several data structures and the rules for their processing, and uses JSON (RFC 4627) as a data format.

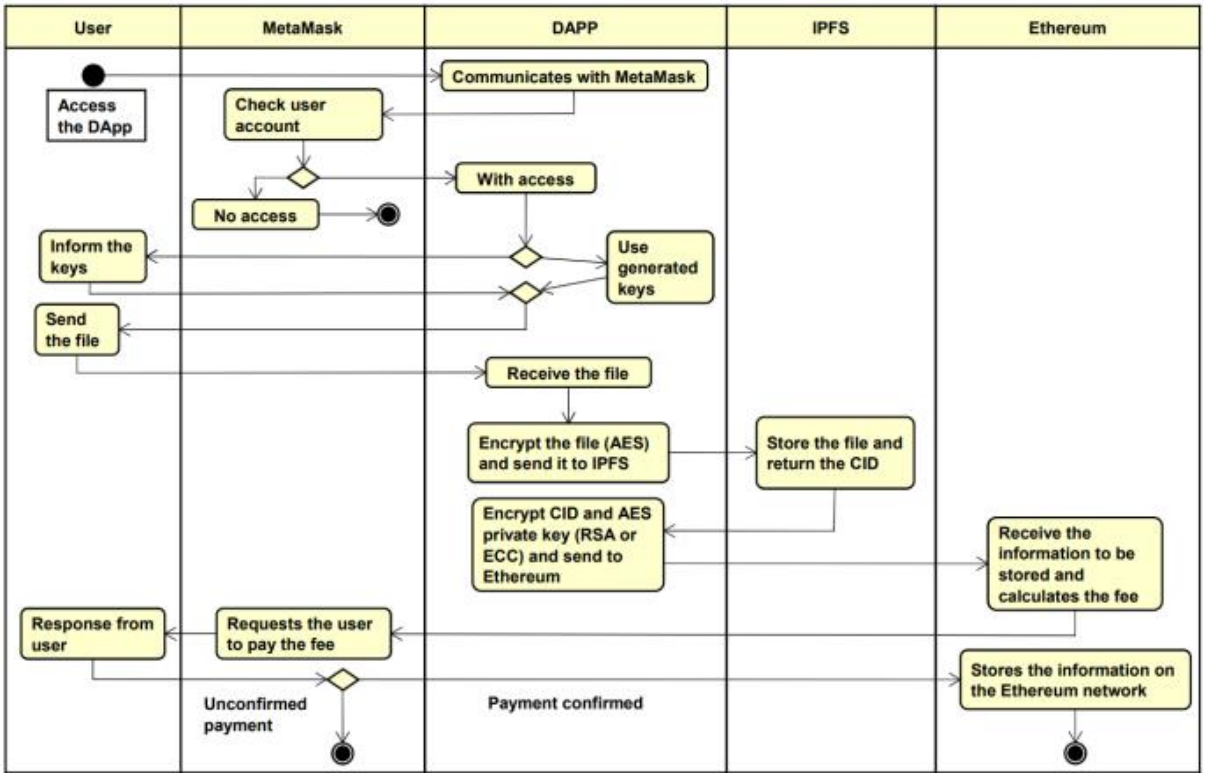
Signer (MetaMask) – After connecting to the blockchain, state of the blockchain can be read. But to write to the state of the blockchain, you need to perform a transaction which needs to be signed using your private key. This is where MetaMask comes in, MetaMask stores the user's private keys in the browser and whenever the frontend needs the user to sign a transaction, it calls on Metamask.

Front-end – It defines the UI logic, with which the user interacts. It also communicates with the application logic defined in smart contracts.

IPFS – IPFS (Interplanetary file system) is a distributed file system for storing and accessing data. The IPFS system distributes and stores the data in a peer-to-peer network. This makes it easy to retrieve data when needed.

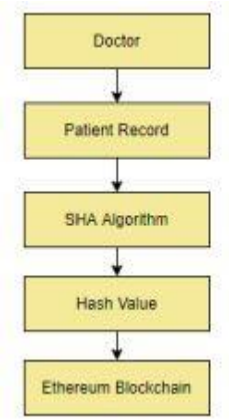
The Graph – The Graph is an off-chain indexing solution that makes it easier to query data on the Ethereum blockchain. The Graph allows you to define which smart contracts to index, which events and function calls to listen to, and how to transform incoming events into entities that your frontend logic can consume.

Sequence of tasks performed when a patient's data is being stored



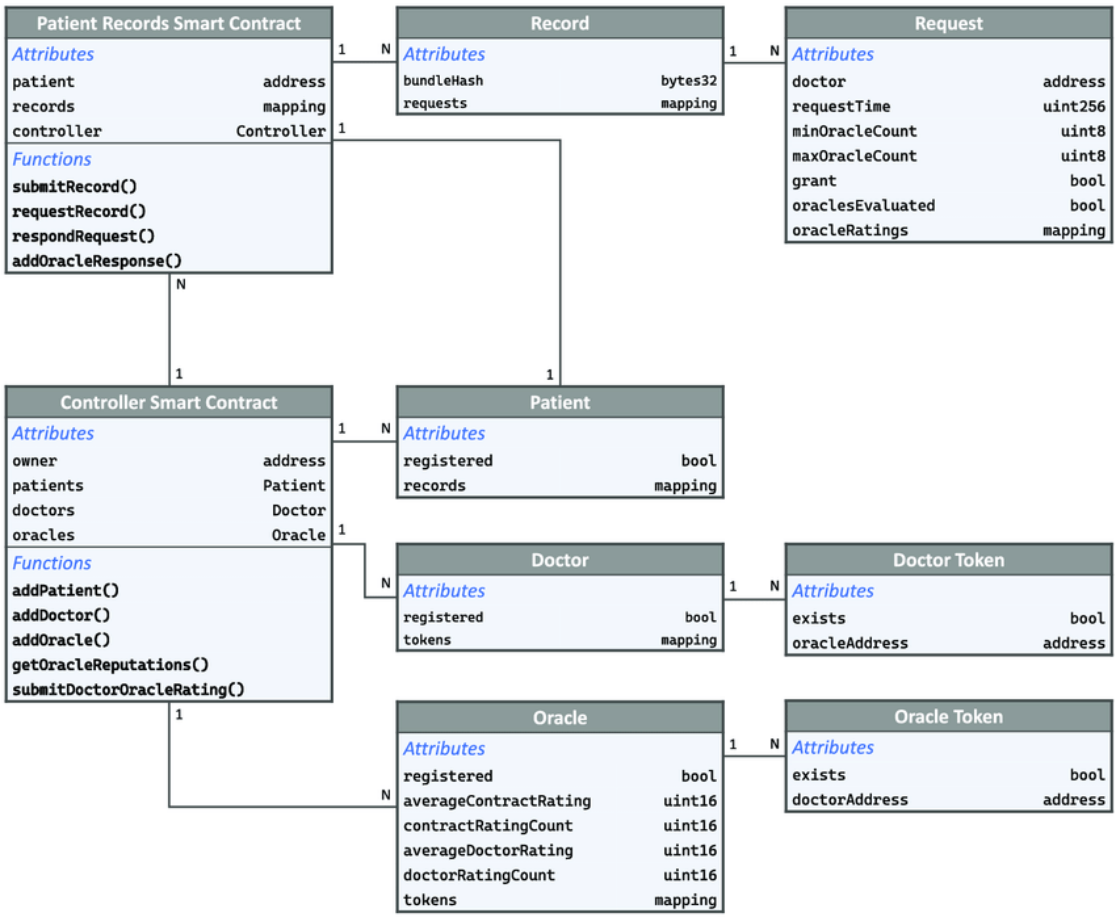
DATA FLOW DIAGRAM

A data flow diagram is generally used to represent the flow of data. The below diagram shows how the data is carried into a block.



The doctor makes note of all the patient's data and then validates it again because once the data is entered the block it cannot be changed, so validation is the most important aspect. Once the doctor finds the data accurate then by generating a hash value by the usage of SHA algorithm the data is entered the block.

ER DIAGRAM


Patient Records Smart Contract
Attributes
patient address
records mapping
controller Controller
Functions
submitRecord()
requestRecord()
respondRequest()
addOracleResponse()
Record
Attributes
bundleHash bytes32
requests mapping
Request
Attributes
doctor address
requestTime uint256
minOracleCount uint8
maxOracleCount uint8
grant bool
oraclesEvaluated bool
oracleRatings mapping
Controller Smart Contract
Attributes
owner address
patients Patient
doctors Doctor
oracles Oracle
Functions
addPatient()
addDoctor()
addOracle()
getOracleReputations()
submitDoctorOracleRating()
Patient
Attributes
registered bool
records mapping
Doctor
Attributes
registered bool
tokens mapping
Doctor Token
Attributes
exists bool
oracleAddress address
Oracle
Attributes
registered bool
averageContractRating uint16
contractRatingCount uint16
averageDoctorRating uint16
doctorRatingCount uint16
tokens mapping
Oracle Token
Attributes
exists bool
doctorAddress address
1
N

UML DIAGRAMS

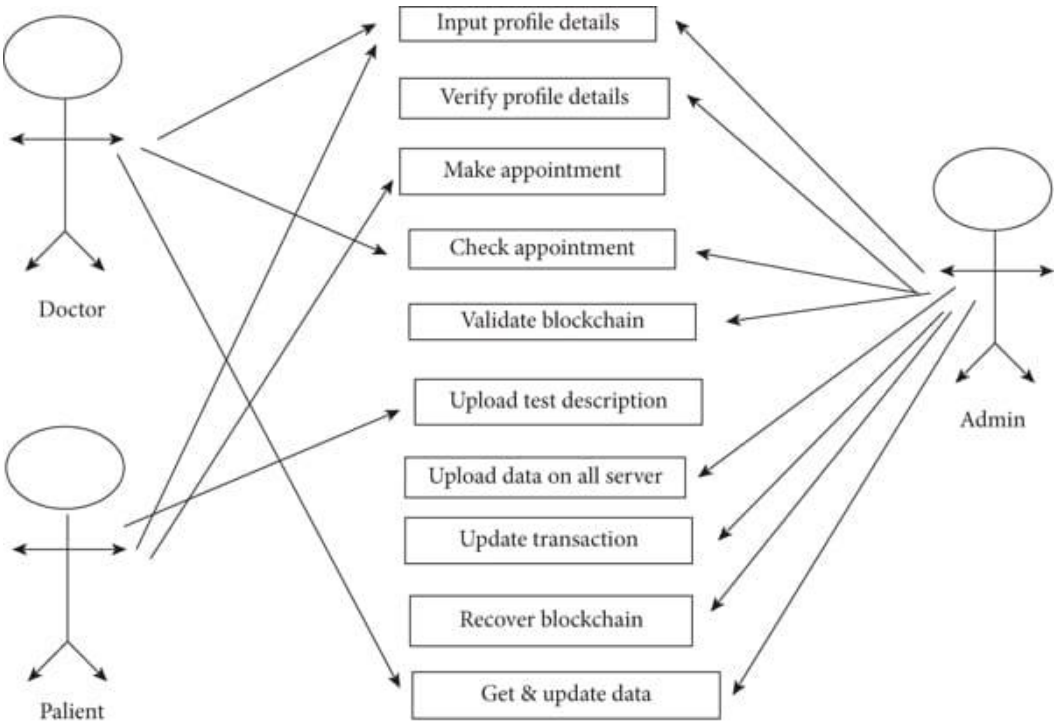
UML represents Unified Modeling Language. UML is an institutionalized universally showing dialect in the subject of program designing.

The goal is for UML to become a regular dialect for design of item in PC programming. In its gift frame UML is contained two noteworthy components: a Meta-show and documentation. Later on, a few type of method or system can also likewise be brought to; or related with, UML.

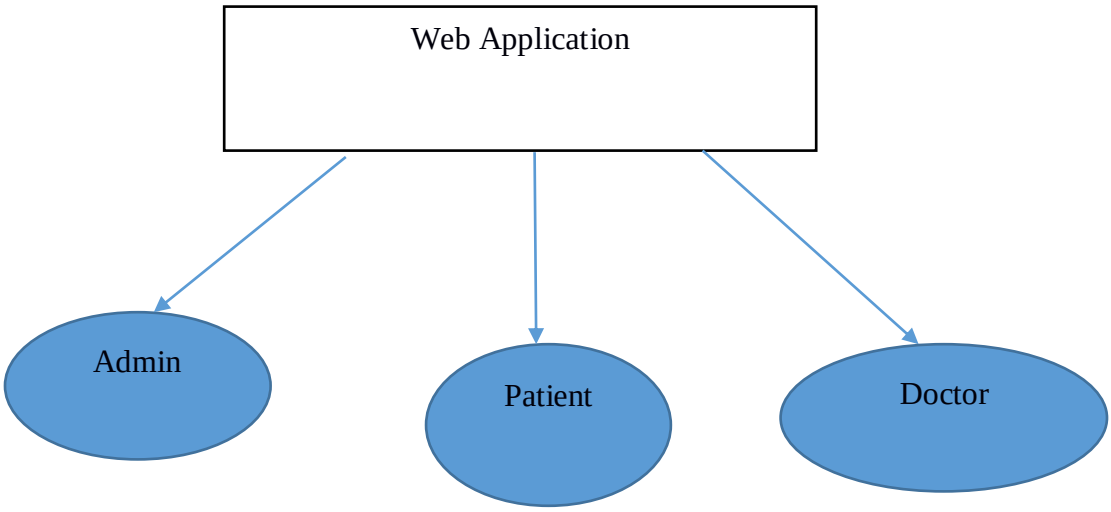
The Unified Modeling Language is a popular dialect for indicating, Visualization, Constructing and archiving the curios of programming framework, and for business demonstration and different non-programming frameworks.

The UML discusses on accumulation of first-rate building practices which have are useful in the demonstration of full size and complicated frameworks.

The UML is a essential piece of creating gadgets located programming and the product development method. The UML makes use of commonly graphical documentations to for programming platforms or systems.



The EHR web application designed for our project has three access logins. It was built upon Blockchain-based architecture. Data can be shared in a peer-to-peer approach which is either by a doctor to patient or patient to doctor. Users are Doctors, Patients, and Admins. Doctor <=> Patient (Transaction of medical data) Fig: Web application structure .



Admin :

- Admin can log in and signup based on the hospital he is working in.
- Admin can create patient accounts.
- Admin can create doctors' accounts who are working in the hospital under different specialities.

Patient:

- A patient can log in and sign up by providing their credentials.
- Patients can book an appointment with the doctor by filling out a form about the symptoms.
- A patient can see their diagnosis results given by the doctor.

Doctor:

- Doctors can log in and sign up by providing their credentials.
- A doctor can see his/her booking appointments on the Dashboard.
- A doctor can see the patient's details and based on the information provided by the patient, he/she can prescribe medications

OTHER SPECIFICATIONS

ADVANTAGES

Interoperability — Currently, systems in different countries are fragmented and don't talk to each other. An electronic health record based on the blockchain can unlock true interoperability by connecting fragmented systems across countries and regions.

Security — With blockchain, healthcare data can be stored immutably in a decentralized manner instead of storing in one database. As a result, there would be no single point of entry for a hacker to retrieve the data. That's how blockchain can ensure better data security for health information.

Authorization — Blockchain enables patients with better control of their data. Once the data is stored on the blockchain and assigned to the public key, the patient can provide access to the data to only the required authorities.

Transparency — Every node on blockchain stores a copy of the data which is updated in real-time. Thus, any alteration or corruption to the health data will be immediately spotted. The system also signs every transaction with a cryptographic stamp which allows tracing back to the origin of every piece of data.

LIMITATIONS

- **Potential Privacy and Cybersecurity Issues** - All computerized systems are vulnerable to attacks by hackers, and EHR systems are not immune. The consequences of private medical information getting into the wrong hands could be dire.
- **Inaccurate Data -** If an EHR is not updated immediately, as soon as new information is gleaned, such as following an exam or after test results come in, anyone viewing that EHR could be receiving incorrect or incomplete information. This could lead to subsequent errors in diagnosis, treatment, and health outcomes, not only by the issuing practitioner but also by any specialists, pharmacists, physical therapists, or personal trainers participating in the patient's care.
- **Frightening Patients Needlessly -** When a patient has access to his or her own medical information at will, it can expose that patient to information he or she may not completely understand. The ability to access information one does not thoroughly understand could lead to a host of misunderstandings, including those that create a panic in the patient or lead him or her to take inappropriate, and potentially detrimental, actions.
- **Malpractice Liability Concerns -** Implementing an EHR system opens the door to several liability concerns, such as how to ensure precious medical data does not get destroyed or lost during the transfer from paper to electronic records. This, in turn, could lead to errors in treatment. Physicians can be held liable for any inability to access all the medical data at their disposal, especially when that data is supposed to be more accessible given their electronic nature.
- **Time and Money -** It can take years to select and set up an EHR system and completely switch over all your paper records to digital ones. Over that time, you must determine your budget and decide what features you require. It also takes time to demo EHR products and negotiate with EHR system vendors to choose and implement the right system for your practice. Then, even after your new EHR system is all set up and running smoothly, you still need to take the time to train your staff in how to use it. There is also the cost involved in setting up and switching over to a whole new medical records system, which, even at competitive prices, doesn’t come cheap. Fortunately, as more and more players enter the EHR system marketplace, increased price competition is becoming more prevalent.
- **Inconvenience and Inefficiency** - As suggested above, maintaining an EHR system requires frequent updates. If your team doesn’t stay on top of that, your records could lose

their accuracy and, subsequently, their value. EHRs can also be inconvenient in that they require computer access and, more, internet access to utilize. If you have a power outage or computer failure, that information can become inaccessible. An essential part of a strong EHR is the ability to have an information technology team available to solve technical problems immediately so that patient care interruptions are minimized.

APPLICATIONS

- **Better Health Records Exchange**

  ARRA 2009 (American Recovery and Reinvestment Act of 2009) needs all qualified healthcare experts to adopt or show "meaningful use" of EHR. This act stimulated a significant increase in EHR adoption. However, most systems are not capable of sharing their health data, which is one of the biggest challenges of health IT and EHR interoperability. Blockchain technology has the potential to address interoperability challenges by being utilized as a common technical standard to securely distribute electronic health data.

- **Increase Data Security and Privacy**

  Security and data integrity issues hinder meaningful coordination and collaboration in healthcare. The threat of cyber-attacks and confusing interoperability standards put data at risk and limit the ways it might be distributed and accessed. However, too often data isn't trusted even though it is exchanged, partly because files are corrupted or include errors, forcing to manually correct them. Blockchain technology assures access control through shared public and private chains. While public information is open to all of the network participants, private information is encrypted and can be accessed only by authorized users. Thus, blockchain-enabled systems defend EHRs and ePHI as well as improve the privacy required by HIPAA.

- **Validate the Correctness of Billing Management**

  Blockchain's independent structure gives a high-integrity tracking option and enables for refreshing data instantly. Any effort of data modification should be reaffirmed by all the blocks in the system. After confirmation, new data becomes a permanent part of the database and cannot be changed or erased. Blockchain can reduce financial failures as well as substantially stop fraud and illegal data shifting.

- **Empower the Medical Supply Chain**

  As per the 2017 WHO research, 10% of medical goods flowing in developing nations are either low or falsified. It is assumed that at least 1% of all drugs on the market are fraudulent. A blockchain-based system can guarantee a chain-of-custody record, tracing each level of the drug supply chain. Also, add-on functionalities (e.g. private keys, smart contracts) strengthen the credibility of the pharmaceutical supplier at any delivery step and better maintain the agreements between different parties.

- **Enhance the Climate of Trust in Medical Research**

  Blockchain technology can address the difficulties of result shifting and data snooping. The system enables transferring time-stamped permanent records of clinical trials and research outcomes, hence, decreasing the incidents of scam and error in clinical test records.

CONCLUSION AND FUTURE WORK

In this study, a systematic literature review regarding EHRs within a Blockchain was conducted, with the objective of identifying and discussing the main issues, challenges, and possible benefits from Blockchain adoption in the healthcare field. The application of Blockchain has exceeded the scope of the field of economics and we have highlighted Blockchain's potential for the healthcare area, while also revealing that it still highly depends on the acceptance of the new technology within the healthcare ecosystem.

Analyzing the results that were obtained from the literature review, we conclude that Blockchain technology might be a future suitable solution for common problems in the healthcare field, such as EHR interoperability, establishing sharing trust between healthcare providers, auditability, privacy, and granting of health data access control by patients, which would enable them to choose whom they want to trust and with whom to share their medical records. However, additional research, trials, and experiments must be carried out to ensure that a secure and established system is implemented prior to using Blockchain technology on a large scale in healthcare, since a patient's health data are personal, highly sensitive, and critical information.

REFERENCES

1. G. Jetley and H. Zhang, ‘‘Electronic health records in IS research: Quality issues, essential thresholds and remedial actions,’’ Decis. Support Syst., vol. 126, pp. 113–137, Nov. 2019.
2. K. Wisner, A. Lyndon, and C. A. Chesla, ‘‘The electronic health record’s impact on nurses’ cognitive work: An integrative review,’’ Int. J. Nursing Stud., vol. 94, pp. 74–84, Jun. 2019.
3. M. Hochman, ‘‘Electronic health records: A ‘‘Quadruple win,’’ a ‘‘quadruple failure,’’ or simply time for a reboot?’’ J. Gen. Int. Med., vol. 33, no. 4, pp. 397–399, Apr. 2018.
4. Q. Gan and Q. Cao, ‘‘Adoption of electronic health record system: Multiple theoretical perspectives,’’ in Proc. 47th Hawaii Int. Conf. Syst. Sci., Jan. 2014, pp. 2716–2724.
5. T. Vehko, H. Hyppönen, S. Puttonen, S. Kujala, E. Ketola, J. Tuukkanen, A. M. Aalto, and T. Heponiemi, ‘‘Experienced time pressure and stress: Electronic health records usability and information technology competence play a role,’’ BMC Med. Inform. Decis. Making, vol. 19, no. 1, p. 160, Aug. 2019.
6. M. Reisman, ‘‘EHRs: The challenge of making electronic data usable and interoperable.,’’ PT, vol. 42, no. 9, pp. 572–575, Sep. 2017.
7. W. W. Koczkodaj, M. Mazurek, D. Strzałka, A. Wolny-Dominiak, and M. Woodbury-Smith, ‘‘Electronic health record breaches as social indicators,’’ Social Indicators Res., vol. 141, no. 2, pp. 861–871, Jan. 2019.
8. S. T. Argaw, N. E. Bempong, B. Eshaya-Chauvin, and A. Flahault, ‘‘The state of research on cyberattacks against hospitals and available best practice recommendations: A scoping review,’’ BMC Med. Inform. Decis. Making, vol. 19, no. 1, p. 10, Dec. 2019.
9. A. McLeod and D. Dolezel, ‘‘Cyber-analytics: Modeling factors associated with healthcare data breaches,’’ Decis. Support Syst., vol. 108, pp. 57–68, Apr. 2018.
10. L. Coventry and D. Branley, ‘‘Cybersecurity in healthcare: A narrative review of trends, threats and ways forward,’’ Maturitas, vol. 113, pp. 48–52, Jul. 2018
11. ‘‘The future of health care cybersecurity,’’ J. Nursing Regulation, vol. 8, no. 4, pp. S29–S31, 2018.
12. D. Spatar, O. Kok, N. Basoglu, and T. Daim, ‘‘Adoption factors of electronic health record systems,’’ Technol. Soc., vol. 58, Aug. 2019, Art. no. 101144.

13. S. Nakamoto, Bitcoin: A Peer-to-Peer Electrnic Cash System. 2008, pp. 1–9.
14. W. J. Gordon and C. Catalini, ‘‘Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability,’’ Comput. Struct. Biotechnol. J., vol. 16, pp. 224–230, Jan. 2018.
15. A. Boonstra, A. Versluis, and J. F. J. Vos, ‘‘Implementing electronic health records in hospitals: A systematic literature review,’’ BMC Health Services Res., vol. 14, no. 1, Sep. 2014, Art. no. 370.
16. T. D. Gunter and N. P. Terry, ‘‘The emergence of national electronic health record architectures in the United States and Australia: Models, costs, and questions,’’ J. Med. Internet Res., vol. 7, no. 1, p. e3, Jan./Mar. 2005.
17. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, ‘‘An overview of blockchain technology: Architecture, consensus, and future trends,’’ in Proc. IEEE Int. Congr. Big Data (BigData Congr.), Jun. 2017, pp. 557–564.
18. C. Pirtle and J. Ehrenfeld, ‘‘Blockchain for healthcare: The next generation of medical records?’’ J. Med. Syst., vol. 42, no. 9, p. 172, Sep. 2018.
19. A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, ‘‘Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives,’’Cryptography, vol. 3, no. 1, p. 3, Jan. 2019.
20. J. Eberhardt and S. Tai, ‘‘On or off the blockchain? Insights on offchaining computation and data,’’ in Proc. Eur. Conf. Service-Oriented Cloud Comput., Oct. 2014, pp. 11–45