IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

HER (ELECTRONIC HEALTH RECORDS) Management System Using Blockchain

Prof. Mohammad Sharique
Sandip Institute of Technology and Research Center
Savitribai Phule Pune University
Nashik, Maharashtra, India

Vedant Patil
Sandip Institute of Technology and Research Center
Savitribai Phule Pune University
Nashik, Maharashtra, India

Atharva Sajgure
Sandip Institute of Technology and Research Center
Savitribai Phule Pune University
Nashik, Maharashtra, India

Sneha Joshi
Sandip Institute of Technology and Research Center
Savitribai Phule Pune University
Nashik, Maharashtra, India

Swapnil Singh
Sandip Institute of Technology and Research Center
Savitribai Phule Pune University
Nashik, Maharashtra, India

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. This paper deals with the use of 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 implementation of blockchain technology for in healthcare sector for EHR. The aim of our publication is to implement blockchain technology for HER and also to provide secure storage of electronic records by defining access rules for the users of the proposed framework. The data is encrypted by the algorithm known as SHA-256. It is used to encrypt all the data of the patients into a single line 256-bit encrypted text which will be stored in the blocks of Ethereum. These records are used for consultation as well as for the creation of historic family health information tree that keeps track of health issues and diseases.

Keywords: Blockchain, Ethereum, SHA-256 algorithm, decentralization, electronic health records, and scalability.

INTRODUCTION

The goal of this project is to provide a user friendly and cost-effective application. A big advantage of this project is security. A secure system is more important to be trustworthy. Electronic Health Records (EHR) provides a convenient medical record storage service that allows traditional paper medical records to be accessed electronically over the Internet.

The system is designed to give a patient control over the generation, management, and sharing of her EHR with family, friends, healthcare providers, and other authorized data users. Furthermore, if healthcare researchers and providers of such services can access these EHRs from anywhere, it is hoped that the Healthcare Solutions Transition Program will be achieved. However, in the current situation, the patient distributes her ePA to different regions. During a life event in which the EHR will be moved from her one service provider database another. Patients may therefore lose control of their existing health data, but providers usually bear the primary responsibility. Patient access to EHRs is very limited and patients typically, cannot easily share this data with researchers or providers.

A blockchain is a decentralized database in which blocks of data are linked in chronological order. In the healthcare industry, there are various parties that need to jointly manage an individual's EHR blockchain (in a consortium blockchain model), including: B. Medical professionals, hospitals, insurance departments, etc. Electronic records systems are designed to be proprietary and centralized. This means you have a single vendor to control your code base, database, and system output while providing monitoring tools. It is difficult for a centralized system to gain the trust of patients, physicians and hospital administrators. An independently verifiable open-source system solves this problem. Cryptographic ownership on the blockchain network ensures patient privacy. Data integrity and integrity prevent medical data from being tampered with. Blockchain can be thought of as a distributed database that stores data on each network node to avoid outage issues. Therefore, it improves stability, consistency, and resistance to attacks. The problem of distributed denial of service (DDOS) attacks in traditional centralized frameworks can be solved by blockchain technology. The use of blockchain in medical record systems not only provides a trusted service, but also speeds up the exchange of medical records. Decentralization returns ownership of medical records to patients, allowing them to directly manage their medical records and manage th eir own health.

Despite these technological advances, storing, reviewing, synchronizing, and sharing
medical records has always been a difficult challenge to overcome. When healthcare providers and researchers need to access and share health data, they are subject to strict policies and technical restrictions. This means that significant time and resources must be expended to perform approval reviews and data reviews. For the most part, each hospital database is managed independently. Each platform has its own standards, lacking incentives and incentives to share data between different medical institutions. Patient cannot manage his medical records. They don't know what's in their

medi

medical record or who has access to their data.

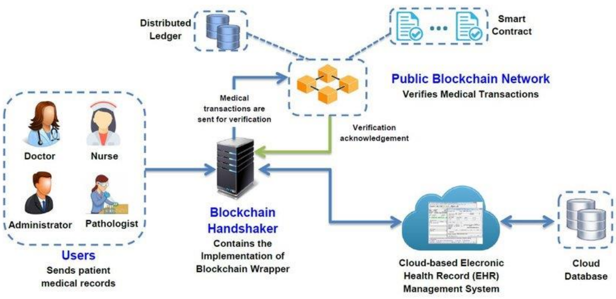
With the recent rapid development of blockchain technology, it has been proposed that blockchains can be used to securely store and manage records such as diagnoses, prescriptions, and payments. This technology can be used to help patients manage their own medical records. Patients have the power to decide who has access to their data and for how long. Data changes are reflected on the blockchain, permanently protecting data storage.

Electronic medical
record (EMR) system. However, hospitals face sev eral issues related to medical record security, data user ownership, data integrity, and more. The solution to these problems is to use new technology. H. Blockchain. User Classes and Functionality: The application mainly has his three types of users: administrators, patients and doctors. A user connects his girlfriend's MetaMask wallet to the application and logs into the application.

1. Administrators - Administrators can register users as patients or doctors. The user's girlfriend's MetaMask wallet address is used to identify the identity.

2. Patients – Patients are the owners of their data and can grant or revoke permission from doctors and other medical institutions such as hospitals, laboratories and health insurance companies.

3. Physician - Physicians can add, edit, view, or delete medical
records for patients granted access to medical records.



BLOCKCHAIN TECHNOLOGY

Definition: A blockchain is a distributed database or ledger that is stored among the nodes of a computer network. It is a peer-to-peer or P2P, distributed database that stores the ongoing transactions on the blockchain in a way that the records remain distributed, decentralized an immutable.

The transactions are stored in the form of blocks chained using cryptography. Each block stores the hash of data in the previous block, except for the starting block, forming a chain of block, hence called genesis block. Every user on the blockchain owns a public key of the user is visible to everyone, others can use the users public key to send transactions, while private key is private to the user and should be kept secret. If a user loses access to his private key, he can no longer access his account or the funds in his account.

Every transactions on the blockchain needs to be signed by the private key of the sender, which authenticates the transactions and protects it from tampering.

But, why is blockchain becoming so popular, what issue does it resolves? Imagine a scenario where you need to transfer some amount of money from one account to another. Mostly these transactions are done through some third-party intermediaries, like bank, brokers, etc. increasing time, cost and also introducing possibility of tampering. These types of transactions are done based on the trust and agreements signed between the account holders and intermediaries. Such agreements can be broken easily by intermediaries which could result in loss of the users. Blockchain comes into play here, it facilitates faster movement of transactions cutting down these intermediaries, saving both time and money, and highly reducing the chances of tampering. Because blockchain works on a decentralized network, no single entity has a complete power over the system, the behavior of system is decided by the consensus mechanism. These nodes are responsible for maintaining the state of blockchain and validate the incoming transactions. These nodes show

their acceptance of a transaction tries by adding the corresponding block to the blockchain.

2. Transactions: Transaction is a transfer of assets between two parties, which could be cash, currency or property. The data of these transactions are stored on the blockchain permanently after the node's validation the transaction.

3. Block: A block is a data structure which stores the transactions. These blocks are chained to each other using cryptography. Each block stores the hash of data of it previous block forming a chain of blocks. Typical contents of a block are-

* **Header** contains the metadata of block, like block hash, etc.

* **Previous block address** is stored to connect the previous block with current block, ith block stores the hash of (i-1) th block's hash

* **Timestamp** is the time date of creation of bock. It is unique for each block and indicates the time when the block was created

* **Nonce (number only once)** lies at the core of PoW (Proof of Work) consensus protocol. Miners need to find a valuable nonce value before adding transaction to the blockchain.

* **Merkel Root** is a data structure that efficiently stores multiple transactions in single block using cryptography

4. Chain: Chain is a concept of connected blocks forming a blockchain. Blocks stores hash of previous block in the chain.

5. Miners: Another word for the nodes is miners, they validate the transactions through the process called mining. They validate each

step of a transaction while operating cryptocurrencies.

6. Consensus: Consensus is a mechanism or agreement that all the nodes agree upon. It is the method of selecting the node for validating a transaction. Rewarding the genuine nodes and penalizing the malicious nodes.

PROBLEM STATEMENT

The current healthcare solution for storing and sharing medical records is highly sensitive electronic medical records.

Due to the lack of reliable and trustworthy health data sharing mechanisms, the majority of EHR data sharing still occurs by mail. This results in significant delays in patient treatment and many other reasons

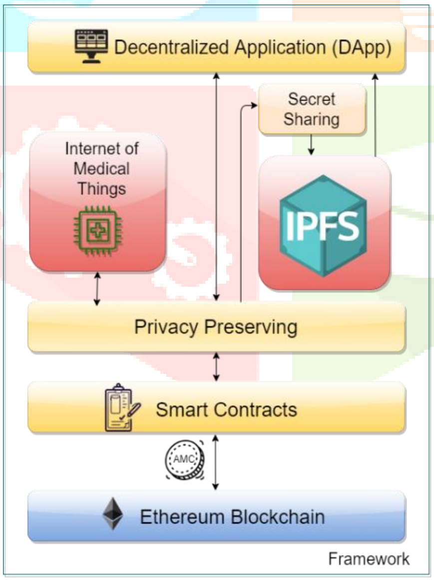
For patients, the decision to participate in a clinical trial is a complex decision, often with unknown and potential medical benefits. The advantages and disadvantages must be weighed side impact risk. The solution is for patients to own their data in order to find suitable and efficient treatments.

Different hospitals and medical facilities have different systems. Therefore, integration and interoperability issues result.

Blockchain features a decentralized system that provides cryptographic guarantees for data integrity, security, privacy, and data access smart contracts. Some EHR management literature addresses these issues by proposing a centralized framework and system for sharing his EHR across cloud infrastructures. While these frameworks provided solutions to many of the above challenges, they were plagued by limitations, especially around transparency, data ownership, and privacy.

Natural disasters present new challenges as health departments need to be prepared and able to respond quickly to crises. This is one of the arguments for how decentralized EHR management and information replication and distribution can guarantee improved performance and availability disaster situations compared to centralize models.

SYSTEM ARCHITECTURE



Ethereum – The Ethereum blockchain is often touted as the "computer of the world". This is because it is globally accessible deterministic state machine managed by a peer-to-peer network of nodes. His state changes in this state machine follow consensus rules followed by peers in the network.

Smart Contract – A smart contract is a program that runs on the Ethereum blockcha defines the logic behind state changes t occur on the blockchain.

Ethereum Virtual Machine (EVM) – The EVM is responsible for executing smart contracts and the handles state changes that occur in this globally accessible state machine.

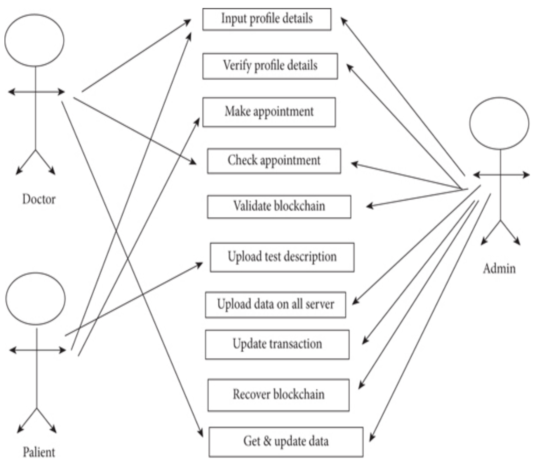
Provider – A node on the blockchain that you connect to interact with the blockchain is called a provider. Each provider implements the JSON-RPC (Remote Procedure Call) protocol. It defines various data structures and their processing rules, and uses JSON (RFC 4627) as the data format.

Signer (MetaMask) – After connecting to the blockchain, you can read the state of the blockchain. However, to write to the blockchain state, you need to perform a transaction that must be signed with the private key. This is where MetaMask comes into play. MetaMask stores the user's girlfriend's private key in the browser and calls MetaMask each time the frontend asks the user to sign a transaction.

Frontend – Defines the UI logic that the user interacts with. It also communicates 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 data over a peer-to-peer network. This makes it easy to get the data when you need it.

UML DIAGRAM



UML stands for Unified Modeling Language. UML is a common dialect institutionalized in the programming field. The aim is for UML to become the usual dialect for designing items in PC programming. UML's gift box includes two notable components of his: meta shows and documents. Depending on the procedure and type of system, it can be dealt with later. Or related to UML. Unified Modeling Language is popular dialect for displaying, visualizing, building, a archiving the weirdness programming frameworks, and is also used for

business demonstrations and various non-programming frameworks. UML descri an accumulation of first-cl build practices that help demonstrate f size and complex frameworks. UML is integral part of how gadgets are creat programmed, and developed. UML often uses graphical documentation for platform a system programming.

SYSTEM REQUIREMENTS

Database Requirements

· Fireb

· NoSQL Database

Software Requirements

· Operating System: Windows 10 (bit) or later / Linux / Mac

· Languag

o Solic

o TypeScr

o HT

o

o Sass

o JavaScript

· Angular

· Node

· Ganac

· JSON

· Git, GitH

· VS Cc

· NPM

Hardware requirements—

· RAM: Hard Disk: 1 GB or more

· Processor: 64-bit, single 2.5 GHz minim per core, core speed.

APPLICATIONS

· Better Health Records Exchange ARRA 2009 (American Recovery and Reinvestment Act of 2009) requires all qualified health professionals to adopt or demonstrate "meaningful use" of an EHR. This legislation has significantly increased adoption of the EHR. However, most systems cannot share medical data. This is one of the biggest health IT and HER interoperability challenges. Blockchain technology has the potential to address interoperability challenges by using it as a common technical standard for the secure distribution of electronic medical records.

· Enhancing Data Security and Privacy Security and data integrity issues hinder meaningful healthcare coordination and collaboration. The threat of cyberattacks and confusing interoperability standards put data at risk and limit how it can be distributed and accessed. Too often, however, the data exchanged is not trusted, perhaps because the files are corrupted or contain errors that need to be corrected manually. Blockchain technology ensures access control through shared public and private chains. Public information is open to all participants in his network, while private information is encrypted and accessible only to authorized users. Thus, a blockchain-enabled system protects his EHR and ePHI and enhances the privacy required by HIPAA.

· Ensure Accuracy of Claims Management The independent structure of the blockchain provides a highly consistent tracking option and enables immediate updating of data. Any attempt to modify data must be reconfirmed by every block in the system. Once approved, new data becomes a permanent part of the database and cannot be changed or deleted. Blockchain can also reduce economic losses and inherently thwart fraud and illegal data movement.

· Strengthening the medical supply chain According to a 2017 WHO study, 10% of medical goods entering developing countries are cheaoor counterfeit At least 1% of all drugs on the market are believed to be illicit. A blockchain-based system can ensure a chain of custody record that tracks every level of the pharmaceutical supply chain. In addition, add-on features (e.g. private keys, smart contracts) enhance trust for pharmaceutical suppliers at every delivery step and better adhere to contracts between various parties.

· Enhancing a culture of trust in medical research Blockchain technology can address the problem of result shifting and data sniffing. The System enables the transmission of time-stamped, permanent records of clinical trials and study results, reducing the incidence of clinical trial record fraud and errors.

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. WoodburySmith, ''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. 4852, 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. G 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.

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