A Blockchain based Electronic Medical Health Records Framework using Smart Contracts

Vardhini B
Department of ISE
CMR Institute of Technology
Visvesvaraya Technological University
Bengaluru , Karnataka, India
vardhinib2008@gmail.com

Shreyas N Dass
Department of ISE
CMR Institute of Technology
Visvesvaraya Technological University
Bengaluru, Karnataka, India
shreyas0820@gmail.com

Sahana R
Department of ISE
CMR Institute of Technology
Visvesvaraya Technological University
Bengaluru, Karnataka, India
bokehlenz@gmail.com

Dr.R.Chinnaiyan
Associate Professor
Dept.of Information Science and Engg.,
CMR Institute of Technology
Bengaluru – 560 037 , Karnataka, India
chinnaiyan.r@cmrit.ac.in

2021 International Conference on Computer Communication and Informatics (ICCCI) | 978-1-7281-5875-4/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICCCI50826.2021.9402689

***Abstract*— The common issues in medical services within the country are mostly associated with doctors' referral process, data transfer between health institutions, and portals for patients to access their medical information. Specific issues arise, such as sharing health Records across institutes or hospitals, problems with misuse of data once shared, no security, etc. The Electronic Health Record (EHR) Framework on Blockchain addresses those issues, resulting from a collaboration of all stakeholders involved. This paper explores the likelihood of representing medical records to make sure data privacy, data accessibility, and data interoperability for the healthcare-specific scenario. Data privacy refers to affording protection to ensure data is available when needed and not used, imparted, accessed, altered, or deleted while being stored or retrieved, or transmitted. Data accessibility is the ability to access the data regardless of natural or artificial accidents, hardware, or others. Improving the accessibility of health data in the healthcare sector while ensuring privacy has been identified as a necessary capability that involves every individual and organization. Traditionally, healthcare interoperability has centered on sharing data between business institutions, such as various hospital systems. The emphasis has lately been on patient-driven information sharing, where the exchange of medical information is patient-mediated and patient-driven. We propose implementing a large-scale information infrastructure to access Smart Contracts sponsored by EHRs as information mediators. The decentralized nature of blockchain technology will aid in making the EHR accessible over a broader network. Using Blockchain will help make far-reaching changes in the healthcare industry by providing immutable, authentic, and accessible medical records, privacy, and faster payments.**

Keywords*— *medical information sharing, Blockchain-based EHR, Consent based Health data sharing, Healthcare Record Management.

I. INTRODUCTION

Blockchain is a decentralized, distributed, and transparent digital ledger used for recording transactions through several machines, such that no precise record will be retroactively changed without modifying all subsequent blocks. The concept of the Blockchain was released as a white paper by Satoshi Nakamoto in the year 2008. Protected Health Information of every patient is the most critical asset of any health care system. Blockchain technology offers an impressive and creative way to maintain references to the dispersed patient data. An Electronic Health Record (EHR) is a comprehensive system collection of patient personal information and health records that are stored electronically in a digital format. EHRs are patient-driven authentic documents that deliver the information available to authorized stakeholders immediately in a secured manner. An EHR includes patients' personal and medical histories. The EHR framework aims to exceed standard clinical data collection to be more inclusive of a broader viewpoint on patient outcomes. Imagine that every EHR submitted updates to an open-source, community-wide trustworthy ledger about medications, issues, and allergy lists, so changes to the medical records are well understood and auditable across organizations. Instead of just displaying data from a particular database, the EHR could show data from any database referenced in the ledger. The outcome would be perfectly balanced community-wide information, with assured credibility from the point of data generation to the time of requirement, without manual human interference.

Key Features Of EHR

- Automate and streamline provider workflow
- Data can be devised and maintained by approved suppliers.
- Maintained in a sharable digital format across multiple organizations.
- Exchange data with parties such as laboratories, consultants, medical imaging centers, pharmacies, emergency departments, and clinics at school and in the workplace.
- Improves quality of care.
- Improves Diagnostics and Patient Outcomes

Reasons For Adopting Blockchain

Blockchain is extremely secure and thus allows the EHR to be secured. It extends the ability to deploy a network of stakeholders who has access in a layered approach. This way, it will enable the patient to control their medical records and authenticate whatever doctor they deem necessary. The patients will also control how little is to be shared using the Blockchain's secure network.

978-1-7281-5875-4/21/$31.00 ©2021 IEEE

This approach differs from the traditional system by making the patient the owner of the records and addressing ease of accessibility and authority by merely using the Blockchain's inherent features. This paper will determine the design, structure, stakeholders in the system, their functionality, and its significant features.

II. DESIGN

A. *Blockchain Structure*

- Block: Every block in the Blockchain contains some data and a hash (AKA digital fingerprint) generated from the data contained within the block using cryptography. The contents of a block are unchangeable.
- Chain: A hash connects one block to another, chaining them together mathematically. It's the concept that ties blockchains together and helps them gain cryptographic trust. The Blockchain hash is generated from the information present in the previous block. The hash is a fingerprint of data and locking blocks in order and time.
- Network: The network consists of "full nodes." Nodes are analogous to the machines running an algorithm that secures the network. Each node includes all of the transactions that are recorded in that Blockchain is a complete collection.

B. *Blockchain Terminologies*

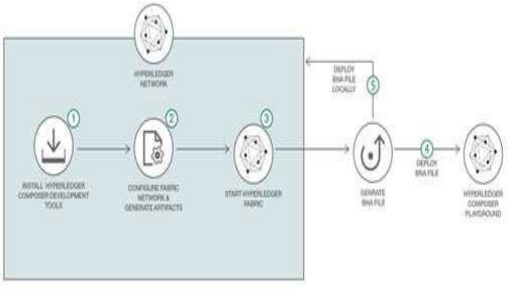
- Cryptography: Cryptography is the way of disguising and exposing information through advanced mathematics, better known as encrypting and decrypting data. Only the intended recipients can only view the data and nobody else.
- Nodes: Nodes form the blockchain infrastructure. They store, distribute, and collect blockchain data, therefore, a blockchain exists on nodes.
- Proof of Work (POW): Proof of work is a protocol with the primary purpose of deterring cyber-attacks such as distributed denial-of-service attack (DDoS), which is meant to drain a computer system's resources by submitting multiple false requests.
- Smart Contracts: A electronic agreement held on the unalterable Blockchain, once authorized, is a smart contract. It describes logical operations that must be done in order to execute tasks such as money or data depositing.
- Distributed Ledger: A distributed ledger is shared by consensus and synchronized across multiple sites, institutions, or geographies across a network.
- Crypto-Tokens: Crypto tokens are a particular form of virtual currency tokens that exist on their blockchains and represent a commodity or usefulness.
- Peer to Peer Network: A Peer to Peer Network is built on top of the Blockchain to distribute information about the state of the network.
- Hash Function: A function that is used to map arbitrary size information to fixed-size data.

C. *Hyperledger Fabric*

Hyperledger Fabric, a blockchain system, is an open-source project hosted by the Linux Foundation. It hosts a smart contract called chain code in a containerized technology that integrates the application logic. Hyperledger Fabric is a permissioned Distributed Ledger Technology platform.

Permissioned Blockchain is carried out by a set of established participants with a certain amount of trust. In DLT, every entity participating in the exchange of value owns a copy of the record referred to as Distributed Ledger.

- Permissioned network - All members have known identities. Need approvals to guarantee accountability for membership. Provides authentication, access protection, confirmation of the transaction.
- Confidential transactions - Participants can track the visibility of transactions.
- No cryptocurrency - It does not require mining and expensive computing to ensure transactions.
- Establishes trust, transparency, and accountability between participants



HYPERLEDGER FABRIC FOR BLOCKCHAIN

III. DIFFERENCE BETWEEN EXISTING SYSTEM AND PROPOSED SYSTEM

A. *Existing System*

India, a country with residents of over 1.3 billion with geographical, socioeconomic, linguistic, religious, and ethnic diversities, certainly requires healthcare infrastructure where each citizen's health data can be processed securely and efficiently accessed.

"Ayushman Bharat Yojana," an initiative taken by the Government of India to offer the National Health Protection Scheme (NHPS), demonstrates its commitment to achieving UHC by 2030. Google's DeepMind Health is to develop a blockchain-like technology capable of securely tracking NHS patient data. DeepMind's Blockchain will also allow the NHS or its hospitals to verify their datasets – unlike traditional Blockchain, which relies on decentralized verification from a group of participants. According to DeepMind, both differences will make the system more efficient. To facilitate patient information exchange between hospitals, pharmacies, and insurers, the medical chain uses dual Blockchain and technological advancement. At present, medical records are extremely centralized and challenging to circulate. Obtaining critical data about a patient's health in front of a doctor shouldn't be as difficult as it is now. The medical chain would allow insurers, physicians, and patients to access medical records with Blockchain's ease, speed, and security.

B. Proposed System

The main problem of the current health care is that the organizations hold multiple and fragmented medical records of patients.

The Proposed System aims to solve the health care sector's current problems by hosting medical record transactions on the Blockchain to create a smart ecosystem. The goal is to provide secure access to patient data, avoiding the third party accessing it without permission.

EHR Framework uses blockchain technology to securely store the records and maintain a single version of the truth. The stakeholders will have to request permission to access a patient's history and commit the transaction to the distributed ledger.

A solution centered on the blockchain, can permit large-scale availability, data confidentiality, cost-effectiveness, and belief in the information system.

Stakeholders

- Patients
- Doctors
- Hospitals
- Clinicals Researchers
- Laboratories
- Pharmacies and Drug Control Departments
- Insurers

Implementation

- Develop a technology plan for the healthcare blockchain
- Develop a Proof of Concept (POC)
- Deploy the Smart contract (Model File, Acl File, Logic and Query File) to generate network Architecture
- Launch a full volume rollout which is connected to a fully functioning front end

Functionality

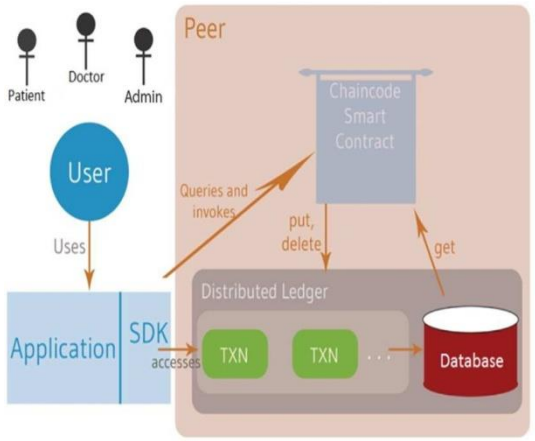
- Healthcare providers will collect medical data from the patient.
- The data is then stored in existing hospital databases.
- A hash is generated from each data source and is forwarded to the Blockchain.
- The patient gets to decide who gets access to their confidential data.
- The required stakeholders can query the Blockchain to gain access to the medical details.

Features

Using Blockchain as the underlying technology to back the EHR provides the following features:

- All stakeholders involved with the patients will have time-limited access to the EHR. The EHR is shared in the form of a Smart Contract.
- The information is always kept private and secure.
- A zero-knowledge protocol is a means by which one party (the prover) confirms to the other party (the verifier) without revealing any information apart from the fact that this specific statement is true. The use of zero-knowledge proof increases privacy.
- Blockchain being universal will ensure that the EHR framework will be compatible across multiple health applications.
- The patient can interact conveniently with different stakeholders while maintaining privacy following the zero-knowledge proof mechanism.
- It ensures the patient owns the EHR, and hence consent and approvals are processed faster.
- Blockchain allows the chain of custody to be transparent in the network.
- Avoid medical errors and improve quality outcomes. This is ensured by involving the Central Drugs Standard Control Organization in the network, which can automatically and speedily notify the Pharmacies and Doctors regarding banned drugs or new drugs.

Architecture



SYSTEM ARCHITECTURE

IV. CONCLUSION

Adopting the Blockchain to deploy the EHR solves the significant issues of accessibility and authority. The Blockchain allows ease of access to the records as it is available to any personnel authorized to access them. Since it is deployed on a Distributed network, it can be accessed from anywhere. However, there are a few issues that could still be addressed in the future. Since it is possible to distinguish the people engaged in the transactions, this could endanger their confidentiality and secrecy. Although certain blockchains offer absolute anonymity, but some sensitive details should clearly not be distributed in this way. The system can be improved by allowing the medical records to be accessed quickly during emergencies. Its structure could be modified to fit a specific disease or modeled on established standards.

REFERENCES

[1] Blockchain Consensus Mechanisms. The buzz around https://medium.com/datadriveninvestor/blockchain-consensus-mechanisms-7aa0176d488a

[2] Clinical EHR (Electonic Health Records) Market https://www.envisioninteligence.com/industry-report/clinical-ehr-electronic-health-records-market/

[3] Electronic Medical Records: Holy Grail for Blockchain https://www.medpagetoday.com/practicemanagement/informationtechnology/74695

[4] G. Sabarmathi and R. Chinnaiyan, "Big Data Analytics Framework for Opinion Mining of Patient Health Care Experience," *2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC)*, Erode, India, 2020, pp. 352-357

[5] G. Sabarmathi and R. Chinnaiyan, "Investigations on big data features research challenges and applications," *2017 International Conference on Intelligent Computing and Control Systems (ICICCS)*, Madurai, 2017, pp. 782-786

[6] G. Sabarmathi and R. Chinnaiyan, "Reliable Machine Learning Approach to Predict Patient Satisfaction for Optimal Decision Making and Quality Health Care," *2019 International Conference on Communication and Electronics Systems (ICCES)*, Coimbatore, India, 2019, pp. 1489-1493

[7] Hohenberger, S., and Waters, B.: Online/offline attribute-based encryption. In: Public-Key Cryptography - PKC 2014 - 17th International Conference on Practice and Theory in Public-Key Cryptography, Buenos Aires, Argentina, March 26-28, 2014. Proceedings, pp. 293–310, 2014

[8] Huang, H., Chen, X., Qianhong, W., Huang, X., and Shen, J., Bitcoin-based fair payments for outsourcing fog devices' computations. Fut. Gen. Comp. Syst. 78:850–858, 2018.

[9] Krist, A.H., Peele, E., Woolf, S.H., Rothemich, S.F., Loomis, J.F., Longo, D.R., and Kuzel, A.J., Designing a patient-centered personal health record to promote preventive care. BMC Med Inf. .Decis. Making 11: 73, 2011.

[10] R.Chinnaiyan and S.Balachandar BDET 2020: Proceedings of the 2020 2nd International Conference on Big Data Engineering and Technology, January 2020 Pages 106–111

[11] Sabarmathi G., Chinnaiyan R. (2020) Envisagation and Analysis of Mosquito Borne Fevers: A Health Monitoring System by Envisagative Computing Using Big Data Analytics. In: Pandian A., Senjyu T., Islam S., Wang H. (eds) Proceeding of the International Conference on Computer Networks, Big Data and IoT (ICCBI - 2018). ICCBI 2018. Lecture Notes on Data Engineering and Communications Technologies, vol 31. Springer, Cham.