Proceedings of the International Conference on Electronics and Sustainable Communication Systems (ICESC 2020)
IEEE Xplore Part Number: CFP20V66-ART; ISBN: 978-1-7281-4108-4

Blockchain: The Novel Way to Secure Confidence!

Jairaj Khushalani
Computer Department
VESIT
Mumbai, India
2016.jairaj.khushalani@ves.ac.in

Sachin Chandwani
Computer Department
VESIT
Mumbai, India
2016.sachin.chandwani@ves.ac.in

Abdus Samad Shaikh
Computer Department
VESIT
Mumbai, India
2016.abdus.shaikh@ves.ac.in

Bhavesha Talreja
Computer Department
VESIT
Mumbai, India
2016.bhavesha.talreja@ves.ac.in

Mrs Rupali Hande
Assistant Professor
Computer Department
VESIT
rupali.hande@ves.ac.in

Abstract— This report intends to play out a precise audit to survey and establish the practicality of blockchain for implementing healthcare service records effectively. Traditional health records are both localized and expensive to operate; they can be improved upon by using blockchain based electronic health records (EHRs). EHRs are just electronic versions of a patient's whole clinical history. EHRs, when stored on blockchain, has some serious advantages when compared to their traditional centrally stored counterparts. The patient's medical records will be stored on a distributed network. An ethereum based decentralized application (DApp) can be incorporated to record and update medical information securely in real time using smart contracts. A decentralized application on a private blockchain network will ensure the integrity of data records and improve interoperability of the system by providing permanent access to essential details like patient's medical track record, prescription history, laboratory/ clinical reports etc. The application uses the efficiency and security of blockchain technology to solve the challenges faced by the healthcare domain.

Keywords—Decentralized Application (DApp), Smart contract, Blockchain, Electronic health records (EHR)

II. INTRODUCTION

In the prevailing healthcare system, if a patient visits multiple organizations for treatment his data is scattered across various independent institutions. It is the provider and not the patient who generally retains the ownership of data [13]. Furthermore, the data present with the patient is mostly on paper and involves a lot of difficulties in maintenance and record keeping. In electronic health records the information exchange is usually restricted to the same organization unless they make use of a designated intermediary for information exchange. An intermediary may vary from a single centralized system or even a private network established between local hospitals to help facilitate information exchange [3]. Even in the case of electronic data, it is the provider who retains access to data. Interoperability challenges between different provider and clinic systems pose extra barriers to effective statistics sharing. Even with data sharing capabilities the issue of compatibility between varied systems also poses a serious problem for all the stakeholders. The absence of coordinated data and transfer means health records are scattered, rather than being cohesive[4], [5]. Health providers are required to maintain the privacy of healthcare data as it is considered to be highly sensitive. However the patient has no access to any mechanism to ensure privacy of their data. The proposed system eliminates the need for using paper records as well as the disintegrated centralized systems [1], [2], [8]. As previously established, using the fundamental qualities of a decentralized system, a network can be created in which each node will accommodate the record. Nodes constitute the basic building blocks of blockchain. A node is essentially a computer which forms a network when connected to other nodes. Blockchain provides a user friendly mechanism using which the data is just a click away from the patient. Blockchain technology is here to disrupt the widely used client server model in sectors such as healthcare by making the entire process decentralized. Blockchain in simple terms is a system of complex code for building trust without any middleman. The transaction data is stored over the block and this data

is highly patient centric. Each block consists of some transactional data as well as the hash value. No single node on the network has full control of the network [6]. It goes to prove that not to involve third parties for the well being of our healthcare data. A blockchain based distributed computing platform called Ethereum can be utilized to solve the problems of privacy and interoperability in healthcare. Ethereum is an open source, public operating system featuring smart contract functionality. Ethereum uses a consensus mechanism called Proof of Work (PoW) which guarantees that a new block can be appended to the chain only if all the nodes present in the network agree upon the hash value provided in the new block. This mechanism provides additional security to blockchain. As the network grows the probability that an organization or a user is able to control the network reduces significantly. Taking advantage of multiple users in the healthcare domain this property works in its favor. All the blocks are immutable once they have been created and agreed upon, to change you cannot delete or change anything without leaving a trace. That is critical in case of healthcare data. It could secure health records, making them highly resistant to illegal alterations.

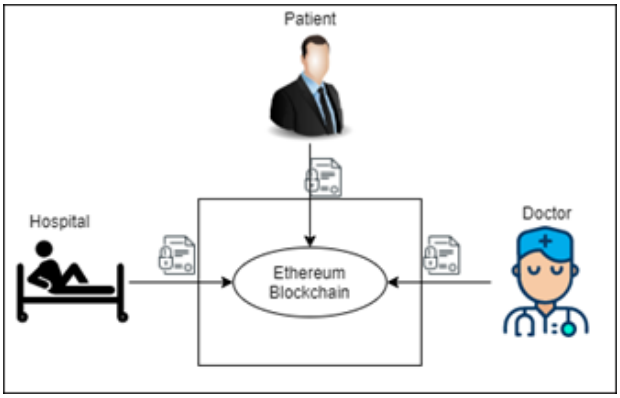

Fig 1- Interaction between stakeholders and the network

III. RELATED WORK

This paper not just considers access control over data uploading and sharing, yet in addition gives a successful data management technique using a decentralized storage system combining Interplanetary File System (IPFS). Various studies have investigated the ability of blockchain to support healthcare data sharing. Blockchain was exploited in [1] to ensure reliable EHRs accessibility for medical users. The authors have excessively relied on theoretical analysis and therefore, the feasibility of the proposed solution was not verified. Rather than hypothetical examination as current investigations, in this work, executing information sharing capacities are centered around. The proposed system allows the addition of arbitrary logic to process, validate, and access the data. This is implemented using logic known as smart contracts, which reside on the blockchain and are synchronized across all nodes. A smart contract is just like the contracts in the real world, but they are written into lines of code and stored within a blockchain. They consist of a string of computer code that executes whenever certain conditions are met and cannot be altered once they are deployed over the network [9]. Moreover, with its inherent distributed nature it becomes impossible for an attacker to force a contract to perform a certain outcome because others on the network will recognize this attempt and mark it as invalid. In the existing approaches, patients have little control over their personal data [5]. Some healthcare practitioners may try to use health data of patients for their illegal purposes, leading to leakage of the sensitive patient information. The ability to create smart contracts makes blockchain suitable for health care, where strict regulations administer how sensitive data can be used [8], [15]. Data sharing occurs on the basis of pre-agreed conditions of the contract therefore smart contracts are immutable. Blockchain uses public key cryptography to create an add-only, immutable and time stamped chain of content [12]. To overcome the problems of information sharing there is a need of storing data using a mechanism where patients are sure about their data security and privacy and simultaneously allowing all the involved stakeholders to be able to see the integrated view of the overall transaction [7]. The system promotes data driven decision making to personalize the experience for every patient and improve the outcome all the way from diagnosis to treatment.

IV. TECHNICAL DESCRIPTIONS

A. Blockchain Technology

Blockchain is a growing chain of records, called blocks which are linked to each other using cryptography. Each block contains a cryptographic hashcode of the previous block, a timestamp, and transaction data. It is designed to be resistant to modification of the data. A blockchain network is like a giant shared database that anyone can interact with using the power of the web. Data discrepancy is averted in the data because all of the participating nodes must agree with each other that they have the same information. In the case of healthcare, blockchain works perfectly as it will keep track of the records and other details like the information appended on the network and its owner. A consensus must be reached between all the participating nodes without which no transaction can take place.

B. Ethereum Decentralized Application (DApp)

Ethereum is a public blockchain platform and the most advanced for coding and processing smart contracts. It boasts of an open-source ecosystem that supports Turing complete operations. To carry out any transaction on the system such as adding information etc and for using computing power "ETH" tokens need to be used. These apps require cryptographic tokens to conduct various transactions and run on decentralized blockchains. A Decentralized App can have frontend code and user interfaces written in any language (just like an app) that can make calls to its backend. However, since Ethereum contracts are code that runs on the Ethereum decentralized peer-to-peer network, then a decentralized app consists broadly of frontend and contract i.e. Decentralized App = frontend + contracts + test RPC(Remote Procedure Call) dummy network. Decentralized applications help to link hospital systems across a shared network. Most importantly, they can mobilize patients to collect, own and manage their own data and be self-reliant.

C. Smart Contracts

A smart contract is a computer protocol intended to digitally facilitate, verify, or implement the negotiation or performance of a contract. A Smart contract is at the heart of every blockchain transaction. It allows the execution of credible transactions and restricts illegitimate transactions. Its unique offering includes the ability to enforce transactions without involving the services of a middleman. A smart contract is typically written as code in languages such as Solidity and committed to the blockchain. The code and conditions of the contract may be available publicly however it cannot be altered once it is deployed on the system. Personal medical records could be encoded and stored on the blockchain with the assistance of a private key which would grant access only to specific individuals and hence regulators will be able to receive important information while still maintaining the privacy of individuals.

V. PROBLEM STATEMENT

Establishment of each clinical account and putting away the printed version is a troublesome activity. Keeping that record unblemished is a challenge in itself. To help us perform this seemingly impossible task there are electronic frameworks that are additionally accessible yet they stay constrained to a solitary clinic/hospital and are therefore not sustainable. There ought to be where the patients can keep their records and it has an entire history of records. This is where blockchain steps in and our proposed system mean to wipe out the need of the paper records or concentrated records and give a decentralized system in which both the provider and receiver can connect seamlessly. A direct relationship is established between a patient and a specialist. With the assistance of blockchain the patient will initially enroll himself and join the chain, subsequent to which he can choose the specialist of his choice from the pool of specialists available for an appointment. In the event that the specialist is chosen he gains access to medical history and the treatment and record will likewise be put away on the Decentralized App itself. Furthermore, that record is immutable and consequently no odds of fraud.

Objectives

- Creating a patient-centric decentralized system
- Promote viable and easy access to all medical records.

Features

- Provides access to doctors only when granted by a patient.
- Medical records are immutable hence no chance of any fraud in case of insurance claims etc.
- Ease of access; no need to carry piles of reports, everything is stored in the patient's block.

VI. SYSTEM ELEMENTS

Contracts can be used to document ownership metadata, permissions and all other forms of user data. Any exchange of information that takes place, will be signed cryptographically. This will assist the system to perform the necessary data transfer operations between the various stakeholders of the system. State-transition functions of the contract carry out policies as specified in the smart contract thereby allowing only legitimate transactions to modify data. These regulations can be structured to enforce any set of rules regulating a specific medical record as long as it can be computationally represented. The entire medical history can be stored using distributed file storage and sharing protocol. Complex healthcare workflows can be designed using blockchain compared to traditional healthcare systems [14]. At every stage of the transaction, the application generates tokens in accordance with a standardized cryptographic algorithm that acts as proof of the value that the nodes will be contributing to the application. Data on the blockchain is altered in real time ensuring that the data available is of utmost relevance. A patient goes to select his doctor, choosing from the list of available doctors already present. who will integrate related medical data as the EHR. Upon appending the EHR, they are indexed to the consortium blockchain. The doctor can be able to see his patient's entire treatment history. A patient may authorize any number of healthcare professionals with the list of authorized data users. A doctor uses a pair of keys (PK, SK) to generate

the content extraction signature on EMRs for authentication.

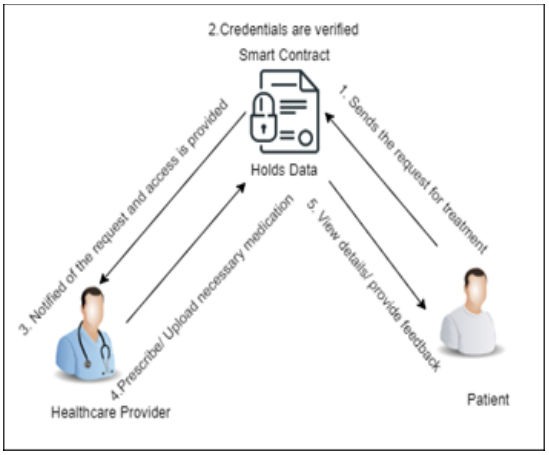

Fig 2- Application Functionality

Figure 2 describes the steps in which data sharing takes place between the stakeholders of the system.

VII. PERFORMANCE METRICS

Sr no	**Performance metrics**
A	Secured data transmission
B	Accessibility
C	Data provenance

A) Secured data transmission

It provides a ubiquitous and secured mechanism for data storage and transfer. It provides secure data transmission mechanisms as well as protects sensitive data. It uses Interplanetary File Systems (IPFS) as a secure data transmission platform. Meanwhile, for EHRs sharing, users are not given the authority to modify the signed transactions to smart contracts. No entity can tamper and change the content of recorded transactions.

B) Accessibility

It allows for verifiable identity and authentication of all the participants. Access control decisions are decided by the terms in the smart contract. If the third parties/unknown entities want to health information of the patient, the smart contract will deny the request. Importantly, users can't have rights to change or modify the agreement in the smart contract and access policies in our scenario.

C) Data Provenance

The very distributed fabric of medical records acts as an obstacle during verification. All the transactions are time stamped and the source of the medical records can be verified. All records are signed by source and their legitimacy can be authenticated as well as false records can be plausibly ruled out.

VIII. SYSTEM IMPLEMENTATION

A. Overview

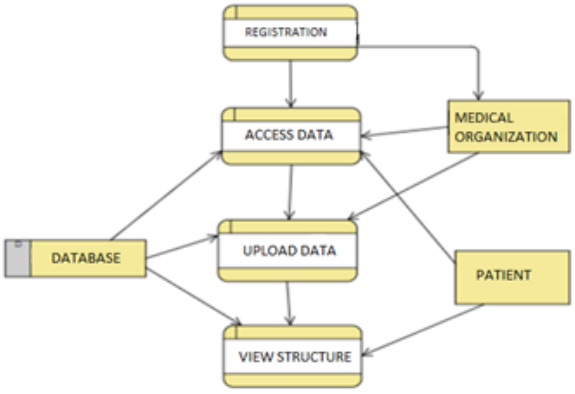

Fig 3- Dataflow Diagram

The frontend of the application is responsible for whatever seen on the webpage and the backend will support the business logic via smart contracts. When the patient registers for the first time they will have to furnish basic details like his health and medical history. The patient will have to first request by selecting one or more doctors from the list of doctors available on the network. When the patient requests an account a block is created and the block is added to the chain of nodes. The assigned node will validate the credentials of the user and if this process is completed successfully then it is broadcasted over the entire network. This particular instance represents the consensus in the patient block. If the consensus is achieved only then the new patient block will be appended. The most remarkable advantage of blockchain is the fact that it expels the requirement for

a centralized trusted third party in distributed applications. A central authority would otherwise introduce a transaction cost. Therefore by the elimination of central authority transaction costs are lowered. In place of a central authority, blockchain uses an accord mechanism to accommodate inconsistencies between nodes in a distributed application.

B. Methodology

The proposed work will considerably cut back the turnaround for EHR sharing, improving decision time for treatment. This provides a novel chance to design and implement a secure, trustable EHR information management and sharing system. There are many benefits to the healthcare sector for managing heterogeneous data and the workflow of the proposed system follows a highly patient centric design. Ethereum which is a decentralized blockchain public network can be used to run our private blockchain by employing Ganache. It can be used to run tests, execute commands etc. MetaMask is a cryptography wallet that allows users to interact with the Ethereum network with the help of a browser. It enables users to sign smart contracts, buy and send ether (ETH) tokens. These tokens are essential for any transaction and an account that wants to request for a transaction spends some gas in a contract execution. The structure of a network can be decoupled into the presentation layer which consists of the web, mobile or desktop interface say a web3.js or web3.py framework. The middle layer or the data sharing layer provides a connection to the Ethereum blockchain run by smart contracts and is responsible for maintaining privacy. These smart contracts are often written in solidity programming language. In this layer, the authorized patients, medical workers and healthcare institutions can request patient's EMRs and utilize them for making personal health plans, improving clinical treatment or carrying out medical research. Patients are the owners of EMRs and have complete control of them. In order to avoid privacy information being leaked in the process of data sharing, patients can remove sensitive information of EMRs and generate valid extraction signatures. To initiate the process the patient will send a request to do a transaction. The request will be sent to the proposed model and it will check the patient's identity using the cryptographic credentials. After the request and patient are verified, the system will process the request; this request could be receiving the medical data from the network. When the verified request is granted, a new block is added to the existing chain that contains the data of this transaction and the new state of data. The patient is provided with what he/ she asked for and the transaction completes. The patient's encrypted EMRs and the extraction signature, meanwhile, outputs the storage location and a timestamp. The patient predefined access permissions in the smart contracts to assure the data sharing securely. likewise, each access request and access activity should be recorded in the blockchain network for future auditing or investigation. Heterogeneous (imbalanced) data is defined as the objects depicted by various features of different forms and architectures. Medical data may have different data types, say for example patient id, age, body temperature, blood pressure, blood sugar level etc. will be stored in float. Whereas details like gender, disease, will be written in textual format, symptoms like pain intensity will be in the ordinal form. Moreover details like X-Ray, Ultrasound, MRI reports will be stored in the form of images along with documents like medical laboratory reports etc. Using all these types of stored data relevant information can be derived combining these data types to extract meaningful insights from the data. Storing patient information in the form of a health record, directly on the block-chain confirms that the data is stored through a highly secured transaction. The blockchain technology doesn't store the different data types directly to the blockchain, such as X-rays or ECG signal data. These are rather stored off-chain. To store data off-chain, the heterogeneous data would require pointers to a new address location. When a user patient or a healthcare specialist creates a patient medical record or prescription an e-Stamp would be generated to verify the user's authenticity of prescription. The heterogeneous data would be converted through encryption techniques and sent to the cloud storage. The shared information made available by blockchain technology would distribute a broad dataset by patients and users from various racial, socio-economic platforms and geographical areas. Blockchain would guarantee constant accessibility to real-time data. Real time accessibility to patient data would improve clinical care patient care in emergency cases.

IX. CONCLUSION

The safety of our data even if it's in the digital form is our right and need to assume control. The proposed system demonstrates how people who deal with value sensitive commodities such as healthcare records will benefit from principles of decentralization. The system can improve trust and materialize interoperability while promoting the security and privacy of information. It provides patients with comprehensive record review abilities especially during times of crisis. It also helps with care auditability and data sharing. It ensures continuity of healthcare services even across organizational borders with the power of data sharing vested in the hands of the beneficiary and not the provider. Blockchain technology in healthcare can serve as an effective method of providing fault tolerance by eliminating a single point of contact for data storage. Its

utility can be beneficial during relief efforts in case of a natural calamity or during an epidemic outbreak. It can also be utilized to ease the process of insurance claims, ensuring authenticity. This technology is still in its infancy in the healthcare domain as it still has a lot of potential areas that haven't been explored. Blockchain technology has seen unprecedented applications in the financial sector and has the ability to revolutionize the healthcare sector.

REFERENCES

[1] Zyskind, Guy, and Oz Nathan. "Decentralizing privacy: Using blockchain to protect personal data." In Security and Privacy Workshops (SPW), (2015) IEEE, pp. 180-184.

[2]Wood, Gavin. "Ethereum: A secure decentralized generalised transaction ledger." Ethereum Project Yellow Paper (2014)

[3]A Case Study for Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data by Ariel Ekblaw*, Asaph Azaria*, John D. Halamka, MD†, Andrew Lippman*

[4] Katuwal, Gajendra & Pandey, Sandip & Hennessey, Mark & Lamichhane, Bishal. (2018). Applications of Blockchain in Healthcare: Current Landscape & Challenges

[5]Ball, M.J. 2003, 'Hospital information systems: perspectives on problems and prospects, 1979 and 2002', International Journal of Medical Informatics, Vol. 69, Iss. 2-3, pp. 83-89.

[6]Wu, Kaidong et al. "A First Look at Blockchain-based Decentralized Applications." ArXiv abs/ 1909.00939(2019): n. pag.

[7] Cheng, Raymond & Zhang, Fan & Kos, Jernej & He, Warren & Hynes, Nicholas & Johnson, Noah & Juels, Ari & Miller, Andrew & Song, Dawn. (2018). Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contract Execution.

[8]https://medium.com/swlh/how-blockchain-technology-can-transform-the-healthcare-sector-604d1bcdc

[9] L. W. Cong and Z. He, "Blockchain disruption and smart contracts," The Review of Financial Studies.

[10]https://www.ibm.com/blogs/blockchain/category/blockchain-in-healthcare

[11]Carter, G., White, D., Nalla, A., Shahriar, H., & Sneha, S. (2019). Toward Application of Blockchain for Improved Health Records Management and Patient Care.

[12]https://hbr.org/2017/03/the-potential-for-blockchain-to-transform-electronic-health-records

[13] P. Zhang, J. White, D.C. Schmidt, G. Lenz, S.T. Rosenbloom FHIRChain: applying blockchain to securely and scalably share clinical data Comput. Struct. Biotechnol. J., 16 (2018), pp. 267-278

[14] Zhang, P., Walker, M. A., White, J., Schmidt, D. C., & Lenz, G. (2017). Metrics for assessing blockchain-based healthcare decentralized apps. 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom). doi:10.1109/healthcom.2017.8210842

[15] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," IEEE Access, vol. 6, pp. 11 676–11 686, 2018.