Smart Electronic Healthcare Record System based on Blockchain technology

Venkat R
Computer Science Engineering
SRMIST, Vadapalani
Chennai, India

Shruti Srinivasan
Computer Science Engineering
SRMIST, Vadapalani
Chennai, India,

S Varsha
Computer Science Engineering
SRMIST, Vadapalani
Chennai, India,

Mrs. Deepa R
Assistant Professor, CSE
SRMIST, Vadapalani
Chennai, India

Abstract-Modern healthcare systems are extremely complex and costly. This can also be minimized by better monitoring of health records, using Blockchain technology. Blockchain was first implemented to provide distributed records of money-related transactions which were not reliant on centralized authorities or financial institutions and seems to pave the way for revolution in the conventional healthcare industry benefitting by its unique features such as data privacy and transparency. This system proposes an Electronic Health Record (EHR) model using Blockchain technology. The implementation of this model is done using Ethereum Dapp. Ethereum is an open-source, public, blockchain-based platform and operating system featuring smart contract functionality. A Dapp is an autonomously operated open-source application that is not managed by any central authority.

Instead it is decentralized over the web built on the top of blockchain technologies. The data of a Dapp is stored cryptographically in a public and also decentralised blockchain to avoid any single point of failure. The proposed model uses different development environments to build a highly effective EHR which is not controlled by a single point of authority and uses a decentralized system for storage.

Keywords—blockchain, ethereum, EHR, healthcare, off-chain storage

I.INTRODUCTION

As discussed earlier, there are various benefits of using Blockchain technology to create an application that stores Electronic Health records. A modern, secure solution is introduced that maintains EMRs in the healthcare departments using blockchain technology. The systems proposed earlier show blockchain implemented EHR that provides access to the data owner and the data requester to read, write, add and revoke records. The given systems do not really concentrate on an efficient storage, storing the data in the main blockchain network. Therefore, a system with an off chain storage can be introduced where the actual data is stored offline and the hash of the data is stored in the blockchain. This way, this distributed storage proposed ensures safety against manipulation and confidentiality of the data.

A. INTEROPERABILITY

It's the way information is shared between various information systems. The information should be exchangeable and should be available for additional purposes. An significant feature of EHR programs is their Health Information Exchange (HIE), or the general feature of data sharing. With a range of EHR systems built in various hospitals they have a varying level of terminologies, technical and functional capabilities which makes it to have no universally detained standard [6]. In addition, the medical reports to be shared would be interpretable at the technical level, and that interpreted piece of information could be further used[6].

B. INFORMATION ASYMMETRY

The biggest issue defined by critics in the healthcare sector today is information asymmetry which refers to one party having better access to information than the other. In the case of EHR systems or in the general healthcare sector this issue is suffering because doctors or hospitals have access to the records of the patient and therefore make it importantIf a patient wishes to access his medical history, a lengthy and boring procedure will have to be followed in order to access them. The knowledge is centralized to a single healthcare agency and only the hospitals or associations are granted oversight over it.

C. DATA BREACHES

Data breaches also call for a stronger forum in the healthcare sector. A study[7] was performed to analyze data breaches in EHR systems and it found that since October 2009 173 million data entries in these systems have been compromised. The research carried out by Argaw et al shows that hospitals have become a focus of cyber-attacks, and there has been an growing increase witnessed by the researchers while conducting this study that a lot of research work has been done in this domain. In addition, many EHR systems are not designed to meet patients 'needs and requirements and resolve issues and inadequate implementation of these systems. The literature also indicates that the use of EHRs has had adverse implications for the production of information. These issues make it rational to nd a platform to be patient-centered, i.e., blockchain, that would be helpful in transforming health care sector. A portal that is safe, open and gives patients 'medical records data integrity as well. This paper proposes a framework that creates such a decentralized platform that would store patient's medical records and give access of those records to providers or concerned individuals, i.e., patient. We also intend to solve the scalability problem of blockchain, as it is not in the design of blockchain to store huge volumes of data on it. So, we would use off-chain scaling method that makes use of the underlying medium to solve the scalability problem by storing the data on that medium. Moreover, our proposed work is intending to solve the above mentioned information asymmetry and data breaches problem faced by the EHR system. This paper is organized as follows the section II of this paper summarizes the basics of blockchain technology and its dependencies; section III narrates the related work done in this domain. The section IV explains the design and architecture of the proposed framework and section V explains the performance of this framework. The last section provides the conclusion and references.

II. LITERATURE SURVEY

Blockchain innovation empowers a decentralized and distributed network environment with no requirement for a central entity. Transactions are secure as well as trustworthy due to the utilization of cryptographic standards. Lately, blockchain innovation has turned out to be in popular, trendy and has infiltrated various areas, generally because of the prevalence of digital forms of money. One field where blockchain innovation has gigantic potential is healthcare because of the requirement for a more patient-centric way to deal with healthcare systems and to increase the interoperability of the systems and increase the precision of Electronic Healthcare Records (EHRs).

The broad use cases are: -

1. Blockchain for Electronic Medical Records – Blockchain can be used to store digital medical records of patient data in a decentralized system. This system is believed to be of great benefit as it guarantees data integrity and protect patient privacy.
2. Blockchain for Tracking and Tracing Medical Fraud – The market is flooded with fake medical drugs. Blockchain can be used to move the fake drugs out of the picture by tracking the drugs from their manufacture to their distribution. This will also help the country in an economical point of view.
3. Blockchain for Artificial Intelligence – AI can be used for the analysis of complex medical data. This requires huge amount of data with diverse range to ensure accuracy and obtain effective results. Blockchain can provide a platform where patients, with the help of an advanced AI doctor, can discuss their medical data and get proper results. Moreover, this huge generated data can also be used as training sets for the AI systems.
4. Blockchain for Secure and Guaranteed Payments – Financial sectors was the first domain in which Blockchain technology was used and it has proved to be very successful. Even for healthcare applications, Blockchain can facilitate payment of fees for treatments.
5. Blockchain for Medical Research – Because of the large audience and huge amount of generated data, it will not become easy to find people who fit a certain medical history or and has the potential for clinical trials. They can even be incentivised with this platform. Moreover, abundant data will be available that can boost the medical research.

Andreas Bogner, in his paper[10] explains the use case of Ethereum blockchain in creating a decentralized application running a smart contract. It focuses on the elimination of TTP (Trusted Third Party)[10]. The main components of the application are the smart contracts hosted on the blockchain, the local Ethereum client, and a web app. The web app provides a GUI for the local Ethereum client, which in turn interacts with the smart contract on the Ethereum blockchain.

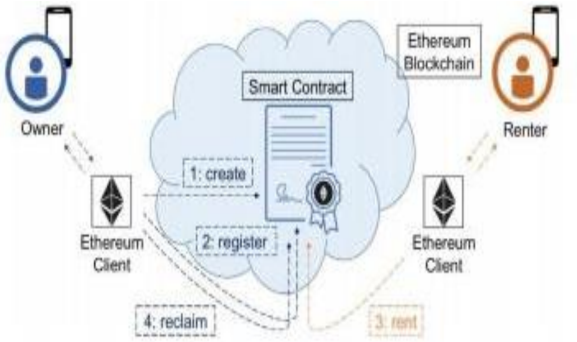

Fig 1: DApp in use

One of the applications of this technology is being worked on by the Truefield team. The practice of medical recordkeeping reduces the healthcare cost and also assure quality health care. The Truefield platform aims at creating a patient centric approach to storing of medical information. They plan to achieve this by creating a unique digital medical IDs for each user. Their objective is to create an EHR system that is secure, private, confidential, easily accessible, cheap, facilitates information sharing etc. They plan on creating a decentralized application that will be accessible to users even without internet access through Trufield's unique protocol USSD. It will be a combination of centralized and decentralized platform. They plan to have their own tokens that can be owned, used and received as rewards.

III. BLOCKCHAIN TECHNOLOGY

Nakamoto invented this technology for his famous digital currency or crypto-currency work, that is, bitcoin. Nakamoto used blockchain technology to address bitcoin's double spending issue but this innovative technology was quickly being used in many other applications. Blockchain is a chain of blocks that are connected together and are that continuously by storing transactions on the blocks. This framework uses a decentralized approach to distribute the information and share ownership of and piece of distributed information, or commonly known as data. Blockchains carry transaction batches that are hashed thus providing them with protection, and are managed by peer-to-peer networks. A blockchain has certain bene_ts such as security, anonymity, and integrity of data with no third party intervention. These benefits make it a reasonable choice to store patient's medical records on it, because the innovation of technology in the healthcare industry has made the security of patient's medical data a top priority. A number of researchers have also identified that using blockchain technology in healthcare would be a feasible solution.

A. Blocks

A block is a sequence of transactions. It contains the transactions chronographically. A Blockchain is made of a series of blocks. Each block contains the hash of the previous block, and thus they make a series. The first block in a Blockchain is also known as the genesis block.

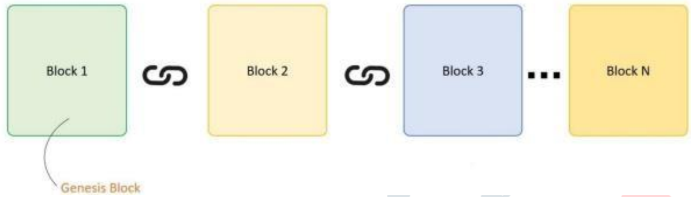

Fig 2: Chaining between blocks in a blockchain

B. Nodes

A node is also stated as the shareholder of the Blockchain. Every node in the network has two keys, a public key and also a private key. The private key is used for decrypting the messages and it allows a node to read that message. The public key is used for encryption of messages sent to a node. Some nodes also act as the miners of the blockchain ecosystem. The miners are referred to as special nodes that uses an algorithm to validate the transactions submitted by other nodes and make a block that will be a candidate for the next block to be added in the blockchain.

C. Types of Blockchain

On the availability of data and what actions can be performed by the user, the blockchain can be classified into three types : -

1. Public permissionless

The data in public blockchain is always accessible and visible to everyone. In a public permissionless blockchain, anyone has the right to join the blockchain and become a node without any approval.

2. Consortium (public permissioned)

The consortium blockchain is a system that is 'semi-private' and has a controlled user group, but works across different organizations. It allows only a particular group of nodes that can take part in the consensus process.

3. Private

A private blockchain allows only particular nodes to be a part of the network either as a node or as a miner. Thus, it is a distributed yet centralized network. They control which nodes can perform transactions, execute smart contracts or act as miners. They are managed by one organization which is the trusted party. It is used for private purposes.

IV. PRELIMNARIES

This section formally describes the preliminaries used in proposed framework. It describes the software platform used for development of this framework and its advantages. Ethereum and IPFS being the most prominent and important for implementation of this framework are also discussed in the following section.

A. ETHEREUM

Ethereum was presented in the paper of Vitalik Buterin[7], and discussed some drawbacks of the scripting language of the Bitcoin. The main contributions are complete Turing-completeness, which means Ethereum supports all forms of computations including loops. Then Ethereum supports transaction status, as well as many other enhancements in the framework of the blockchain.Ethereum is a blockchain with a Turingcomplete built-in programming language. It offers an abstract framework that allows everyone to establish their own rules of ownership, transaction types, and state transition functions. This is achieved by means of smart contracts, a collection of cryptographic rules which are only applied if certain conditions are met[7].The consensus within the Ethereum network is based on the modified GHOST (Greedy Heaviest Observed Subtree) protocol[8]. This is designed to fix the network's issue of stale blocks. The stale blocks will arise when one group of miners combined in a mining pool has more computing power than the others, which means the blocks from the first pool can contribute more to the network, cauTtsing the centralisation problem. GHOST protocol integrates such old blocks into the longest chain calculations.The centralization problem is removed through providing block rewards to stales, where the stale block receives 87.5% of the reward, and the nephew of that stale block receives the remaining 12.5% of the reward. In this way, the miners are still rewarded even if their block didn't become the part of the main blockchain (those blocks are called uncles). Ethereum uses the modification of the

GHOST protocol which includes uncles up to seven generations [9].

B. SMART CONTRACTS

A smart contract is a computer protocol designed to digitally facilitate, check or execute a contract's negotiation or execution. Smart contracts allow the performance of credible transactions without third parties. These transactions are trackable and irreversible. They permit trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for a central authority, legal system, or external enforcement mechanism.

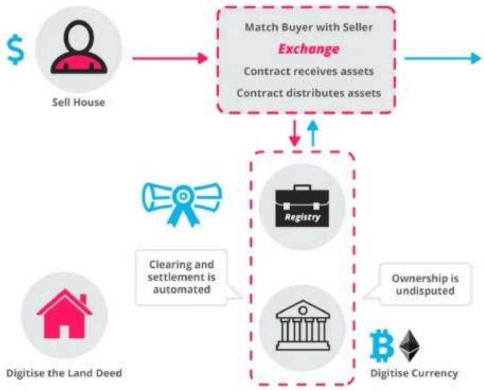

Fig 3: How Smart Contracts work

C. IPFS

IPFS or InterPlanary File System is a protocol that uses peer-to-peer network for data storage. It provides secure data storage as data stored on IPFS is protected from any alteration. It uses a cryptographic identifier that protects the data from alteration as any attempt to make change on the data stored on IPFS could only be done by changing the identifier. All the data _les stored on IPFS contains a hash value that is generated cryptographically. It is unique and is used for identification of stored data on the IPFS. This secure storage strategy of IPFS protocol makes it a favourable choice for storing critical and sensitive data. The cryptographic hash that is generated could be stored on the decentralized application to reduce the exhaustive computational operations over the blockchain. IPFS protocol works using a peer-to-peer (P2P) network, this network contains a data structure known as IPFS object that contains data and link in it. Data is unstructured binary data and link consists of an array. The IPFS protocol works in the following way: Files stored on IPFS are assigned a unique cryptographic hash. Duplicates are not allowed to exist on the IPFS network. A node on the network stores content and index information of the node.

V. SYSTEM DESIGN AND ARCHITECTURE

The systems proposed earlier show blockchain implemented EHR that concentrate on access control ,data sharing. The given systems do not really concentrate on an efficient storage, storing the data in the main blockchain network. Therefore, a system with an off chain storage is proposed where the actual data is stored offline and the hash of the data is stored in the blockchain. IPFS is used for this purpose of off-chain storage and we take advantage of its scaling features. Moreover, Ethereum is used for the overall implementation of the proposed system.

A. SYSTEM DESIGN

There are three entities or components within the proposed structure or scheme. Such entities or modules have additional definitions which need to be clarified as discussed below.

The conceptual system consists of participants who may be patients, clinicians, admins and Lab technicians. There are different access rights for different participants namely- Read, Write, Modify and Revoke.

1. NETWORK

This consists of an interconnection of peers/nodes that enables the transfer of data without any central authority playing the middle man. This ensures complete privacy of data. This creates a distributed system where no one controls the network. All the computers in the network are treated equally and have equal powers.

2. TRANSACTIONS

The system has the following functionalities :

Create Medical Record(By patient/Clinician): This adds a medical record to the existing patient records. For a clinician to be able to create records, the need the access permission of the patient beforehand. Only those clinicians with access permission can create medical entries. A patient ,by default has the access right to add medical data to their profile.

The specific medical records of the patient are stored alon g with the IPFS hash, which includes the uploaded file contai ning the patient's test reports or other medical information.

Grant Access (To Clinician/Lab) :This functionality allows patient to grant access to the above mentioned records and information to the clinician / Lab.

Revoke Access(To Clinician/Lab): This would let the patient revoke the access of clinician/Labs to add or view data after a certain point or after their treatment is over.

View Medical Record(By patient/Clinician): This operation Is used both by doctors and patients. This function also requires access permission of the patient. Only after the patient grants access to view , the participants can access those data. The patient has access rights to view their own data.This data is stored in a decentralised way in IPFS and accessed through the hash of the data.

3) SYSTEM IMPLEMENTATION

The implementation of the business logic of the system is done through smart contracts.It consists of three smart contracts :

Migration contract: This is present in all Ethereal DApps that lets us migrate the contracts to the blockchain via the truffle framework.

Record contract:This defines the access rules and has information regarding which users have what access rights over the record.

Patient contract: This consists of the logic behind the operations that the patient has access to.It also initializes the patient address

A. ALGORITHMS USED

Create Medical records:

```
If ( msg.sender == patient && msg.sender IN PID || Granted ( msg.sender ) && msg.sender IN CID )
    then
    add data to patient's profile
    else
    Permission    Denied
    end if
```

View Medical records:

```
If ( msg.sende r== patient && msg.sender IN PID || Granted ( msg.sender ) && msg.sender IN CID )
     then
    fetch data from IPFS and display
    else
    Record  Access  Denied
    end if
```

Assign Roles:

```
     function Roles (New Role, New Account )
    add new role and account in roles mapping
    end function
```

CID represents the list of authorised Clinicians and PID represents the list of authorised patients.msg.sender in Ethereum using Solidity language which denotes the Ethereum address of the user/ sender of the request/ message.

VI. CONCLUSION

As discussed earlier, there are various benefits of using Blockchain technology to create an application that stores Electronic Health records. A modern, secure solution is introduced that maintains EMRs in the healthcare departments using blockchain technology. The systems proposed earlier show blockchain implemented EHR that provides access to the data owner and the data requester to read, write, add and revoke records. The given systems do not really concentrate on an efficient storage, storing the data in the main blockchain network. Therefore, a system with an off chain storage can be introduced where the actual data is stored offline and the hash of the data is stored in the blockchain. This way, this distributed storage proposed ensures safety against manipulation and confidentiality of the data.

VII. REFERENCES

[1] 'Review Paper on Untwist Blockchain: A Data Handling Process of Blockchain Systems' by Zeal College of Engineering

[2] 'BinDaaS: Blockchain-Based Deep-Learning as-a-Service in Healthcare 4.0 Applications' – IEEE Paper Published on 25th December 2019

[3] Efficient key management scheme for health blockchain- IEEE Paper Published on 28th June 2018

[4] 'Managing lifelong learning records through blockchain' – Springer Open Published in 2019

[5] 'A Novel EMR Integrity Management Based on a Medical Blockchain Platform in Hospital' - Department of Computer Engineering, Jeju National University, Jeju-si 63243, Korea Published on 25th April 2019

[6] Off-chain Data Fetching Architecture for Ethereum

[7] Smart Contract - IEEE Explore published in July 2019.
V. Buterin, "Ethereum white paper: a next generation smart contract

[8] &decentralized application platform," 2013

[9] Y. Sompolinsky and A. Zohar, "Secure high-rate transaction processing in Bitcoin," Financial Cryptography

[10]
Ethereum Community, "A next-generation smart contract and

[11] decentralized application platform"

[12] Andreas Bogner, Arne Meeuw, Mathieu Chanson, "A Denetralised Sharing App running a Smart Contract on the Ethereum Blockchain," Research Gate, Conference Paper November 2016