# Electronic Health Record: Blockchain Technology

Shruti Gaikwad,Nikita Kirad,Shubhangi Gayake
Department of Information Technology
MIT College of Engineering
Pune, India
shruti2835@gmail.com,2nov.nk@gmail.com,
shubhangigayake123@gmail.com

Dr. Pradnya Kulkarni
Department of Information Technology MIT
College of Engineering Pune, India,
Federation University, Australia
pradnya.kulkarni@mitcoe.edu.in

*Abstract*— Electronic health record (EHR) is a systematic collection of compact real-time patient-centric information which includes all types of treatments the patient has undergone along with the lab results, medical prescriptions etc.EHR allow faster sharing of records and information retrieval.EHR is about helping the medical practitioners provide quality treatment to their patients while also maintaining the safety and efficiency of their records. But, one of the exasperating problem that the health care systems face is the ability to share medical records with more than one stakeholders, while maintaining complete security and ensuring data integrity. Storage and sharing of medical records securely have been one of the important aspects of the EHR.Medical data consists of sensitive information that the patient expects to be kept confidential. At present, the biggest issue of health care systems is the central administration of data. Regardless of various advancements in the healthcare industry, the EHRs have still been suffering from various data breaches. Storing patients sensitive health records on the Blockchain based storage can help in rectifying these shortcomings. The Blockchain technology is decentralized and a unique approach of storing data on a distributed network without any central authority. The blockchain has the ability to transform the healthcare industry, by placing the patient at the center of the ecosystem and increasing quality, security, interoperability of health records. Blockchain offers a set of tools for solving many issues related to patients consent for data sharing.Recent findings indicate that the blockchain research has been increasing in the healthcare industry and is mainly used for managing health records and access control.

***Index Terms*—Electronic Health Records, Blockchain, Privacy**

## I. Introduction

The interest in the Blockchain technology has been increasing since the year 2008[6][9].In recent years, the blockchain technology has become one of the most trending technology and has been entering in different domains mainly because of the popularity of cryptocurrencies[8]. The blockchain technology has the tremendous potential to transform the healthcare industry.A blockchain supported Health information systems can solve the frequently discussed problem of the lifelong recorded patient health data.

Blockchain can store any kind of data on the distributed ledger which can also track the history of the data. Transactions are carried out with the use of cryptographic principles which makes them secure and trustworthy. Three basic and commonly used models followed by the medical institutions to achieve interoperability of medical data are push, pull and view[6]. Blockchain offers fourth model which provides complete security to the medical records[6]. It also ensures the secure sharing of medical records across different institutions.

## II. Basic terminologies in blockchain

Distributed Network Architecture: Blockchain replaces the centralized architecture with a distributed one. The Blockchain software runs on thousands of nodes in a distributed network. The transaction which is processed is distributed across these nodes in the network and it is cleared only when all the nodes reach an agreement (also called consensus) to accept the transaction in the ledger[6][7].

Peer to Peer transmissions: Communication occurs directly between the peers. Every node stores and forwards the information to the next node. Every node maintains their own copy of data. The system has to ensure that all individual copies are consistent i.e the local copies at every node are identical and are always updated based on the global information[6].

Public Ledger: Public Ledger works like a database where it contains historical information and it utilizes this information for future computations.

Transparency: Blockchain provides higher levels of security and privacy by ensuring that the details of transactions are shared with only those who have access to the transactions or who are involved in the transactions. The data belongs to various clients involved in the transactions and hence the privacy and authenticity are maintained. In blockchain transactions, there is no third party intervention. Every transaction or value will be visible to only those who had access to the system[6][7].

Mining: The process of validating the transactions in the block is known as Mining. Mining is the mechanism that provides decentralized security in the blockchain. Mining is an important concept that should be taken into consideration as it

affects the overall performance of the system. Miners collect all transactions for a particular duration and try to build a new block and connect it using some cryptographic hash computation[5].

Immutable Transaction Ledger: Since the ledger is immutable no one can erase or update the records. Updates include date, time location, entity making the update. All the information is encrypted and stored on the blockchain and can be decrypted by the parties who have the corresponding private key[6][7].

Smart Contracts: The term "Smart Contract" was coined by Nick Szabo. He claimed that smart contracts cab be realized with the help of public ledger. Smart contracts can be thought of as an agreement or contractual clauses that can be embedded in the hardware or software[5][2].

Public Key Cryptography: It is an encryption system that makes use of a key pair, a public key, a private key. Public key is the one which is available to everyone whereas the private key is the one that is available only to its holder. Either one is used to encrypt the message while the other one is used to decrypt it[5][2].

The interplanetary file system also is known as IPFS is a peer to peer hypermedia protocol to make the web faster and safer. There have been many peers to peer applications, some of them are very successful while some of them failed completely. HTTP is one of the most successful distributed file system protocol and is being used worldwide. However, IPFS aims to replace HTTP with a novel peer to peer system. It provides content addressable storage model[3][5].

## III. TYPES OF BLOCKCHAIN

There are different types of blockchains available depending on the type of data, availability of the data and the corresponding actions the user performs on them. They are:

1) Public Permissionless

2) Consortium (public permission)

3) Private

Public Permissionless work in an open environment and over a large network of users. All data in the public permissionless is accessible to the public. Some parts can be encrypted to preserve the participant's anonymity. In the public permissionless anyone can join the chain either as a simple node or as a miner. The users need not reveal their identity to their peers.

The consortium type blockchain allows only a selected group of nodes to participate in the process. It is partially centralized and open for a limited public use.

A private blockchain allows only certain nodes to join the network. It is a decentralized yet a centralized network. It is used for private purposes only. They are managed by a single organization only. Private blockchains are permission and control the transactions on the nodes. Hyperledger Fabric is an example of private blockchain[8].

## IV. NEED FOR BLOCKCHAIN IN HEALTHCARE

There are several problems with centralized EHR systems. These can be summarised as follows

### *A. Single point of failure*

Dependency on the systems that are mostly centralized often suffer from the fear of data crashes as most of the data is present in one place. Failure in one node/server leads to failure of the entire system.

### *B. Privacy Issues*

Privacy issues in the health sector have resulted in decrease in patients trust in the EHR. If the privacy of sensitive health information is weaker then public trust in the health care delivery system cannot be maintained. Inspite of the increased feasibility and convenience that the EHR's offer, the patients are in constant fear about the integrity and privacy of their health information[4].

### *C. Data Breaches*

EHRs are prone to attack by hackers who have a complete understanding about the navigation of network which is not protected. Healthcare documents contain a vast amount of personal information of the patients can be rewarding for the cybercriminals. Patients fill out details such as their name ,addresses, medications, history records, payment information. Attackers can see all this information within the EHR files.EHR benefits the health care process but can also be susceptible to attacks if they are not properly secured[7].

### *D. Lack of Interoperability*

Powerful EHR interoperability is crucial for providing efficient patient-centered care. However, recent findings show that it is lacking in most of the EHR systems. When a patient receives treatment from a different provider either in an emergency situation or just by visiting a specialist it is important that the new healthcare provider have access to the patient's health history. All practitioners, in fact, require a broader, up-to-date view of the patient information conveyed at the point of care to ensure the highest levels of clinical quality. Varying data standards also make systems less interoperable because not all records are compatible with the

systems. Effective interoperable systems are likely to improve the provider's productivity[1].

Health care is one such field where blockchain is considered to have a greater potential. The above-mentioned problems can be solved by the implementation of patient-controlled blockchain based EHR system. Focus should be given on the management of data and efficient storage of data that will increase the accuracy of the EHRs. Storage of sensitive health records is very important and these records are prime targets of attackers. Blockchain technology is robust against attacks and failures, and hence it provides a good framework for healthcare data[8].

Blockchain works on the basis of three principles. First, the data is stored on a public ledger that anyone can read. In blockchain, a committed transaction cannot be rolled back so there will always be a complete record of all the transactions. Even if errors are encountered in the previous transaction, then we have to enter an new transaction saying the previous one was invalid. Second, blockchains are implemented in a decentralized network ,where no one controls the blockchain. This makes them robust against possible failures and attacks. Third, the metadata of each transaction is available to everyone in the system, which does not mean the data stored on the chain is readable. Blockchain stores the record using public key cryptography and pseudo-anonymity. This allows the data to be encrypted in such a way that they become expensive to crack[8].

In the context of EHR, the transactions would contain the documentation of specific appointments of patients and the healthcare services provided. Practitioners and patient can contribute to the encrypted data which would be stored on the public blockchain. This information stored on the blockchain will be in the encrypted form which can be decrypted only by those parties having patient's private key. In addition to this, as the ledger is immutable, and no one can alter the records, blockchain based EHRs system will be self-auditing[7].

## V. Advantages of Blockchain

A patient becomes controller of his records. This replaces the traditional methods where patients had to acquire copies of their records and transfer it to other providers while receiving treatment.

As the data is stored on a decentralized network, there is a low risk of data being hacked or robbed as there is no central authority in control of the data[7].

The encrypted data can be decrypted only by the patients private key, so even if the attacker wants to read the data or hack the data he will not be able to read the patients data[7].

[7] Ivan, Drew. "Moving toward a blockchain-based method for the secure storage of patient records." ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST. 2016

Time stamping is used in the blockchain methodology which authenticates changes to the dataset. This infrastructure therefore, provides self-auditing capabilites[7].

## VI CONCLUSION

In recent years there has a been successive rise in the adoption rate of EHRs, but the expectation of safe, secure, easily transported electronic patient data is still not met[7]. The blockchain approach can prove to be an ideal solution to problems. The most significant advantage of the block-chaining approach is that data is secured and protected from data breaches. Cryptography can prove to be an important part in the way the healthcare systems work. With the rapid increase in patient numbers, the hospitals have to manage more and more data on daily basis. In this situation having secure information sharing services are crucial for providing proper medical services. Using this technology when the data is encrypted and decrypted it is impossible to alter the data which ensures robust security. As this technology uses time to stamp it is also possible to know the providers who contributed to the chain as well as the time when the changes were made. Every device or a block in the chain stores a copy of the transactions. It is therefore, possible for the users to identify the owner of a particular block at any time. Blockchain is therefore, a secure and reliable method of storing and sharing sensitive medical records.

## References


[1] Assaf Halevy,"Game-changing Interoperability for Healthcare".

[2] Gábor Magyar,"Blockchain: solving the privacy and research availability tradeoff for EHR data",2017 IEEE 30th Jubilee Neumann Colloquium.

[3] Yongle Chen, Hui Li∗ , Kejiao Li and Jiyang Zhang,"An improved P2P File System Scheme based on IPFS and Blockchain",2017 IEEE International Conference on BigData (BIGDATA).

[4] Mario Sicuranza,Angelo Esposito,"An Access Control Model for easy management of patient privacy in EHR systems",The 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013).

[5] Nabil Rifi, Elie Rachkidi, Nazim Agoulmine, Nada Chendeb Taher,"Towards Using Blockchain Technology for eHealth Data Access Management",2017 Fourth International Conference on Advances in Biomedical Engineering (ICABME)

[6] Halamka, John D., and Ariel Ekblaw. "The potential for blockchain to transform electronic health records." Harvard Business Review 3 (2017).

[8] Hölbl, Marko, et al. "A Systematic Review of the Use of Blockchain in Healthcare." *Symmetry* 10.10 (2018): 470.

[9] Yli-Huumo, Jesse, et al. "Where is current research on blockchain technology?—a systematic review." *PloS one*11.10 (2016): e0163477.

[10] Uddin, Md Ashraf, et al. "Continuous Patient Monitoring With a Patient Centric Agent: A Block Architecture." *IEEE Access* 6 (2018): 32700-32726.