

PATIENT DRIVEN ELECTRONIC HEALTH RECORD USING BLOCK CHAIN

¹Vinithra.G,²Nandhini.S, ²Tharunya.R

¹Asst.Professor,²Final Year Students, Dept. of Computer Science & Engineering
Sri Sairam Institute of Technology, Chennai-600044
vinithra.cse@sairamit.edu.in

ABSTRACT:

An electronic Medical record (EHR) is a of a computerized version of a patient's paper record. Our reality has been drastically changed by advanced innovation like – PDAs, tablets, and web-empowered gadgets have changed our day to day lives and the manner in which we impart. Medication is a data rich enterprise. EHR incorporate the clinical and treatment chronicles of patients, an EHR framework is worked to go past standard clinical information gathered in a supplier's office and can be a more extensive perspective on a patient's consideration. Electronic Health Record (EHR) frameworks face issues with respect to information security, honesty and the board. We could execute blockchain innovation to change the EHR frameworks and could be an answer of these issues. The main goal of our proposed structure is to implement and execute blockchain innovation for EHR and furthermore to give secure capacity of electronic records by characterizing granular access rules for the clients of the proposed framework. Thus this structure furnishes the EHR framework with the advantages of having a versatile, secure and necessary integral chain-based arrangement

INDEX TERMS :blockchain, health records, electronic health records, decentralization, and scalability

I. INTRODUCTION¹

The quick take-up of digitization in human healthcare has prompted a huge electronic records about patients. Such development presents exceptional requests for social insurance information security while being used and trade. The ascent of blockchain innovation as a capable and straightforward system to store and appropriate information is making ready for new possibilities of fathoming genuine data privacy, security, and uprightness issues in medicinal services. Blockchain innovation has pulled in impressive consideration from industry just as scholastics in the course of recent years.

The blockchain technology has given rise to numerous smart contract applications in several areas, ranging from energy resources , financial services and healthcare.

Blockchain innovation offers straightforwardness and destroys the requirement for third-parties or administrators.. It uses consensus mechanisms and cryptography to verify the legitimacy of a transaction in a trustless and unreliable environment In a blockchain distributed P2P network of transactions, the receiving node checks the message; if the message is correct, then stores it in a block. A consensus algorithm then used to confirm the data in each block; this is called "Proof-of-work(PoW)".

A blockchain innovation is identified as a circulated record of innovation for shared (P2P)-an organized computerized information exchanges that might be openly or secretly appropriated to all clients, permitting any sort of information that is put away in a reliable and in a verifiable manner. Another principle idea of the

blockchain is the brilliant concept, a lawfully restricting approach that comprises of adjustable arrangement of rules under which various gatherings consent to associate among one another as decentralized automation

The capability of block chain in medicinal services(EHR) is to invoke the provokes identified with information security, protection, sharing and capacity ,One of the necessities for the social insurance industry is Interoperability. It is the capacity of two gatherings, either human or machine, to trade information or data definitely, efficiently, and reliability.

The goal of interoperability in healthcare is to facilitate the exchange of health-related information, such as electronic health record(EHR), among healthcare providers and patients so that the data can be shared throughout the environment and distributed by different hospital systems .Moreover, interoperability enables providers to securely share patient medical records (given patient permissions to do so), regardless of the provider's location and trust relationships between them ,This is specifically important considering that the source of healthcare data is diverse.

This part of interoperability is settled by utilizing blockchain innovation which showed potential to store, oversee and share EHRs securely among social insurance networks.

Moreover, expanding expenses of social insurance frameworks and programming in the business have caused colossal weight on world. In the medicinal record part, blockchain innovation is emphatically influencing social insurance results of organizations and partners to enhance business forms, improve understanding results, persistent information the board, upgrade consistence, lower costs, and empower

better utilization of human services related information

BLOCK CHAIN AND ITS TECHNOLOGIES

This technology was introduced by Satoshi Nakamoto , for his popular work of digital currency or crypto-currency, i.e., bitcoin. Nakamoto used blockchain technology to solve the double spending problem of bitcoin but soon this novel technology was being used in many other applications. Blockchain is a chain of blocks that are connected together and are continuously growing by storing transactions on the blocks. This platform uses a decentralized approach that allows the information to be distributed and that each piece of distributed information or commonly known as data have shared ownership.

Blockchain holds bunches of exchanges that are hashed in this way giving them security and they are managed by distributed systems. A blockchain has certain advantages, for example, security, obscurity, and respectability of information with no outsider verification . These advantages settle on it a sensible decision to store patient's clinical records on it, on the development of innovation in the medicinal services industry has made the security of patient's clinical information a top need. Various analysts have likewise distinguished that utilizing blockchain innovation in medicinal care would be a feasible solution

ARCHITECTURE

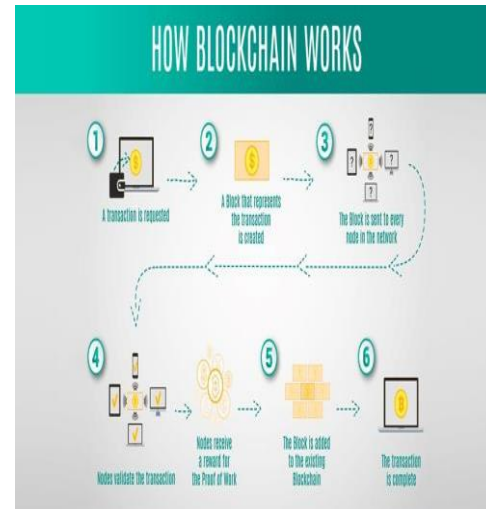
The blockchain architecture explains the whole process of a transaction being sent from a user on the blockchain network.

1. A new transaction being sent by a user on the blockchain network suggests that a new block is created. A block in the blockchain is used for keeping transactions in them and these blocks are distributed to all of the connected nodes in the network. That transaction placed inside a block is broadcasted to all of the nodes in the network. All the nodes in the network have a copy of the complete blockchain that helps them in verification process. When a block containing the 3 user transaction is broadcasted to all of the connected nodes, they verify that the block is not tampered by any means. If this verification results in success then the nodes add that block in their own copy of blockchain.

2. This whole process of the block being added on the blockchain is done by the nodes reaching upon a consensus where they decide which blocks are valid to be added on the blockchain and which are not. This validation is performed by the connected nodes using some known algorithms to verify the transaction and to ensure that sender is an authenticated part of the network. When a node succeeds in performing the validation that node is rewarded with crypto-currency. This process of validating the transaction is known as mining and the node performing this validation is known as miner.

3. After validation is done the code of block is added to the blockchain structure.

4. After the whole process of validation is performed the transaction is completed.



A. BLOCK

A blockchain are formed together by a number of blocks connected together in a peer-to-peer network thus making a decentralized application. The header of these blocks contains hashes of previous blocks in them. A block contains three things in it which are data, hash of current block and hash of previous block. The data could be anything as it depends on the type of blockchain. As in case of bitcoin, the data consists of coins that are actually acts as electronic cash for ease transaction .The hash that is stored in these blocks contains a SHA-256 cryptographic algorithm which is used for unique identification of a block on the chain.

B. CONSENSUS ALGORITHM

Each block that is added on the chain would need to follow some consensus rules for it to be added on the blockchain. For this purpose blockchain technology uses consensus algorithms. The most common consensus algorithm used is Proof of Work (PoW) algorithm and it was used in bitcoin network.

The basic working of this algorithm is that there are number of nodes or participants on a blockchain network so when a transaction is requested to be added on the network by any participating node it needs to be calculated. This process is called mining and the nodes that are performing these calculations are miners

D. KEY FEATURES OF BLOCKCHAIN

Decentralization: With blockchain the information is distributed across the network rather than at one central point. This also makes the control of information to be distributed and handled by consensus reached upon by shared input from the nodes connected on the network. The data that was before concentrated at one central point is now handled by many trusted entities.

Data transparency: Achieving data transparency in any technology is to have a trust based relationship between entities. The data or record at stake should be secured and temper proof. Any data being stored on the blockchain is not concentrated at one place and is not controlled by one node but is instead distributed across the network. The ownership of data is now shared and this makes it to be transparent and secure from any third party intervention.

Security and Privacy: Blockchain technology uses cryptographic functions to provide security to the nodes connected on its network. It uses SHA-256 cryptographic algorithm on the hashes that are stored on the blocks. SHA stands for Secure Hashing Algorithm, these hashes provide security to the block chain as data integrity is ensured by them. Cryptographic hashes are strong one way functions that generate checksum

for digital data that cannot be used for data extraction. This makes blockchain as such a decentralized platform made secure by the cryptographic approaches which makes it to be a good option for privacy protection of certain applications.

SYSEM IMPLEMENTATION

A. ETHEREUM

Ethereum was formally introduced in year 2015 and the idea behind Ethereum was to create a trustless smart contract platform that would be open-source and would also hold the feature of programmable blockchain. This technology also shares the peer-to-peer networking that makes it distributed. This platform also makes use of its own crypto currency known as Ethers. This crypto currency can be used for sharing it between accounts connected on Ethereum blockchain. Ethereum also provides the programmers a language in which they can customize their own blockchain, this language is known as Solidity. It was developed for smart contracts that are the main feature of Ethereum

SMART CONTRACTS

Smart contract are known as the piece of code that is used to perform any task on the blockchain. This piece of code is executed when the users send the transactions [30]. They run on the blockchain directly thus making themselves secure from any kind of tampering and alterations. Smart contract commonly use solidity language and they can be used to program any kind of operation that a programmer wants to do on the blockchain

ETHEREUM VIRTUAL MACHINE (EVM)

The major benefits of using Ethereum platform is that it offers include the programmable blockchain. It provides its users with the choice to create their own applications functioning on the Ethereum.

IMPLEMENTATION

Blockchain innovation offers straightforwardness and destroys the requirement for third-parties or administrators.. It uses consensus mechanisms and cryptography to verify the legitimacy of a transaction in a trustless and unreliable environment In a blockchain distributed P2P network of transactions, the receiving node checks the message; if the message is correct, then stores it in a block. A consensus algorithm then used to confirm the data in each block; this is called "Proof-of-work(PoW)".

The user will be able to access their records on their own data from the place where they are. It also provide a means for easy access and security. EHR enhances information security, protection, sharing and capacity of the information

Patient Granting Access

- Patient X grants access to EHR to Practitioner X
- Practitioner X's ID is added to Patient X's authorised asset on the ledger
- Patient X's ID is added to Practitioner X's authorised asset on the ledger
- The Symmetric key for the EHR is decrypted with Patient X's private key
- Symmetric key is then encrypted with Practitioner X's public key

Patient Revoking Access

- Patient X revokes access from Practitioner X
- Practitioner X's ID is removed from Patient X's authorized asset

Patient X's ID is removed from Practitioner X's authorized asset

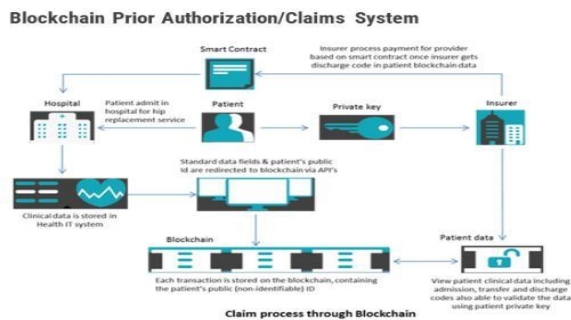
- Patient X's private key is used to decrypt Symmetric key for EHR which is used to decrypt theHER
- The EHR is encrypted with a new Symmetric key
- The new Symmetric key is encrypted with Patient X's public key and the public keys of all the remaining IDs that have permission

The patient has access to their own EHR this will enable the following key features.

1. Medical record not only provides this established and successful format of consultation, but will accommodate the doctor by enabling them to interact live with the patient's records during the consultation.
2. Health record offers unique value and provides patients with privacy controls. Patients are able to choose the level of detail visible and allocate viewing rights to their chosen doctor for as long as they feel necessary.
3. Users could allow health insurers access to



their health records. In return, insurers (who provide insurance) could rest assured that the information they are making decisions upon is trusted, verifiable and patients could be rewarded for their transparency in the form of lower premiums.



proposed approach. The proposed system also provides the ownership rights to the user by giving them authority using the smart contracts and hence can monitor the transaction. It also provides a limited access to researchers, insurance companies and others. Thus implementing Electronic Health Record using blockchain will ensure a more secured health care system.

REFERENCES:

- https://www.researchgate.net/publication/328208535_A_Systematic_Review_of_the_Use_of_Block_chain_in_Healthcare
- <https://www.semanticscholar.org/paper/A-Case-Study-for-Blockchain-in-Healthcare>
- www.computer.org/publications/tech-news/research/blockchain-health-medical-records-cloud-security
- https://www.academia.edu/39373366/Block_chain_Review_and_Directions_for_Future_Research
- <https://journals.sagepub.com/doi/full/10.1177/1460458219866350>
- <https://synapse.koreamed.org/DOIx.php?id=10.4258/hir.2010.16.4.281> Erstad T. Analyzing computer based patient records: a review of literature.
- J Healthc Inf Manag. Kaushal R, Shojania KG, Bates DW. Effects of computerized physician order entry and clinical decision support systems on medication safety: a systematic review. Arch Intern Med. advancedmd.com/emr-ehr-software

MOST SUITED SYSTEM

In the current healthcare system, patients have their health information spread over multiple systems, hospitals, networks and potentially countries. It provides the user, being the owner of their own medical records, full access and control over their data.

The user will have the capability to provide differing levels of access to various users, by assigning a set of access permissions and also a double encryption mechanism on a closed, permission-based blockchain

CONCLUSION

In this paper we notice that by combining the blockchain technology with the Electronic Health Record the shortcomings of the available health record such as interoperability, security, data integrity have been overcome by this