International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *22 August 2023* ***Revised:*** *12 October 2023* ***Accepted:*** *22 October 2023*

Healthcare Record sharing and management using Blockchain

Dr. Dhanamma Jagli[1], Dr. Subhash Chandra[2], Nakirekanti Laxmi[3], Sudhakar Jangili[4]
[1]Assistant Professor
Vivekanand Education Society's Institute of Technology,
Mumbai University, Mumbai, Maharashtra, India
e-mail: dsjagli.vesit@gmail.com
[2]Professor,
Department of Computer Science and Engineering,
CVR Engineering College, Ibrahimpatnam, Telangana, JNTU Hyderabad, India
e-mail: subhashchandra.n.cse@gmail.com
[3]Associate professor,
Visvesvaraya College of Engineering and Technology, JNTU Hyderabad, India
e-mail: laxmiprakash09@gmail.com
[4]Assistant Professor,
Geethanjali College of Engineering & Technology, Medchal (D) and
Research Scholar, JNTUCE Telangana, INDIA
e-mail: sudhakarj80@gmail.com

Abstract---We experience various health problems due to the hectic pace of life, which includes daily hustle and work life, and the deteriorating ecosystem. There are numerous health records produced and every individual has to maintain these many important pieces of private information. Health records are extremely sensitive information that must typically be shared with peers for numerous examinations in the medical field. Healthcare records are managed manually in the current scenario, which raises efficiency, security, and other concerns. This paper puts forward a web application that uses blockchain technology to offer a simple method for securely sharing private medical records. It offers real-time tracking of medical records, enhancing security, boosting productivity, and lowering total costs. By enabling infrequent knowledge transfer between healthcare professionals, insurance agencies, pharmaceuticals, scientists, and caregivers of the patient, it will streamline data exchange, enhance decision-making for healthcare, and ensure availability and genuineness. Doctors could use the application to review the healthcare data of the patients by whom they have been granted access, while individuals could use it to upload their data, grant access to the doctors, and read their own records.

Keywords- Healthcare Records, Blockchain, Ethereum, Smart Contracts, IPFS, security, privacy**.**

I. INTRODUCTION

Blockchain is an emerging, developing technology for distributed databases that uses cryptography to ensure the security, incorruptibility, and integrity of data. These characteristics make for reliable and secure data storage. Blockchain operates without a central authority and keeps all transactions in a chronological order that users can access at any time. This technology guarantees knowledge security and control of patient and medical field data that are susceptible. This technique has many advantages, including being immutable, transparent, hassle-free, and upholding integrity. The principles and different protocols used in cryptography, including digital signature and hashing, made it possible to implement all of these functions.

One of the numerous areas that blockchain has influenced is healthcare. Handling records in the healthcare sector is simple and secure because to blockchain's many benefits, including transparency and data integrity. Patients are given complete control over their access permissions and become the data's sole owners. Blockchain can be used to undertake multiple medical and clinical investigations, but doing so compromises the privacy and security of patient healthcare data. In these circumstances, it can serve as a solution to all of these problems. Healthcare researchers are working diligently to use this technology to address each of these problems.

In the supply chain for pharmaceuticals, it can also be utilized to detect fraud. Since most individuals rely on these pharmaceuticals for life, it is essential to safeguard them from fraud. Any agreement reached in this matter may have an impact on a specific patient's health. Due to the extensive people involvement, many supply chains are vulnerable to such fraudulent actions.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *22 August 2023* ***Revised:*** *12 October 2023* ***Accepted:*** *22 October 2023*

Smart contracts can be used to authenticate every record on a blockchain, which overcomes most of the problems with conventional systems that can provide a good level of security. But sustaining a blockchain is challenging.

Health has been rapidly degrading in this fast-paced world, and to reverse this, numerous tests and medical records are needed. We must always have reports, reported medical records, MRIs, X-MRIs, and past prescriptions, with us when we visit the doctor. Keeping all of these records in one place is a tough task.

Health records must be shared between health insurers, medical professionals, chemists, and research professionals, which is exceedingly difficult because patients' histories are always changing. Anyone who has experienced a major illness, such as cancer or Aids, has gone through treatment, recovery, and post-recovery. For example, understanding the chemo dosage for add - on therapy is essential because the patient might attend multiple healthcare centers for treatment or might be moved from one facility to some other. Having a thorough medical history is crucial for the right treatment. A patient must sign a statement outlining the information they consent to sharing with the receiver if they want to transfer their clinical information from one hospital to another or share it for research purposes.

Unless the data is anonymous, the patient must also consent to the collection of the information for research purposes. Relying on a single central authority to store and handle data can be the framework's single point of failure.

Due to its centralization, existing traditional systems have several flaws, including authentication, confidentiality, and security. Our study intends to present a framework for a decentralised approach that keeps patient healthcare data and allows certain clinicians or researchers to have access to such records. We even made an effort to address the issue of patient privacy.When healthcare records are stored using IPFS, the issue of scaling the blockchain is even handled.

II. BLOCKCHAIN AND ETHEREUM

Blockchain is an irreversible distributed database that may be used for virtually everything, including financial transactions. Some examples include the maintenance of digital identities and tracking of the weekly goods that we buy. This technology was implemented by Satoshi Nakamoto to produce Bitcoin, the first blockchain-based digital currency.

There are already over 4,000 digital currencies available now. Near real-time, Peer to Peer, Verified, and Immutable are some of the key characteristics of blockchain, which increase trust and lower the chance of fraud for a blockchain-based transaction.

These attributes are strengthened by blockchain: -

1. Independence

Since there is no single owner of a blockchain, no single person can exert authority over it. The modifications are the responsibility of every stakeholder. The possibility of experiencing a fraudulent operation can be reduced by doing this.

2. Faith

Blockchain assists in decentralizing a specific application. No one has the authority to delete or modify a previous transaction. Any effort to engage in this kind of conduct will not be recognized as a legitimate transaction.

3. Intermediaries

Blockchain technology can be used to eliminate all intermediaries. Let's say that individual A, who resides in India, wants to send his friend B, who resides in Germany, some money. The transfer of funds will be validated and verified by several banks. Aside from the banks of the sender and receiver, there are other intermediaries present here that can be eliminated with the aid of blockchain technology.

4. Integrity

Cryptography is used to secure all of the blockchain's transactions and state, making it difficult to alter.

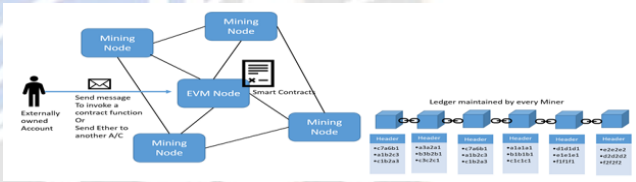

Fig 1: Blockchain, Ethereum, and smart contracts.

A. Ethereum Architecture

Some of the most crucial elements of Ethereum include the virtual machine, Transactions, Blocks, Miner, Smart Contracts, Consensus mechanism, mining nodes, gas, and Ether.

Together, these components form a distinctive architectur e for how they interact with one another and work. There are many nodes in a blockchain network, some of which are utili zed for mining and others
which assist in the execution of transactions and smart contra cts. Blockchain features a large number of nodes that are inte rconnected. Multi-
node communication is established using the peer-to-peer protocol.

The instance of the ledger, which is maintained by miners, contains every block on the chain. There are numerous miners in the network, thus it's possible that their ledgers differ from those of the other miners. To ensure that every miner has access to the same ledger, care has been made to synchronize the ledger amongst numerous miners.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 22 August 2023 **Revised:** 12 October 2023 **Accepted:** 22 October 2023*

Smart contracts are also hosted by Ethereum virtual machines. Business logic that is applied as part of the transaction and complies with the mining process is contained in smart contracts. Every action a person does, such as calling a smart contract function or sending a message, is regarded as a transaction. The individual doing the transaction must have an account on the network where the gas fee of Ether transfer is carried out. To confirm the sender's identity, each transaction is digitally signed using the account holder's private key.

All transactions are committed on the blockchain network. Blocks play a crucial function in ensuring that everyone is in a synchronized state. To prevent all transactions from being put in a single block, each block has a gas limit. They are stored in the new block when the gas limit is surpassed. A hash tree constructed by hashing transactions has a root known as the Merkel root, and each block has a block hash that is produced by obtaining the root hash of the tree. This makes it so that if someone tries to modify a transaction, the block hash will change and all subsequent blocks will be deleted. Transactions become permanent as a result.

1. Ethereum virtual machine (EVM)

The main purpose of the EVM is to run the smart contract's code. It has transaction-related information in it. In the transaction pool, all of the submitted transactions are gathered before being executed.

2. Mining Nodes

The miners use mining nodes to gather transaction details and then add them to fresh blocks. and after that, the blockchain gains access to that specific block.

3. Ether

The cryptocurrency utilized on the Ethereum network is called ether. When miners successfully add a block to a chain, they are rewarded with some Ether. A charge that can be paid with ether is typically associated with any operation that modifies the state of Ethereum.

4. Transaction

They are instructions that have been signed using cryptography. Accounts will start transactions that will update the blockchain's status. These transactions could include sending digital assets or Ether from one account to another, calling a smart contract function, sending messages to smart contracts, etc. When submitting a transaction in Ethereum, the recipient, signature value, data, gas limit, and gas cost are all included.

5. Smart Contracts

It is only a piece of code that operates on the Ethereum blockchain. It typically consists of a set of information (states) and programming (functions) that is kept in one particular place on the network. Smart contracts are simply normal contracts that specify certain rules, and the codes within the smart contract take these rules into account automatically.

III. TECHNOLOGIES

Technologies Used:

Ethereum Network for Blockchain.

Solidity for constructing Ethereum blockchain smart contracts.

Data off-chaining using IPFS (Interplanetary File Storage).

To pay a transaction fee: cryptocurrency wallet Meta Mask.

1. Ethereum

The blockchain network used by the cryptocurrency bitcoin is called Ethereum. The goal of Ethereum's official launch in 2015 was to create open-source smart contracts. It is distributed because it is a peer to peer. Our framework employs ether coin to carry out a variety of tasks on the platforms. The blockchain can be modified by programmers using the solidity programming language.

2. Solidity

Smart contracts are written in Solidity. It is a language for object-oriented programming. It is utilized to put Ethereum smart contracts into action. It was introduced by several Ethereum contributors, including Lex Beregszi and Christoph Reitwiessner.

3. IPFS (Interplanetary File Storage)

To create a flexible system of file storage and sharing, IPFS operates on a decentralized system of users that each own a portion of the overall data. To make sure that every report is seen uniquely by every machine in the network, IPFS uses content addressing. It is based on cryptographic hashes, which may easily be stored on a blockchain. Users of IPFS can no longer share documents with specific organisations. If sensitive or private details are to be disclosed, then this is required.

4. Meta Mask

A cryptocurrency wallet called Metamask communicates with the Ethereum network. Customers may access their Ethereum wallets via this browser extension, which can subsequently be used to communicate with decentralized applications. ConsenSys Software Inc., a blockchain software company that specializes in Ethereum infrastructure, is the developer of Metamask.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 22 August 2023 **Revised:** 12 October 2023 **Accepted:** 22 October 2023*

METHODOLOGY

A. Design

The patient records are kept in this application on a blockchain. Because files are not stored in the system, but access information is, the blockchain is a hybrid.

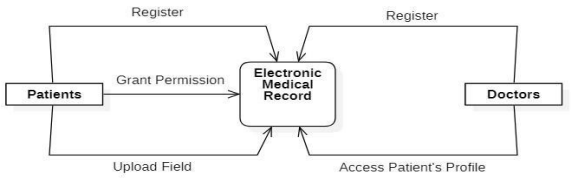

Fig 2: Working

B. Implementation

The application has been built for both patients and doctors.

1. Doctor

Doctors can create an account and log in to their dashboard. Once a patient grants a doctor access, the doctor can view the patient's data and address in their dashboard.

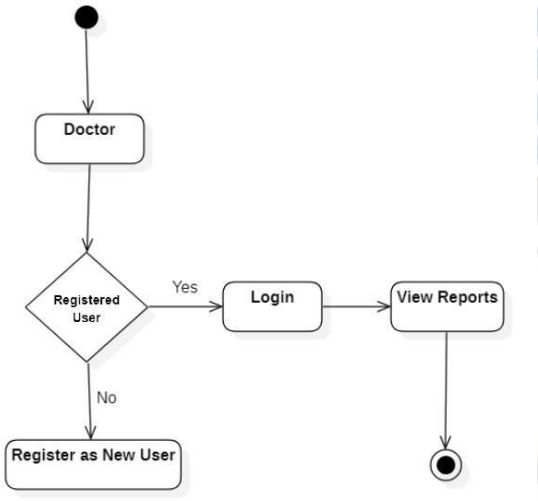

Fig 3: Doctor Module

2. Patient

By entering their meta mask information, patients can register and sign in to their dashboards. The files that the patient uploads will be uploaded to IPFS and their cryptographic hashes will be preserved on a blockchain. Patients may provide access to specific doctors.

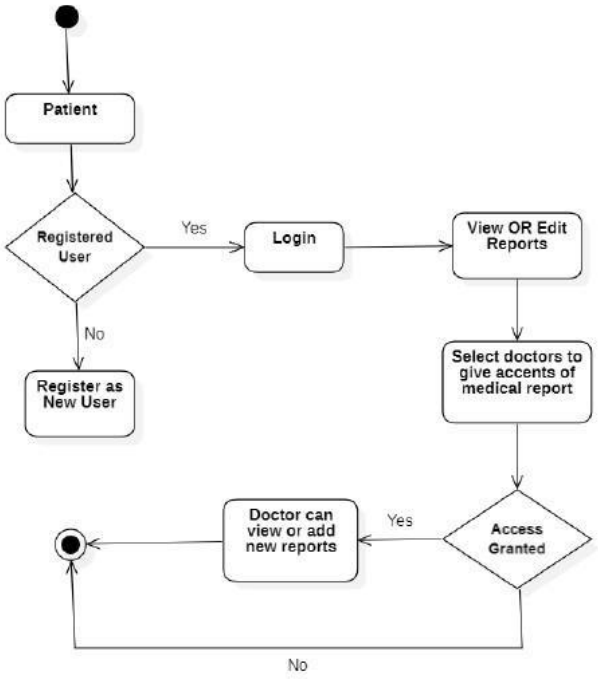

Fig 4: Patient Module

C. Features

1. Scalability

Scalability can be summed up as the system's capacity to carry out operations even as its storage needs increase or decrease. Due to the use of IPFS, our suggested framework functions whether the storage volume increases or decreases. Since both the IPFS file hash and the patient's data are stored. This eliminates the blockchain's scalability problem. The content on blockchain would still be fairly small, therefore transactions will proceed more quickly even if the size of the patient's data increases. The scale issue can be solved with IPFS while maintaining security because hashes are kept in a decentralised way.

2. Access Control

The system ensures that nobody who isn't supposed to have access to the system can. To protect itself from outside incursions, it offers security via specific safety protocols.

3. Content Addressable Storage

The storage techniques use IPFS or Content Addressable Storage. The hash is generated by IPFS, which also stores the patient's record. Now that the hash is saved on the blockchain network, both patients and doctors can access it. It guarantees the safe storage of patient records.

4. Integrity

Any system's integrity is determined by how much its users can rely on it. It must be genuine and durable. This is not

compromised because it is blockchain-based. The information is secure and cannot be changed by someone without authorization. No other person has the authority to edit the patient's data; they are the only owners of that information. The IPFS protocol secures the confidentiality of medical reports.

IV. CONCLUSION AND FUTURE WORK

The functionality of this system has been demonstrated in this research. It enables effective management and simple access to healthcare data for easy record-sharing. All users who are concerned about waiting in long-lines, long wait periods, and unsafe sharing protocols now can be comfortable. Our suggested system allows for both easy access and safe records. The application is simple to learn and can be used easily. Because IPFS is used, the system also makes sure to handle the issue of storage of data.

Later, these characteristics could be included:

1. Adding more people working in the healthcare profession, such as insurers, pharmacists, and researchers.
2. Integration of the patient consultation.
3. Include the payment method.
4. The incorporation of fitness trackers into health tracking applications.

REFERENCES

[1.] P. Roschin and D. Efanov, "The All-Pervasiveness of the Blockchain Technology," ScienceDirect, vol. 123, pp. 116-121, 2018.

[2.] B. V, " A Next-Generation Smart Contract And Decentralized Application Platform," White Paper; Ethereum Foundation (Stiftung Ethereum), 2014.

[3.] W. Liu, U. Krieger and S. S. Zhu, "Advanced block-chain architecture for e-health systems," IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom), pp. 1-6, 2017.

[4.] K. Fan, W. Shangyang , . R. Yanhui, . L. Hui and Y. Yintang , "MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain," Springer Link, 2018.

[5.] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma and J. He, "BlocHIE: A BLOCkchain-Based Platform for Healthcare Information Exchange," 2018 IEEE International Conference on Smart Computing (SMARTCOMP), pp. 49-56, 2018.

[6.] A. Omar, M. S. Rahman, A. Basu and S. Kiyomoto, "MediBchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data," International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, 2017.

[7.] M. A. Engelhardt, "Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector," Technology Innovation Management Review, vol. 7, no. 10, 2017.

[8.] P. Tak and Shing Liu, "Medical Record System Using Blockchain, Big Data and Tokenization," International Conference on Information and Communications Security, pp. 254-261, 25 November 2016.