International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 04 | Apr 2022 www.irjet.net p-ISSN: 2395-0072

Blockchain based system to store and retrieve healthcare records

Aditya Singh[1], Akash Salvi[2], Kaushal Pawar[3], Aayush Prabhu[4],

Dnyaneshwar Bavkar[5]

[1,2,3,4]*Computer Engineering, Terna Engineering College, Nerul, Maharashtra, India*
[5]*Assistant Professor, Dept. of Computer Engineering, Terna Engineering College, Nerul, Maharashtra, India*

Abstract - *Blockchain technology and its use case domains are growing rapidly due to the features and benefits offered over the existing systems. These features include decentralization, immutability, complete transparency, faster traceability, enhanced security and trust, automation without human involvement, and increased efficiency and speeds. These features are beneficial to many industries including supply chains, banking and financial sector, healthcare and pharmaceutical sector, governments, and insurance companies. The handling of patient records has been a recurrent issue in the healthcare sector as it is difficult to implement the right privacy and security measures in the existing systems. Data breaches, cyber-attacks, and identity theft are major threats in today's digital environment, and existing solutions have proven ineffective at managing these challenges. The threat of a single point of failure also looms over the existing centralized systems. Our research intends to address concerns with existing systems for accessing, managing, and securing health record data and offer a blockchain-based alternative for storing and retrieving health information. Ethereum blockchain platform is used to implement the data structure of our system. We also discuss the trade-offs in the adoption of blockchain technology.*

Key Words: **Blockchain, Solidity, IPFS, Healthcare, Smart Contracts, Ethereum, Decentralization, Secure transactions, Transparency**

1. INTRODUCTION

In recent years, medical practices have grown in prominence, with the primary goal of addressing ways to improve an individual's quality of life. In this data-driven environment, information systems are also becoming more important, as they can improve access to healthcare and business. Users can easily access their data thanks to the rapid development of technologies like information systems and cloud computing. Users are more than often connected to the internet with all the information they require being a click away. The traditional healthcare system is more doctor-centric. All the medical reports are stored by the healthcare institutions or medical professionals in the form of physical or digital files. These institutions use a centralized repository for storage which could become a cause for concern in maintaining privacy, accessibility, and security.

1.1 Reason to use Decentralization

In the health record management system, information from multiple sources like prescriptions, medical prognosis, and scans. This type of sensitive information is critical to patients' treatment. Currently, physical file repositories and centralized databases are used to store this critical information. These methods are prone to a single point of failure issue. Another issue is the inter-accessibility of these records as a patient may visit multiple doctors in different medical institutions and it may not be possible for two different entities to share the patient records. These systems should also be tamper-proof and only authorized individuals should be able to access and change the records. The authorized individuals are usually from medical institutions but this becomes are privacy and security issue individuals are prone to errors. Maintaining a timeline of reports is quite difficult to achieve in these systems. A personal ledger could maintain a timeline of reports which would streamline the process of diagnosis.

1.2 Advantages of Blockchain Solution

The proposed solution to these problems is a blockchain-based electronic health record system. A blockchain provides features that could solve the existing issues in the health record systems. The proposed system is user-centric and decentralized which also means no single institution is in charge of maintaining the system. A blockchain is a public database this is up to date and shared throughout many computer systems in a community. This increases the accessibility and transparency of the system. In the personal blockchain, the best recognized and identifiable set of members are explicitly admitted to the blockchain community. This reduces the presence of malicious actors in the community. As the data are saved in a blockchain that's programmed to be permissioned, the information may be very secure and guarded against any tries to tamper with it. The information may be decentralized and could allow the person to clean and rapidly get the right of entry to their personal information. The blockchain could be very stable in storing healthcare personal files due to the fact if a person attempts to tamper with one block, all of the different determine blocks need to be modified for this reason and comply with this. Hacking a blockchain community isn't any clean task, it requires tremendous computational electricity that can fail if the information itself is encrypted. Hence the proposed system can provide a viable solution for storing the health records of a patient.

2. PROBLEMS WITH CURRENT SYSTEM

The current system of sharing medical records is as such that they are feasible and compatible within a specific institution only. They can use their private networks in which the patient documents can be circulated between different departments. But this situation is not always ideal as a patient does have unexpectedly changing behavior when it comes to their health. It becomes a crucial necessity that such reports are interoperable and formats understood by multiple institutions participating in the medical lifecycle of a patient. Presently major of healthcare data depends on the interaction between the medical profession and the patient, and less importance is given to the data analysis part for the diagnosis. This makes such procedures long and difficult and is not welcoming to the patient. The presence of a complicated medical onboarding process also discourages the participation or active check-ups by people who then reach out to inexperienced and unprofessional opinions.

The amount of data generated related to healthcare is massive and needs proper collection and management. Patients have multiple doctors and physicians and the medical reports are scattered and non-standardized. In current systems, the medical reports rely on doctor-patient interactions, and these reports are scattered across different systems making the data less secure and less reliable. Even now in some cases, medical institutions use handwritten reports and physical files for managing patient data. This method of data management is very unreliable as human mistakes happen while forming reports and files could be lost and misplaced in poorly managed file repositories. Proper and truthful record keeping is required along with compatibility of data across different systems.

3. RELATED WORK

A whitepaper in early 2009, the notion of blockchain began to garner public interest, resulting in the first extensive application of blockchain, a digital currency known as Bitcoin[1]. They envisioned an online transactional system that would allow users to send digital currencies to one another without the requirement of a financial intermediary. Peer-to-peer transactions enable decentralization, and all transactions are cryptographically hashed to provide high levels of security. All transactions are recorded on a distributed ledger network, which ensures that they are transparent.

Many blockchain-based platforms for decentralized applications began to emerge as the popularity of blockchain technology and its possible uses expanded, one of which was Ethereum[2]. Due to the rapid development enabled by blockchain platforms like Ethereum, the applications of blockchain beyond digital currency are diverse and ever-growing.

An electronic medical record system that makes the use of Inter Planetary File System to store and retrieve data with corresponding hash and encrypted data for decentralization and the encrypted keyword information of the medical data is stored on the Ethereum blockchain[3]. This method of storage helps reduce the load on the blockchain as high-frequency access can be stressful. It is much more efficient in terms of the resources used to store such large amount of data in Inter Planetary File System instead of the blocks in the blockchain, as the medical data can have large sized files for which a blockchain is not suitable as a storage service, instead it should be used for recording the transactions and file locations[4].

To mitigate the raised privacy concerns in existing and centralized health record systems and the need for privacy mechanisms in health record systems, blockchain due to its immutability and irreversibility is a potential solution for incorporating privacy and security in health record systems but it also comes with its drawbacks[5].

Proposals for a private blockchain based on the Ethereum protocol, where sensors communicate with smart devices which invokes the smart contracts that write records on the blockchain were made[6]. This provides real-time patient monitoring and keeps a secure record of patients' data. This also resolves the security problems related to sending notifications to the patient in a HIPAA-compliant manner.

It becomes important for the patient to have the access control over their health records. Such proposals were made to use an Ethereum blockchain solution that will use smart contracts to ensure the trustful and secure access of data by the patient and other concerned entities involved with the treatment[7].

There are already conducted systematic reviews of blockchain technology applications in the healthcare industry. In conclusion, a large number of healthcare application prototypes are being developed using the blockchain platform, and the number of publications in this field has increased in recent years. Blockchain is still a field in which more research is needed to determine its utility in healthcare[8]. For a better use of the blockchain storage structure which provides the advantage of immutability, it can store the metadata of the files and of the stored medical data whereas the medical data files itself can be stored with the help of Distributed Hash Tables as it offers decentralized storage and distributive processing[9].

There are some limitations which are identified in this solution for storing the records in such applications. It includes the cost-effective implementation of processing and storing data which will be on the chain and issues regarding the scaling of the blockchain system even on a public ledger[10].

4. BACKGROUND

4.1 Blockchain Cryptography

The concept of blockchain revolves around the system of Distributed Ledger technology. It is a decentralized growing chain of blocks that are linked together. The new blockchain architecture is a peer-to-peer network that was introduced with Bitcoin in 2008. Programmatically these cryptographic functions are called Hash functions. Such functions aim to take the input of arbitrary length and generate an output of fixed length. There are different types of hash functions used in different blockchain architectures. For instance, to make a collision-resistant cryptographic hash function Merkle–Damgård hash function is used. A practical example of such will be the SHA-256 used for Bitcoin. Another way is using Sponge construction, and the example would be SHA-3 used for Ethereum.

The ledger in a blockchain can be replicated and maintained. In an event where one copy is edited, it should trigger a chain reaction that causes the other copies to update simultaneously[11]. This eliminates the requirement for anyone else to validate if the transaction occurred or not.

4.2 Blockchain structure and transactions

The purpose of the development of the blockchain would be about developing a trust less system where we can program our ethical and legal practices in the smart contract and store the rules of operation on the ledger. This will help to mitigate the doubt of human error in following the code of conduct and ethics while interacting with the system as everyone will have to come to a common consensus. These problems are countered when a certain practice has the support of a large population and is peer-reviewed. Blockchain ultimately refers to a chain of connected blocks that stores information about all the actions and transactions that are occurring on the network on which the blockchain exists. It will contain information on current transactions and the history of occurred transactions as well[12]. Each block is linked to the previous one by a hash code, which may be generated by the algorithms used by the platform, some of which are discussed above, and a new block becomes a part of this chain as soon as it is created. Blockchain networks can use public key infrastructure, such as Bitcoin, which uses the users' private and public key addresses to authenticate the user from their network-connected wallets. All information blocks are stored in disc space called nodes, which keep records of all network transactions and check the authenticity of any occurring transaction [13].

The transactions in the networks are chained with the previous block transactions using the hash of the preceding block, and this achieves the blockchain's immutability[14]. If an attacker tampers with the information stored in the blocks over the network, the local copies of the blocks will no longer be validated because the linking bridge, which is the hash code, will be changed upon the execution of any transaction on the chain by the hash function. In a further development of the technology blockchain, second-generation or blockchain 2.0 uses the concepts of smart contracts which are just scripts of a code that can execute itself upon fulfilment of a condition. It is helpful in domains of ownership, sharing data, and maintaining digital signatures. Blockchain uses the consensus mechanism to agree on the true state of a node.

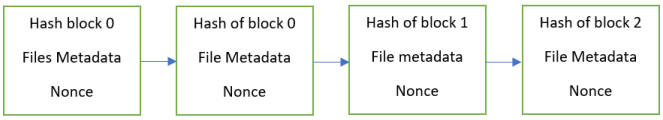

Fig -1: Blockchain structure

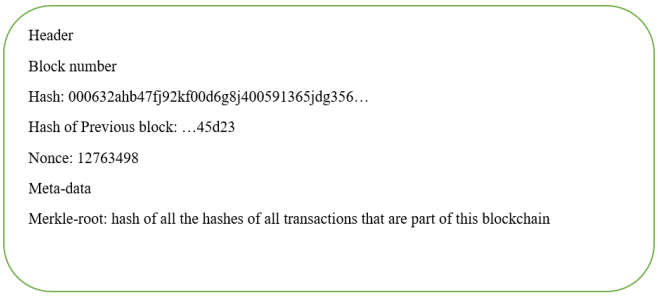

Fig -2: Block details

5. PROPOSED SOLUTION

5.1 Storing Data on Blockchain

When data is added to the blockchain, it is encrypted, making it immutable and difficult to decipher. It authorizes transactions using a personal identification key known only to the user. As a result, unlike current healthcare data technology, a healthcare provider would only be able to access a patient's medical data if they had explicit access to the blockchain record. Blockchain technology can keep patient information safe and secure while allowing them to share it with any service provider of their choice. It ensures the authenticity of anti-counterfeiting techniques and provides proof of ownership of medical records.

Users' signature is used to ensure the validity of the health data stored. All healthcare metadata can be stored in a single block for a particular patient. Generally, the blockchains are not suitable for storing large data files such as images or report files which can accompany the rest of the data. So, to overcome this a cloud storage system stores the data files and on the blockchain we can store the corresponding hash values or metadata pointing to the access of a particular file.

5.2 System Architecture

When the new data is created, a hash value will be calculated corresponding to the generated or uploaded data. We will use the hash algorithm called SHA-2. With the public key of

the owner to ensure the confidentiality of the records, metadata of the data is generated. This will help us to develop a search functionality which can be used to map the data files which will be stored in the cloud so that users with certain permissions can access those files just with the metadata which points to the file on cloud. This way we do not need to store the massive files on the chain which first of all it is not optimized for and saves a lot of additional changing of datatypes. Keys are provided to the person who has the permission to access these files. After the record files are stored on the cloud, its mapped hash value is taken and mapped to a generated id unique to the associated data with the hash value. A signature is generated for this data and then the metadata, hash values, ids and owners public address are stored in a block and appended to the blockchain network.

The use is able to get the access information of the health records from the metadata stored in the blockchain which is associated with a data file on the cloud. Using the users' signature to check the authenticity of the request and allowed permissions and decrypts the data on the cloud, effectively giving the access to the requesting user.

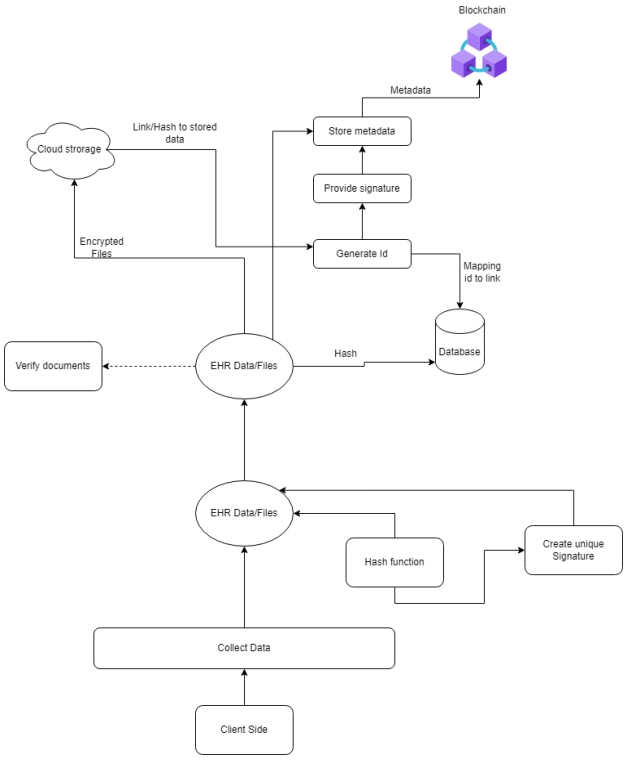

Fig -3: Data flow diagram

5.3 Development Methodology

We layout a decentralized accessed framework with the use of permissioned blockchain generation with Ethereum for Health and medical data. It eliminates the critical dependence on centralized computing assets for storing, processing and gaining access. The ensuing structure can assist in growing and promote sustainable implementations.

In the system there will be multiple datatypes which can store the essential information and provided certain access to other parts of the system. We create the data structure for storing the doctor's information, patients' information which includes the byte array of files where the hashes of the records will be stored for a patient. Next, we also have the address or public key array corresponding to the doctor's profile in the patient structure. Similarly, the doctor's structure will have an address array which will contain the patient private keys so for the doctor to use. The file structure will contain certain fields such as file name, type, hash and the metadata will be stored in the additional information about a file.

We map the address or the public key of the patient to its corresponding doctor structure profile who is currently diagnosing the patient. Another mapping is made which maps a byte32 datatype which will be the hash value of a file uploaded to the "filesInfo" data structure which contains the metadata of the file records. Some more mappings are present in the contract which maps the public keys of the user to the permissions of access to files. In the contract we first execute a constructor where the owner address is set to the address which is currently executing the contract.

Using modifiers, we verify if the user is a registered doctor or a registered patient or if the user has access to the file or not and some functions which can only be executed by the owner of the contract. They are helpful in checking if a function is being executed by the right type of user or if some predefined conditions must be checked before moving on. The contract provides the functionality to sign up a patient and a doctor. It can provide certain access to the doctor for the files. The contract allows the patients to upload files which are essential and required for the medical services. These functions are called transactional functions as when such functions are executed by the user calling the contract, the state of the contract is changed which causes the generation of a new block in the chain. Before saving the block, it has to be verified on the chain. This is done by using the proof of stake concept used in blockchain transactions.

It is consensus model which allows the updating the blocks in the chain securely. In Ethereum we can use the Proof of stake model for multiple users to reach a consensus on a particular transaction which makes it valid. POS algorithm is a development over the proof of work mechanism which does have high-cost implications.

The contract can be used to check profiles of a patient or doctor. Whenever the contract state changes in any way, a new block is created. Some functions do not need to change the state of the current contract and hence there is no transactions performed upon calling such functions on the contract. In the client side the user is give multiple options to check the permission level and accessed files via such call function on the contract like getting the file info for a patient, doctor information. While adding a file for a patient, the hash is returned using the data collected from the client side as an

input. Keccak256 is a built-in cryptographic function I Solidity, it will take any number of inputs and convert it into a 32-byte hash. This is an irreversible operation as you cannot regain the original data by converting the hash value to the original string or byte array of data. The algorithm is designed in such a way to prevent it from happening and breaching the privacy of users.

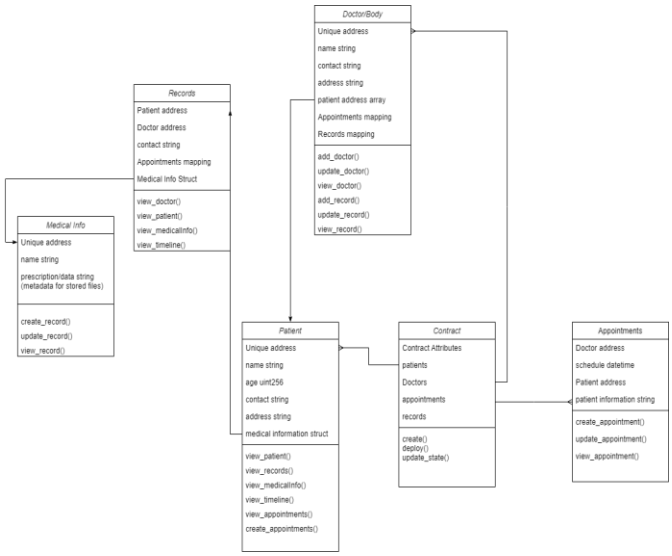

Fig -4: Entity Relationship Diagram

6. CONCLUSIONS

In this paper a blockchain based solution is approached for upgrading the current existing methods for storing and accessing the electronic healthcare records. The proposed solution considers the requirements of the health record systems and the loopholes centralized systems which are in practice. Heavy consideration is given to preserve the privacy of the health records according to medical practices followed and mentioned in associated research papers. A good quality system for storing the records which provides the non-tampering architecture and restricted access based on the permissions given to different parties is required where personal information is constantly under threat. Other requirements which pushed the development of such systems are the limited storage, synchronizing the medical records for multiple entities involved such as labs, pharmacies, hospitals, private medical professionals etc., Keeping the clear transaction logs for every change in the data to improve transparency of the system, and avoiding a central point of failure using a decentralized system.

REFERENCES

[1] Satoshi Nakamoto, 2008, "Bitcoin: A Peer-to-Peer Electronic Cash System" .

[2] Vitalik Buterin, 2014, "A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM", Ethereum White Paper .

[3] Sun J, Ren L, Wang S, Yao X, 2020, "A blockchain-based framework for electronic medical records sharing with fine-grained access control", PLoS ONE 15(10): e0239946.

[4] Ayesh Shahnaz, Usman Qamar, Ayesha Khalid, 2019. "Using Blockchain for Electronic Health Records", IEEE Access, Digital Object Identifier 10.1109/ACCESS.2019.2946373.

[5] Thein Than Thwin, Sangsuree Vasupongayya, 2019, "Blockchain-Based Access Control Model to Preserve Privacy for Personal Health Record Systems", Hindawi Security and Communication Networks Volume 2019, Article ID 8315614.

[6] Kristen N. Griggs, Olya Ossipova, Christopher P. Kohlios, Alessandro N. Baccarini, Emily A. Howson, Thaier Hayajneh, 2018. "Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring", Mobile & Wireless Health.

[7] Mohammad Moussa Madine, Ammar Ayman Battah, Ibrar Yaqoob, Khaled Salah, Raja Jayaraman, Yousof Al-Hammadi, Sasa Pesic, Samer Ellahham, 2020, "Blockchain for Giving Patients Control Over Their Medical Records", IEEE Access Volume 8, 193102-193115

[8] Cornelius C. Agbo, Qusay H. Mahmoud and J. Mikael Eklund, 2019. "Blockchain Technology in Healthcare: A Systematic Review", Healthcare 2019, 7, 56; doi:10.3390/healthcare7020056.

[9] Saqib Ali, Guojun Wang, Bebo White, Roger Leslie Cottrell, 2018,"A Blockchain-based Decentralized Data Storage and Access Framework for PingER", 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering.

[10] Suveen Angraal, Harlan M. Krumholz, Wade L. Schulz, 2017. "Blockchain Technology Applications in Health Care", American Heart Association, Inc., DOI: 10.1161/CIRCOUTCOMES.117.003800.

[11] Iansiti M, Lakhani K, 2017, "The truth about blockchain", Harvard Business Review, 2017 Jan–Feb.

[12] Khatoon, A.; Verma, P.; Southernwood, J.; Massey, B.; Corcoran, P. "Blockchain in Energy Efficiency": Potential Applications and Benefits. Energies 2019, 12, 3317

[13] Yli-Huumo, J.; Ko, D.; Choi, S.; Park, S.; Smolander, K. "Where is current research on blockchain technology?—A systematic review": PLoS ONE 2016, 11, e0163477

[14] Baliga, Arati. "Understanding blockchain consensus models." Persistent 4 (2017): 1-14.