IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Medical Supply Chain Management using Blockchain: An Overview

Pooja Thorat[1], Divya Patil[2], Vishwas Khemnar[3], Dr. Sunil Khatal[4]

Student, Computer, Sharadchandra Pawar College of Engineering, Otur, India [1 2 3]

Dr. Prof. Computer, Sharadchandra Pawar College of Engineering, Otur, India[4]

Abstract: In the last decade, blockchain technology has come into being and has gained a lot of traction in many sectors, including banking, government, energy, health, etc. This paper provides a detailed analysis of blockchain technologies in the medical field. Indeed, in this field, on-going research is advancing rapidly. We have therefore produced many state-of-the-art use cases using blockchain technology, such as the sharing of electronic medical records, remote access for patients, the supply chain of medicines, etc. In the healthcare sector, stakeholders need interoperability, security, authenticity, transparency and seamless transactions. The Internet-based blockchain technology promises to enable peer-to-peer and interoperable use of current health data using a patient-centred approach that excludes third parties. Applications for managing and exchanging safe, transparent and immutable systematic fraud audit trails can be created with this technology. In order to identify key challenges faced by different health stakeholders and to analyse the features of blockchain technology that could solve identified problems, the present study analyses existing literature. We also concentrated on finding the limitations of the approaches studied and finally discussed some open research concerns and potential areas of research. However, future studies must be focused on the concerns and disadvantages of this technology.

***Index Terms* -** Blockchain, Smart contracts, PHR (Personal Health Records), healthcare, access control.

I. Introduction

Basically the document certificate and privacy is a very essential to provide security to private information, various platform has already exist to store such a kind of large data in a secure manner. Some centralized cloud storage provides data Encryption strategies for achieve highest security for documentation. In real time large document verification is very tedious process which required much resources as well as time also. Where manual systems are has been followed by different organization since couple of years, for employee verification, student document verification as well as any other government document verification by particular agencies. Sometime industrial organizations and colleges should be verifying the students and employees documentation. This research basically eliminate such time consuming process introduce the cost of traditional existing systems.

Background of System

Blockchain: Basically blockchain is the technique which provides decentralized approach data storage for different transactional systems. Basically it is introduced to achieve the highest data security during the data transactions and eliminate various network as well as data attack from malicious requests.

Decentralization: To guarantee strength and adaptability and to wipe out many-to-one traffic streams we need a decentralized framework. Utilizing such decentralized frameworks, we can likewise take out the single purpose of disappointment or data postpone issues. In our model, we are utilizing an overlay decentralized system.

Authentication of data: User's System or cloud administrations store unpreserved information that should be moved to blockchain systems. During transmission, the information could be changed or lost. The protection of such off base altered information builds the weight to the framework and can cause the loss of the patient (demise). Along these lines, to guarantee that information isn't adjusted, we utilize a lightweight advanced mark [2] plot. On the recipient side, information is confirmed with the client's advanced mark, and whenever got effectively, it sends a receipt of information to the patient.

Adaptability: Solving Proof of Work (PoW) is computationally escalated; in any case, IoT gadgets are asset confined. Likewise, the IoT system contains numerous hubs and blockchain scales inadequately as the quantity of hubs in the system increments. We dispense with the idea of PoW in our overlay system and separation our overlay arrange into a few bunches rather than a solitary chain of squares, and in this way a solitary blockchain isn't in charge all things considered. Rather we spread the hubs more than a few groups. Our model depends on the circulated nature and other extra security properties to the system.

Data Storage:: Storing IoT huge information over blockchain isn't reasonable and in this manner we use cloud servers to store scrambled information squares. The information is protected over the cloud because of extra cryptographic security like the advanced signature and exclusive requirement encryptions which will be examined later. In any case, it might cause an issue about confided to outsiders. For this reason, we store all exchanges in various squares and make a consolidated hash of each square utilizing Merkle Tree and move it to the dispersed system. Along these lines, any adjustments in cloud information can be effectively perceivable. Doing the capacity as such likewise saves the decentralization over certain degrees.

Anonymity of users: Medical information of a patient may contain touchy data, and in this manner information must be anonymized over the system. For obscurity, we are utilizing lightweight Ring structure [2] alongside advanced marks. Ring mark enable an endorser to sign information namelessly, that is the mark is blended with different gatherings (named ring), and nobody (aside from real underwriter) knows which part marked the message.

Security of data: Medical gadgets or wellbeing information must be precise and can't be changed by programmers. To spare the information from programmers, we are utilizing a twofold encryption plot. Here twofold encryption does not allude to scrambling similar information utilizing two keys yet rather encryption of the information and again encryption of key which was utilized to encode information. We scramble the information utilizing lightweight ARX calculations and after that encode the key utilizing the open key of the beneficiary. Likewise, we are utilizing the Diffie Hellman key trade strategy to move the open keys and in this way getting the keys is practically incomprehensible for an aggressor

Digital Certificate : Digital Certificate is a one kind of document which illustrate the data into to soft format. In today's era various sections in computer science is E-certificate has used fore end uses of indication as well as private data transmission. In this work who proposed E- certificate generation for educational documents using blockchain Technology. Basically this certificate has generated by system based on automatic methodology using various secure algorithms.

II. Literature Survey

Patients have authority over their medical records thanks to blockchain [1]. Smart contracts based on the Ethereum blockchain allow patients control over their data in a decentralized, immutable, transparent, traceable, trustworthy, and safe way. To securely collect, store, and exchange patients' medical data, the proposed solution uses decentralized storage of interplanetary file systems (IPFS) and trusted reputation-based re-encryption oracles. Algorithms are presented together with complete implementation information. We assess the suggested smart contracts based on two key performance indicators: cost and accuracy. We also explore the generalisation elements of our technique and give security analysis. The suggested approach's drawbacks are outlined. On Github, we make the smart contract source code openly accessible.

IPFS [2] provides a blockchain-based secure storage and access solution for electronic medical data. We built an attribute-based encryption scheme for safe storage and efficient exchange of electronic medical records in IPFS storage environment based on the ciphertext policy attribute-based encryption system and IPFS storage environment, paired with blockchain technology. Our method is based on ciphertext policy attribute encryption, which effectively regulates access to electronic medical data while maintaining retrieval efficiency. Meanwhile, we store encrypted electronic medical data in the decentralized Interplanetary File System (IPFS), which not only provides storage platform security but also eliminates the single point of failure concern. Furthermore, we use blockchain technology's non-tamperable and traceable characteristics to enable safe storage and search for medical data. Our approach delivers selective security for pick keyword assaults, according to the security proof. Our approach is efficient and viable, according to performance analysis and actual data set simulation studies.

Blockchain technology is being used to handle health records [3]. a patient-centered, entirely decentralized strategy that can detect data theft, prevent data modification, and gives patients control over access. Blockchain technology is the most effective way to solve all issues and meet all demands. As a decentralized and distributed ledger, blockchain has the potential to affect billing, record sharing, medical research, identity theft, and financial data crimes in the future. Smart contracts in health care may help to simplify things even further. On the Blockchain, invocation, record generation, and validation will all take place. on a patient-driven model of record maintenance based on Blockchain technology, with smart contracts to be added in the future, allowing for more data sharing possibilities. Finding its vast reach, I hope that additional study will be conducted and actual applications will be realised.

A medical data exchange and protection method based on blockchain[4]. To enhance the hospital's electronic health system, a medical data exchange and protection strategy based on the hospital's private blockchain was developed. For starters, the system may meet a variety of security requirements, including decentralisation, openness, and tamper resistance. Doctors will be able to retain medical data or retrieve patient history data via a secure approach that respects their privacy. A symptom-matching technique is also provided between patients. It enables patients who have the same symptoms to complete mutual authentication and generate a session key for future disease communication. PBC and OpenSSL libraries are used to implement the suggested approach.

HealthyBlock is a blockchain-based IT architecture for electronic medical records that is resistant to network outages. [5]. a patient, posing a direct danger to the person and resulting in large public health expenses for governments. The creation of electronic medical record (EMR) systems using blockchain networks is one of the proposed solutions to this problem; however, most of them fail to account for the occurrence of connectivity failures, such as those found in various developing countries, which can lead to data integrity failures. To address these issues, Healthy Block is described in this paper as a blockchain-based architecture that proposes a unified electronic medical record system that takes into account multiple clinical providers, has data integrity resilience during connectivity failure, and has usability, security, and privacy characteristics. A prototype for patient care in a network of hospitals was developed based on the Healthy Block architecture. The evaluation's findings revealed a high level of efficiency in maintaining patients' EMRs unified, updated, and secure, regardless of which network healthcare provider they contact.

[6] A blockchain-based personal health record sharing system with certified data integrity. A novel blockchain-based personal health record sharing system with certified data integrity. The new scheme uses searchable symmetric encryption and attribute-based encryption techniques to achieve privacy protection, keyword search, and fine-grained access control in the process of personal health record sharing, addressing the problems of privacy disclosure, limited keyword search ability, and loss of control rights. In comparison to other comparable methods, the new approach enables patients to give attribute private keys to users, eliminating many of the security issues that the scheme's attribute authority causes. Furthermore, the new scheme manages keys in the scheme using blockchain, reducing the single point of failure concern associated with centralised key management. The new technique, in particular, maintains the hash values of encrypted personal health information in blockchain and the corresponding index set in a smart contract, which may boost data integrity verification efficiency even further.

An efficient consortium blockchain for the exchange of medical data [7]. a new business approach for exchanging medical data and a blockchain-based platform Our solution takes use of the benefits of blockchain in the recording and exchange of medical data. The distributed network's participants may store, exchange, and reliably verify information. A novel consensus method and a universal anonymous sharing mechanism are also proposed. These techniques improve the efficiency and security of medical data exchange among users. To avoid manipulation and fraud, both the information and the traces of the transaction may be maintained in a dispersed manner in this fashion.

For improved privacy, scalability, and availability, blockchain is being used to retain patient information in electronic health records [8]. consortium blockchain to create a distributed system using existing EHRs utilizing Hyper ledger Fabric. The address of a patient record in an EHR is recorded on the same ledger held by peer nodes. Individual patients are recognized by one-of-a-kind certificates issued by local certificate authorities who operate together in a network channel. When transferring data, we employ a proxy re-encryption mechanism to preserve a patient's privacy. We created and implemented a number of chain codes to handle business logic that was agreed upon by the network's member organizations.

In healthcare, a poll on blockchain-based self-sovereign patient identification [9]. Blockchain (BC)-based self-sovereignty and patient data records in healthcare are at the cutting edge. Our objective is to look into the possibilities of using BC technology in patient data and identity management. BC may be particularly advantageous as a distributed decentralized technology, providing patients ownership over their own data and self-sovereign identification. To the best of our knowledge, no literature exists that addresses the same issues. More particular, solutions aimed at realizing comprehensive BC-based Electronic Health Records (EHR) and Patient Health Records are the emphasis (PHR). EHR and PHR are used to keep track of patient information such as doctor's notes and radiological pictures. As a result, they include crucial information on the patient's privacy and identity. As a result, in terms of architectural and technological framework, developing pure decentralized Healthcare Information Systems (HIS) is a significant problem. Designing a strong and dependable EHR and PHR, which serve as the basis for a variety of other healthcare services, requires carefully balancing a number of aspects, including decentralisation, privacy, scalability, and data throughput.

Using blockchain to protect the privacy of electronic health records [10]. a way to use blockchain technology to build EHRs and make them more safe and private. Using cryptographic methods and decentralisation, blockchain technology will maintain control over information access. It will also strike a balance between data security and data accessibility. This project's major goal is to frame data privacy and security challenges in electronic healthcare

III. Proposed System

This system highlights the implementation of e-transaction using blockchain for such a proposal from a practical point view in both development/deployment and usage contexts. Concluding this work is a potential roadmap for blockchain technology to be able to support complex applications. Building an electronic transaction system that satisfies the legal requirements of legislators has been a challenge for a long time. Distributed ledger technologies are an exciting technological advancement in the information technology world. Blockchain technologies offer an infinite range of applications benefiting from sharing economies. This paper aims to evaluate the application of blockchain as service to implement distributed electronic transaction systems.

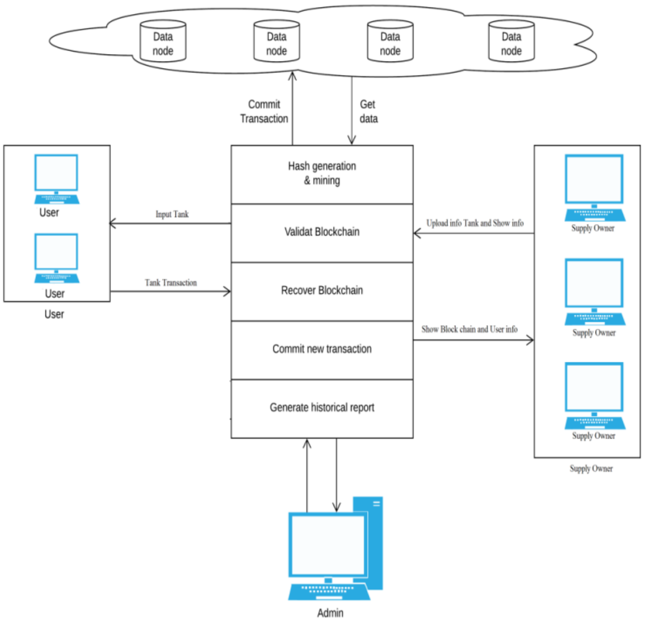

Figure 1.1: Proposed System Architecture

Module Description

Admin (Company):- A Company is first entity in medicine supply chain, first one to invoke smart contract for trading.

Supply Group: The maintains warehouse by (processing, storing & managing) supply of goods from producers & certification

of various product standards & authentication regarding quality.

User's Group: Purchasing Medicine products from a supplier.

Distributed Block chain: The Blockchain is the distributed ledger used to represent the current state of delegated access rights

in the system. Permissions to interact with the Blockchain are handled by the Root Authority and the Attribute Authorities.

Results Generation

- The central outline of the proposed algorithm is the implementation of sup- ply chain management distribution data storage using block chain.
- System creates the trustworthy communication between multiple parties without using any third party interface.
- We use the Hash generation algorithm and the Hash will be generated for the given string.

- Before executing any transaction, we use peer to peer verification to validate the data.
- If any chain is invalid then it will recover or update the current server blockchain.
- This will validate till the all nodes are verified and commit the query.
- Mining algorithm is used for checking the hash generated for the query till the valid hash is generated.

IV. Algorithm Design

```
Algorithm 1: Hash Generation
Input: The "Genesis block" refers to the first block in a blockchain. "Previous hash" is the cryptographic hash of the previous block in the chain. “Plain text data d" represents the information stored in a block.
Output: Created a cryptographic hash, denoted as H, based on the provided data.
Step 1:  Enter the input as plain text, and assign it to variable D_plain_text.
Step 2: Utilize the SHA 256 algorithm from the SHA-256 family.
Step 3: Current Hash_Values= SHA256(d)
Step 4: Return Current Hash_Values
Algorithm 2: Protocol Peer-to-Peer Verification
Input: The user is provided with the IP address and the transaction ID.
Output: Activate the IP address or current query if there is a valid connection.
Step 1: For the purpose of generating a few transactions (DDL, DML, or DCL), kindly add a query.
Step 2: Retrieve the present Internet Protocol (IP) address
For each (read IP_values into IP address)
If (connection (IP_values) equals (true))
Flag_values true
Else
Flag_values false
End for
Step 3 : if (Flag == true)
Peer-to-peer verification works as intended.
Else
Peer to Peer Verification is not valid.
End if
End for
Algorithm 3: Mining Algorithm for valid hash creation
Input: The user transaction query represents the current node chain as CNode[chain], while Nodes-Chain[Nodeid][chain] represents the remaining nodes in the blockchain.
Output: If a chain turns out to be invalid, try to recover it; if not, continue with the current query.
Step 1: Please provide a query to generate transaction data.
Step 2: Retrieve the most up-to-date blockchain of the server.
    Current_chain ← Current_node [Chain data]
Step 3: For each
            $NodesChain\ [Treancation\_id, Chain] = \sum_{bc=1}^{n} (GetChain)$
    End for
Step 4: For each (read BL into Nodes_Chain)
  If(! Equals NodeChain [bc] with (Current_chain))
                Flag 1
Else Carry on Commit query
Step 5: if (Flag == 1)
   Similar_Values = SimilaryNodesBlockchain ()
Step 6: Calculate the server's majority ratio. Restore invalid blockchain data to designated nodes.
 Step 7: End if
           End for
Algorithm 4: An algorithm for creating a valid hash
Input: The current hash values, hash_Val, are being validated according to the Hash Validation Policy P[].
Output: Valid hash values
Step 1: The system utilises Algorithm 1 to create the hash value for the ith transaction.
Step 2: if (Hash_Values.valid with Plan_Text[])
            Valid hash
             Flag =1
Else
         Flag=0
           Mine over randomly
Step 3: Return valid hash when flag=1
```

IV. RESULTS AND DISCUSSION

4.1 Results

In the results section, we assess the effectiveness of both sections by employing the recommended classification approach to quantify the efficiency of blockchain execution and the precision in identifying fake news. The device runs on an Intel(R) Core(TM) i3-2328M CPU @ 2.20GHz and has 4 GB of RAM. The system employs a distributed architecture on the Java-based 3-tier analytics platform. We obtained the Liar dataset from the website www.kaggle.com to use in a limited implementation. Figure 2 depicts the duration required to reach a consensus by utilizing Proof of Work (PoW) to authenticate the blockchain across at least 4 nodes. In order to verify the results, we carried out an initial empirical investigation on the implementation of the blockchain.

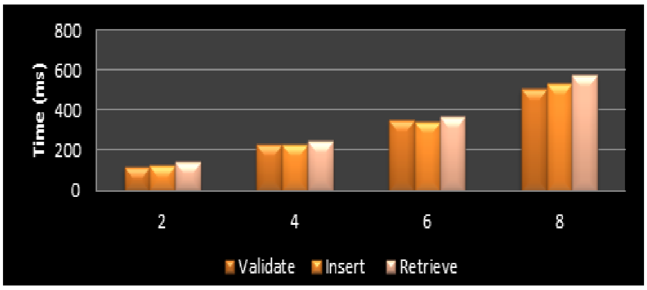

Figure 2: Duration of transactions and number of transactions processed by a blockchain

In the following experiment, we will assess a system that incorporates smart contract validation for a certain consensus technique. This evaluation will be conducted using varying numbers of data nodes inside a peer-to-peer environment.

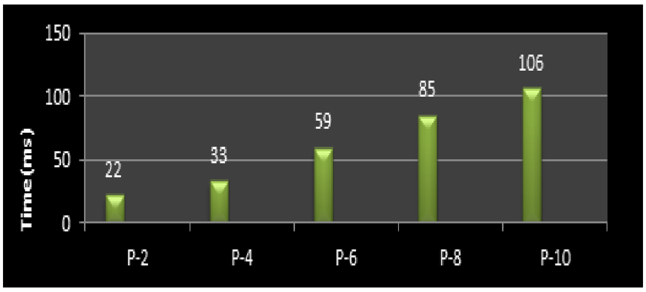

Figure 3: The blockchain necessitates a certain amount of time to authenticate smart contracts across many peer-to-peer networks.

The analysis explicitly evaluates the total level of variability that arises from the proposed SHA value in the third test instance. The objective was to authenticate the proposed hash sequence in accordance with the specified mining methodology. The system frequently ignores the computing policy while generating a SHA-256 code for the given transactional data. To adhere to the mineral extraction policy, it is crucial to generate several iterations of the text sequence that are tailored to the specific mining conditions. Figure 4 illustrates the time required to create the accurate SHA-256 string for individual transactions. The blockchain necessitates a certain amount of time to authenticate smart contracts across many peer-to-peer networks.

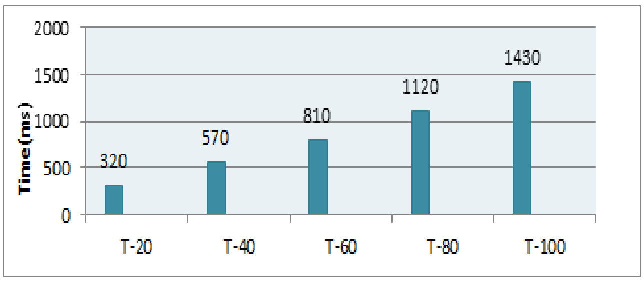

Figure 4: Duration needed to generate a valid hash for a given amount of transactions

The provided data illustrates the time required to generate valid hashes for different transactions, depending on the specified smart contracts. The production of a valid hash is sometimes contingent upon the algorithm's complexity and the processing environment. A smart contract uses the maximum nonce to generate a valid hash when it encounters more challenges.

V. Conclusions

Because of the complexities of this area and the need for more stable and efficient information management frameworks, there are several research directions to apply Blockchain technology to the transaction industry. In several cases of transaction usage that face similar data exchange and communication problems, an interoperable architecture will certainly play a significant role. Further research on safe and efficient software practise for the use of Blockchain technology in transactions is also required to educate software engineers and domain experts on the potential and also limitations of this new technology, whether to build a decentralised application using an established Blockchain. The algorithm has chosen the acceptable complexity, efficiency and complexity of implementation to operate the system. Through empirical studies, we have a better understanding of the pace of knowledge creation in the supply chain. There are several important hurdles to getting on the blockchain reaching its full potential and applying it to health is the most important issue technology scalability and data controls.

References

[1] [1] Madine, Mohammad Moussa, et al. "Blockchain for giving patients control over their medical records." IEEE Access 8 (2020): 193102-193115.

[2]Sun, Jin, et al. "Blockchain-based secure storage and access scheme for electronic medical records in IPFS." IEEE Access 8 (2020): 59389-59401.

[3]Harshini, V. M., et al. "Health record management through blockchain technology." 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI). IEEE, 2019.

[4] Liu, Xiaoguang, et al. "A blockchain-based medical data sharing and protection scheme." *IEEE* Access 7 (2019): 118943-118953.

[5] Gutiérrez, Omar, et al. "HealthyBlock: Blockchain-Based IT Architecture for Electronic Medical Records Resilient to Connectivity Failures." International Journal of Environmental Research and Public Health 17.19 (2020): 7132.

[6] Wang, Shangping, Dan Zhang, and Yaling Zhang. "Blockchain-based personal health records sharing scheme with data integrity verifiable." *IEEE Access* 7 (2019): 102887-102901.

[7] Du, Mingxiao, et al. "An optimized consortium blockchain for medical information sharing." *IEEE Transactions on Engineering Management* (2020).

[8] Tith, Dara, et al. "Application of blockchain to maintaining patient records in electronic health record for enhanced privacy, scalability, and availability." *Healthcare informatics research* 26.1 (2020): 3-12.

[9] Houtan, Bahar, Abdelhakim Senhaji Hafid, and Dimitrios Makrakis. "A survey on blockchain-based self-sovereign patient identity in healthcare." *IEEE Access* 8 (2020): 90478-90494.

[10] Sharma, Yogesh, and B. Balamurugan. "Preserving the privacy of electronic health records using blockchain." *Procedia Computer Science* 173 (2020): 171-180