ISSN:0975-9646

Medical Supply Chain Management using Block Chain

Shalaka S. Wagh[1]

Student, Department of Computer Network Engineering, Smt. Kashibai Navale College of Engineering, Off Sinhgad Rd, Vadgaon (Bk),Pune-411041 , India

Email Id:shalakawagh24@gmail.com

Poonam N. Railkar[2]

Department of Computer Engineering, Smt. Kashibai Navale College of Engineering, Off Sinhgad Rd, Vadgaon (Bk),Pune-411041, India

Email Id:poonamrailkar@gmail.com

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.

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.

II. Background of System

A. *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.

B. *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.

C. *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.

D. *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.

E. *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.

F. *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.

G. *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

H. *Digital Certificate:* Digital Certificate is a one kind of document which illustrate the data into too 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.

III. Literature Survey

A.G. Said et. al. [1] proposed a system authentication System Using Blockchain In short, the program's purpose is: a valid registry with electronic certificates, i.e. an electronic credential is generated at the applicant's request. At the same time, that student's record is preserved by using hash values in blockchain blocks. The customer is also presented with a particular QR code or serial number, in accordance with the E-certificate. And instead the demand unit (e.g. company to which the applicant has applied for a job) must verify the authenticity of the electronic file using the QR code or the relevant serial number based on the reported details in the blockchain

Jiin-Chiou Cheng et. al. [2] proposed a system Blockchain and smart contract for digital certificate, then build an electronic paper document file that follows those related details into the database and thus decides the hash value of the electronic file. Finally, the hash value within the ring is stored in the chain process. To be affixed to the paper credential, the software will produce a related QR code and question string data. It will involve the demand device for paper certificate validity verification via mobile phone scanning or web site inquiries. Since of the blockchain's unchangeable property, the network not only increases the credibility of unique paper-based certificates but also the authentication risks of various types of certificates electronically types of certificates

Marco Baldi et. al. [3] Certificate Validation The program solves the problem through Shared Ledgers and Blockchain's by introducing a mechanism in which several CAs share a transparent, shared and stable database where CRLs are received. To this end, we find the concept of blockchain-based shared ledgers implemented for use of cryptocurrencies, which is becoming a common solution for many web applications of high protection and reliability requirements.

Oliver et. al. [4] illustrates Using blockchain as a Government degree tracking and assessment tool: a business analysis based on two financial factors comparing the service price as the main players between the customer and the employer. Students need a low-cost and easy-to-check evidence of competence, and employers also need swift and accurate documentation of their degree before recruiting. All models are built for growing regional markets and shares to discover ways of extending this sector in the European Union.

Because of the arbitrary existence of hashing is never a guarantee of producing an appropriate object. Thus, Bitcoin mining is a competitive enterprise where miners are effectively hashed and admitted into the blockchain by awarding new Bitcoin for each block [5]. Miners, a collaborative consumer network, verify and check transactions and set up specialized computation equipment called "hashes." They vote with their CPU strength, demonstrating their approval of legitimate blocks by working to expand them and by declining to operate on invalid blocks [6]. These record strings (hashes) that keep track of any Bitcoin transaction and are repeated on any device in the Bitcoin network.

Blockchain is a decentralized LEDGER used for safe trading of digital currencies, deals and transactions [7], and peer-to-peer network management. All nodes adopt the same internode contact protocol, and verify new objects. If the data is validated in every block no block will change it. To modify individual block data, all corresponding block data will be modified, resulting in network cooperation and denial of the transaction by all nodes. The power used to "farm" the cryptocurrency is a key aspect since its costs are rising.

According to the Bitcoin statistics site Digiconomist, citizens worldwide use more than 30 terawatts-hours of electricity are mining the crypto-currency. This is greater than, at least, the human energy use 159 countries like Hungary, Oman, Ireland, and Lebanon [8].

Bitcoin mining is a Creation of new Bitcoin process by verifying Bitcoin Network transactions. That transaction is stored in a shared ledger, and all of the machines involved in the Bitcoin network check and manage the ledger. This "net" of transactions is known as the ledger, and. transaction is basically a timestamp for the database that may involve data [9]. Narayanan et al. [10] describe a block string as a data structure composed of a related array of hash pointers. Every entity in the list is a block containing some previous block data and hash. This renders it a tamper-evident file, implying the data can only be applied to the list and the prior data cannot be changed without detection.

Hyper ledger Saw tooth employs a flexible design, which distinguishes different sections of the device. This means the degree of blockchain is decoupled from stage of implementation. The flexible architecture often ensures that it is possible to modify various elements of the network, based on the project requirement. Examples of the modules that can be modified involve transaction laws, making and consensus algorithm. [11] Lamport et al. [12] present algorithms under different circumstances that let the generals reach consensus. In a structure where the generals can send recorded, unforgeable letters, the writers illustrate that the dilemma can be solved with any number of generals and traitors. Nonetheless, because of the huge number of communications this approach would be very costly necessary.

Proof of elapsed time (PoET) is a Built consensus approach to be more effective than PoW. PoET can be seen as a function which makes a node wait randomly. In a "trusted execution setting" the feature to determine the amount of time a node should wait this helps the system to identify any users who try to function until their random time elapses. [13]

A distributed ledger, or a website, they have a global environment. The global state is all the material that is contained in the ledger, including the present status. The knowledge used in the global state differs considerably depending on the context of blockchain. [14]

In Hyper ledger Saw tooth, and for other blockchain applications, the transactions are put in batches. Batches are used where transaction order is important. The transactions should be done in the right order by placing certain transactions in the same set. If a transaction does not rely on every other transaction than those that have already been authenticated and deposited in the blockchain, the sender may build a new batch only for that transaction. [15].

IV. 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.

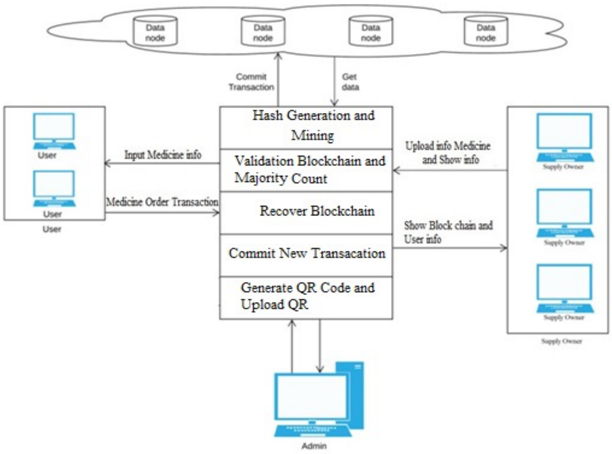

Figure 1.1: Proposed System Architecture

- The central outline of the proposed algorithm is the implementation of supply 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.

V. Proposed Algorithms

Algorithm 1: ***Hash Generation***

```
Input: Genesis block, previous hash, data d,
Output: Generated hash H according to given data
Step 1:  Input data as d
Step 2: Apply SHA 256 from SHA family
Step 3: Current Hash= SHA256 (d)
Step 4: RetrunCurrentHash
```

Algorithm 2: ***Protocol for Peer Verification***

```
Input: User Transaction query, Current Node Chain CNode [chain], Other Remaining Nodes blockchain Nodes Chain [Nodeid] [chain],
Output: Recover if any chain is invalid else execute current query
Step 1: User generate the any transaction DDL, DML or DCL query
Step 2: Get current server blockchain
        Cchain ←Cnode [Chain]
Step 3: For each
      $NodesChain\ [Nodeid, Chain] \sum_{i=1}^{n} (GetChain)$
   End for
Step 4: For each (read I into NodeChain)
        If (!.Equals Node Chain[i] with (Cchain))
            Flag 1
Else Continue Commit query
Step 5: if (Flag == 1)
      Count = SimilaryNodesBlockchian ()
Step 6: Calculate the majority of server
        Recover invalid blockchain from specific node
 Step 7: End if
        End for
        End for
```

*Algorithm 3: **Mining Algorithm for valid hash creation***

```
Input: Hash Validation Policy P[], Current Hash Values hash_Val
Output: Valid hash
Step 1: System generate the hash_Val for ith transaction using Algorithm 1
Step 2: if (hash_Val.valid with P[])
        Valid hash
         Flag =1
Else
      Flag=0
Mine again randomly
Step 3: Return valid hash when flag=1
```

VI. Result and Discussions

Calculate the matrices for consistency in the device output assessment. The machine runs in a distributed environment on a java 3-tier architecture platform with an INTEL 2.4 GHz i3 processor and 4 GB RAM. The time required for a consensus algorithm to validate the blockchain in four nodes is shown in Figure 2. In evaluate the number of variations derived from the proposed SHA256 value by the algorithm. Basically, the aim of this experiment was to see whether the proposed hash string was correct or not in terms of a given mining policy. When the system produces SHA256 codes for given transaction data, it often fails to follow the mining policy. To enforce the proposed mining policy in accordance with the provided scenario mining in order to generate multiple variations on a given string. Figure 2 shows the time it takes to produce a correct SHA string for a specific transaction in milliseconds.

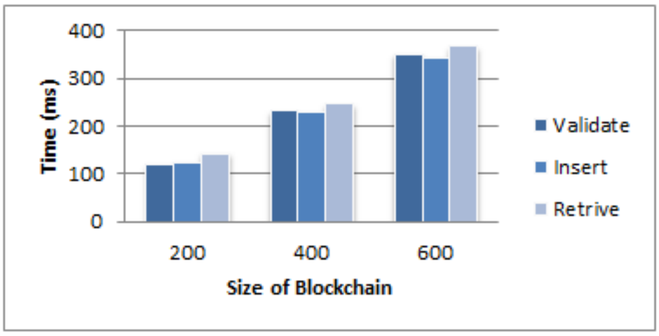

Fig.2.Time required (in milliseconds) for complete transaction with different records blockchain using 4 data nodes in P2P Network

In Figure 3, we evaluate the proposed system with smart contract validation by consensus algorithm in a different number of peer to peer nodes

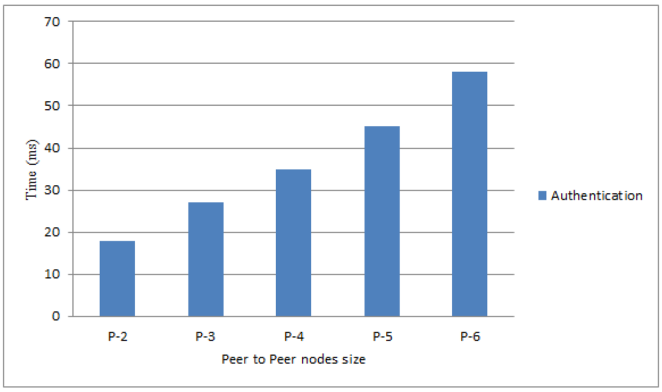

Figure 3: Time required for smart contract validation with different no. of P2P network in the blockchain

VII. 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] A.G. Said, R.P. Ashtaputre, B. Bisht, S.S. Bandal, P.N. Dhamale, "*E-Certificate Authentication System Using Blockchain*," International Journal of Computer Sciences and Engineering, Vol.7, Issue.4, pp.191-195, 2019.

[2] Cheng JC, Lee NY, Chi C, Chen YH. "*Blockchain and smart contract for digital certificate.*" In2018 IEEE international conference on applied system invention (ICASI) 2018 Apr 13 (pp. 1046-1051). IEEE.

[3] Baldi M, Chiaraluce F, Frontoni E, Gottardi G, Sciarroni D, Spalazzi L. Certificate Validation Through Public Ledgers and Blockchains. InITASEC 2017 (pp. 156-165).

[4] Oliver M, Moreno J, Prieto G, and Benítez D. "*Using blockchain as a tool for tracking and verification of official degrees: business model*".

[5] George F. Hurlburt and Irena Bojanova, "*Bitcoin: Benefit or Curse?*" in IEEE, 2014

[6] Satoshi Nakamoto, "*Bitcoin: A Peer-to-Peer Electronic Cash System*", 2008, White Paper.

[7] Nirmala Singh and Sachchidanand Singh, "*Blockchain: Future of financial and cyber security*," in IEEE, Noida, 2016.

[8] Henrique Rocha, Marcus Denker and Stephane Ducasse Santiago Bragagnolo, "*SmartInspect: solidity smart contract inspector*," in IEEE, Itly, p. 2018.

[9] GWYN D'MELLO. (2017, Dec.) https://www.indiatimes.com/technology/news. [Online]. https://www.indiatimes.com/technology/news/bitcoin-miners-are-using-more-electricity-than-irelandother-159-countries-no-kidding-335114.html

[10] Narayanan A., Bonneau J., Felten E., Miller A. & Goldfeder S. (2016) "*Bitcoin and Crypto currency Technologies: A Comprehensive Introduction. Princeton: Princeton University Press*"

[11] *"Introduction to Hyper ledger Saw tooth"* (2018) Retrieved January 4, 2019 from https://sawtooth.hyperledger.org/docs/core/releases/latest/introduction.html) 49

[12] Lamport, L., Pease, M., & Shostak, R. (1982). "*The Byzantine general's problem. Menlo Park*", CA: SRI International.

[13] PoET 1.0 Specification (2018) Retrieved January 4, 2019 fromhttps://sawtooth.hyperledger.org/docs/core/releases/latest/architecture/poet.html

[14] Global State (2018) Retrieved January 4, 2019 from https://sawtooth.hyperledger.org/docs/core/releases/latest/architecture/global_state.ht ml

[15] Transaction and Bathces (2018) Retrieved January 4, 2019 from https://sawtooth.hyperledger.org/docs/core/releases/latest/architecture/transactions_and_batches.html