Medical Supply Chain Management using Blockchain: An Overview

Prashant Sadaphule[1], Pratiksha Munot[2], Ritu Narayani[3], Rachana Ghodke[4], Snehal Ghodke[5]

Department Of Computer Engineering, Savitribai Phule Pune University

[1] prashant.sadaphule@aissmsioit.org

[2] pratikshamunot99@gmail.com

[3] ritunarayani654@gmail.com

[4] ghodkerachana44@gmail.com

[5] snehalghodke2000@gmail.com

Abstract

Blockchain technology has been developed over the past decade in various industries, including banking, government, energy, health, etc., and has gained significant traction. This paper offers a detailed description of medical blockchain technology. In reality, ongoing research in this field is progressing rapidly. We have thus created many modern cases of use of blockchain technology, including electronic medical records sharing, remote patient access, the medical supply chain, etc. Stakeholders in the fields of medical services need to be interoperable, secure, authentic, accountable and seam-free. The Internet-based blockchain platform aims to allow peer-to-Peer and interoperable use of current health data using a patient centered approach that excludes third parties. This technology allows applications to be built to manage and share systemic fraud audit trails that are secure, transparent and immutable. This research analyzes current literature to identify major challenges facing different health workers and to assess the features of blockchain technology that could solve problems identified. We also concentrated on finding the limitations of the approaches examined and eventually addressed open-ended study and further areas of research. However, future research needs to focus on the challenges and disadvantages of this technology.

Keywords— *Supply Chain Management, Blockchain Technology, Smart Contract, Distributed Ledger, Business Process Re-engineering*

I. INTRODUCTION

Basically, to provide private information with security, the document certificate and privacy is a very important thing, there have already been various platforms to store such a type of large data in a secure way. To achieve the highest documentation efficiency, data encryption techniques are supported by certain centralized cloud storage. Real-time verification of big documents is a very tedious process that takes a lot of resources as well as time. Student document verification as well as any other government document verification by various agencies for employee verification, where manual procedures have been practiced for a few years by different organizations. Students and employees' documents can sometimes be reviewed by industrial organizations and universities. This research effectively eliminates the cost of certain time-consuming procedures of traditional current systems.

Blockchain: Blockchain is fundamentally a technique that provides data storage with a decentralized method for different transactional processes. Basically, it is introduced during data transactions to achieve the highest data security and remove malicious requests from various networks as well as data attacks.

Decentralization: To guarantee power and adaptability and wipe out many-to-one traffic sources, we need a decentralized framework. Using such decentralised systems, we can also take out the single goal of frustration or data postponement issues. In our model, we use a decentralised overlay system.

Data Authentication: In the user system or cloud management, unpreserved information that should be passed to blockchain networks is stored. During transmission, the data can be altered or lost. The protection of such information altered off base builds the system's weight and can cause the patient to lose weight (demise). To ensure the data is not altered, we use a lightweight advanced mark [2] plot along these lines. Information is verified with the advanced client mark on the receiver side, and it gives the patient a receipt of information if it succeeds.

Adaptability: Computationally escalated job proof (PoW) is solved; in any event, IoT gadgets are asset-limited. Likewise, as the amount of hubs in the system increases, the IoT system requires several hubs and blockchain scales inadequately. We dispense with the idea of PoW in our overlay scheme and break our overlay into a few bunches rather than a solitary chain of squares, so a solitary blockchain is not liable for all considered material. Instead, over more than a few schools, we spread the hubs. Our model is based on the system's distributed nature and other additional security properties.

Data Storage: Via blockchain, it is not fair to store big IoT information and we use cloud servers to store scrambled data squares in this way. The data is protected over the cloud because of extra cryptographic security such as the advanced signature and exclusive prerequisite encryptions that will be checked later. In any case, it can lead to a problem of trusting outsiders. For this reason, we store all exchanges in different squares using the Merkle Tree and make a consolidated hash of each square and move it to the dispersed scheme. Along these lines, certain improvements in cloud data can be seen easily. Doing the skill as such also saves those decentralisation degrees.

Consumer Anonymity: The medical records of a patient can include touchy details, and in this way, information must be anonymize through the system. Along with advanced marks for obscurity, we use the lightweight ring structure[2]. The ring mark allows an endorser to sign information namelessly, i.e. the mark is mixed with multiple meetings (named ring), and no one knows which part of the message is signed (apart from actual underwriter).

Data Security: Health gadgets or well-being knowledge must be correct and cannot be changed by programmers. To save the data from programmers, we use a double encryption map. Double encryption here does not refer to the use of two keys to scramble similar information, but rather to the encryption of information and key encryption used to encode information. The information is scrambled using lightweight ARX calculations and the key is then encrypted using the recipient's open key. We often use Diffie Hellman's key trade strategy to move the open keys since it is practically incomprehensible for an aggressor to get the keys this way.

Digital Certificate: A single form of document is a digital certificate that is too soft to clarify the specifics. In various parts of computer science in today's era, E-certificate has used advanced end uses of indication as well as private data transfer. In this work, who suggested the generation of E-certificates using blockchain technology for educational documents. Basically, via a framework based on automated methodology, this credential was generated using different stable algorithms.

II. Literature Survey

The A.G. Said to et. Al. [1] Proposed system authentication system Using Blockchain for short, the purpose of the programme is to: establish a valid electronic certificate registry, i.e., at the request of the applicant, generate an electronic credential. At the same time, the record of that student is preserved by the use of hash values in blockchain blocks. The customer is also issued with a specific QR code or serial number in conjunction with the E-Certificate. Instead, the demand unit (e.g. the company to which the applicant has applied for a job) must, on the basis of the details reported in the blockchain using the QR code or the related serial number, verify the authenticity of an electronic file.

Cheng Jiin-Chiou et. Al. [2] A digital certificate system Blockchain and smart contract were proposed, then an electronic paper record file was created to follow the relevant information into the database and thus decide the hash value of the electronic file. Lastly, the hash value within the ring is stored in the chain process. In order to be affixed to the paper credential, the programme will generate a related QR code and query string information. The demand unit will be included for paper certificate validity verification by cell phone scanning or website inquiries. The network not only strengthens the credibility of unique paper-based certificates as the unchanging property of the blockchain, but also the authentication risk of electronic certificate forms of various types of certificates.

And Marco Baldi et. Al. [3] Certificate Validation The software solves the problem through Shared Ledgers and Blockchains through the implementation of a mechanism in which several CAs share a free, shared and protected database where CRLs are obtained. To this end, we see the principle of decentralised blockchain-based ledgers used for the use of cryptocurrencies, which for many web applications is becoming a common solution for high security and reliability requirements.

About Oliver et. Al. [4] It illustrates the use of blockchain as a government degree tracking and assessment mechanism: a price comparison based on two financial factors comparing the cost of the service as the main player between the consumer and the employer. Students need low-cost and easy-to-check evidence of competence, and employers also need quick and accurate verification of their degree prior to hiring. Both models are planned to discover ways of expanding this sector in the European Union with a view to growing regional markets and shares.

Due to the arbitrary nature of hashing, hashing is never a guarantee of producing a suitable entity. Consequently, Bitcoin mining is a competitive business where miners are hashed and effectively admitted into the blockchain by awarding fresh Bitcoin for each block [5]. Miners, a collective network of users, verify and monitor transactions and set up specialized computing equipment called "hashes." They vote with their CPU power, showing their approval of legitimate blocks by working to expand them and refusing to operate on illegitimate blocks [6]. These record strings (hashes) that keep track of any bitcoin transaction and are repeated on any machine on the Bitcoin network.

Blockchain is a decentralised LEDGER used for the secure exchange and control of the peer-to-peer network of digital currencies, transactions and deals [7]. All nodes are accompanied by the same internode interaction protocol and new objects are tested. In any block, no block can alter it if the information is validated. In order to change individual block data, all related block data will be changed, resulting in network cooperation and rejection of the transaction by all the nodes. As its costs rise, a key factor is the electricity used to "farm" the cryptocurrency. The crypto-currency is mined by individuals worldwide using more than 30 terawatt-hours of energy, according to the Bitcoin statistics website Digiconomist. This is greater than at least 159 nations using human capital, such as Hungary, Oman, Ireland and Lebanon [8].

A new Bitcoin process generated by verifying transactions from the Bitcoin Network is Bitcoin mining. The transaction is held in a shared ledger and all of the computers involved in the Bitcoin network verify and manage the ledger. This "net" of transactions is known as the ledger, and. The transaction is essentially a timestamp for a database which can contain data [9]. A block string is defined as a data structure composed of a linked sequence of hash pointers by Narayanan et al. [10]. Any entity in the list is a block containing any prior block data and hash. This makes it a tamper-evident file, meaning that data can only be added to the list and previous data cannot be changed without detection.

Hyperledger Sawtooth, which separates different parts of the device, uses a versatile design. This means the stage of the blockchain is decoupled from the process of execution. The flexible architecture also means that various elements of the network can be modified, depending on the project requirement. The algorithm for transaction laws, making and consensus contains examples of modules that can be changed. [11] Lamport et al. [12] present algorithms in various circumstances that enable the generals to reach consensus. With any number of generals and traitors in a system where the generals can send recorded, unforgivable letters, the writers show that the issue can be solved. Nonetheless, the vast number of interactions would make this strategy very costly.

Proof of elapsed time (PoET) is a workaround for a built consensus to be more powerful than PoW. PoET can be seen as a function which makes a node wait randomly. In a "trusted execution setting" the role to determine how long a node should wait allows the system to detect any users who are trying to run until their random time elapses. [13]

They have a global climate, a library that is distributed, or a website. The global state is all the data that is contained in the ledger, including the current status. The information used in the global state differs considerably depending on the context of the blockchain. [14]

In Hyper ledger Sawtooth, the transactions for other blockchain applications are installed in batches. Batches are used where transaction order is important. Transactions should be carried out by placing certain transactions within the same set of transactions, in the correct order. If a transaction does not rely on transactions other than those already authenticated and stored in the blockchain, only a new batch can be created for that transaction by the sender. [15]

III. Proposed System

From a functional point of view, this system illustrates the implementation of public using blockchain in both innovation and utilization contexts for such a proposal. A future roadmap for blockchain technology to be able to support complex applications is to complete this work. For a long time, creating an electronic payment system that meets legislators' legal requirements has been a challenge. In the digital world, distributed ledger systems are an exciting technical development. An endless number of applications benefiting from shared economies are provided by blockchain technologies. The purpose of this paper is to examine the use of blockchain as a service to incorporate electronic distributed transaction systems.

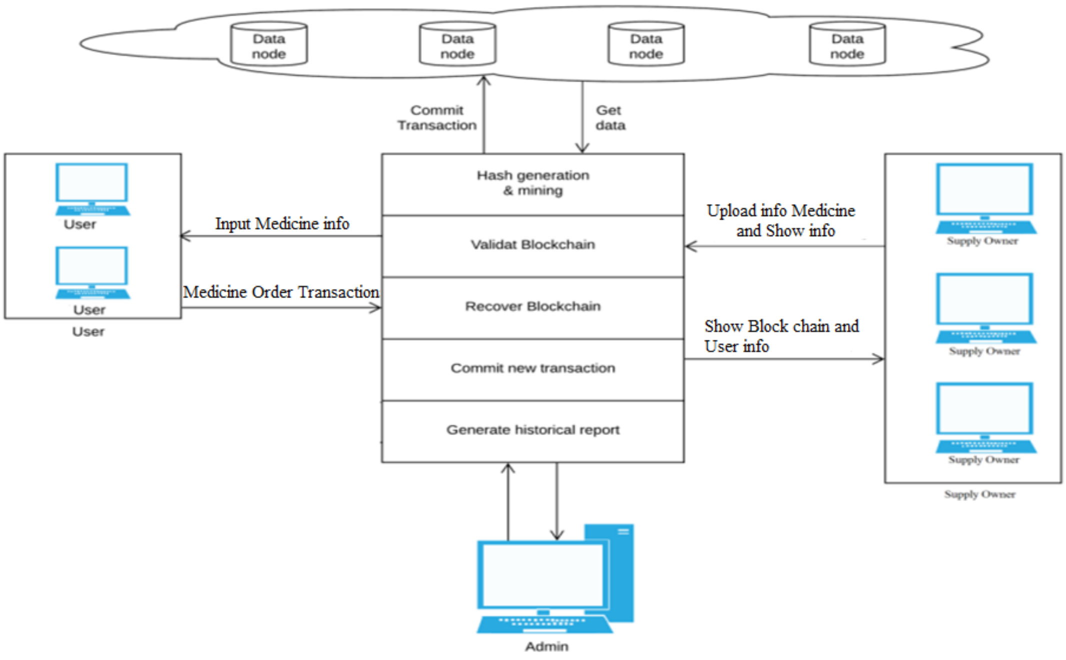

Fig. 1. Proposed System Architecture

Module Description

The system contains following modules:

1: Admin.

2: Create Transaction.

3: Block Generation and Blockchain Validation.

4: Consensus Algorithm Validation and Blockchain Recovery.

5: Results Generation.

- The management of operations management data delivery storage using the block chain is the core outline of the proposed algorithm.
- Without using any third party interface, the device creates trustworthy contact between different parties.
- We use the algorithm of Hash generation and for the given string, the Hash will be generated.
- To validate the data, we use peer to peer verification before executing any transaction.
- If a chain is null, the current server blockchain will be restored or modified.
- This will be checked before the query is confirmed and committed to all nodes.
- The mining algorithm is used to verify the generated hash for the query until the current hash is generated.

Algorithm Design

1 : SHA 256 based Hash Generation

Input : Initial transactional or input data Data[]

Output : Generation hash using SHA256 algorithm

Step 1 : Input data data[]

Step 2 : Perform SHA 256 from SHA suitable algorithms

Step 3 : NewHash= SHA256(data[])

Step 4 : Retrun String(NewHash)

2 : Protocol for Peer to Peer Node Verification

```
Input : User input query, Current Node blockchain Current_Node[chain], Additional
Outstanding Nodes blockchain NodesChain[Node_id] [Node_chain]
Output : Automatic recover blockchain if nodes fails
Step 1 : Transactional data or any event data for input to blockchain
Step 2 : Extract kth server's blockchain of time[t]
         Current_chain □ Current_node[Chain]
Step 3 : foreach
                NodesChain [Nodeid, Chain] $\sum_{i=1}^{n}$    (GetChain)
         End for
Step 4 : foreach (i into Node_Chain)
        If (!.equals NodeChain[i] to (Current_chain))
            FlagVal 1
otherwise continue;  commit query into the nodes
Step 5 : if (FlagVal == 1)
       CCount = SimilarityyNodesBlockchian()
Step 6 : Determine the most of all server
         Unacceptable blockchain recovery from accurate node
Step 7: end if; end for; end for
```

3 : Transaction Mining Algorithm to Generate Valid Hash

```
Input :  Smart contract SC[], Transactions current hash  CH[], Previous hash or genesis block
PH[]
Output : Generate of valid hash and nonse
Step 1 : Generate the hash_Value for kth transaction consuming Algorithm no. 1
Step 2 : if (hash_Value.valid to smart_contract [])
         Current hash is validate
          FlagVal =1
      Else
        FlagVal=0
          Continue;
Mine the current hash again for next iteration
Step 3 : Return validated_hash[] till when flagVal = 1
```

IV. CONCLUSION

There are several research recommendations to apply Blockchain technology to the transaction industry because of the complexities of this field and the need for more robust and effective information management frameworks. An interoperable architecture can undoubtedly play a significant role in many instances of transaction use that face related data sharing and communication problems. In order to educate software engineers and domain experts on the potential and also limitations of this new technology, whether to create a decentralized application using an existing Blockchain, more research on secure and efficient software practice for the use of Blockchain technology in transactions is also needed. To run the method, the algorithm has chosen the appropriate complexity, performance and complexity of implementation. We have a clearer understanding of the speed of information formation in the supply chain through longitudinal studies. There are some major barriers to achieving the full potential of the blockchain and the most critical thing is the scalability of technology and data controls to apply it to health.

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, 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 Cryptocurrency Technologies: A Comprehensive Introduction. Princeton: Princeton University Press

[11] Introduction to Hyper ledger Sawtooth (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 generals problem. Menlo Park, CA: SRI International.

[13] PoET 1.0 Specification (2018) Retrieved January 4, 2019 from https://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.html

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