TRANSACTION OF HEALTHCARE RECORDS USING BLOCKCHAIN

Mrs. S. Kavitha[1], S. Abinaya[2], V. Ramya[3], S. Famidha Sabnam[4]

[1]Assistant Professor, Velammal College of Engineering and Technology, Madurai
[2,3,4]UG Scholar, Department of CSE, Velammal College of Engineering and Technology, Madurai

***Abstract*:-** The major crucial portion of any field is to maintain the large set of data that is being collected from various distributed areas and to protect those data from the interventions of the third party.One such field is Healthcare which faces many problems in maintaining the patient's records. One of the best solutions for the above mentioned problem is creating blockchains. This paper involves the creation and implementation of the private Blockchain for healthcare using Proof of work algorithm and analysing the performance.

***Keywords*—Third party intervention, Distributed, Secure, Blockchain, Healthcare.**

I. INTRODUCTION

Healthcare systems faces many challenges in case of security, flexibility of the data records.Blockchain is one of the most important Technologies and acts as a better platform that maintains large, enormous set of data and also solves the above problem. [1]One of the best examples that implemented blockchain is Bitcoin. It involves in many transactions that transfers money between two parties without the help of any third party intervention. Data are present in the form of blocks which cannot be altered by anyone[2].This helps in maintaining the Sensitive data and also provide Data integrity, Reliability, Secure transactions for the trust worthy patients.[3]

II. BASIC COMPONENTS OF BLOCKCHAIN

There are many components that are involved in blockchain in which each of the components have its own role in the implementations of the blockchain that involves many transactions.

A. Block

The Block is a container and a structure that holds many components such as Data, hash of previous block and Timestamp.

B. Chain

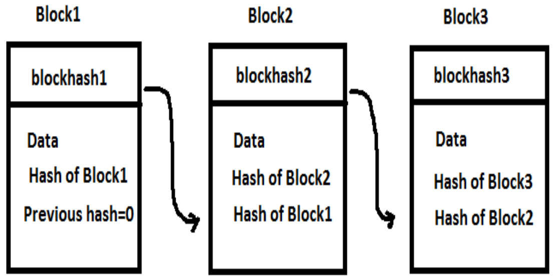
It is the sequence of blocks that connects the multiple blocks to form a chain just like a Data Structure, Linked list.

C. Data

Large set of medical records of the patients that has to be maintained, transferred and the integrity of the data has to be maintained between two parties or within an Organisation.

D. Hash

It is a function that converts the input into the output of fixed length. The output are in the form of the encrypted text using some cryptographic algorithms[4].



III. USE CASES OF HEALTHCARE IN BLOCKCHAIN

There are various possible use cases of Blockchain in Healthcare industry. This involves the data exchange, Interoperability among data, Cyber security handling, Clinical trial management, Integrity of supply chain.

A. Interoperability and exchange of clinical data

This provides a good solution for problems that are face by the healthcare industry in managing large set of data, data interoperability, data integrity and security. This helps in accessing the historical data anywhere and anytime.

B. Healthcare IoT and Cyber security handling

This ensures the data security, privacy and reliability that should not be affected by hackers or third party vendors.

C. Provenance and Integrity of Drug Supply chain

This process in which blockchain helps in gaining trust and confidence among the customers in order to supply the drugs and prevent the fake drug distribution.

D. *Clinical trials and Research result management*

Clinical trials can vary in size and cost, and they can involve a single research center or multiple centers, in one country or in multiple countries. Clinical study design aims to ensure the scientific validity and reproducibility of the results[5].

IV. PROOF OF WORK ALGORITHM

Consensus algorithms are a decision-making process for a group. Blockchain consensus models are methods to create equality and fairness in the online world. One of the consensus algorithms is Proof of work(PoW). Proof of work is the first Blockchain algorithms introduced in the blockchain network. Many blockchain Technologies uses this Blockchain consensus models to confirm all of their transactions and produce relevant blocks to the network chain.[6]

A. *Rise of Proof of work*

At its core, the Byzantine Generals' Problem is achieving a consensus across a distributed network of devices, some of which could be potentially faulty, while also being weary of any attackers attempting to undermine the network. Byzantine Fault Tolerance means an incoming message is repeated to other recipients of that incoming message. All of the nodes make the assumption that the act of repeating a message rules out the issue of Byzantine nodes.Thus, the proof of work protocol deals with the above problem through nonces and combining messages into blocks. Each block has its own distinct nonce. They are only used once in order to add another element of difficulty in generating valid hashes, specifically to prevent precomputation and ensure fairness.[8]

B. *Purpose of PoW:*

PoW offers Distributed Denial of Service(DDoS) protection and lowers the overall of stake mining. This blockchain algorithms offer a fair deal of difficulty for the hackers. The system requires a lot of computational power and effort[6]. This combines the concepts of cryptography and computational power to validate the records that are involved in the transaction and it tries to ensure the authenticity and security of the data in the blocks[7].

C. *Steps:*

Actually the proof of work comes in the form of answers to the mathematical problems.The only way to solve these mathematical riddles is through nodes on the network, running a long and random process that presents answers on a trial and error basis.This means that the problem could be solved on first attempt, although this is extremely unlikely, to the point where it is practically impossible. [8]

1)*Block creation:* Initially the blocks of the block chain will created with the data that has been sent by various sections of the hospital management. The Block will contain the hash of the current block, hash of the previous block and the timestamp that indicates the time at which the block has been created.

2) *Hash calculation:* Hash is being calculated by using the SHA-256 algorithms which provides the output as a message digest. This algorithms usually takes input of any size and produces an output of fixed size.

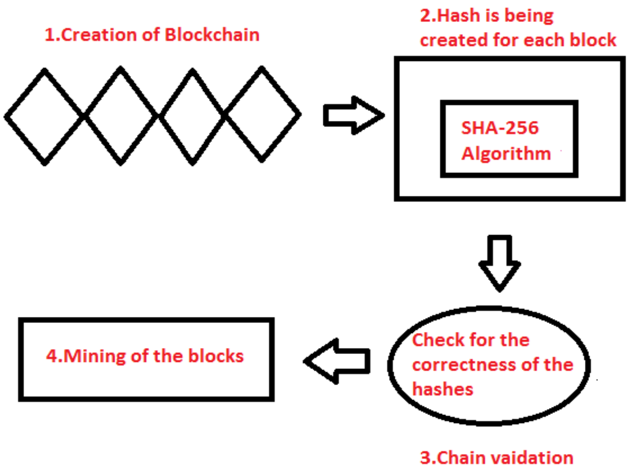
3) *Chain validation:* After the creation of the blocks, the entire chain is validated by comparing the registered hash and the hash that has been calculated for the block. The same process is done for the current as well as the previous block. If the hashes are same then the Chain is a valid one. The Current block's previous hash and the previous block's current hash is checked, whether they are equal.

```
if(previousBlock.hash.equals(currentBlock.previousHash))
{

return true;

  }
```

4)*Mining of blocks:* Target hash will be generated. Target hash is the hash that has to be lower the hash of the current block. Lower the target hash, lower the creation of new blocks. The block will be mined with their hash values.

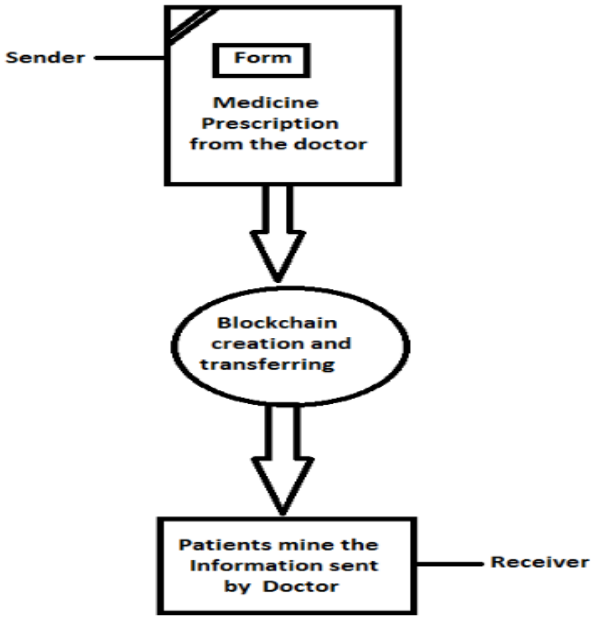


V. STRUCTURE OF BLOCKCHAIN

The above diagram shows the implementation of the healthcare in Blockchain, in which each block contains data that is being sent by the doctor. Blocks in the chain cannot be tampered any third person and it can be retrieved whenever wanted. Doctor will send his/her medicinal prescription with the digital signature to the patients through a private Blockchain. At the receiver end, patient can ensure the validity of the information by the signature of the doctor that is provided in the data before mining the medicinal data. Data that is being added to the blocks by the doctor that involves the generation of new hash value for each block in the blockchain. Then the blocks will be connected by their previous hashes that is, current block will have the hash of its own as well as the hash of the previous block. If there is any changes/modification done by the third party in any of the block, then new hash will be created. If someone want tamper the data, he/she has to change the data of the entire blockchain. During validation part, the hashes are checked, newly generated hash by the tampered block will not match with current node's previous hash and hence sender can easily find that the data has been tampered by someone, can conclude that the chain is not the valid one. If the chain is valid, then the blocks will be mined by the user for the further steps.

1) *Sender:* The Doctor acts as a Sender. This contains the form which has the information that is being sent by the doctor to the patient. The information contains the medicinal prescription like tablet details.

2) *Receiver:* Patient acts as a Receiver. Patient will mine the information that is being sent by the doctor. Before mining, the blocks are being validated by using the SHA Algorithm.


Sender
Form
Medicine Prescription from the doctor
Blockchain creation and transferring
Patients mine the Information sent by Doctor
Receiver

BLOCKCHAIN ON HEALTHCARE

VI. BENEFITS

The main benefit of the Proof of Work algorithms is for deterring cyber-attacks such as a distributed denial-of-service attack (DDoS) which has the purpose of exhausting the resources of a computer system by sending multiple fake requests.

This algorithms is also being used by various cyptocurrencies like Bitcoin, Ethereum, Litecoin, Monero as they consider the algorithm to be very safe for performing money related transactions.

It does not need any third person to look after/monitor the processes that are involved in the transaction. It involves various type of blockchains like pivate or public blockchains..

VII. LIMITATIONS

Like the saying,'Coin has the two sides', PoW algorithms has some limitations eventhough it has advantages.

1) *Greater Energy Consumption:*

The security level of blockchain network based on PoW needs more energy. If the system needs to be more secure, then the energy consumption will be more.

2) *Cost of Electricity*:

The greater consumption is becoming a problem where we are running out of energy – miners on the system have to face a large sum of cost due to the electricity consumption.

3) *51% attack:*

A 51 percent attack, or majority attack, is a case when a user or a group of users control the majority ofmining power.The attackers get enough power to control most events in the network.They can monopolize generating new blocks and receive rewards since they're able to prevent other miners from completing blocks.They can reverse transactions.

VIII. CONCLUSION

Block chain may be considered as one of the best technologies in case of transactions. It uses multiple algorithms in which the first and foremost algorithm used by it was PoW. The proof of work(PoW) algorithms helps better in creation of blockchain based on the storage and maintenance of the data. This algorithms works better in case of making the health related data to be protected with the help blockchain. This data will be present forever in the chain. Even we can retrieve the historical data from the blocks and can view it whenever we want to refer the data.This would create greater impact in the field of Healthcare.

IX. FUTURE CONSIDERATION

Though there are lot of advantages, there are some disadvantages related to the consumption of computation power and cost that has been spent over the electricity bills. Hence, the next process of the project will step towards the implementation of the algorithms that works better than the above algorithms by ensuring that the enhanced algorithm will overcome the disadvantages of the Proof of Work algorithms.

REFERENCES

[1]Advanced Block-Chain Architecture for e-Health Systems by W. Liu,School of Science and Technology,G.G.C,S.S. Zhu.Department of Computer Science,Shantou University, T. Mundie,School of Science and Technology,G.G.C,U. Krieger,Computer Science in Communication and Networks,University of Bamberg

[2] Blockchain Technology beyond Bitcoin by Michael Crosby, Google, Nachiappan, Yahoo, PradhanPattanayak, Yahoo, SanjeevVerma, Samsung Research America,VigneshKalyanaraman, Fairchild Semiconductor.

[3]https://insights.daffodilsw.com/blog/possible-use-cases-of-blockchain-in-healthcare-industry

[4] A Systematic Review of the Use of Blockchain in Healthcare by Marko Hölbl, Marko Kompara, Aida Kamišali´c and LiliNemecZlatolas, University of Maribor, Faculty of Electrical Engineering and Computer Science, Maribor, Slovenia.

[5]https://insights.daffodilsw.com/blog/possible-use-cases-of-blockchain-in-healthcare-industry

[6]https://101blockchains.com/consensus-algorithms-blockchain/

[7] Proof of Work and Proof of Stakeconsensus protocols: a blockchain applicationfor local complementary currencies Sothearath SEANG_ Dominique TORRE_February 2018

[8] https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/proof-of-work