BLOCKCHAIN: MINING OF HASH FUNCTION USING POW ALGORITHM

Vaishali Sharma[1], Nilufar Yasmin[2]

1 &2 Department of Electronics & Communication Engineering, AKGEC, Ghaziabad
APJ Abdul Kalam Technical University, Lucknow (INDIA)

Abstract

Cryptography is an art of secret writing. Major cryptography applications are Cryptographic hash functions (message digests), block chain, MAC, digital signature and digital time stamping. The cryptographic hash work is essentially utilized for security objectives for example, credibility, computerized marks, uprightness and many more. Blockchain is a growing list of transactions record. Blockchain-based applications are covering many fields including financial services, reputation systems, Internet of Things (IoT), healthcare, asset management, Insurance, Voting and Supply chain management. In this paper, the basic structure of blockchain is presented and general steps or procedure for utilizing blockchain in health care sector for managing patients records have been discussed. The concept of mining is related to the proof-of-work consensus algorithm. Although blockchain technology faces two major problems scalability and security. This paper contains an overview of healthcare services which are used to make sure that the patient's health management is given top priority. Federal regulations are made in the health sector in order to provide effective patient care. It affects many sectors like business, industry and financial area. Security, data sharing and Trust computation are major problems that are being faced in health care domain. The structure of blockchain procedure is defined in terms of mining of hash functions for different blocks. Proof-of –work (POW) consensus algorithm is used to find the value of hash functions, previous hash functions, digital time stamping, and nonce value for each block in terms of results. Mainly Blockchain transaction procedure is used for better security. Using Mining technique, it is proved that the proposed method performs better than the existing methods.

Index Terms - Computer Security, Hash functions, Message digest, Blockchain, Mining.

I. INTRODUCTION

Cryptography is the technique for hiding information. It provides basic cryptographic services and send the information to authorized person secretly. The basic goals of cryptography are Confidentiality, Data Integrity, Authentication, and Nonrepudiation. W.Diffie, et.al (1996) [1] introduced the concept of public-key cryptography in order to solve the key management problem. Each person gets a pair of keys, one called the public key and the other called the private key. Each person's public key is published while the private key is kept secret. Today there exist many hash functions, but SHA-256 of hash functions are widely used because of the trust in its security and the execution speed it offers. In this paper, we focus on the cryptographic hash functions and cryptography applications (blockchain in healthcare).

A cryptographic hash function is used to ensure the integrity of the transmitted data or stored data. Sometimes it is also called digest of a message. Hash function generates a fixed size message, digest of a given message and this message digest is treated as a signature of that message. There are many algorithms designed to implement the hash function. MD-2, MD-4, MD-5, SHA-0, SHA-1, SHA-256 and SHA-2 are the best known algorithms for message digest [2].

Blockchain is distributed ledger system for recording and storing transactions. Blockchain is a shared, immutable record of peer-to-peer transactions built from linked transaction blocks and stored in a digital ledger. In a blockchain system [3], there is no central authority, transaction records are stored and distributed across all network participants. In blockchain, we don't use the central bank. For health care organizations, it is decided to initiate blockchain projects. There are two primary use cases to consider: (1) verify and authenticate information (2) transfer value. The working process of blockchain are-Firstly, the sending node records the new data and broadcast the network. The receiving node checked the message from those data what is received, if the message was correct then it will be stored to a block. All the receiving nodes use the consensus algorithms to the block. The block will be stored into the chain after executing the consensus algorithms. Every node in the network admit this block and continuously extend the chain base on this block.

The rest of the paper is summarized as follows: Section 2 describes a consensus algorithm; Section 3 presents healthcare industry; Section 4 describes the challenges in the block chain; Section 5 presents proposed method including hash function, data mining, and transaction record. In Section 6 results has been discussed and then in section7 conclusion is described.

II. CONSENSUS ALGORITHMS

Consensus function is a mechanism [4] that make all blockchain nodes have agreement in same message. It makes sure that the latest block have been added to the chain correctly, guarantee the message that stored by node was the same one and won't happened “fork attack", even can protect from malicious attacks.

.

4.1 Proof of Work (POW): A proof of work is a piece of data which is difficult (costly or time-consuming) to produce but easy for others to verify and which satisfies certain requirements. Producing a proof of work can be a random process with low probability so that a lot of trial and error is required on average before a valid proof of work is generated. Bitcoin uses the Hash cash proof of work system. When calculating POW, it's called “mining". Each block has a random value called “Nonce" in block header, by changing this nonce value, POW have to generate a value that makes this block header hash value less than a “Difficulty Target" which has already been set up. Difficulty means how much time it will take when the node calculating hash value less than target value. In order for a block to be accepted by network participants, miners must complete a proof of work which covers all of the data in the block. The difficulty of this work is adjusted so as to limit the rate at which new blocks can be generated by the network to one every 10 minutes. Due to the very low probability of successful generation, this makes it unpredictable that the worker computer in the network will be able to generate the next block.

4.2 Proof of Stake (PoS) - PoS (Proof of stake) is an energy-saving alternative to POW. Miners in PoS have to prove the ownership of the amount of currency. It is believed that people with more currencies would be less likely to attack the network. The selection based on account balance is quite unfair because the single richest person is bound to be dominant in the network. As a result, many solutions are proposed with the combination of the stake size to decide which one to forge the next block. In particular, Black coin uses randomization to predict the next generator. It uses a formula that looks for the lowest hash value in combination with the size of the stake. Peer coin favours coin age based selection. In Peer coin, older and larger sets of coins have a greater probability of mining the next block. Compared to PoW, PoS saves more energy and is more effective. Unfortunately, as the mining cost is nearly zero, attacks might come as a consequence. Many block chains adopt PoW at the beginning and transform to PoS gradually. For instance, ethereum is planning to move from Ethash (a kind of PoW) to Casper (a kind of PoS). Proof of Work method will cause a lot of electricity power and computing power be wasted, Proof of Stake doesn't need expensive computing power. With Proof of Stake, the resource that's compared is the amount of Bitcoin a miner holds - someone holding 1% of the Bitcoin can mine 1% of the Proof of Stake blocks. A Proof of Stake method might provide increased protection from a malicious attack on the network.

4.3 Proof of Elapsed Time- C.Duma,et.al (2006) [5] recommended that In this variant, consensus is achieved by having every potential validator node request a secure random waiting time from a trusted execution environment which is embedded into the computing platform (such as Intel's SGX). Every node waits for the assigned time, and the first to finish claims validation leadership. Since each trusted computing environment in any node has a chance of being chosen, the probability for any entity of being in control of the validation leader is proportional to the amount of resources contributed to the overall network.

4.4 Proof of Concept- To build a simple system to examine new services and systems and carry out the confirmation using said system.

III. HEALTHCARE INDUSTRY

Blockchain technology has a no. of advantages in healthcare applications. This paper describes [6] blockchain technology and how Bitcoin is using some compelling specific applications in healthcare. We will then look at some problems which we are facing in Healthcare and how blockchain can serve as a solution to these problems. The healthcare industry (also called the medical industry or health economy) is an aggregation and integration of sectors within the economic system that provides goods and services to treat patients with curative, preventive, rehabilitative, and palliative care. It includes the generation and commercialization of goods and services lending themselves to maintaining and re-establishing health.

IV. CHALLENGES IN BLOCKCHAIN

There are many challenges in blockchain [7]-

(a) Nascent technology: Resolving challenges such as transaction speed, the verification process, and data limits will be crucial in making blockchain widely applicable.

(b) Uncertain regulatory status: Because modern currencies have always been created and regulated by national governments, blockchain and Bitcoin face a hurdle in widespread adoption by preexisting financial institutions if its government regulation status remains unsettled.

(c) Large energy consumption: The Bitcoin blockchain network's miners are attempting 450 thousand trillion solutions per second in efforts to validate transactions, using substantial amounts of computer power.

(d) Control, security and privacy: While solutions exist, including private or permissioned blockchains and strong encryption, there are still cyber security concerns that need to be addressed before the general public will entrust their personal data to a blockchain solution.

(e) Integration concerns: Blockchain applications offer solutions that require significant changes to, or complete replacement of, existing systems. In order to make the switch, companies must strategize the transition.

(f) Cultural adoption: Blockchain represents a complete shift to a decentralized network which requires the buy-in of its users and operators.

(g) Cost Blockchain: offers tremendous savings in transaction costs and time but the high initial capital costs could be a deterrent.

V. PROPOSED WORK

A method is presented for the data mining and transactions in blockchain technology. In this method [8], blockchain technology is the process of adding transactions to the large distributed public ledger. Blockchain is best known term for its association with Bitcoin. Other technologies that are using blockchain employ data mining. Blockchain transaction is processed on a blockchain, in seven steps [9]:

Step1: A user signs off on a transaction from their wallet application, attempting to send a certain crypto or token from them to someone else.

Step2: The transaction is broadcasted by the wallet application and is now waiting to be picked up by a miner on the according blockchain. As long as it is not picked up, it hovers in a 'pool of unconfirmed transactions'. This pool is a collection of unconfirmed transactions on the network that are waiting to be processed. These unconfirmed transactions are usually not collected in one gaint pool in small subdivided local pools.

Step3: Miners on the network select transactions form these pools and form them into a block. A block is basically a collection of transactions in addition to some extra metadata. Every miner constructs their own block of transactions. Multiple miners can select the same transaction to be included in their block.

Step4: By selecting transactions and adding them to their block, miners create a block of transactions. To add this block of transactions to the blockchain, the block first needs a signature, this signature is created by solving a very complex mathematical problem that is unique to each block of transactions. A hash function is simply a mathematical problem that is very hard to solve, where the answer is very easy to verify. It contains the hash functions, the mining of hash functions of different blocks and finding the value of hash functions, previous hash functions, digital time stamping, and nonce value using the Proof-of -work consensus algorithm in experimental results.

Step5: The miner that finds an eligible signature for its block first, broadcasts this block and its signature to all the other miners.

Step6: Other miners now verify the signature's legitimacy and hashing it to see if the output hash indeed matches the included signature. If it is valid, the other miner will confirm its validity and agree that the block can be added to the blockchain (they reach consensus, they all agree with each other, hence the term consensus algorithm).That's why Proof of the work performed (the computational power that was spent).

Step7: After a block has been added to the chain, every other block that is added on top of it counts as a confirmation for that block.

5.1 Project Workflow:

In this section [10] implementation steps used in proposed algorithm is mentioned in detail along with their respective output. User will require miners to do proof-of-work by trying different variable values in the block until its hash starts with a certain number of 0's.In Fig 5.1 shows the overall implementation of blockchain. Here a method is presented for the data mining and transactions in blockchain technology.

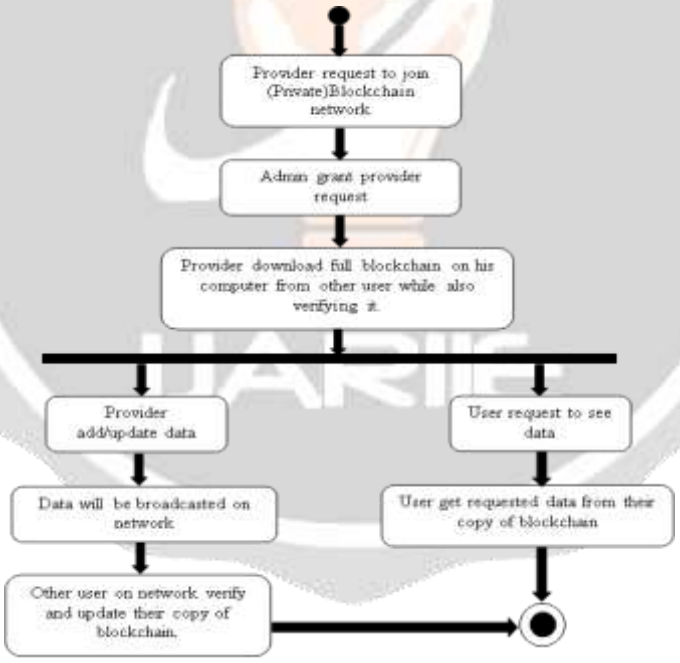

Fig 5.1 Project Workflow

VI. EXPERIMENTAL RESULTS

To evaluate the performance of this work data mining is used. Datasets contains data mining. Dataset is used with proposed SHA-256 algorithm. All the experiments are performed over Java (Eclipse IDE).

6.1 Introduction: This section [11] comprises the results of proposed work. In this chapter the step by step development of the proposed algorithm is mentioned. It comprises the resulted output of the blockchain. For every steps operations

are performed on blockchain according to the proposed algorithm. The output is studied in the form of hash value, data mining and status of blockchain transactions.

6.2 Implementation steps

A blockchain is a chain/list of blocks where each block in the blockchain have its own digital signature, digital signature of the previous block, and have some data (this could be transactions for example).Each block doesn't just contain the hash of the block before it, but its own hash is in part, calculated from the previous hash. If the previous block's data is changed then the previous block's hash will change (since it is calculated in part, by the data) in turn affecting all the hashes of the blocks there after. Calculating and comparing the hashes allow us to see if a blockchain is invalid.

Basic block contains a string hash that holds digital signature. The variable previous Hash is used to hold the previous block's hash and string data is used to hold block data. SHA-256 algothims finds the way to generate a digital signature. It will import java.security.Message Digest package to get access to the SHA-256 algorithm. User uses SHA256 and String Util 'utility' class for handling data mining.

Here user simply takes a string and applies SHA256 algorithm to it and returns the generated signature as a string. After that SHA-256 is applied in a new method in the block class to calculate the hash. It is necessary to calculate the hash for all blocks of the chain. Each block contains the previous Hash, the data and timestamp [12].

6.3 output:

This section comprises the result of the proposed work. Here, the step by step development of both proposed algorithm [13] is discussed. It comprises the resulted output of the blockchain. For each step, operations are performed on blockchain according to the proposed algorithm. The output is studied in the form of hash value and data mining. After performing all the steps according to the proposed work on the blockchain, data has been taken for producing final results. The output of the data mining clearly show the value of mined data. The proposed technique gives the output of hash functions successfully. Fig 6.1 represents the hash value or blocks and Fig 6.2 represents the hash value, previous hash value, data, timestamp and nonce value. Fig 6.3 shows the value of block hash, how to add/append transaction using Merkle tree, how to validate the block transactions and then combining the transaction into Blocks using mining proof of work.

Fig 6.1 Hash Value

Fig 6.2 Data Mining

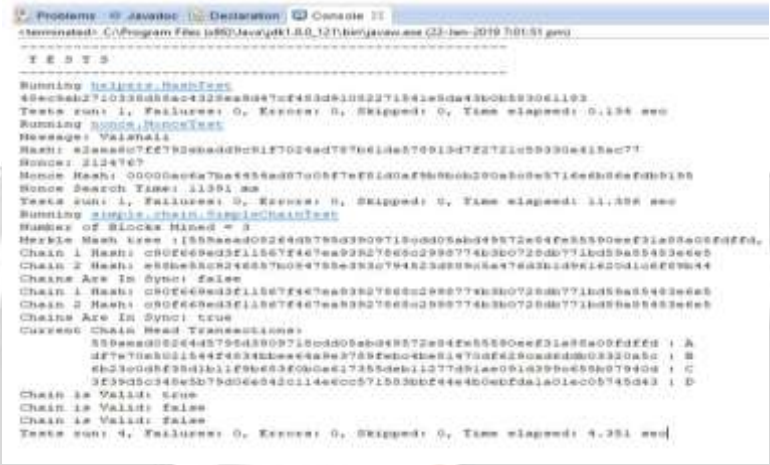

Fig 6.3 Blockchain Transactions

VII. CONCLUSION AND FUTURE SCOPE

This paper gives the overview about all the integrity algorithms. All attempts have been made to give a complete picture of cryptographic hashes, its design techniques and vulnerabilities. Potential of blockchain for healthcare highly depends on the acceptance of the new technology within the healthcare ecosystem in order to create technical infrastructure. Though there are certain concerns and speculations regarding blockchain's integration with current healthcare systems and its cultural adoption, the technology is still popular in the healthcare sector. It has taken the healthcare industry by storm over the past year and many solutions are being developed to adopt it. With so many potential use cases and possibilities, blockchain is sure to disrupt the healthcare landscape for good. The goal of blockchain is to implement a user-oriented, user-friendly, and voluntary method for maintaining any health information (like patient records or prescription scripts). The future scope includes in blockchain healthcare- Full stack blockchain, Decentralized prediction platform, Decentralized borderless virtual nation, Electronic contracts, Anti-counterfeit Platform, Helping local economies to grow, Asset Protection, Internet of Things, Data Storage on Network. Future work can be done on this to reduce the time delay and also some work can be done to improve the internal strength of this algorithm**.** Efforts has been made on these algorithms to improve the scalability and security services further. It is possible to design tools like the modified version of present day errors to improve these.

ACKNOWLEDGMENT

Authors are thankful to Ajay Kumar Garg Engineering College (AKGEC), Ghaziabad for providing the necessary research environment.

REFERENCES

[1] W. Diffie and M. E. Hellman, (1976) "New Directions in Cryptography", IEEE Transactions on Information Theory, Vol. 22, No. 6.

[2] X. Wang, H. Yu,(2005),How to Break MD5 and Other Hash Functions, Advances in Cryptology, proceedings of EUROCRYPT 2005, Lecture Notes in Computer Science 3494, pp. 19–35.

[3] S. Nakamoto (2008),"Bitcoin: A peer-to-peer electronic cash system", journal of cryptology, vol.3, pp.1-8.

[4] Weizhi Meng , Elmar Wolfgang Tischhauser, Qingju Wang, Yu Wang , And Jinguanghan, (2018) "When Intrusion Detection Meets Blockchain Technology: A Review" Special Section On Research Challenges and Opportunities in Security and Privacy of Blockchain Technologies Received November 30, 2017, accepted January 21, 2018, date of publication January 30, 2018, date of current version March 15, 2018 pp10179-10188.

[5] C. Duma, M. Karresand, N. Shahmehri, and G. Caronni, (2006), ''A trust-aware, P2P-based overlay for intrusion detection'', in Proc. DEXA Workshop, vol.18, No.2, pp. 692–697.

[6] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, (2017),"An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", IEEE 6th International Congress on Big Data, vol. 4, No.17, pp.557-564.

[7] Iuon-Chang Lin and Tzu-Chun Liao, (2017)," A Survey of Blockchain Security Issues and Challenges", International Journal of Network Security, vol.19, No.5, pp.653-659.

[8] Michael Crosby, Nachiappan, Pradhan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman, (2015)," Blockchain Technology beyond Bitcoin ", Sutardja Centre for Entrepreneurship & Technology Technical Report,pp.1-35.

[9] Han, Kamber, Pel, Jaiwei, Micheline, Jian, (2011),"Data Mining: Concepts and Techniques ", international Standard Book Number 978-0-12381479-1.

[10] J. Barcelo, (2014), "User privacy in the public bitcoin blockchain", Proc.of Electronics Commerce, vol.6, pp.1-4.

[11] C. Badertscher, U. Maurer, D. Tschudi, and V. Zetas, (2017), ''Bitcoin as a transaction ledger: A composable treatment", in Advances in Cryptology— CRYPTO (Lecture Notes in Computer Science), vol. 10401, pp. 324–356.

[12] M. Mettler, (2016), ''Blockchain technology in healthcare: The revolution starts here, 'Proc. of IEEE International Conference on e-Health Networking, vol.20, No.1, pp. 1–3.

[13] R. Bhanot, Rahul Hans, (2015), "A Review and comparative Analysis of Various Encryption Algorithms", International Journal of Security and its Applications, vol 9, No. 4, pp.289-306.

Vaishali Sharma received his Bachelor in Technology degree in Electronics & Communication Engineering from Lord Krishna College of Engineering in 2016. She is presently pursuing his Masters of Technology in Electronics & Communication Engineering from Ajay Kumar Garg Engineering College, Ghaziabad, affiliated from Dr. APJ Abdul Kalam Technical University, Lucknow. Her working fields are cryptography and currently

working in blockchain in healthcare. She worked on a project on Android Based Home Automation System during his graduation. The prototype was successfully fabricated later**.** She presented a paper on "Latest Trends in Wireless Mobile Communication (4G-5G) Technologies" in Emerging Trends on Electronics and Communication Engineering – 2017 at AKGEC, Ghaziabad.

She published his one research paper and one review paper in International Journal of Advance Research in Science and Engineering in 2018. She presented his paper on Blockchain in Healthcare-an overview at National Conference on Emerging Trends on Electronics and Communication Engineering 2019 at AKGEC, Ghaziabad. She was awarded as Best Session Speaker.