International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 12 | December - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

Implementation of Blockchains as a Distributed Ledger

Namratha Vasudeva

Information & Communication Technology, Manipal Institute Of Technology

---

Abstract - The need for security and privacy calls into question the need for a model which control a large quantity of personal information. Block chain is used to link blocks using cryptography. SHA256 algorithm is used to implement blockchains. It consists of a database that is placed across the nodes on a peer-to-peer network where a copy of the ledger and updates are made independently. Once the update is made it cannot be altered without altering the subsequent blocks. The block chains concept can be extended to form a good solution for problems related to trust issues in society.

***Key Words*:** blockchain, distributed ledger, SHA256, security

1.INTRODUCTION

The early stage of blockchain was in the form of a hash tree known as the Merkle tree. Ralph Merkle patented the hash tree in 1979. It was important to maintain the integrity of the data and made sure inappropriate data was not sent during the transfer. a few years later in 1991, secured chain of blocks were created from the Merkle tree which held blocks connected to each other. Satoshi Nakamato [1] brought up the concept of Blockchain in 2008. It was developed to provide peer to peer connection to check the data exchange and manage without a central authority. As a result of which bitcoins came into existence in the world of cryptocurrencies. The basic concept of blockchain is to provide a transaction that is tamper proof [2]. The first block in a blockchain is known as the genesis block. When a new block is created, the hash value of the preceding block is appended. In case any changes are made to the previous block, different hashcode will be shown which is visible to all other users. As a result of which it is extremely hard to tamper and hence considered as the tamperproof distributed transaction ledgers. Bitcoin has emerged as a digital currency and has been known as the public ledger. Leon et al., [3] states that the problem of double-spend can be solved using public-key cryptography in which a private key and a public key is assigned to each user and shared among all users.

2. Body of Paper

The most important concept of blockchain is a distributed database containing all the transactions. Every transaction is checked and verified making sure no malicious users can manipulate. Over the years there has been an enormous talk about blockchains and a number of industries has implemented it as well. The major reason for adopting blockchains in only few industries is due to trust issues as it is a recent technology. Blockchain supports a decentralized consensus mechanism which allows users to exchange data without the involvement of any trusted third-party. Roman Beck [4] explains that blockchains have created a much 1 trustworthy ledger that help to organize relationships among the organizations which leads to the global economic growth. Records are maintained in hospitals, educational institutes, financial institutes and are maintained by third parties. They are susceptible to be corrupted by humans or through failure in systems. This can be mitigated using blockchains. The authors Marten Risius and Kai Spohrer performed research to explain the outlines, scope and approaches to blockchains [5]. They have given a systematic survey on blockchains and its status in the field of information systems and is well explained in the paper. A number of consortiums like the R3 consortium have come up in the industry of blockchains inorder to enhance and influence the technology of blockchains [6]. A significant work has been carried out to explain the blockchain approach to solve know-your-customer (KYC) problems in the banking sector. It reduces the burden for banks as a single KYC verification is sufficient for various financial institutes. It ensures that there is transparency and beneficial for the customers as well as the insitution [7]. Further research is done which explains a prototype for trading used cars known as proof-of-concept. It contained the history of the vehicles, autorities and other third parties. Blockchains played an important role to keep a track on the history of ownership, asset and helps prevent frauds from claiming insurance for parts of car [8]. In the coming years researchers [9] have found that blockchains are really helpful to keep a track on taxes as well. It prevents tax evasion and double taxation when taxes are paid. Benjamin Egelund-Muller [10] presented a classic domain-specific approach using modeling language for financial contracts. Ethernum blockchains were used to demonstrate the complicated rules and its execution.

The concept of blockchain as a distributed ledger is gaining importance in a wide range of industries. A distributed ledger use nodes to keep a record, share and synchronize the transactions instead of maintaining a centralized data. In order to implement the simple blockchains it is necessary to make use of SHA256 to generate the hash functions. It is a 256-bit key and makes a good function for Advanced encryption standard. The research work is implemented using Java Script where initially the simple blockchains are created. Blockchains work in such a way that it contains an initial block which is called the genesis block. a simple block is made up of index, timestamp, data, hash and some amount to be transferred. The index value of this block is set to zero. The blocks created after the genesis block contains the hash value of its previous block. The hash functions are generated using the SHA256. A smart contract is a code that verifies and put forward the negotiation of a transaction. The simplest form of decentralized automation is seen in smart contracts. Proof of work consensus algorithm is implemented which confirms transactions and generate new blocks. The miners compete with one another in a network to complete transactions. All the transactions are

gathered in a decentralized ledger into blocks. It carries a process called mining by the miners in a network.

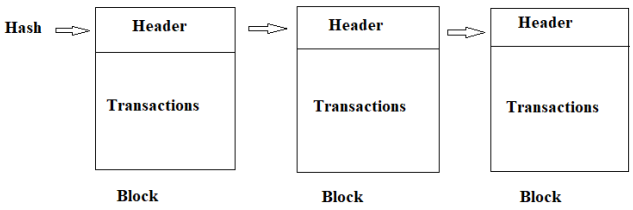

Fig -1: Blockchain Structure

3. CONCLUSIONS

In this paper, efforts are made to understand the various aspect of blockchain as it is still in the early stage and it is needed to understand the distributed ledger techniques and adopt it in wide range of domains. The previous work limits itself in the aspects of security and limited scope. This paper works on the idea of blockchains as a distributed ledger and challenges it faces.

ACKNOWLEDGEMENT

The author is grateful to the friends who reviewed the paper and gave valuable comments which was helpful in improving the paper.

REFERENCES

1. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008
2. What is blockchain technology? a step-by-step guide for beginners. https://blockgeeks.com/guides/what-is-blockchain-technology/. Accessed: 2019-01-21. 2
3. J. Leon Zhao, Shaokun Fan, and Jiaqi Yan. Overview of business innovations and research opportunities in blockchain and introduction to the special issue. Financial Innovation, 2(1):28, Dec 2016.
4. Roman Beck, Michel Avital, Matti Rossi, and Jason Thatcher. Blockchain technology in business and information systems research. Business Information Systems Engineering, 59, 11 2017.
5. Marten Risius and Kai Spohrer. A blockchain research framework. Business & Information Systems Engineering, 59(6):385–409, Dec 2017.
6. Ye Guo and Chen Liang. Blockchain application and outlook in the banking industry. Financial Innovation, 2, 12 2016.
7. Jos´e Parra Moyano and Omri Ross. Kyc optimization using distributed ledger technology. Business & Information Systems Engineering, 59(6):411–423, Dec 2017.
8. Benedikt Notheisen, Jacob Benjamin Cholewa, and Arun Prasad Shanmugam. Trading real-world assets on blockchain. Business & Information Systems Engineering, 59(6):425–440, Dec 2017.
9. Hissu Hyv¨arinen, Marten Risius, and Gustav Friis. A blockchain-based approach towards overcoming financial fraud in public sector services. Business & Information Systems Engineering, 59(6):441–456, Dec 2017.
10. Benjamin Egelund-M¨uller, Martin Elsman, Fritz Henglein, and Omri Ross. Automated execution of financial contracts on blockchains. Business & Information Systems Engineering, 59(6):457–467, Dec 2017.