© 2018 IJSRSET | Volume 4 | Issue 8 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

Blockchain Evolution - A Survey Paper

S. S. N. L. Priyanka*, A. Nagaratnam
CSE, Anil Neerukonda Institute of Technology & Sciences,Visakhapatnam, Andhra Pradesh, India

ABSTRACT

In the modern era, all continents are drifting promptly towards digitization. All financial transactions are being digitized. Leave transactions being digitized. Its an old monk story. Now, the recent drift is money itself is being digitized. Tailoring the digitization processs, ruling out the interference of the third party which controls the cash flow, Bitcoin is the recent invention for Digital money. The need for digitization throughout the globe is the necessary step towards future technology advancement. Blockchain is a incredible technology that is immensely taken by storm in the recent days. Blockchain technology is being used collaboratively with digital money (Cryptocurrency) to streamline all the peer to peer transactions secure, decentralized, non-transparent and accountable.

Keywords: Blockchain, Cryptocurrency, Bitcoin, Distributed Ledgers, SHA-256 Algorithm

I. INTRODUCTION

Blockchain is an incredible technology that is immensely taken by storm in the recent days. Blockchain is a combination of numerous blocks. This combination of blocks is formed by a ledger of records arranged in data batches. These data batches itself are called blocks. Distributed ledger technologies (DLTs), including blockchains, are extensively getting affinity from established and renowned industries. This technology is especially established among financial service firms, which are starting to see DLTs as a great interest in infrastructure and back-office processes. But before going deeply into blockchain, let us understand Cryptography[1].

II. REVIEW OF BASIC CONCEPTS

A. Cryptography: Cryptography is the practice and study of methods/techniques for secure and reliable communication.

B. Hashing: Among the cryptography practices, Hashing is one of the best implemented techniques. A hash value is a numeric value of a unique and fixed length that represents some data.

C. Nonce: A nonce is a number generated for a specific use, such as block generation. A nonce is only for a single use [2].

III. DISTRIBUTED LEDGER TECHNOLOGIES (DLTS)

Distributed ledger technologies (DLTs), including blockchains, are increasingly getting a massive interest from many B2B applications and industries. It is especially used in financial service firms, in infrastructure and back-office processes. In simpler words, a distributed ledger is a database that is shared and synchronized across a network, spread across a network, spread across multiple sites, institutions and geographies. A blockchain is typically implemented as a distributed ledger. In distributed ledger, the entire

blockchain is replicated by each peer (node), and the chain is highly tamper proof[2].

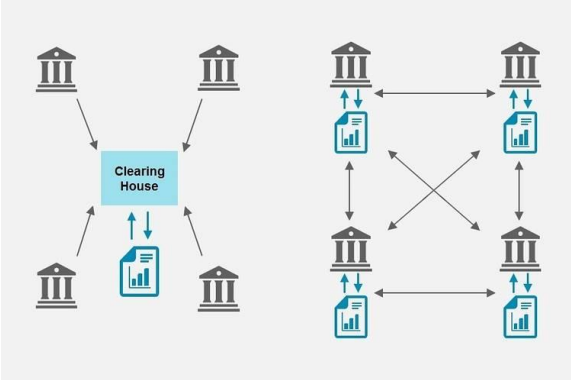

Figure 1. Distributed Ledger Technology

Blockchains are one form of distributed ledger technology. Necessarily, not all distributed ledgers employ a chain of blocks to provide a secure and valid transaction. A blockchain is distributed across the system and regulated by peer-to-peer networks. Since it is a distributed ledger, it can exist without a centralized authority or server managing it, and its data quality can be maintained by database replication and computational trust. However, the structure of the blockchain makes it distinct from other kinds of distributed ledgers. Data on a blockchain is grouped together and organized in blocks. The blocks are then linked to one another and secured using cryptography techniques[3].

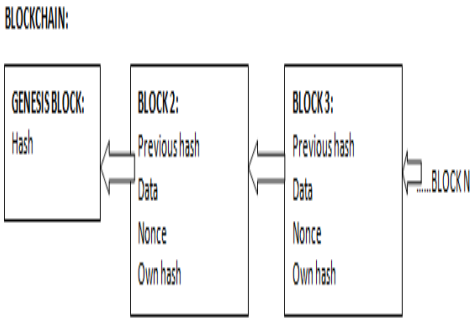

Figure 2. Usage of BlockChain Components

IV. BLOCKCHAIN ARCHITECTURE

Blockchain is a ledger of records arranged in data batches called blocks, that uses cryptographic validation to link themselves together. Put simply, each block reference and identifies the previous block's hash forming an unbroken chain[4].

Each block is a typical blockchain has at least the following components:

Table 1. Components of BlockChain

COMPONENTS	DETAILS
INDEX(BLOCK#)	The position of the block to know sequence/order of the block(Genesis block has the index 0)
PREVIOUS HASH	This lets us know whether previous block is valid or not
TIMESTAMP	This holds the information of the time when the block is added
DATA	The type of information that is stored on a block
NONCE	A number generated for a specific use, such as block generation, to be used only once.
HASH	The hash that is generated for the present block

All the above information that is Index, previous Hash, Timestamp, Data and Nonce are used for the creation of the present block's Hash. As each transaction occurs, it's put into a block. Each block is connected to the one before and after it. All the transactions are blocked together.

Modifying/Changing a block will change its Hash. This will invalidate all the subsequent blocks in the chain. The reason for this is the present block's hash is derived from previous block's hash.

Types of Blockchain

There are two types of block chain[4]:

A. Public Blockchain: The public blockchain is accessible and open to anyone who wants to participate using open source software. This behaves as the decentralized system. All participants can add to the chain. An open network that anybody can access like the bitcoin model. That is the users can add to the chain by creating new blocks but the new users have no right or permission to modify/change the existing blocks as this may result in the wrong derivation of the hash.

Example: bitcoin, ethereum and factom etc.

B. Private Blockchain:

The private blockchain incorporates permission to review and modify the contents of blocks. So this behaves as centralized system. The most preferred option of the banks is that, it is a closed, confidential and non-transparent system which checks all the details and the accessing capacities are being controlled at a central level.

Example: quorum, hyperledger(corda, fabrix and sawtooth) etc[6],[7].

V. CHARACTERISTICS OF BLOCKCHAIN

A. Decentralization: In conventional centralized transaction systems, each transaction needs to be validated through the central trusted party (central bank) which results in high end cost and the performance bottlenecks at the central servers. Differently, a transaction in the blockchain network can be conducted between any two peers (P2P) without the authentication by the central party. In this manner, blockchain can significantly reduce the server costs (including the development cost and the operation cost) and optimize the performance bottlenecks at the central server.

B. Persistency: Each of the transactions spreading across the network needs to be confirmed and recorded in blocks distributed in the whole network. It is almost impossible to tamper. Additionally, each broadcasted block would be validated by other nodes and transactions would be thoroughly checked. So any manipulation is not possible and could be detected very easily.

C. Anonymity: Each user can interact with the blockchain network with a generated address. A user can generate many addresses to avoid identity exposure. There is no longer any central party keeping users private information. This mechanism preserves a certain amount of privacy on the transactions included in the blockchain. Note that blockchain cannot guarantee the perfect privacy preservation due to the intrinsic constraint.

D. Auditability: All the transactions on the blockchain is validated and recorded with a timestamp, users can easily verify and trace the previous records through accessing any node in the distributed network. In Bitcoin blockchain, each transaction could be traced to previous transactions iteratively. It improves the transparency of the data stored in the blockchain.

VI. SHA-256 ALGORITHM IN BLOCKCHAIN TECHNOLOGY

SHA – 256 algorithm, abbreviated as Secure Hashing Algorithm is used in blockchain to get a constant hash of 256 bits every time. This algorithm is also a part of encryption technology[5].

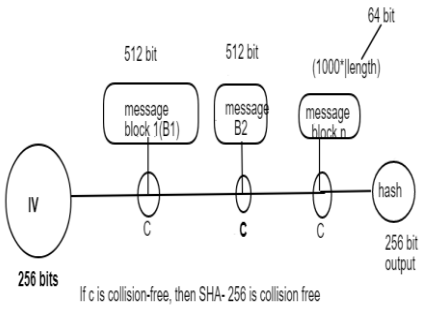

Figure 3. Working of SHA-256 Algorithm

SHA – 256 algorithm, abbreviated as Secure Hashing Algorithm is used in blockchain to get a constant hash of 256 bits every time. This algorithm is also a part of encryption technology.

In the above figure you can see the prototype of algorithm. In this there is some data called **IV** which is of **256 bits**. Now the input we get will be in the very large. So be break it in size of 512 bits. As the input will always be not a perfect multiple of 512 bits, so some part of input will be left. To this left input we do a padding – concatenate the input with 10* bits before it. Now our input is perfect multiple, so we can proceed further. Now **512-bit input** is added with **256-bit IV** to get a total of **768 bit.** This 768 bit is passed through a compression function 'c' to get an **output of 256 bits** only. This output 256 bit is again merged with 512 bits input from **block B2**. Again the total is passed through the compression function to yield a 256-bit output. This loop goes on till the last block (block n). Again a compression function starts and gives final 256 bits output, what we call it as hash of input data. The important concept here is that if function c is collision free, then SHA – 256 is collision free.

VII. CONCLUSION

Blockchain is highly applauded technology in the recent times all over the globe. As it supports decentralized system and peer-to-peer nature, it is being employed by many renowned companies like Microsoft Azure(2016), IBM etc. Blockchain is also extensively applicable under many domains like Internet of Things, Finance, Security, Public Services, E-Commerce etc. Blockchain is gaining huge craving with its key characteristics like auditability, decentralization, anonymity and persistency. There are many algorithms that can be applied to the blockchain. But we discuss the application of SHA-256 algorithm used in blockchain.

VIII. FUTURE WORK

As blockchain is designed as a decentralized system, its growing popularity will allow maximum population of enterprises to use this technology. As the blockchain is not intended to serve a few organizations, some methods should be proposed to solve this problem. Blockchain technology can also be used for data analytics and this trending technology can also bring advancement in areas like artificial intelligence and data mining.

IX. REFERENCES

[1]. https://jfinswufe.springeropen.com/articles/10.1186/s40854-016-0040-y
[2]. https://www.msm.nl/resources/uploads/2017/10/Working-Paper-No.-2017-3.pdf
[3]. https://bravenewcoin.com/assets/Industry-Reports-2016/UN-How-Can-Cryptocurrency-and-Blockchain-Technology-Play-a-Role-in-Building-Social-and-Solidarity-Finance-Brett-Scott.pdf
[4]. https://www.youtube.com/watch?v=9mNgeTA13Gc
[5]. https://www.youtube.com/watch?v=IqtRKWJ1aPc
[6]. Glaser, F., M. Haferkorn, M.C. Weber and K. Zimmerman. 2014. "How to Price a Digital Currency? Empirical Insights on the Influence of Media Coverage on the Bitcoin Bubble." Banking and Information Technology
[7]. Noizat, P. 2015. "Blockchain Electronic Vote." In Handbook of Digital Currency, edited by David Lee Kuo Chuen, 453-461. San Diego, CA: Academic Press.