Blockchain-The More Secure Way Forward

Shruti Mukhedkar

Bangalore
India.

***Abstract*- This Whitepaper explains blockchain concepts to improve security for any transaction. This security is provided using public key cryptography where public key address is used in encrypted form and used for authentication.**

***Index Terms*- blockchain, bitcoin, cryptography**

I. INTRODUCTION

Blockchain – These are digital records that are securely linked to each other via cryptographic hashes. These records are stored in a block comes after previous block in sequence.

It collects information together in groups known as 'Blocks' Blocks have certain storage capacity so, when filled are closed and linked to previously served block for same transaction and forms a chain of data known as the Blockchain. New data and transactions are introduced by adding a new block to chain.

Blockchains are typically managed by a peer-to-peer (P2P) computer network for use as a public distributed ledger, where nodes collectively adhere to a consensus algorithm protocol to add and validate new transaction blocks. Although blockchain records are not unalterable, since blockchain forks are possible, blockchains may be considered secure by design and exemplify a distributed computing system.

II. HISTORY

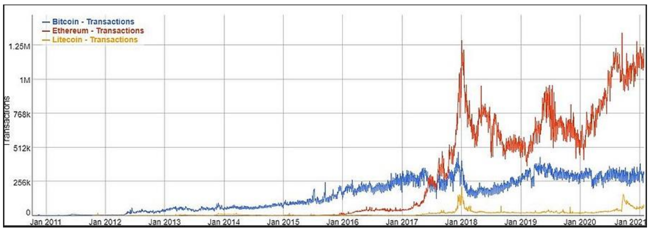
The first decentralized blockchain was conceptualized by a person (or group of people) known as Satoshi Nakamoto in 2008. Nakamoto improved the design in an important way using a Hashcash-like method to timestamp blocks without requiring them to be signed by a trusted party and introducing a difficulty parameter to stabilize the rate at which blocks are added to the chain. The design was implemented the following year by Nakamoto as a core component of the cryptocurrency bitcoin, where it serves as the public ledger for all transactions on the network.

In August 2014, the bitcoin blockchain file size, containing records of all transactions that have occurred on the network, reached 20 GB (gigabytes). In January 2015, the size had grown to almost 30 GB, and from January 2016 to January 2017, the bitcoin blockchain grew from 50 GB to 100 GB in size. The ledger size had exceeded 200 GB by early 2020

The words block and chain were used separately in Satoshi Nakamoto's original paper, but were eventually popularized as a single word, blockchain, by 2016.

According to Accenture, an application of the diffusion of innovations theory suggests that blockchains attained a 13.5% adoption rate within financial services in 2016, therefore reaching the early adopters' phase. Industry trade groups joined to create the Global Blockchain Forum in 2016, an initiative of the Chamber of Digital Commerce.

In May 2018, Gartner found that only 1% of CIOs indicated any kind of blockchain adoption within their organizations, and only 8% of CIOs were in the short-term "planning or [looking at] active experimentation with blockchain". For the year 2019 Gartner reported 5% of CIOs believed blockchain technology was a 'game-changer' for their business.



III. STRUCTURE OF BLOCKCHAIN

A blockchain is a decentralized, distributed, and mostly public, digital ledger consisting of records called blocks. These blocks are used to record transactions across many computers so that any involved block cannot be altered.

Any change is needed for any of the block (i.e., for any specific transaction) all blocks belong to the chain for specific transaction must be changed.

Blocks are arranged in chain form as shown in figure1. In Which first block of a particular transaction (Green Block)
is called genesis block. Blocks after genesis block (blue blocks) form main blockchain. Few blocks added but remain unused later (orange blocks) are the orphan blocks

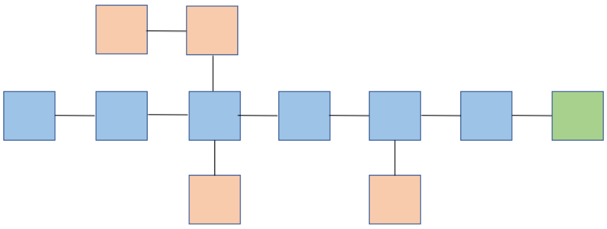


Figure1: Blockchain Structure

A. *Ledger*

Blockchain is a form of distributed ledger like a book maintained for all the transaction for an organization. Each block stores a transaction related data which is a part of whole transaction. Such blocks connected to each other in sequence to form a chain of data related to any transaction. These blocks are nothing but records which keep on growing by simply addition of more blocks with data in it.

As shown in Figure2, every block contains:
1. Data
2. A unique and cryptic Identifier which is Hash computed
3. Timestamp which informs when it was created
4. Unique Identifier of previous block

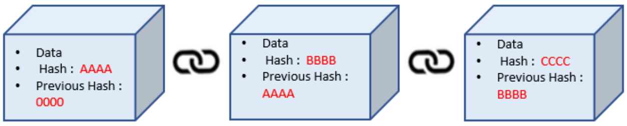


Figure2: Block contents in a Blockchain

Data is transaction related data and may have some additional data added by sender. Hash computed value for whole data present in that block. This Hash computed value is unique as each block has different data and hash computed value for such data is also unique. Each block contains certain timestamp which represents time of creation or modification of that block. This timestamp once created can not be changed by anyone which helps to keep track of any alteration of data. Except first block of transaction i.e., Genesis blocks all blocks should have hash value of previous block. Since each block contains information about the previous block, they effectively form a chain with each additional block linking to the ones before it. Consequently, blockchain transactions are irreversible in that, once they are recorded, the data in any given block cannot be altered retroactively without altering all subsequent blocks. Alteration of all blocks involved in that transaction is nearly impossible with high values of proof of work and if transaction contains a greater number of blocks.

B. *Decentralization*

Blockchain uses Decentralized control, meaning no one organization can control data. So, control to blockchain is done by multiple organizations. For this reason, entire blockchain is copied and stored in a decentralized, distributed and mostly public network computers. As shown in figure 3 below. Blue colored nodes have control on blockchain.

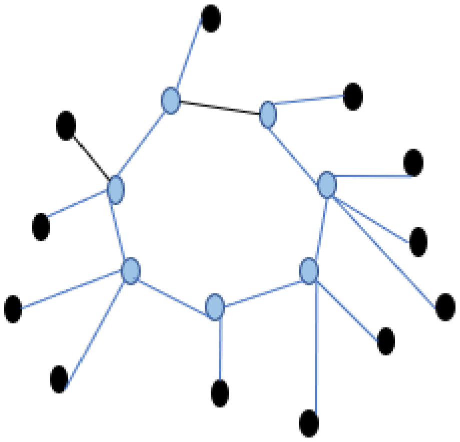


Figure3: Decentralized approach for blockchain

This distributed control handling removes dependency on a reliable third party to supervise and verify all transactions. All transactions are open and publicly declared. No centralized "official" copy exists, and no user is "trusted" more than any other.
So, if any modification is needed for any block, those must be published to all controlling nodes and need approval from them to allow the new changes. If no approval received, Data can not be modified once it is created. In other words, if a randomly

chosen validator proposes a block, the rest of validators vote on it, and, if a supermajority decision approves it, the block is irreversibly committed into the blockchain.

Each block is cryptographically chained to the previous block (i.e., Hash value of previous block present in next block) Alteration of any block anywhere in the chain would result all the upcoming blocks to be invalid, as any change in data of any block would result in change in its hash value which is already added in next block.

There is no limitation for number of blocks to add in chain so there are no restrictions for transaction data. It provides Authentication and authorization in between recipients.

These operations are controlled by a piece of code that executes when specific criteria are met called as Smart Contract. It defines the rules for any transaction. It can vary as per requirement. These smart contracts present in each block, and it interacts with other blocks and with other smart contracts.

Blockchain provides overall more secure and more reliable approach for any transaction.

Blockchain can be implemented with following layers:

- infrastructure (hardware)
- networking (node discovery, information propagation and verification)
- consensus (proof of work, proof of stake)
- data (blocks, transactions)
- application (smart contracts/decentralized applications, if applicable)

IV. Types of Blockchain

A. Public Blockchains

A public blockchain has no access restrictions. Anyone with an Internet connection can send transactions to it as well as become a validator. Usually, such networks offer economic incentives for those who secure them and utilize some type of a proof-of-stake or proof-of-work algorithm. Proof-of-stake are the protocol are class of consensus mechanism for blockchains that work by selecting validators in proportion to their quantity of holdings in the associated cryptocurrency. This is done to avoid computational cost of proof-of-work schemes. Proof of work is a form of cryptographic proof in which one proves to others that a certain amount of a specific computational effort has been expended. Verifiers can subsequently confirm this expenditure with minimal effort on their part.

B. Private Blockchains

A private blockchain is permissioned. The network administrators should invite and give access to participants and validators. Their access is restricted. To distinguish between open blockchains and other peer-to-peer decentralized database applications that are not open, the terminology Distributed Ledger (DLT) is normally used for private blockchains.

C. Hybrid Blockchains

A hybrid blockchain has a combination of centralized and decentralized features. The exact workings of the chain can vary based on which portions of centralization and decentralization are used.

D. Consortium Blockchains

A consortium blockchain is a type of blockchain that combines elements of both public and private blockchains. In a consortium blockchain, a group of organizations come together to create and operate the blockchain, rather than a single entity. The consortium members jointly manage the blockchain network and are responsible for validating transactions. Consortium blockchains are permissioned.

V. USES OF BLOCKCHAIN

1. Cryptocurrencies - Most cryptocurrencies use blockchain technology to record transactions. For example, the bitcoin network and Ethereum network. Governments can have mixed policies on the legality of their citizens or banks owning cryptocurrencies.
2. Smart contracts - Blockchain based Smart contracts can be operated without human interaction, it can work in automated way. So, it removes dependency on a reliable third party to act as mediator in between contracting entities.
3. Financial services - with implementation of distributed Ledgers along with Private Blockchain, more secure and fast transaction can be achieved in financial sector. New research labs dedicated to blockchain technology are establishing to explore how blockchain can be used in financial services to increase efficiency and reduce costs.
4. Supply chain management - The Food Supply Chain still relies heavily on manual interventions when it comes to coordinating between players to find out the shipment location and condition. If the refrigerator fails or the food truck breaks down, it is difficult to determine and take real-time action. Data inaccessibility is affecting the overall profitability and productivity of the system. Most of these issues can be solved by implementing Blockchain infrastructure as explained in above sections for tracking and tracing.
5. IoT (Internet of Things) - By using Public blockchain for IoT devices, tracking and updating the state of devices can be achieved. Monitoring and Tokenizing of these devices also can be implemented. For e.g., for self-driving cars, traffic congestion information it can receive or update to a server. Exchange of this information in real time can be achieved using digital tokens that exists in blockchain.
6. 5G IoT products - 5G IoT agricultural products traceability platform is based on blockchain. The application of 5G technology to the traceability of agricultural products on the Internet of Things can effectively solve the problem of slow transmission of massive data generated in real-time. Blockchain can ensure that information will not be tampered with, and the consortium blockchain has strong controllability, which is suitable for the traceability system of agricultural products with multiple responsibility subjects along with traceability platform.

7. IPv6 Technologies - With the development of IPv6 services and the increase in traffic, data center networks face new challenges. The traditional IPv6 network provides best-effort forwarding. To make this IPv6 transactions more secure blockchain concepts can be reused such as hash computation for source and destination addresses. This will achieve goal for completely authenticated and authorized transactions over IPv6 to prevent Man-In-The-Middle attacks.

V. CHALLENGES

1. Blockchain Technology is still emerging technology not developed yet so with this state there can be doubts about stability and reliability. Before implementation there are doubts about scalability and security also for any organization.
2. For this technology regulations and laws are not yet available by authority there will be difference when used widely when complexity to Blockchain added
3. No standardization available yet in some area such as interoperability with other blockchain. So, integration of technology becomes difficult.
4. While start using this technology into existing environment, has high level of complexity and risk associated with it. For e.g., This Decentralized system must work with one or more centralized, multi-layered systems, both, inside and outside organization.
5. Blockchain provides just infrastructure while implementing, still some factors need to work on e.g., which type of smart contracts to deploy, and which component should interact with them

V. CONCLUSION

Blockchain is a sequential distributed database used in cryptocurrencies. This infrastructure gives platform for more secure transaction, which has distributed control so that data will be open to multiple parties and no single administrator can modify data. This way data becomes open to all and very difficult to change once created. Blockchain concepts can be applied in various technologies to make best out of it. With this blockchain yet need to grow, improve in some of the aspects to be usable with less restrictions. With the increasing number of blockchain systems appearing, even only those that support cryptocurrencies, blockchain interoperability is becoming a topic of major importance. The objective is to support transferring assets from one blockchain system to another blockchain system.

REFERENCES

1. Nakamoto, Satoshi (October 2008). "Bitcoin: A Peer-to-Peer Electronic Cash System" (PDF). bitcoin.org. Archived (PDF) from the original on 20 March 2014. Retrieved 28 April 2014.
2. External video Blockchain Basics & Cryptography, Gary Gensler, Massachusetts Institute of Technology
3. IPv6 Enhanced innovation (IPE); IPv6 and Cloud using DataBlock Matrix for Food Supply Chain Tracking and Tracing, ETSI GR IPE 006 V1.1.1,2022