Asian Journal of Convergence in Technology **Volume V Issue I**
ISSN NO: 2350-1146 I.F-5.11

Overview of Blockchain Technology

Janvi Dattani, Harsh Sheth

Computer Engineering Department
Mukesh Patel School of Technology Management and Engineering, NMIMS

***Abstract*— A blockchain is distributed, decentralized database of records which enables fast reliable transactions without a centralized management overlooking it. The cryptocurrency may or may not be enthralling in the future but role of blockchain technology in various fields of finance and non-finance sectors should not be underestimated. In this paper we will provide an overview on how blockchain works, types of blockchain, and a short overview of different blockchain platforms.**

Keywords*— *blockchain, distributed ledger, hash, transaction cryptography, mining.

I. INTRODUCTION

A system can follow two architectural approaches i.e. distributed & centralised. Blockchain follows a distributed approach where there are several nodes connected to each other without a central node of control.[1] Blockchain is the technology behind bitcoin and other cryptocurrencies. Bitcoin and other cryptocurrency are the popular example tied up to blockchain but blockchain has been applied beyond financial application which are increasing as time goes on. Blockchain is a open ledger where every transactions taking place are recorded and everyone are connected to each other. Blockchain implements a unique P2P (peer to peer) distributed database communication which allows for storage, verification and auditing of transaction by the peers present in the network. Once a transaction is added to the blockchain it is impossible to change, delete or tamper with the transaction this is one of the critical technical features of blockchain technology. For transaction to be led effectively they should be affirmed by blockchain. These affirmations are carried out by consensus mechanisms. In simple terms, it is easy to steal cookie from a jar kept in a sequestered place than stealing a cookie from a jar kept in place governed by hundreds of people [2] - this statement sums up blockchain neatly.

II. TYPES OF BLOCKCHAIN

A. Permission less blockchain

Bitcoin is the best example describing Permission less blockchain. There is no barrier as to who can use it. Anyone can run a node, mining software. Anyone can access a wallet, write data onto the transactions as long as they are following rules of the blockchain. These types of blockchain are open and transparent anyone can review it at any given point of time They are also known as public blockchains and this blockchain network power ups most of the digital currency in the market. e.g. bitcoin & lite coin

B. Permissioned blockchain

They are also known as private blockchain. They act as closed ecosystem where people cannot readily join the blockchain network, see the history or issue transaction they need some sort of permission to do the mentioned task. It belongs to private individual or an organization where there is a central authority who looks after the permissions. The consensus mechanism may be the same as public blockchain or some other maybe used. e.g. ripple

C. Consortium or federated blockchain

This type of blockchain removes the power which is vested on the single individual. So here instead of giving power to a single entity it is given to a group of people or individual who form groups called consortium or federation. e.g. Quorum, Hyperledger, Corda

III. ARCHITECTURE OF A BLOCK

Blocks are files where data related to blockchain network are permanently recorded. It records most of the transaction in blockchain network. Blocks act like a page of a record book. A chain of these blocks evolves into a blockchain

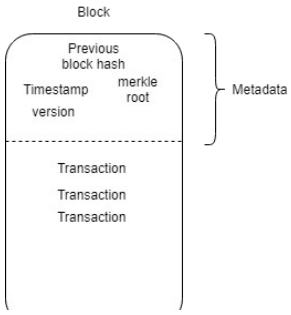

Fig. 1. A block in Blockchain

- **Version**- Current version of the block
- **The Previous block's hash** – A block is a linked list which includes transaction data and a hash pointer. A hash pointer works similarly to a pointer but instead of storing the address of the previous block it contains the

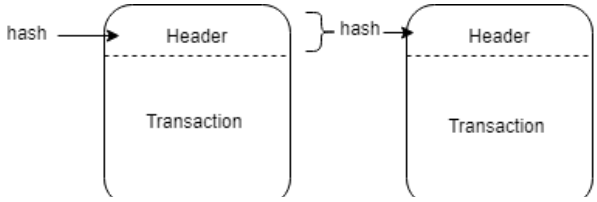

Fig. 2. Linked blocks in Blockchain

- **Merkle root tree -** A cryptographic hash of all the transaction in the block. The transaction which are in a block are in stored in a data structure called Merkle tree. This Merkle tree is created by hashing pair of nodes in a tree until a single hash is left called the Merkle root [3]. Cryptographic algorithm like SHA-256 is used as a hashing algorithm. Some other hashing algorithm can also be used.

  For example- Let's take a block with four transaction.

  const tH ="Hi people"

  const tI ="is this a bat"

  const tJ ="open the door"

  const tK ="do you like this"

  Now for constructing a Merkle tree we start from bottom and go all the way up until a single Merkle root is left. So now taking a single transaction and double hashing them.

  const sha256 = require('js-sha256'). sha256

  const hH = sha256(sha256(tH))

  const hI = sha256(sha256(tI))

  const hJ = sha256(sha256(tJ))

  const hK = sha256(sha256(tK))

  This hashing of the data will produce some output

  Pairing together hH and hI

  const hHI = sha256(sha256(hH + hI))

  Pairing together hJ and hK

  const hJK = sha256(sha256(hJ + hK))

  Now the final step pairing hHI and hJK

  const HIJK = sha256(sha256(hHI + hJK))

  This is our Merkle root.

  Example of cryptographic hash functions are

  MD5, SHA 1, SHA 256, KECCAK (used by Ethereum)

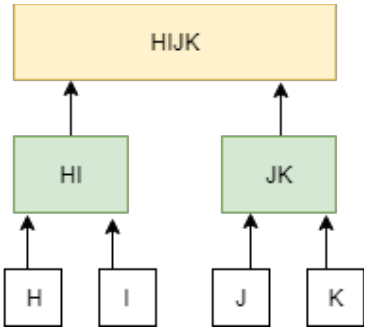

Fig. 3. Merkle root tree

- **Time-** The time at which the block was created.
- **Transaction**

We constructed a block using the technicalities mentioned above and implemented a blockchain consisting of 3 nodes. Platform Node.js and Microsoft visual studio Code were used. SHA-256 cryptographic function is used to provide encryption.

```
const SHA256 = require("crypto-js/sha256");
class Block{
    constructor(index,timestamp,data,previousHash=''){
        this.index=index;
        this.timestamp=timestamp;
        this.data=data;
        this.previousHash=previousHash;
        this.hash=this.calculateHash();
    }
    calculateHash(){
return SHA256(this.index+this.timestamp+this.previousHash+JSON.stringify(this.data)).toString()
    }
}

class Blockchain{
    constructor(){
        this.chain=[this.createGenesisBlock()];

    }
    createGenesisBlock(){
        return new Block(0,"01/01/2018","this is the genesis block","0");

    }
getLatestBlock(){
    return this.chain[this.chain.length-1];

}
addBlock(newBlock)
{
    newBlock.previousHash=this.getLatestBlock().hash;
    newBlock.hash = newBlock.calculateHash();
    this.chain.push(newBlock);
}

}

let block1 =new Block(1,"02/01/2018",{mybalance : 100});
let block2 =new Block(2,"03/01/2018",{mybalance : 100});
let myBlockchain = new Blockchain();
myBlockchain.addBlock(block1);
myBlockchain.addBlock(block2);
```

Fig. 3. A code for Implementation of Blockchain

Fig. 4. Output for the Code

IV. Different Blockchain Platforms

- **Ethereum -** It is an open source, Public blockchain based distributed system that allows developers to build and deploy software application and it is fuelled by its own cryptocurrency token called ether. It also provides users with Ethereum virtual machine which acts as an environment for Ethereum based smart contracts
- **Hyperledger-** It is an open source distributed ledger technology platform designed for enterprises. It uses a Permissioned distributed ledger and being the first distributed ledger to allow smart contracts to be written in general programming languages like Java, Google go and Node JS so no additional training is required by enterprises for learning domain specific languages. [4] The main difference between this and other platform is the support of pluggable consensus which allows the platform to be more efficient for a particular use case.
- **R3 Corda-** It was created by a consortium of top banks of the world. It is a distributed ledger platform. [5] It is based on the infrastructure that has nodes which are responsible for implementing smart contracts. It is a completely permissioned network.
- **Ripple-** Ripple is an open source protocol that is designed for cheap and fast transactions. It uses a common ledger which is managed by a network of independent nodes. The interesting thing is ripple token XRP cannot be mined like bitcoin or another cryptocurrency but it is issued at its inception.
- **Quorum-** Developed by JP Morgan. It is the first step taken towards implementing blockchain in financial sector. It is a Permissioned Blockchain which is specifically designed for financial use cases. It is built off Go Ethereum. It aims to provide confidentiality of Records which being the main concern for financial institutions.

Table. 1. Comparison of different blockchain platforms

Parameter		Blockchain	Platform		
	Ethereum	Hyperledger	R3 corda	Ripple	Quorum
Industry focus	Cross industry	Cross industry	Financial services	Financial services	Cross industry
Governance	Ethereum developers	Linux foundation	R3	Ripple labs	Ethereum dev and JP Morgan
Ledger type	Permission less	Permissioned	Permissioned	Permissioned	Permissioned
Consensus Algorithm	Proof of work	Pluggable framework	Pluggable framework	Probabilistic voting	Majority voting
Currency	Ether	No currency	No currency	XRP	---
Smart Contract functionality	Yes	Yes	Yes	No	Yes

Conclusion

Blockchain which was the main technology behind bitcoin is now not only used in financial sector but now it has cross industry application. Through this paper we provide an easy access to blockchain technology and how it works.

References

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash,2008
[2] Dhiren Patel,Jay Bothra,Vasudev Patel,”Blockchain exhumed”,IEEE 2017.
[3] Blockchain: what is in a block?
URL: https://dev.to/damcosset/blockchain-what-is-in-a-block-48jo
[4] Hyperledger fabric
URL: https://www.hyperledger.org/projects/fabric
[5] Difference between Ethereum,Hyperledger Fabric and R3 corda
URL:https://medium.com/@micobo/technical-difference-between-ethereum-hyperledger-fabric-and-r3-corda-5a58d0a6e347