International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072

# Blockchain Technology

**Mrs. Vrushali Khandare**

*Lecturer, Dept. of Computer Engineering, V.P.M's Polytechnic, Thane, Maharashtra*

---

***Abstract*** *- Blockchain is a rising innovation for decentralized and value-based information sharing over a vast system of untrusted members This paper talks about to create an understanding of the blockchain technology and how it is different from the currently used centralized transactions systems. It additionally talks about how blockchain innovation can be utilized as a part of some business forms in the retail area to profit the clients and the retailers as it were. The paper also describes the advantages of block chain and various evaluation techniques.*

***Key Words***: **Blockchain technology, Bit Coin, Block Chain Evaluation, Decentralised Ledger, data mining.**

## 1. INTRODUCTION

The interest in Block chain technology has been increasing, since the idea was coined in 2008. A blockchain is a decentralized ledger of all transactions in a network. Using blockchain technology, participants in the network can confirm transactions without the need for a trusted third party intermediary. Powerful applications include fund transfers, voting, and many other uses. A blockchain is defined as a public space including all Bitcoin transactions that have been made until the current transaction or the last transaction. As finished blocks are enclosed to it as and when the transactions are complete, the blockchain is becoming bigger and bigger. These blocks are coming into the blockchain following a chronological order, in a linear way. The computers which are part of the Bitcoin network are called nodes. All of these nodes receive a copy of the blockchain, this taking place automatically when a client joins the Bitcoin network. There is a lot of information included in the blockchain, for example the addresses and their balances from the beginning until the newest completed block

.

### 1.1 Bitcoin concept

"Bitcoin is a Peer-To-Peer Electronic Cash System". Bitcoin is digital money that is not issued or controlled by anyone. It is used to securely store and transfer any amount of value anywhere in the world. It is used to buy goods and services, store wealth, or send value to anyone without the permission a cryptocurrency and worldwide payment system. The word cryptocurrency is the label that is used to define all networks and mediums of exchange, uses cryptography to secure transactions; against those systems where the transactions are channeled through a centralized trusted organization or entity.

## 2. BLOCKCHAIN TECHNOLOGY

Blockchain (BC) is a distributed database that maintains a growing list of blocks that are chained to each other. BC was first proposed by Satoshi Nakamoto as the underlying technology behind Bitcoin. BC has been shown to possess a number of salient features including security, immutability and privacy and could thus be a useful technology to address the aforementioned challenges.

The structure of BC is shown in Figure 1. BC is managed distributedly by a peer to peer network. Each node is identified using a Public Key (PK). All communications between nodes, known as transactions, are encrypted using PKs and broadcast to the entire network. Every node can verify a transaction, by validating the signature of the transaction generator against their PK. This ensures that BC can achieve trustless consensus, meaning that an agreement between nodes can be achieved without a central trust broker, e.g. Certificate Authority (CA). A node will periodically collect multiple transactions from its pool of pending transactions to form a block, which is broadcast to the entire network. The block is appended to the local copy of the BC stored at a node if all constituent transactions are valid. A consensus algorithm such as Proof of Work (PoW), which involves solving a hard to-solve easy-to-verify puzzle, is employed to control which nodes can participate in the BC. Once a block is appended, it (or the constituent transactions) cannot be modified, since the hash of each block is contained in the subsequent block in the chain, which ensures immutability. A node can change its PK (i.e. identity) after each transaction to ensure anonymity and privacy.

Blockchain is of two kinds, permissioned and unpermissioned.

Permissioned ones work the very same way, yet are fit for limiting who in the system can approve the exchanges. A blockchain encourages secured online exchanges using cryptography by making cryptographic key combine with a wallet programming.

Unpermissioned one uses open dispersed record innovation that implies the data isn't claimed by any one individual or database, rather it is shared crosswise over different PCs in the system. Anybody can join the system and view those exchange records. Once an exchange is recorded, the information put away is time stamped, with the goal that it can't be erased or refreshed further. The ensuing augmentations to the record or new records are followed

and refreshed continuously for everybody with the entrance. Because of its circulated nature blockchain is hard to hack as every one of the duplicates are situated at better places.

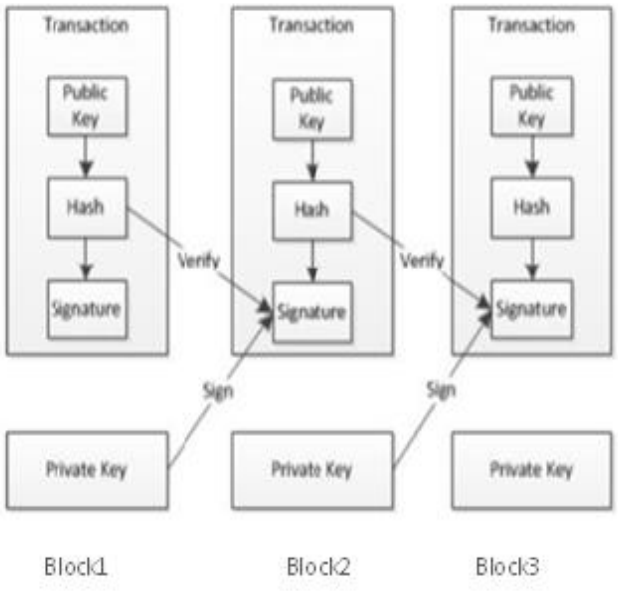


Fig -1 : Working of blockchain

## 3. BLOCK CHAIN IN FINANCIAL SERVICES

Blockchain technology enables people to perform transactions in a fully transparent way. No one mediates this transaction and therefore this entire technology makes things easier and much cheaper. There are numerous companies that began to use this accessible blockchain technology. The entire network is made up of nodes that are distributed servers. The nodes receive and process the transactions, and share the information further on. Thus, the business models are much more accessible to understand and seem quite impressive. These transactions which are recorded will permanently remain there. The entire network of computers which have Bitcoin software is responsible for the performance and the overall maintenance of the chain. In an entire hour, a number of approximately six blocks are created, and appended to the chain, and then transmitted to the nodes. The Bitcoin software will notice quite quickly when a Bitcoin amount has already been spent.This last feature is a lot utilized by organizations such as banks, developers, entrepreneurs. Among them, there is Santander Bank, which is in top 10 largest banks. They have also researched this technology and communicated that their team is working in order to find solutions to apply this innovation. International banks which are also interested in blockchain are Citi and JPMorgan. A lot of the startups start their business taking into consideration this technology. Companies like KPCB manifested their interest for an investment in these types of startups. There are startups such as Coinometrics that collect information and research regarding the qualitative and quantitative data about blockchains. BTCJam offers loans based on bitcoins.. All kinds of financial institutions are interested more and more in the blockchain technology and only Santander Bank has found around 25 cases to be used with this technology. This bank made an ample research and found that using blockchain by banks might reduce costs in infrastructure by up to $20 billion a year. UBS Bank have organized a research lab around blockchain in London. Goldman Sachs developed an investment in Circle, which is a Bitcoin startup. Also, NASDAQ does thorough research regarding this technology. This technology is most important because it allows people to perform transactions even if they're strangers, but in a fully transparent way. No mediator exists between the two entities of a transaction and in this way the whole process is performed not only easier, but also cheaper. This type of concept can be used in digital applications in the world, making transactions and exchanges secure.

## 4. CONCLUSIONS

It is a decentralized environment for transactions, where all the transactions are recorded to a public ledger, which will be visible to everyone. BlockChain helps by removing the involvement of third parties in any transaction. It can be implemented in the financial sector to avoid fraudulent activities. Blockchain technology runs the Bitcoin cryptocurrency. The goal of Blockchain is to provide anonymity, security, privacy, and transparency to all its users. Despite, these attributes set up a lot of technical challenges and limitations that need to be addressed.

## 5. REFERENCES

[1] http://blockgeeks.com/guides/what-is-blockchaintechnology/.

[2] N.Anderson, "Blockchain Technology A game-changer in accounting?," unpublished.

[3] http://letstalkpayments.com/financialinstitutions-blockchain-activity-analysis/

[4] https://www.investopedia.com/terms/b/blockchain.asp

[5] https://www.coindesk.com/information/what-is-bitcoin/

[6] http://letstalkpayments.com/financial-institutionsblockchain-activity-analysis/

[7] http://appliedblockchain.com/

[8] http://www.investopedia.com/terms/d/distributedledgers.