Block Chain Technology

Ajay Tomer, ,Swarnika Vishnoi, Diksha Raghav, Assistant Proff Mr. Deepak Kumar
CCSIT, TMU, Moradabad, India
ajaytomerimt@gmail.com
swarnikavishnoi@gmail.com
diksharaghavimd@gmail.com
deepakchaudhary008@gmail.com

Abstract: **-A blockchain is a distributed database of records and a singly LinkedList of block, which iscontains number of transaction. Decentralized ledger used for exchanging digital currency, perform deals and transactions in a very secure manner. Each & every transaction is verified by each number of the network so as to validate the transaction made.Blockchain is a digital ledger which is programmed to record virtually everything of value. Bitcoin a form of virtual or digital money is based on open source cryptography protocol which makes the use of blockchain.**

I. .INTRODUCTION

The introduction of cryptocurrencies ("Bitcoin") is mainly responsible for bringing the blockchain technology into the mainstream. Blockchain is a distributed database of records; decentralized ledger most commonly used for exchanging digital currency, performs deals and verified transaction in a secure manner each transaction in public ledger is verified by consensus of a majority of the participants on the system[1].

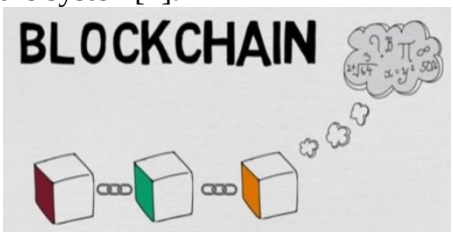

Figure 1

Block chain technology is not only limited the financial system but also provide great solution for almost any platform or product that require trustworthiness.The block of blockchain is not corruptible digital ledger of economic transactions that cannot be record just financial transactions but almost everything of significance."

A. Distributed Database:

Blockchain has exists information as a publicand continually acquiescent database. The database of blockchain is stored publicly and easily showable. A hacker doesn't corrupt this information because it not exist centralized database. The blockchain data is accessible to anyone on the internet by millions of computer simultaneously. [3].

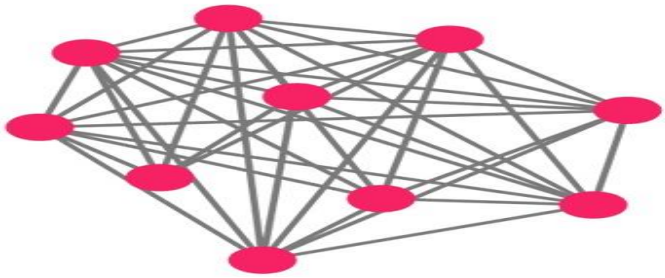

Figure 2

B.Durability and Robustness:

Blockchain technology has the information of every transaction block that's secure transactionin-built robustness. The blockchainstoring blocks of information which are identical on its network, the blockchain cannotbe controlled by any single node. That means if any single node is failed transaction are not affected.

C.Transparent and Incorruptible:

The blockchain is work on the consensus, that means when the transaction isgoing this information is float all the network of blockchain. Every 10 minutes it checks itself automatically.

1. *Transparency:* All the data are public on its network which is shared by sender.
2. *Incorruptible:* To transfer any information on the entire blockchain network it consume huge amount of computing power for encoding or decoding the information. That means the information is incorruptible for its security. [5].

D.Decentralization:

Blockchain is a decentralized technology.A blockchain technology uses by worldwide network of computers to mutuallyachieve the database that record bitcoin transactions. Blockchaindoes not have any one central authority.It is managed by its network. Decentralization means the network works on a peer-to-peer basis. [5]

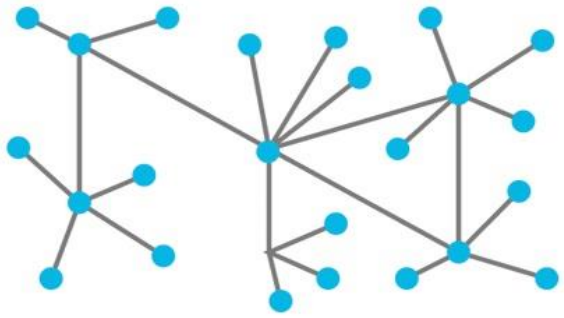

Figure 3

II. WORKING

We explain the idea of the blockchain by clarifying how Bitcoin works since it is innately linked to the Bitcoin. However, the blockchain technology is not applicable only to financial but also to non –financial world applications.

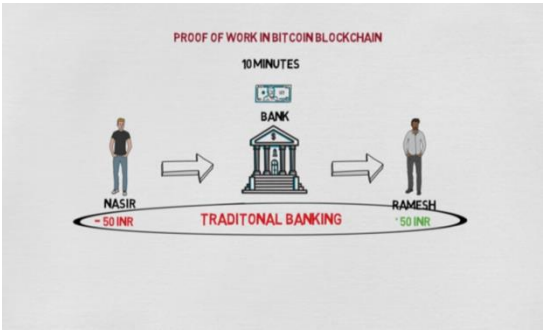

Figure 4

Bitcoin doesn't use third party interaction forthe transaction between two partiesto execute online transaction over the Internet. It usesthe concept of cryptography for every transaction [2].

Digital Signature is used to protect each transaction. For each transaction to transit, sender digitally signs in using "Private Key" and that transaction is received by receiver using "Public key".

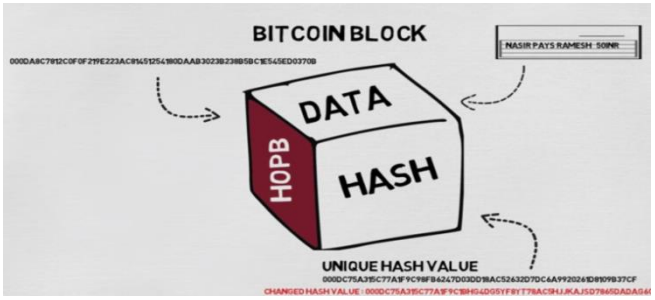

Figure 5

In order to spend money, owner of the cryptocurrency desires to show the ownership of the "private key". The objectgetting the digital currency proves the digital signature –thus ownership of equivalent "private key"--on the transaction using the "public key" of the sender. Every single transaction is broadcast to every node in the Bitcoin network and is then documented in a public ledger after verification. Each transaction needs to be verified for validitybefore it is recorded in the public ledger.

Before recording any transaction verifying node needs to ensure that two things that is:

1. Spender keeps the cryptocurrencydigital signature verification on the transaction.
2. Spender has suitable cryptocurrency in his/her account:make sure that he/she has sufficient balance in his/her account for every transaction against spender's account ("public key") in the ledger.

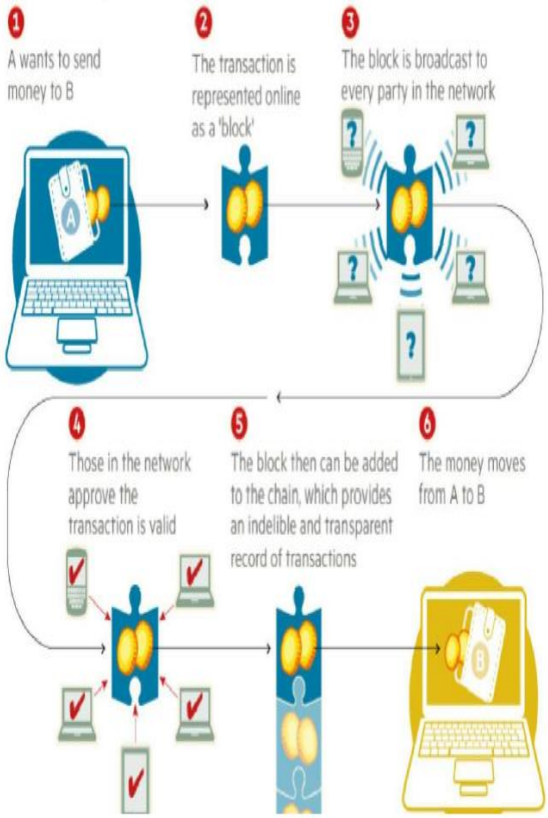

Figure 6

Eachtransactionis passed node by node over the Blockchain network, but there is no guarantee that orders in which they are received at a node are the same order in which these transactions were generated.

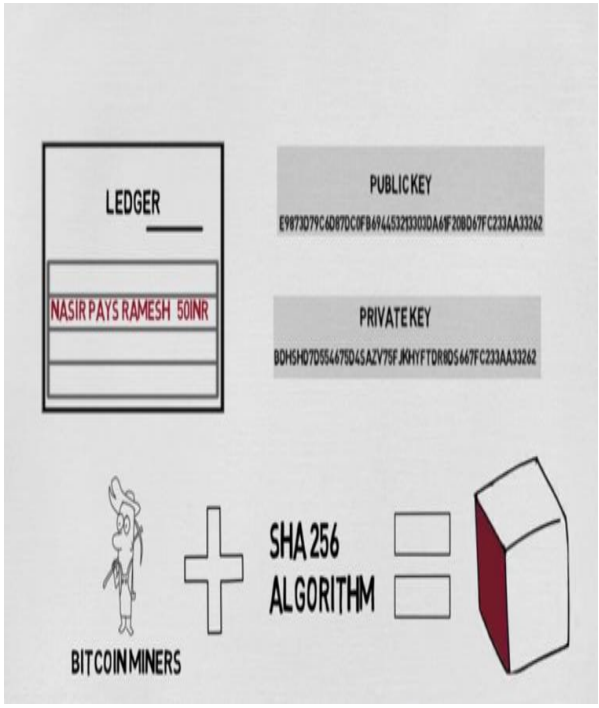

Figure 7

This means that there is need to develop a mechanism so that the entire Blockchain network can agree regarding the order of transactions, which is a daunting task in a distributed system.

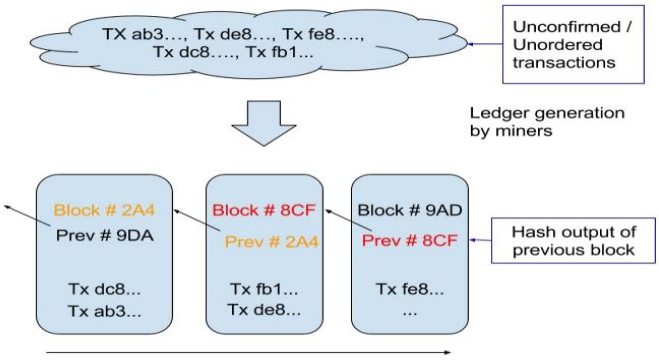

Figure 8

Double spending due to propagation delays in peer-to-peer network [4].

III. APPLICATION

Iinternational payments: If one wants to transfer money to a person in another country, they use

a bank/money exchange based wire transfer. This process of wire transfer takes two business days. Using Blockchain, this transaction would be done in less than 10 minutes with transaction fees of around 15–50 US cents [2].

Trade Finance:A document issued by the bank guarantees a seller about the accuracy of time and value from the buyer. If a buyer is unable to make payments, the bank will cover the full or remaining amount of the purchase. This is a widely tool due to difference in laws and economy of multipleregions and countries involved, where the possibility of valid and timely payments are not guaranteed.

Securities Trading**:**Stock exchanges are experimenting with Blockchain technology to streamline time-consuming and inefficient processes involved in trading securities. Certain long-winded, complex processes like pre-trade, trade, post-trade and custody, and securities servicing involved are time consuming. For this reason, exchanges are experimenting with blockchain technology [2].

Smart Contracts**:**A Smart contract is nothing but a piece of code stored on all computers of the blockchain network. It defines a set of conditions to which all parties using the contract mutually agreed upon. Once the required conditions are met, certain actions are executed and all members of the network get to the same result by executing this action. This enables smart contracts to execute contractual obligations without any human intervention.

Supply Chain Tracking: Blockchain can ease the tracking of items across the global supply chain. By the blockchain technology a product is tracked at every stage when it is created and all information about this item who handled it and when.

IV. LITRATURE SURVEY

ADVANTAGE

- Disintermediation:Blockchain is that it enables a database to be directly shared without a central administrator. The blockchain is a consensus mechanism to confirm the nodes on a network and all transactions are verified and treated independently.

- High Quality Data: Blockchain data is complete, consistent, timely, accurate, and widely available.

- Durability, reliability, and longevity: Blockchain Does not have a central point of failure because it uses the decentralized network.

- Process Integrity: Users can trust the transaction will be executes exactly, it does not need trusted third party.

- Transparency and Immutability: It creates transparency when any changes to public blockchain are publicly viewable by all vendors. And all transaction they cannot be deleted that means transaction are immutable.

- Faster Transaction: It can reduce transaction time to minutes and are processed 24/7 [7].

V. DISADVANTAGE:

- **Performance**

  The Blockchain database is used the concept of decentralization this is the cause it is slower than centralized databases. When a transaction is being processed, a blockchain has to do all the same things just like a regular database do, but it carries three additional burdens as well:

  A. **Signature verification:** Every blockchain transaction must be digitally signed using a public-private cryptography scheme such as ECDSA.The generation and verification of these signatures is computationally complex, and constitutes the primary bottleneck in products like ours.

  B. **Consensus mechanisms:** Blockchain technology is depend on the consensus that means if we want to transfer any data to other node it doesn't transfer whenever all the network miners are not verify this information.Centralized databases must also deal with inconsistent and cancelled transactions.

  C. **Redundancy.** In blockchain technology if the transaction process once or twice they must be processed individually by every node in the network. That means there is lot of work are doing for the same result.

- Nascent Technology**:** To making for widely applicable of blockchain use this technology. It resolves such as verification process, transaction speed and data limits.

- Large Energy Consumption**:** The blockchain technology uses the substantial amount of computer power to validate transection Bitcoin blockchain miners.

- Control, Security and Privacy**:** When the transaction is processed, all the miners have the full information about the transaction or sender and receiver this should be harmful for cyber security.

- Cultural Adoption**:** Blockchain shows full information to a decentralized network which needs the buy-in of its users or operators.

- Cost**:** Blockchain saving in transaction cost and time but the high initial capital costs could be deterrent [7].

VI. FUTURE SCOPE

The future of finance could be dominated by blockchain technologies. A Blockchain technology completes with awell-organized infrastructure.

Control: New technologies such as blockchain have the potential to reduce cyber risks by offering identity authentication through a

Crime: The blockchain technology startup software helps to track down criminal faster and cheaper claimed.

Banks: If the central bank is adopt blockchain concept then all branches hasinformation about the particular userand cryptographically secured currencies will become widely used.

Industries: The blockchain has ability to decree se or discardtrustworthy counterparties in the transaction process.

Governments: The future of finance in many nations could be dominated by Bitcoin and cryptocurrencies.Blockchain technology could be used to distribute social welfare in developing nations [6].

VII. CONCLUSION

To conclude, Blockchain is the technology which is backbone of Bitcoin crypto currency. The distributed ledger

functionality is united with security of Blockchain, makes it very attractive and smart technology to resolve the present Financial as well as non-financial commercial problems.

The Bitcoin Cryptocurrency is based on the Blockchain technology. This is either in the downward slope of overstatedbeliefs or in trough of disillusionment.

REFRENCES

[1]Bitcoin: A peer-to-peer electronic cash system. S. Nakamoto. 2008.

[2] Bitcoin: An innovative alternative digital currency. R Grinberg. 2012. *HeinOnline Hastings Sci. & Tech. LJ*.

[3] The Future of Bitcoin: Mapping the Global Adoption of World's Largest Cryptocurrency through Benefit Analysis. JK Darlington III. 2014

[4]SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. Bonneau J, Miller A, Clark J, Narayanan A, Kroll JA, Felten EW. S&P '15.

[5] The Bitcoin Backbone Protocol: Analysis and Applications. Garay J, Kiayias A, Leonardos N. EUROCRYPT '15.

[6] Distributed Cryptography Based on the Proofs of Work. Andrychowicz M, and Dziembowski S. '14.

[7]https://en.wikipedia.org/wiki/Blockchain

[8]https://www.hindustantimes.com/tech/blockchain-technology-explained-here-are-its-top-features/story-HtaoYSTbL8d4bfHeCUK6tM.html

[9]https://www.newgenapps.com/blog/future-of-blockchain-technology-applications

[10]https://blockchaintechnologycom.wordpress.com/2016/11/21/advantages-disadvantages/