BlockChain Technology

Ajay Tomer
Student MCA (LE)
CCSIT, TMU, Moradabad, India
ajaytomerimt@gmail.com

Swarnika Vishnoi
Student MCA (LE)
CCSIT, TMU, Moradabad, India
swarnikavishnoi@gmail.com

Diksha Raghav
Student MCA (LE)
CCSIT, TMU, Moradabad, India
diksharaghavimd@gmail.com

Mr. Deepak Kumar
Assistant Professor
CCSIT, TMU
Moradabad, India
deepakchaudhary008@gmail.com

ABSTRACT: - A blockchain is a distributed database of records and a singly LinkedList of block, which is contains 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.

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].

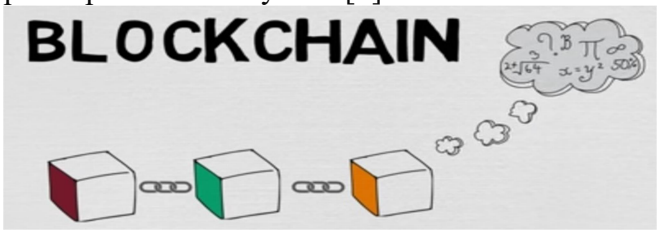

Figure 1

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 blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value."

A Distributed Database:

Information held on a blockchain exists as a shared and continually reconciled database. The blockchain database isn't stored in any single location, meaning the records it keeps are truly public and easily verifiable. No centralized version of this information exists for a hacker to corrupt. Hosted by millions of computers simultaneously, its data is accessible to anyone on the internet [3].

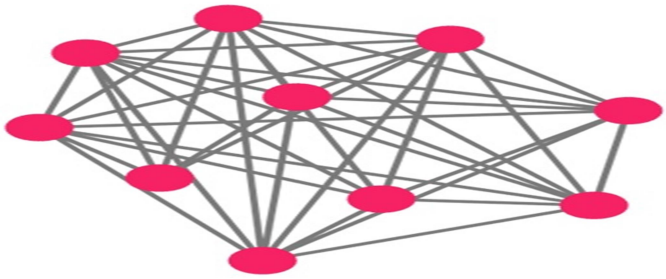

Figure 2

Durability and Robustness:

Blockchain technology is like the internet in that it has a built-in robustness [5]. By storing blocks of information that are identical across its network, the blockchain cannot:

1. Be controlled by any single entity.
2. Has no single point of failure.

Transparent and Incorruptible:

The blockchain network lives in a state of consensus, one that automatically checks in with itself every ten minutes. Each group of these transactions is referred to as a "block".

1. **Transparency** data is embedded within network as a whole, by definition it is public.
2. **It cannot be corrupted** altering any unit of information on the blockchain would mean using a huge amount of computing power to override the entire network [5].

Decentralization:

Blockchain is a decentralized technology. A global network of computers uses blockchain technology to jointly manage the database that records Bitcoin transactions. That is, Bitcoin is managed by its network, and not any one central authority. Decentralization means the network operates on a user-to-user (or peer-to-peer) basis. The forms of mass collaboration this makes possible are just beginning to be investigated [5].

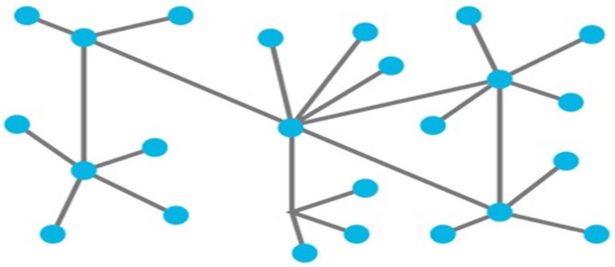

Figure 3

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.

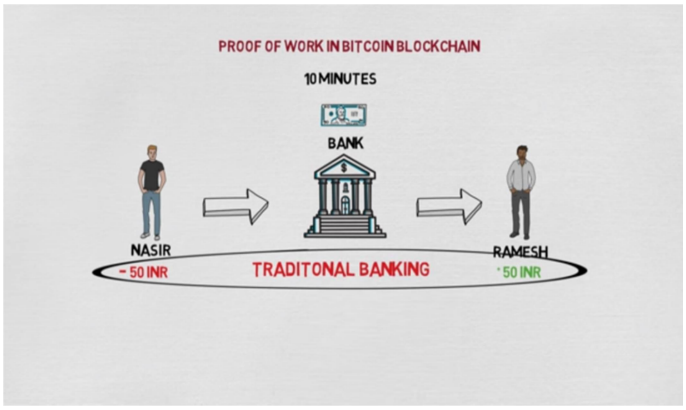

Figure 4

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

theDigital 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".

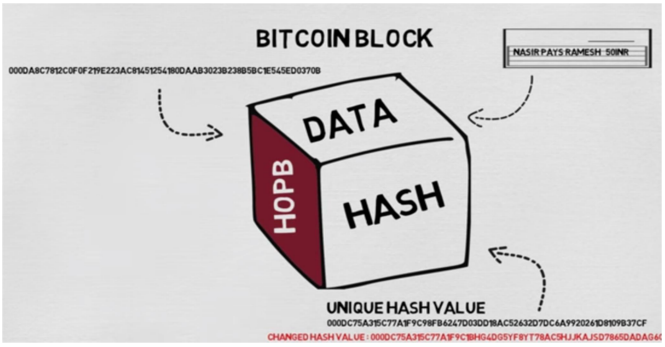

Figure 5

In order to spend money, owner of the cryptocurrency desires to show the ownership of the "private key". The object getting 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 validity before 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 cryptocurrency digital 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.

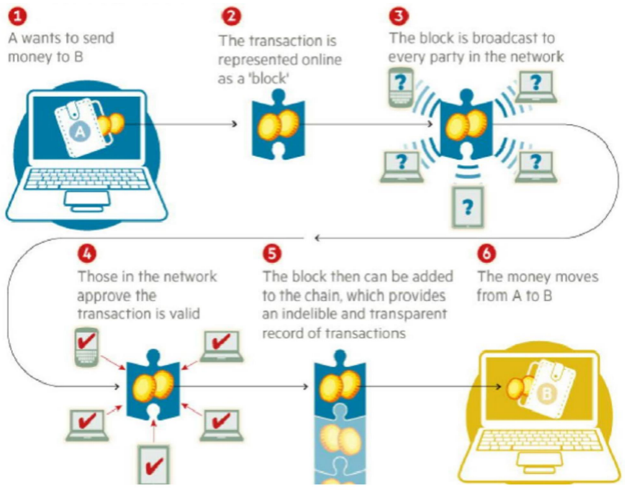

Figure 6

Each transaction is 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.

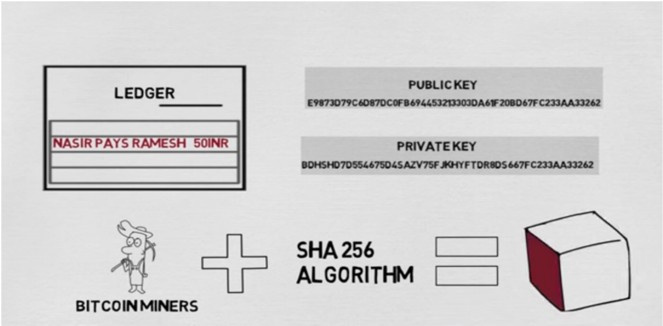

Figure 7

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.

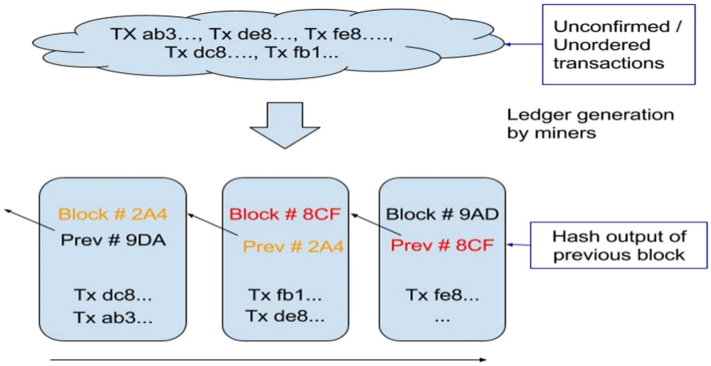

Figure 8

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

APPLICATION

Payments

International 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 multiple regions 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. The product can be tracked at every stage creating the record of the location, who handled it and when.

LITRATURE SURVEY

ADVANTAGE

- **Disintermediation:** Blockchain is that it enables a database to be directly shared without a central administrator. The blockchain acting as a consensus mechanism to ensure the nodes stay in sync, transactions can be verified and processed 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].

DISADVANTAGE:

- **Performance**

  Because of the nature of blockchains, it will always be 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, effort must be expended in ensuring that nodes in the network reach consensus. Centralized databases must also contend with conflicting and aborted transactions, these are far less likely where transactions are queued and processed in a single location.

  C. **Redundancy**. This centralized database process transactions once (or twice); in a blockchain they must be processed independently by every node in the network. So lots more work is being done for the same end result.

- **Nascent Technology:** This technology resolve such as transaction speed, verification process, and data limits to making blockchain widely applicable.

- **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].

FUTURE SCOPE

The future of finance could be dominated by blockchain technologies. A traceable global currency complete with an efficient infrastructure will not only result in massive.

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

Crime: A new blockchain startup has claimed its software could help track down criminals faster and cheaper than ever.

Banks: Blockchain will be adopted by central banks and cryptographically secured currencies will become widely used.

Industries: Time and education will need to play a role as other industries are just realizing one of the core innovations of the blockchain is its ability to reduce or eliminate trusted 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].

CONCLUSION

To conclude, Blockchain is the technology backbone of Bitcoin. The distributed ledger functionality coupled with security of Block Chain, makes it very attractive technology to solve the current Financial as well as non-financial business problems.

As far as the technology is concerned, the cryptocurrency based tech is either in the downward slope of inflated expectations or in trough of disillusionment as shown in Figure

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/