BLOCKCHAIN TECHNOLOGY: AN INTRODUCTION

Neerja Arora
Assistant Professor, Ajay Kumar Garg Engineering College Ghaziabad, U.P., India
aroraneerja@akgec.ac.in

Abstract: **Blockchain Technology allows the exchange of digital assets through online mode in a secured and transparent way i.e. it facilitates the new path forcompleting the transactions and conducting the business online.Many Businesses have initiatedto invest in the blockchain market with expectations to gethuge profit in upcoming years. Blockchain has become more popular because of its enhanced security and ability to eliminate digital identity theft issues because of usingthe distributed public ledger in a decentralized network and implementing the Encryption techniques.This article includes theintroduction about Blockchain technology, various types of blockchain architectureavailable in the market, how it works, benefits and various applications or use cases of blockchain in different fields.**

Keywords: **Transactions, Blocks, Ledger, Hash, Nonce, Previous Hash, Smart Contracts, Encryption, Immutable, Cryptography, Consensus**

I. INTRODUCTION

With an increase in the number of smartphones and the adoption of digital payments and e-commerce, India's digital payment ecosystem is rapidly growing. Digital payment transactions have grown by 76% in the past one year, with several new digital payment users. However, as the number of digital payments continues to grow, cyber-threats and security concerns are also growing. Therefore, some technology is needed to facilitate secured transactions. An emerging and revolutionary Blockchain technology is attracting a lot of public due to its capability to reduce various risks and frauds associated with transactions. Basically, itfollows peer-to-peer network architecturewhere the public ledger isshared to all nodes of the network that makes the records of any digital asset- transparent and immutable and works without the involvement of any third-party as intermediary.

Blockchain also facilitates to record all the transactions and track anything valuableon the network.A*digital asset* may be anything visible (a house, vehicle, money) orinvisible (copyrights, computer softwares, trademarks, intellectual property, patents, etc.

Bitcoin is one of the most popularexamples ofcryptocurrency which follows blockchain technologyand uses a shared distributed ledger. Blockchainfacilitates the framework tostore and transit bitcoins(cryptocurrency)through thepowerful computational algorithm which is storedon a decentralized blockchain network.Blockchain technologyisnot limited todoing transactions but, it canalso be used as repository and inventory for the digitalassets[1].

Who Proposed Blockchain Technology?

In 1982, acryptographer David Chaum proposed the concept of blockchain technology. After that in 1991, Stuart Haber and W. Scott Stornetta presented their work on Consortiums. But, it was Satoshi Nakamoto (a fictitious name representing a individual or group of people) who deployed the Bitcoin (world's first crypto- currency) and invented the first blockchain network.

Consider a current banking system in which users have their account in some bank/Financial Intermediary which manage their all the money. User cannot do any transaction without the involvement of the third party (Bank/Government/Financial Intermediary) and all the transaction records of a user are maintained at centralized Ledger and managed by the Bank itself. There are many issues related to Traditional Banking System, which are as follows*:*

- **High transaction fees:** You cannot access or send the money to someone without the permission from the bank and also have to pay transaction fees to the bank.
- **Double Spending issue**: Sometimes, digital money can be spent twice. Because in traditional banking system second transaction can be initiated without the confirmation of first transaction
- **Hacking:** Traditional banking system uses centralized network i.e. all details and transaction recordsare stored at single point which are vulnerable to attacks.

As Blockchain is a peer-to-peer network with secure, trusted and shared public ledger which storesthe recordsof all the transactions across various participants(computer nodes) so that data cannotbechanged. So, all the issues related to current banking system can be resolved by using Blockchain technology.

II. BASIC PRINCIPLES OF BLOCKCHAIN

a) Decentralization

In Blockchain technologythere is no single authority (user) that controls the transaction, each participant in the network has equal authority to manage the transactions, which means no single person can hack, modifies or end the blockchain or can shut it down.

Thus, blockchain network is free from any hacks or frauds.

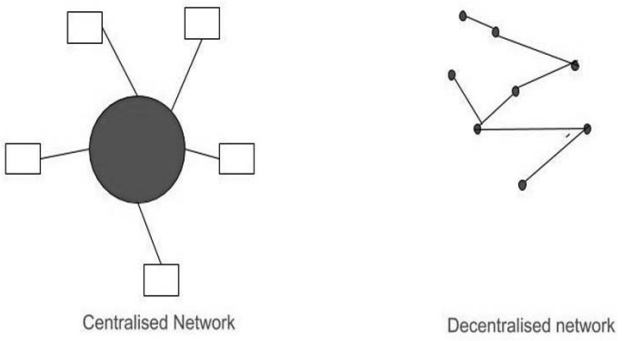

Figure 1: Centralized and Decentralized Network

In Blockchain Networks, transactions are executed only if all the participants involved in consensus mechanism verified the requested transactionwhich results in smoother, safer and faster transactions[6].

b) Shared PublicLedger

Blockchain networks uses public distributed ledger that makes transaction records to be stored across many computers.In case of centralized ledger,there is a chance that ledger get corrupted and the data being tampered. But, public distributed ledger solves this problem because if someone manipulates the data at any node, then that will be noticed at other nodes As transactions are verified and approved by all the active participants available in the blockchain network, making it less prone to cyberattack.

c) Immutable Records

Since in a Blockchain network, each user has copy of the transaction details(block) and every block contains the hash of its previous block, therefore if intruder tries to tamper with the data in some block then the hash of the following blocks will be changed.

So, he needs to change the 'Previous hash' field of all the following blocks, which is not easy at all. Hence, the data in the Blockchain is tamper proof and authentic.

d) Enhanced Security using Encryption

Blockchain Networks uses powerful cryptographic algorithms which ensure that all the transactions of Blockchain are kept secure and integrity is also maintained. Thus,users have to put their trust in cryptographic algorithms instead of relying on third-party. By using cryptographic algorithm (SHA256) unauthorized access to blockchain is eliminatedand blockskept secure.

e) Consensus

Blockchains are growing because of implementing consensus algorithms. These algorithms areused for making decisions for updating Blockchain network by the active participants (miners) of the network. Consensus method basically speeds up the process.

The consensus method is required for the network because of trust issues among participants.

Participants can trust the algorithms rather than trusting each other.

Consensus method [5] is important for a system so that transactions can be completed smoothly, when large number of nodes are involved in validating a transaction.In this process, decision is go with the majority.

Various Consensus Algorithms:

- Proof of Stake
- Directed Acyclic Graphs
- Proof of Weight
- Proof of Activity
- Proof of Capacity
- Proof of Work
- Proof of Burn

f) Smart contracts

These are the computer programs stored on the Blockchain networks to automate the execution of transactions. They automatically execute when predetermined terms and conditions defined in contracts are satisfied.

Processing time and cost is also saved by using smart contracts and everything about the project stays fair to both seller and buyer.

III. TYPES OF BLOCKCHAIN ARCHITECTURE

Various types of blockchainsare explained as below:

a) Public Blockchains

These are accessible to anyone who wants to request for new transaction or interested to participate in validation process of transactions. Participants who are involved in validation process of transactions will receive rewards. Proof-of-work or Proof-of-stake consensus methods are used by these public blockchains. Ethereum (ETH) and Bitcoins are two examples of public blockchains.

b) Private Blockchains
These blockchains are not available to everyone and have access restrictions. People cannot join these blockchains without getting permission from the system administrator. Organisationsuse private blockchains to customize their accessibility and authorizationpreferences, networkparameters and for other importantsecurity options. Private blockchains are managed by single authority that means they are centralized.

Hyperledger is a example of private, permissioned blockchain.

c) Consortiums/ Hybrid Blockchains
These Blockchains are created by combining both public and private blockchains. Thus, they contain features of both. Also sometimes known as Permissioned blockchains which allow access to individuals who are authorized. Organizations uses these Hybrid blockchains to get the best features of both andit provides better solution when decision is to be taken that who can participate in the network and in what transactions.

Energy Web Foundation, Dragonchain, and R3 are Hybrid Blockchain examples.

d) Parallel Blockchains/Sidechains
These are the blockchain which runs parallel to the main chain. Using these blockchains users can move their digital assets from main blockchain to sidechain or vice-versa.It improves the scalability and efficiency of the system.
Liquid Network is an example of sidechain.

IV. WORKING OF BLOCKCHAIN NETWORK

All Transactions through Blockchain Networks are executed by following the below steps[5]:

Step 1: A transaction is initiated and requested by a user on a blockchain Network. This transaction is about either to transfer somevaluable information or monetary value.

Step2: Details of the requested transaction are stored in a block which is created to represent the transaction.

For each transaction, there exists a block which stores all the related information of a transaction. Basically, a chain of blocks that stores information of all transactions occurred is called Blockchain.

Each block contains:

a) **Data (Transaction Details) –** Aggregated information of a transaction that need to occur. In case of Bitcoin, it contains address of the Sender and Receiver and amount of the Transaction.

b) **Nonce-**A 32-bits arbitrary number that is randomly generated whenever a new block is created. It is used by cryptographic algorithm so that unique hash address can be generated for each block.

c) **Hash value:** It uniquely identifies a block and used to provide security to a block. For calculating Hash value for a particular block, Hash function is used which takes (Data, Nonce and Previous Hash) as input and generates the (Hash Value) as output of fixed size i.e. 256 bits.

d) **Previous Hash:** Previous hash value refers to the immediate previous block i.e. every block is linked to its previous block.

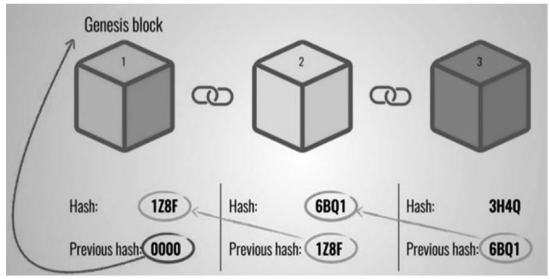

Figure 2: Chain of Blocks

The first block is called as **Genesis Block.**

Step3: The created block for the requested transaction is now forwarded to other participants of the network. In public blockchains, block is forwarded to all the participants of network.

Step4: All active nodes now start validating transaction using consensus algorithm. For Bitcoins, Proof of Work (PoW) method is used.

Step 5: Once the transaction gets validated, the active nodes involved in validation process receives reward for their effort and block is added to the blockchain.

Step 6: The transaction is now complete.

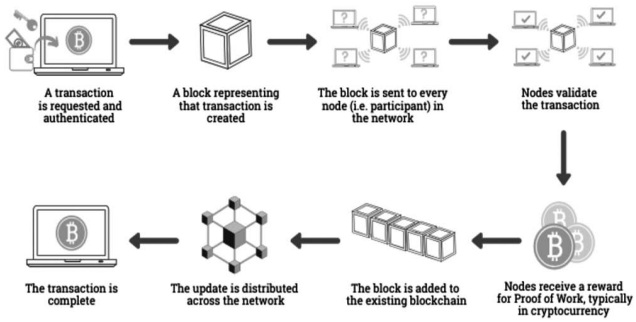

Figure 3: How does a transaction get into the Blockchain

The process of updating the blockchain or adding new block/ (transactional details) to the existing Blockchain is known as **'Mining'.**[6]

People who add blocks in a chain are known as **Blockchain miners**, they do so by solving a mathematical problem using computational cryptographic algorithms, which is known as **Consensus problem** andthe miner who solves this problem first receives a monetary reward.

In the Mining process, hash value of a block is generated, which is hard to forge. Thus, the security of the Blockchain is ensured without the needof centralized authority.

Consensus algorithm-(Proof-of-work)

It is a mechanism to add a new block to existing blockchain in a secured manner. Use of consensus method makes it difficult to tamper with the blocks, because if someone manipulates one block then, he needs to solve the proof-of-work problem for all the following nodes.

So, blockchains get secured by creative use of hashing as well as the proof-of-work algorithm.
Every block of the blockchain contains **unique 32 bitnonce value, its own hash value** and **hash value of immediate prior block** of the chain. So, mining is a difficult process, especially for the large sized chains.

To solve thecomplex mathematical problem (Proofofwork) miners uses specific software to find a correct **nonce**value so that **accepted hash value**can be generated.

As,the size of nonce value is 32 bits and size of hash value is 256 bits, there are about 4 billion possible nonce-hash combinations that must be mined before the accepted hash valuecan be found.

For accepted hash value, the corresponding nonce value is known as **"golden nonce**" and the first miner to solve the problem will broadcast his solution to the network, and others can approve his work and earn their share of the transaction fee. In this way, it can be ensured that only the miner who has invested enough work will earn the right to update the Blockchain.

V. APPLICATIONS/USE CASES OF BLOCKCHAIN IN REAL WORLD

a) Cryptocurrencies
Cryptocurrencies are the major application of blockchain for example, Bitcoin. Bitcoin is a decentralized distributed shared public ledger digital currency introduced by Santoshi Nakamoto which facilitates secured transactions.

b) Blockchain as a Use Case in Banking
The banking system employs concepts of Blockchain. In current scenario, whenever a user visits a bank, his identity needs to be validated in order to perform a transaction. But with use of blockchainand its concepts like truffle, ganache, ethereum etc., the transaction gets validated repeatedly by cryptography employed with blockchain and funds gets transferred as required.

With the use of blockchain the middleman costs incurred per year can be reduced to a great extent, amounting to approximately 19.8 billiondollars. Blockchain and its applications also includes solving double spending issue as hacking of accounts would be difficult or near to impossible.

c) Real Estate
Real estate industry is the one which can be greatly benefitted by use of blockchain technology and smart contracts as it would ease out the whole process of buying and selling a property. Currently the whole ecosystem of real estate is lacking efficiency as the process of sale and purchase of property is quite trouble some and takes a lot of time to complete the whole transaction process. With use of smart contracts, the whole ecosystem of real estate will be benefitted as buying and selling will be automated and ownership proofs and checks can be done in a reliable fashion. Apart from reliability and automation whole process will be cost effective, which would be an added advantage of employing blockchain.

d) Music
Since the advancement of music industry by use of digital media, issues of piracy and money related matters involved with it are not transparently handled. The use of blockchain could resolve this issue to a great extent, by preventing ill practices of unauthorized sharing and distribution of music related content. The artists can be compensated well if the piracy and illegal sharing issues are resolved.

e) Cyber Security
Blockchain also has its impact in cyber security as many of the tech giants like Lockheed Martin is employing it to ensure smooth operation among its cyber division. Sensitive information and data can be properly protected using cryptography features employed with blockchain. The whole process of protecting and authenticating users and devices using passwords is replaced by the use of public private keys used for encryption and decryption of sensitive data.

f) Voting
Voting and election process can also be benefitted using Blockchain technology. The whole process of blockchain is free from irregularities so that data and identities of voters can't be compromised, which would prove to be effective for validating users.[3]

g) Human Resources

Another domain in which blockchain can be effectively used is human resources.The human resource employment and hiring involves various validation and verification checks to be performed on potential candidates for a job. Operations like verification of previous employment details and packages could be ascertained using blockchain in an easy and error free manner.

h) Law Enforcement

Blockchain could also prove to be effective technology solution for law enforcement agencies as it would help them to maintain centralized record of criminals and their associated crimes for effective management. Criminals previous history can be maintained easily in a confidential manner with no issue of security breach or unauthorized access to information maintained in centralized criminals database. [3]

i) IoT(Internet of Things)

The concepts of blockchain are now a days employed in the field of IOT also. IOT involves a lot of digital data moving around the network among devices or nodes connected in a particular fashion. Employing blockchain concepts could prevent the unauthorized access to the whole digital data moving around to unauthorized users.[3]

j) Energy Market

Another field which would be benefitted by use of blockchain will be energy sector. The concepts in the blockchain technology network can help energy sector related companies to provide easy and error free services to their customers. The whole energy sector related companies are revolutionizing their ecosystem by switching towards use of blockchain technology in order to provide consumers with easy to manage services without any interference from centralized authority.

VI. CONCLUSION

Blockchain is a revolutionary and growing technology as it is capable to complete all the transactions among users in a secured, trusted, faster and transparent wayand evolved as a game changer for many industries.

Blockchain has attracted various entrepreneurs with its features and changed the way of conducting the businesses by eliminating the frauds, corruption and establish the ownership of common mass. This decentralized technology definitely contribute to economic growth and will also bring new possibilities in future. It is not easy to predict what lies ahead, but it is sure that the best is yet to come through blockchain technology.

REFERENCES

[1] "Understanding Blockchain Technology" article by Simanta Shekhar Sarmah available at https://www.researchgate.net/publication/336130918_Understanding_Blockchain_Technology.

[2] What is Blockchain Technology? available at https://www.ibm.com/in-en/topics/what-is-blockchain.

[3] Most Popular Application of Blockchain available at www.educba.com/applications-of -Blockchain.

[4] How Blockchain works? availableat https://www.builtin.com/blockchain

[5] How Does Blockchain Work: Simply Explained available at https://101blockchains.com/how-does-blockchain-work

[6] What is Blockchain Technology and How Does It Work? Available at https://www.simplilearn.com/tuorials/blockchain-tutorial/blockchain-technology.

ABOUT THE AUTHOR

Ms. Neerja Arora, is currently working as Assistant Professor (CSE department) in Ajay Kumar Garg Engineering College, Ghaziabad. She has completed her B.Tech from Lingayas's College, Faridabad (formely affiliated to Maharshi Dayanand University, Rohtak and now a deemed university) and M.Tech from TIT&S College, Bhiwani. She has more than 7 years of teaching experience. Her area of interests is image processing and machine learning.