Blockchain

Blockchain is a decentralised and distributed digital ledger which takes only similar types of information also called records and store that records in a series of blocks and the order should be in chronological system. Each block has three things cryptographic hash of the previous block, a timestamp, and transaction data. Here all the blocks are connected/linked together via a cryptographic mechanism. These blocks create a chain of data values as an asset, it maybe tangible or intangible moves from place to place. All the blocks give the surety about the exact time and also sequence of transactions. Each block link securely altogether to restrain any block from being altered or a block being inserted between two existing blocks. Miners create a new block on the chain system through a process which is called mining. Here transactions are blocked together in an irreversible chain. In case of security it provides high security because of its decentralised mechanism in which no central authority can enter into it. This technology is running by millions of computer chain and the transaction copies are shared to everyone those who are connected in the transaction process. Here in this Blockchain technology initially client initiates the transaction through peer to peer network after that check validation and verification and then adding to the ledger and in between Stakeholders verifies the transaction details.

The problems that we are facing in the current central authority system, in case of banking system if we want to send some money from one party to another, here central authority first check the first party's account is the money available is his account or not if it is ok then he/she will give the permission to the first party to send the money after that the money will send to the receiver side, here many problems may arise first of all time delay issues are there then if any mistake happen in center side then both party will face the problems. In the current system if we want to send money for example from India to USA then there is a multistep process that involves a lot of intermediaries which takes lots of time and also requires a hefty amount of money. Other problems are in case of Supply Chain Management system and Health care system also we are facing lots of problem in our day to day life and many more. So, it's a very big issue now-a-day. We can overcome all these issues by Blockchain technology. It will act as the bridge that covers the trust deficiency during a transaction and reduce time complexity. It improves transparency, immutability and efficiency aspects, which set it unique from other.

There are various types of underlying technology present in the Blockchain technology such as:

Distributed Systems: It is also called as computing paradigm whereby two or more nodes working together in a coordinated fashion to achieve a common outcome. All the nodes in the system are capable of sending and receiving messages to and from each other.

Asymmetric Key Encryption: It is known as public-private key cryptosystem technique, serves to create identities on a Blockchain. Here user creates two elements, a public key which is basically used for identify their transactions on the Blockchain system, and a private key which is required to conduct a transaction with the public key.

Hash Values: It is an algorithm which is used to convert the verified transaction into set of unique numbers and letters, similar like RPG (random password generator). Bitcoin uses SHA256 algorithm for generating hash number.

Peer-to-Peer Networks: It allows the computers which are connected in the network they can directly connect with each other without any reference, instruction, or routing of a central authority and also allow for the sharing of files, computational resources, and network bandwidth among those in the network.

Merkle Trees: It is a hash-based data structure. It is look like a tree structure in which each leaf node is a hash of a block of data, and each non-leaf node is a hash of its children. It is mainly used in distributed systems for efficient data verification.

Blockchain have several properties:

i. Distributed ledger technology (DLT), makes the historical backdrop of any digital resource unalterable and straightforward using decentralization and cryptographic hashing.
ii. Immutable records, any records after validation are irreversible
iii. Smart contracts, the features in Blockchain 2.0 that executes contracts upon completion of another event, a computer code that can be built into the Blockchain to facilitate, verify, or negotiate a contract agreement.

iv. Secure, here in this technology all the records are individually encrypted.
v. Anonymous, the identity of any participants is either anonymous or pseudonymous.
vi. Distributed, all the participants that are working in the network have a copy of the ledger for the complete transparency.
vii. Time stamped, recorded on a block for further transaction process.

History of Blockchain:

Cryptographer name David Chaum was first proposed a Blockchain-like protocol in his 1982 dissertation "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups". It was outlined in 1991 by Stuart Haber and W. Scott Stornetta, these two researchers who wanted to implement a system where document timestamps could not be tampered with. In 1998 Computer scientist Nick Szabo works on 'bit gold', a decentralized digital currency. In 2000 Stefan Konst publishes his theory of cryptographic secured chains, plus ideas for implementation. In 2008 Developer(s) working under the pseudonym Satoshi Nakamoto release a white paper establishing the model for a Blockchain. In 2009 Nakamoto release the first Blockchain as the public ledger for transactions made using bitcoin. In 2014 Blockchain 2.0 is born, referring to applications beyond currency. By following Blockchain, smart contract was concocted in 1994 by Nick Szabo. A set of executable codes are Smart Contracts that can straightforwardly run on top of the Blockchain systems. Agreement between untrusted parties without the requirement of an outsider is implemented by this technology system. Smart contracts are permitted in monetary exchanges than Bitcoin.

By market capitalization Bitcoin and Ethereum are the two major Blockchain applications in the market now-a-days**. Bitcoin** is the first and the largest cryptocurrency by market capitalization. In 2008, the first Blockchain was conceptualized by Satoshi Nakamoto, an anonymous person by his publishes "Bitcoin: A Peer to Peer Electronic Cash System". In 2009, the first effective Bitcoin (BTC) transaction occurs between computer scientist Hal Finney and the mysterious Satoshi Nakamoto. It is mainly used SHA256 algorithm to 'hash' data into a 256-bit number. **Ethereum** is a decentralized and open-source Blockchain technology with the functionality of smart contract system. Ether is the native cryptocurrency sysetm. After Bitcoin cryptocurrency system, it is the second-largest by market capitalization. **Hyperledger** is a global enterprise Blockchain project that offers the necessary framework, standards, guidelines, and tools to build open source Blockchains and related applications for use across various industries.

Gas, for creating a block, each transaction is charged with a certain amount of gas, whose purpose is to limit the amount of work that is needed to execute the transaction and pay for execution at the same time.

After the competition of the transaction how we can ensure that this transaction is valid or not? To solve this problem there is a technique called Transaction Validation. It is the process of determining if a transaction conforms to specific rules to deem it as valid. Validators tying to check if transactions meet protocol requirements before adding the transactions to the distributed digital ledger as part of the validating process.

How the block is created in the Blockchain system? Actually, the block is created by the Miners. They create new blocks on the chain through a process called mining. In a Blockchain technology every block has its own unique nonce and a hash value, but also references the hash of the previous block in the chain, so mining a block in the Blockchain system isn't easy, especially on large chains. The previous block hash value links the blocks together and prevents any block from being altered or a block being inserted between two existing blocks. In case of bitcoin cryptocurrency, the block creation time is 10 minutes.

How the Mining process is done? In order to verify a block to add in the Blockchain a miner must use a computer to solve a cryptographic problem. Once the computer able to solve the problem, the block is considered "mined" or verified. After solving the cryptographic hash value in case of Bitcoin or Ethereum Blockchain, the first computer who mine or verify the block receives reward as a bitcoin or ether, respectively.

Consensus is the process used by a group of consisting of nodes that is responsible for maintaining the distributed ledger use. It is a used when a majority of participants in the network system are agree on the validity of a transaction. It has several algorithms to be resilient to failure of nodes, message delays and corrupt messages and also unreliable,

unresponsive or even deliberately malicious nodes. The algorithms are Proof of Work (Pow), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), Proof of Authority (PoAu), Proof of Burn (PoB) etc.

POW was developed to limit denial of service attacks on internet resources. Initially this algorithm was used by Bitcoin after that Ethereum and many others. Miners emulate with each other to add a new block in the existing Blockchain system by solving a cryptographical puzzle of generating a hash output that starts with a number of consecutive zeros in the most significant positions. This algorithm give the rewards to that participants who solve this cryptographic puzzlefirst in order to validate transactions and create new blocks. The drawback in this algorithm are, it needs high consuming electricity, it can process about 7 transactions per second (1Mb block size), 1 block take 10 minutes time and the other problem is 51% attack may possible.

POS was developed to replaces computational work with a random selection process, where the chances of successful mining with PoS is proportionally related to the wealth of validators. It needs lower electricity consumption and also decreased 51% attack problem. The main vulnerability of PoS algorithm is known as the 'nothing at stack' problem. Here transaction fee can be claimed only. Now Ethereum Blockchain has moved from PoW to PoS solutions.

With the help of **PoAu,** block generation requires granting special permission to one or more members to make changes in the Blockchain. It is also known as a modified PoS algorithm, where validators stake is their own identity. Network members put their trust into authorized nodes and a block is accepted if the majority of authorized nodes signs the block. If any new validators want to add something it can be added to the system via voting.

Benefits of Blockchain

Blockchain have several benefits: **Better Transparency,** makes transaction histories more transparent because it is a type of distributed ledger. All the nodes in the network share a copy of the document and data are easily accessible.

Enhanced Security, it is better than any other record keeping system like DBMS when it comes to security by all type of standards. The documents of the transactions which are shared can be updated and/or modified with consensus on a Blockchain network only if everyone or a majority of nodes agree to update it.

Reduced Costs, as Blockchain eliminates the need for third-parties and middlemen, it saves enormous costs specially for business management system.

True Traceability, in complex supply chain system, it is very much hard to trace products back to their origin. In Blockchain, the exchanges of all the goods are recorded. So, we get an audit trial to learn where a particular asset come from.

Improved Speed and Highly Efficient, with traditional paper work process for long time there might be a speed problem and/or an error occur. With the help of Blockchain, it removes the risk of mistakes. Only one ledger is there, so everyone in the network have the access to the same information.

Auditability, as we already know that each transaction in the Blockchain system is recorded for its complete lifetime, there is an audit trail that already exists for us to see and check the authenticity of our asset.

Types of Blockchain network such as:

Public Blockchain networks, where anyone can join and participate in, example- Bitcoin. **Private Blockchain networks**, similar to a public Blockchain network, is a decentralized peer-to-peer network, example- Hyperledger and R3 Corda. **Permissioned Blockchain networks**, Participants need to obtain an invitation or permission to join, example- Bitcoin. **Consortium Blockchains**, it is also known as Hybrid Blockchain**,** combination of public and private Blockchain, Multiple organizations can share the responsibilities of maintaining a Blockchain. Example: Dragon chain

IOTA is an example of Blockchain technology**.** It is a cryptocurrency system; its architecture is called as IOTA Tangle. Tangle basically uses the consensus algorithm known as proof-of-work (PoW) system for authenticating transactions on a distributed ledger. Tangle's PoW system is similar to bitcoin, but it uses less energy and takes less time than other PoW

systems. It is a distributed ledger developed to handle transactions between connected devices in the IoT ecosystem, and its cryptocurrency is known as mIOTA.

EOS, a performance-based and self-governing Blockchain that provides an operating system for creating large scale consumer facing distributed applications.

Challenges of Blockchain:

Performance and scalability, it is coming under technological challenges where decentralised architecture works slower than the traditional systems. Performance affected due to calculations associated with encryption-decryption and hashing at every node. Scalability are affected by the factors for example architecture, network bandwidth, configuration of block, block size, variable requirements for processing power, file system, Consensus algorithm, Transaction validation mechanism etc.

Storage, Blockchain is allow to be an append only data storage mechanism. After data store in the Blockchain it cannot be altered, it becomes perpetual and also available at all the nodes in the network system. In this case it demands huge resources and may create an issue as the chain grow.

Privacy, as we know that Blockchain data is stored on every node on the network system and hence we can say that privacy is not an inherent feature that Blockchain traditionally provides. Here the data need to be stored in such a way that the privacy of an individual is not compromised.

Regulations, the state of regulations and compliance for Blockchain applications is still ambiguous. It is mainly related to the privacy of the information shared through this Blockchain technology which may be user identity documents or health records. The adoption would be smooth and quicker when the regulations are well defined.

Security, use of existing Certificate Authorities- Every entity including the node and the users in the Blockchain network have a public keys, private keys and certificates. The choice of certificate authority would depend on the nature of application that is targeted.

High development cost, the creation of block in the Blockchain technology takes high cost in terms of power consumption and other things.

Legal challenges for Blockchain in Adoption in India

The RBI has put fourth restriction with respect to virtual currencies that are based on Blockchain technology and there is circular to halt the usage of crypto currency transactions in India. The section 43A of the IT Act currently does not have the safeguards mentioned from the privacy perspective when we talk about Blockchain. Digital signatures are the main part of Blockchain networks and application, currently there exist no details in the Schedule I of the Information Technology Act, 2000

Risk with Blockchain technology

51% attacks, in case of Mining it requires a huge amount of computing power, especially for large-scale public Blockchains. It occurs when a single cryptocurrency miner or group of miner’s gains control of more than 50% of a network's Blockchain, that means one or more miners takes control of more than 50% of a network’s mining power, computing power or hash rate. If it is successful, the miners responsible essentially control all the network and certain transactions occur within it.

Proof of Stake vulnerabilities, here the attack is known as Bribe Attack, the attacker performs a spending transaction that he wants to reverse later. Immediately after the transaction happen, the attacker tries to starts to build an alternative chain based on the block prior to the one containing the transaction. The attacker creates an alternative chain in secret. After the transaction acquires the important number of affirmations and the attacker’s chain is longer than the valid chain, the attacker publishes it whole. The attacker 's chain is acknowledged as the new substantial Blockchain, and the transaction is switched.

Double spending, there is a danger that a member with, for instance, one bitcoin can spend it twice and falsely receive goods to the value of two bitcoins before one of the providers of goods or services realizes that the money has already been spent. The most serious risk for double-spending comes in the form of a 51% attack, which can happen if a user controls more than 50% of the computing power maintaining the distributed ledgers of a cryptocurrency. If these user controls the Blockchain technology they will be able to transfer bitcoins to their wallet multiple times by reversing the Blockchain ledger as though the initial transactions had never occurred.

Blockchain application:

Transfer of Land Records that will comes under property record management, Power management, In agriculture and other supply management, eVoting system, Electronic Health record management, IOT device management, In pharmaceutical sector for supplying purpose, In e-Notary service system.

In all over the world many countries now-a-days have launched their platforms and services using Blockchain technologies for example China uses BSN (Blockchain based service network) aims to helping companies and individuals and support in digital economy and smart city initiatives. KSI (Keyless Signature Infrastructure) designed by Estonia and it is deployed by their government network, it helps to prove the authenticity of the e-Data mathematically. United Arab Emirates has started their initiative for “Smart Dubai”, which aims to become the “first city fully powered by Blockchain technology by 2021”. In US, UK, Brazil, Chile, Canada they also adopted this advance technology in their different fields. Samsung, LG, Amazon, Microsoft, IBM, Oracle, these top brand companies also adopted this technology for authentication, transparency and other purpose.

If we say about National Scenario about Blockchain technology, Ministry of Electronics and Information Technology (MeitY) has recognized that this technology as one of the important research areas having application potential in different domains such as Governance, Banking & Finance sector, in Cyber Security and so on. MeitY has likewise help a multi institutional project titled “Distributed Centre of Excellence in Blockchain Technology with C-DAC, IDRBT and VJTI as executing agencies. Centre of Excellence (CoE) was established by NIC in association with NICSI which is basically a Blockchain based project. NITI Aayog has confirmed that the Blockchain is a promising technology which have several features like decentralization, transparency and accountability. RBI also planning for adopting this technology in banking sector also.