بسم اللہ الرحمن الرحیم

Blockchain

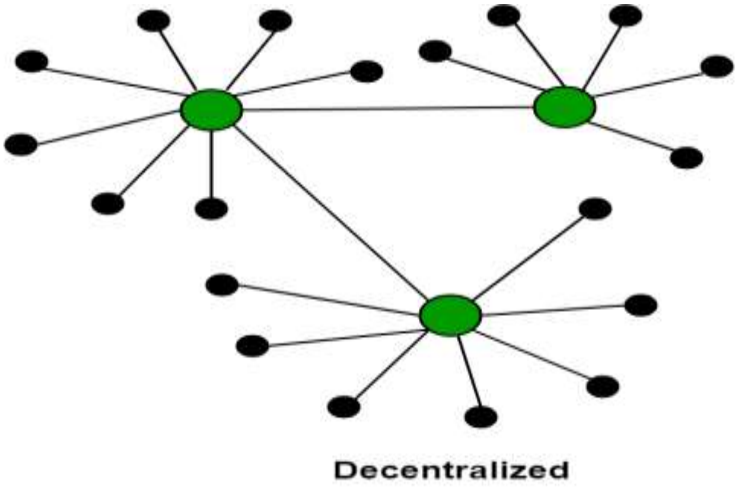
BLOCKCHAIN

Definition:

- Blockchain is a chain of data records that are distributed across a decentralized network of computers.
- Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network.
- The blockchain is a technology that allows data to be stored and exchanged on a peer-to-peer network, without the need for a central authority or intermediary. The data is organized in blocks, which are linked together by cryptographic hashes, forming a chain.

Blockchain Decentralization:

There is no Central Server or System which keeps the data of the Blockchain. The data is distributed over Millions of Computers around the world which are connected to the Blockchain. This system allows the Notarization of Data as it is present on every Node and is publicly verifiable.



Types:

There are four major types of blockchain technologies:

- **Public blockchain** is a permissionless distributed ledger technology where anyone can join and participate in the network, without the need for a central authority or intermediary. Public blockchains are open, transparent, immutable, and decentralized. Examples of public blockchains are Bitcoin, Ethereum, and Litecoin.
- **Private blockchain** is a permissioned distributed ledger technology where only a selected group of entities can join and validate transactions or data in the network. Private blockchains are more secure, efficient, and customizable than public blockchains, but they are also less transparent and decentralized. Examples of private blockchains are Hyperledger Fabric, Corda, and Quorum.
- **Hybrid blockchain** is a combination of public and private blockchains, where some parts of the network are open and some are closed. Hybrid blockchains aim to achieve the best of both worlds, by balancing the trade-offs between security, privacy, scalability, and transparency. Examples of hybrid blockchains are Dragonchain, Kadena, and XinFin.
- **Federated blockchain** is a type of private blockchain where multiple organizations or entities collaborate to form a consortium and share the governance and operation of the network. Federated blockchains are more flexible, scalable, and interoperable than private blockchains, but they also require more trust and coordination among the participants. Examples of federated blockchains are R3, IBM Blockchain, and Cosmos.

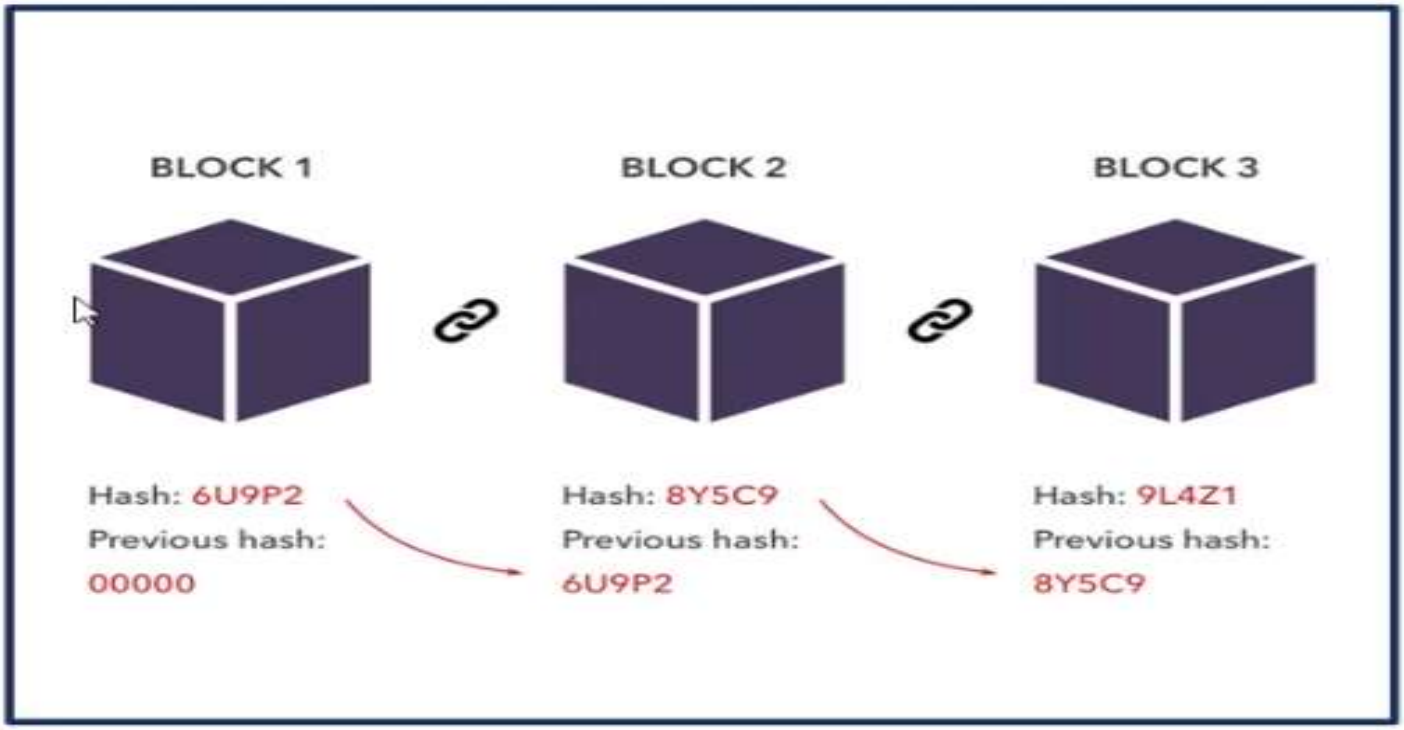
What are the benefits of Blockchain?

- **Time-saving:** No central Authority verification is needed for settlements making the process faster and cheaper.
- **Cost-saving:** A Blockchain network reduces expenses in several ways. No need for third-party verification. Participants can share assets directly. Intermediaries are reduced. Transaction efforts are minimized as every participant has a copy of the shared ledger.
- **Tighter security:** No one can tamper with Blockchain Data as it is shared among millions of Participants. The system is safe against cybercrimes and Fraud.
- **Collaboration:** It permits every party to interact directly with one another while not requiring third-party negotiation.
- **Reliability:** Blockchain certifies and verifies the identities of every interested party. This removes double records, reducing rates and accelerating transactions.

How does Blockchain work?

Blockchain works by storing data in blocks that are linked together by cryptography. Each block contains a hash of the previous block, a timestamp, a nonce, and a Merkle root that summarizes the transactions in the block. The blocks form a chain that cannot be altered or tampered with, as any change would invalidate the hashes and break the links.

Blockchain relies on a peer-to-peer network of nodes that communicate and validate the data. Each node has a copy of the entire blockchain, and can verify the transactions and blocks using a consensus algorithm. The most common consensus algorithm is proof-of-work, which requires nodes to solve a mathematical puzzle to create new blocks and earn rewards. This process is also known as mining, and it ensures that the network is secure and decentralized.



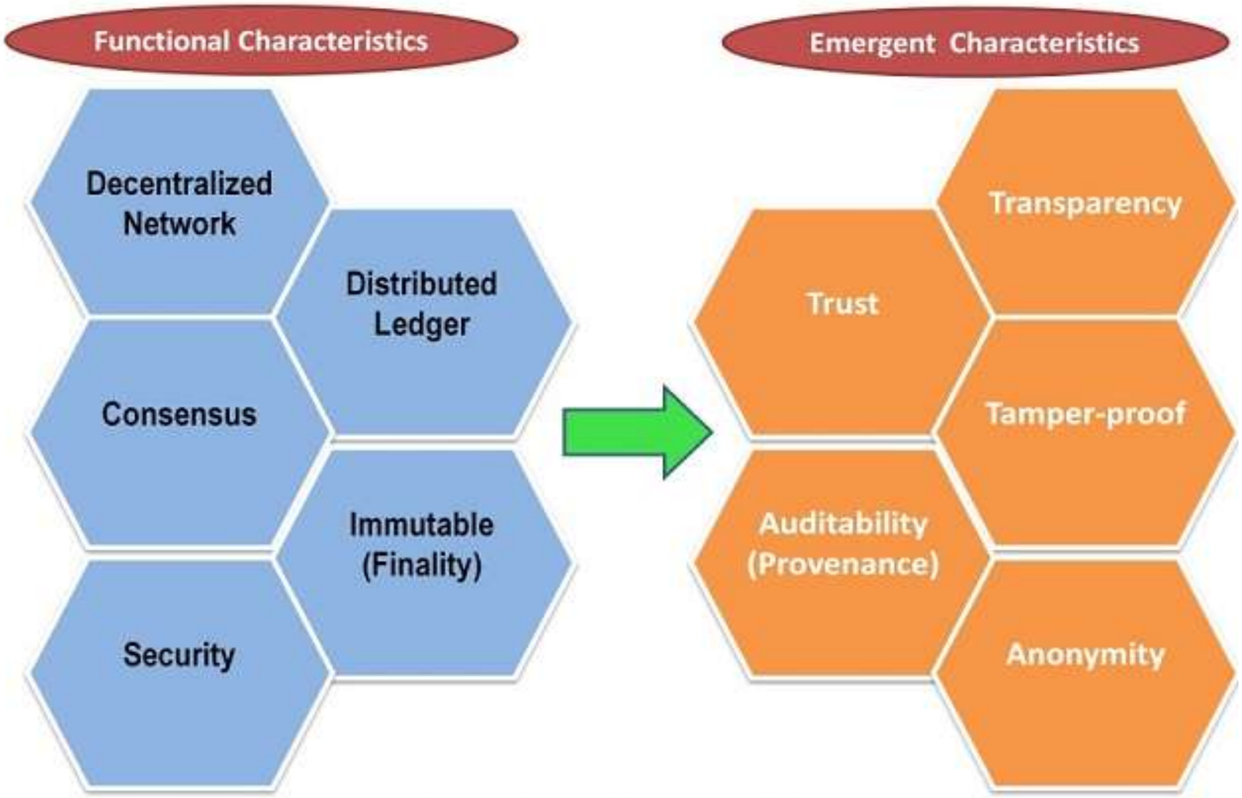
Blockchain and Data Privacy

Blockchain security is the process of protecting the data and transactions on a blockchain network from unauthorized access, manipulation, or attacks. Blockchain security is based on the principles of cryptography, decentralization, and consensus, which ensure the trust and integrity of the system.

Characteristics:

Blockchain characteristics are classified into functional characteristics and emergent characteristics.

- **Functional characteristics** are those which are mandatory for functioning, without which the system may not exist or function properly. Functional Characteristics of Blockchain are Decentralized network, Distributed Ledger, Consensus, Immutable (Finality) and Security.
- **Emergent characteristics** are derived are emerged as a result of functional characteristics. In the case of Blockchain, the emergent characteristics are Trust, Auditability (Provenance), Transparency, Tamper-proof, and Anonymity.



Block Chain Characteristics

Functional Characteristics:

- **Decentralized Network**
- **Distributed Shared Ledger**
- **Consensus**
- **Immutable**
- **Security**

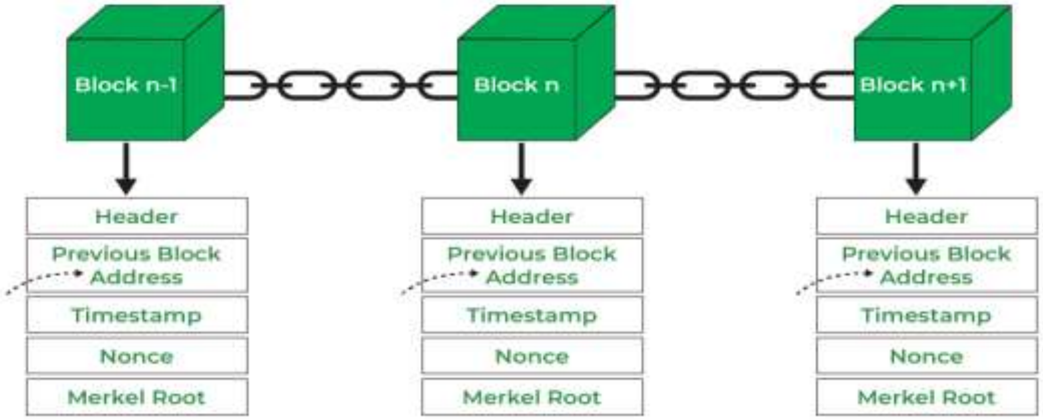
Emergent Characteristics:

- **Trust**
- **Auditability (Provenance)**
- **Transparency**
- **Tamper-proof**
- **Anonymity**

What is Blockchain Architecture?

Blockchain architecture is the design and structure of a blockchain system, which consists of various components and elements that interact with each other to enable the functionality and features of the system. Blockchain architecture can vary depending on the type, purpose, and characteristics of the blockchain, but some common components are:

- Node - user or computer within the blockchain architecture (each has an independent copy of the whole blockchain ledger)
- Blocks: These are the data structures that store a set of transactions that have been validated and verified by the nodes. Each block contains a header and a body. The header contains metadata, such as the hash of the previous block, the timestamp, the nonce, and the Merkle root. The body contains the actual transactions and their details.



- Transaction - smallest building block of a blockchain system (records, information, etc.) that serves as the purpose of blockchain
- Chain - a sequence of blocks in a specific order
- Miners - specific nodes which perform the block verification process before adding anything to the blockchain structure
- Consensus (consensus protocol) - a set of rules and arrangements to carry out blockchain operations

Smart contracts:

Smart contract is a computer protocol (code) that is stored inside the blockchain, and is intended to digitally facilitate, verify, or enforce the negotiation or performance of contract.

Ethereum:

Ethereum is a platform that is built specifically for creating smart contracts.

Smart contract steps:

1. Coding
2. Distributed ledger
3. Execution

Solidity:

Solidity is an object-oriented programming language for writing smart contracts.

Ledger:

Ledger is the database that records all transactions in blockchain.
There are two types of ledger (public ledger, private ledger).

Blockchain Architecture Vs Database:

Parameters	Blockchain Architecture	Database
Control	Blockchain is decentralized because there is no single point of failure and there is no central authority to control the blockchain.	The database is Centralized.
Operations	Blockchain has only an Insert operation.	The database has Create, Read, Update, and Delete operations.
Strength	It is robust technology.	The database is not fully robust technology.
Mutability	Blockchain is immutable technology and we cannot change it back or we cannot go back.	The database is a fully mutable technology, The data can be edited in the database.
Rights	Anyone with the right proof of work can write on the blockchain.	In the database reading and writing can do so.
Speed	It is slow in speed.	It is faster as compared to blockchain.