Pakistan Blockchain Institute

PAKISTAN BLOCKCHAIN INSTITUTE

MODULE-2
BLOCKCHAIN AND SMART CONTRACT BASICS

Class-1

Raja Rizwan Saleem
Lead Blockchain Trainer

Edversity.

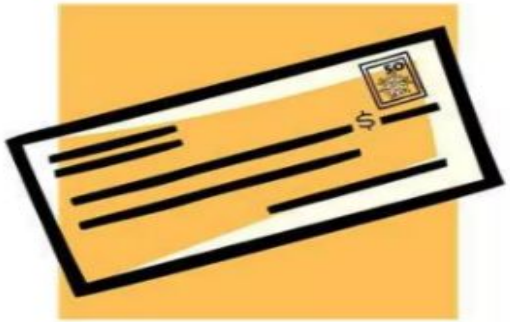
WHAT IS TECHNOLOGY

Technology is the collection of techniques, skills, methods, and processes used in the production of goods or services or in the accomplishment of objectives, such as scientific investigation.

EXAMPLE OF TECHNOLOGY

ADVANTAGES OF TECHNOLOGY

1. **Reduces the time it takes to perform a task.**



DISADVANTAGES OF TECHNOLOGY

3. Technology can cause individuals to become inactive because the use of the devices does not require much energy to be expended.

SUMMARY

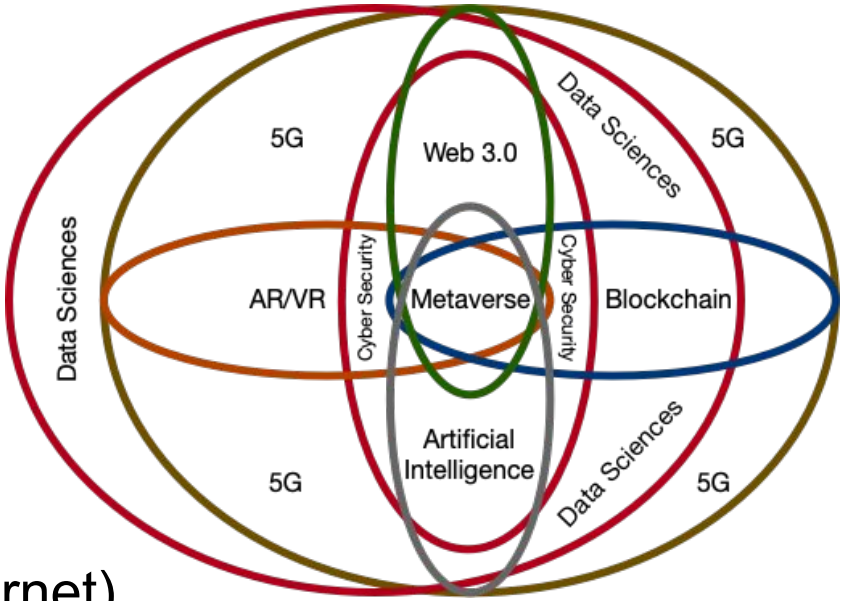
- **What is Technology?**
- Technology is the application of science (the combination of the scientific method and material) to solve problems.
- Technology is the making, usage and knowledge of tools, machine, techniques, crafts and system of organization to solve problems

EMERGING TECHNOLOGIES

Edversity.

COMPONENTS

- Data Sciences
- Cloud Computing
- Internet of things
- Internet of everything
- Artificial Intelligence
- Blockchain
- 5G
- Metaverse (AR/VR + Internet)
- Cybersecurity



Edversity.

WHY IT'S IMPORTANT

Edversity.

WHY IMPORTANT TO UNDERSTAND

- Why this is important to understand all these technologies
- As an Architect or As a Strategist we must understand the application of it
- To build the scenario or case-study
- Be very clear what we need.

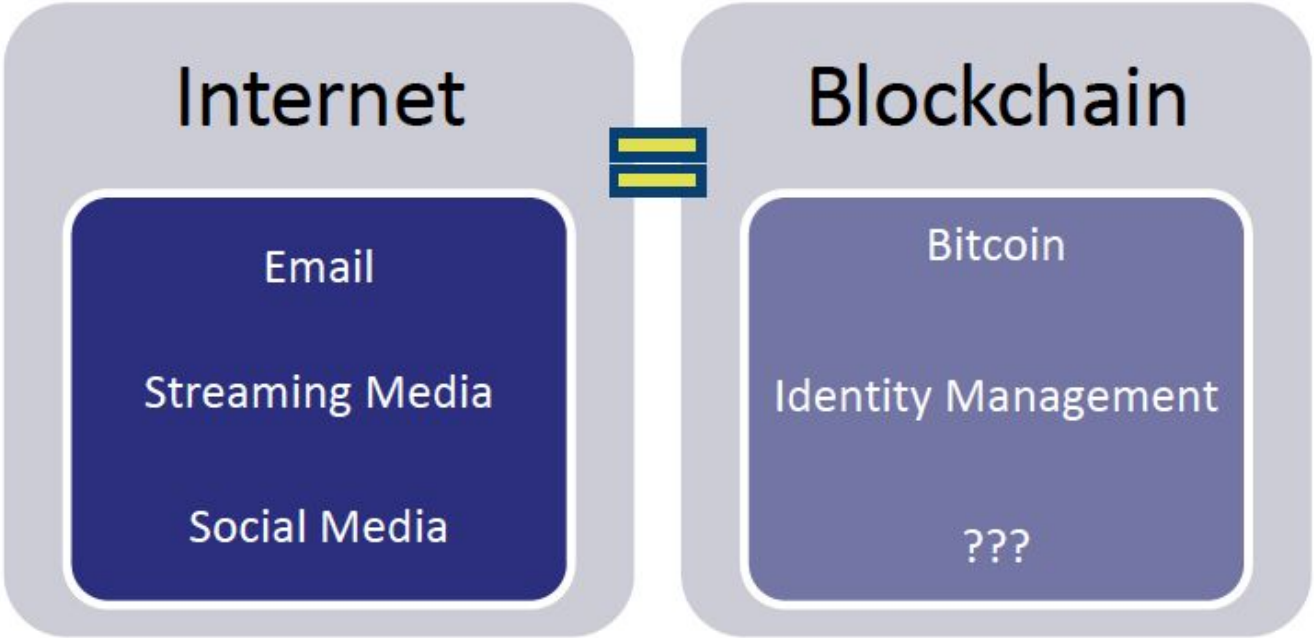
BLOCKCHAIN

Edversity.

MISCONCEPTIONS ABOUT BLOCKCHAIN

- Blockchain = Bitcoin
- blockchain.com is a Blockchain
- Blockchain can only be used for financial sector
- Everyone can see private information on the Blockchain
- Smart Contracts have the same legal value as regular contracts
- Blockchain can only be public

BLOCKCHAIN



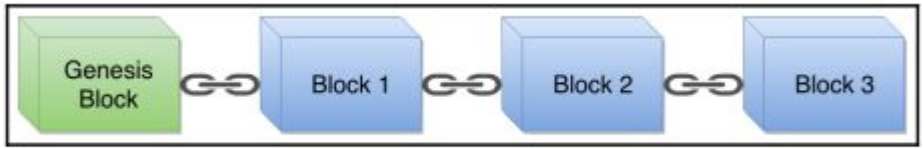
WHAT IS BLOCKCHAIN?

- In its simplest form, Blockchain is a distributed database, an unchangeable record (or Ledger) of asset ownership.
- Blockchain is primarily defined as a shared immutable ledger, or just an “unchangeable record of who owns what”
- Global, peer to peer, and distributed immutable record of transactions.
- Used to transfer and permanently record any change of assets between two or more parties without intermediaries.
- Assets are defined as anything of value that requires accountability of ownership, i.e. money, cryptocurrency, real estate, records of any kind, identities, personal property, etc.

Definition?

- Each computer that participates in this P2P network is called a node. Each node maintains the records of transactions in multiple consecutive blocks.

- Blockchain technology is also called Decentralized Ledger Technology (DLT), as each node in the network keeps the same copy of the ledger. Please have a look at the following diagram



Chain of connected blocks

OLD TECHNOLOGIES USING BY BLOCKCHAIN

- Blockchain is a combined use of existing older technology.
  - Ledger – 7,000 year old technology, triple-entry accounting
  - Cryptography – “coding messages” has been used for thousands of years, and still used in complex S/W algorithms for military and business applications like Blockchain
  - Computer Networking Technology – Blockchain makes extensive use of P2P networking architectures

FEATURES BLOCKCHAIN

FEATURES BLOCKCHAIN

Distributed Ledger Technology

Programmable
A blockchain is programmable (i.e. Smart Contracts)

Secure
All records are individually encrypted

Anonymous
The identity of participants is either anonymous or pseudonymous

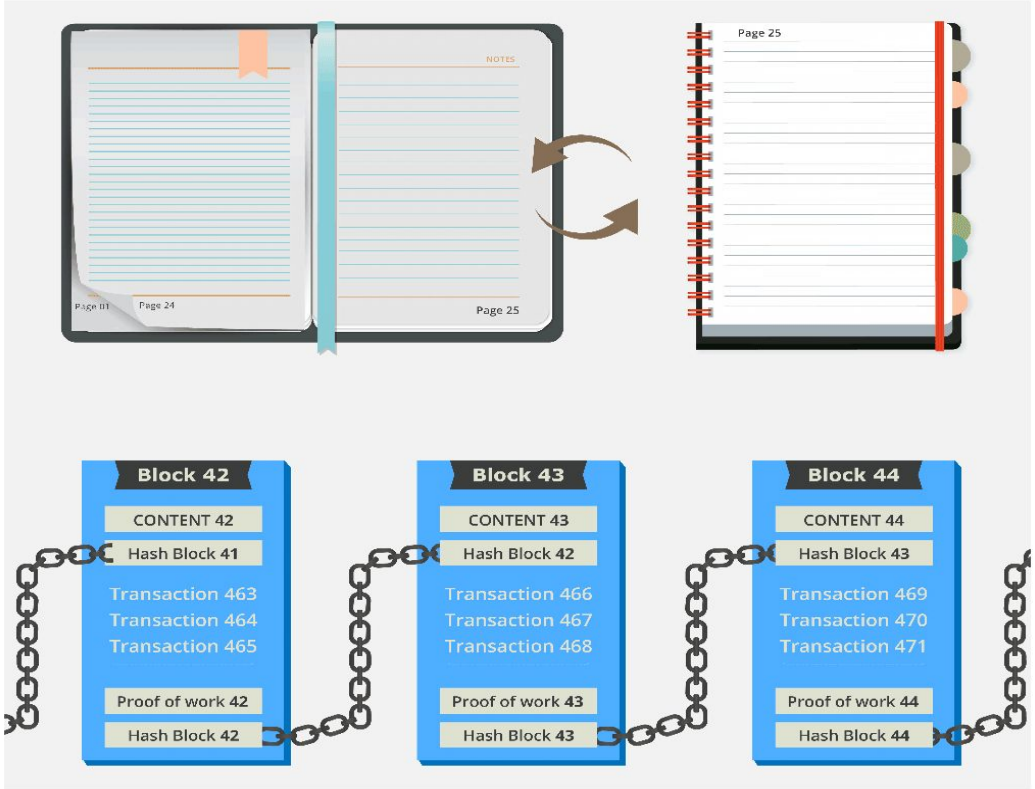
Distributed
All network participants have a copy of the ledger for complete transparency

Immutable
Any validated records are irreversible and cannot be changed

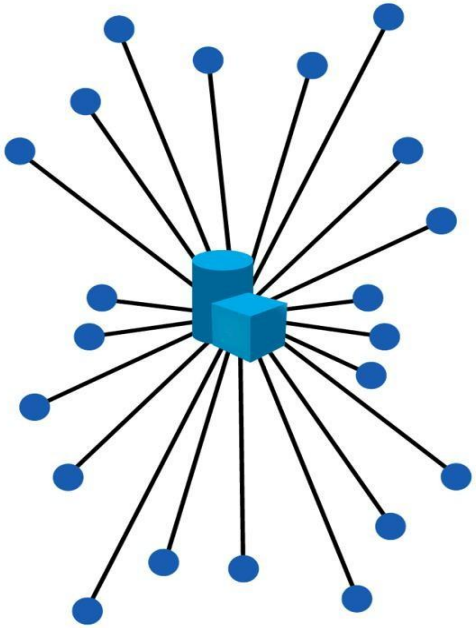
Time-stamped
A transaction timestamp is recorded on a block

Unanimous
All network participants agree to the validity of each of the records

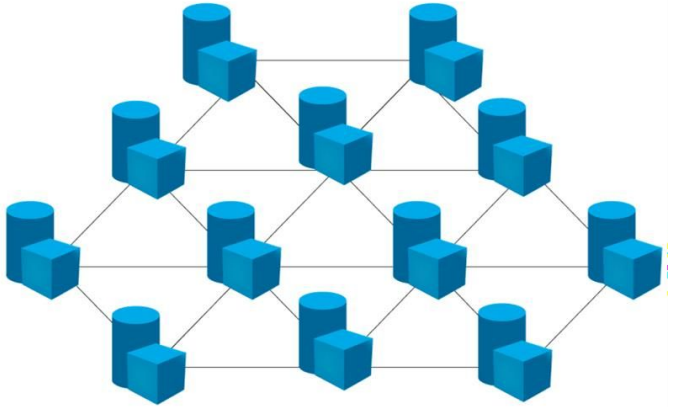
WHAT IS BLOCK & WHY IT'S CALLED BLOCKCHAIN?



Centralized Vs. Decentralized Network

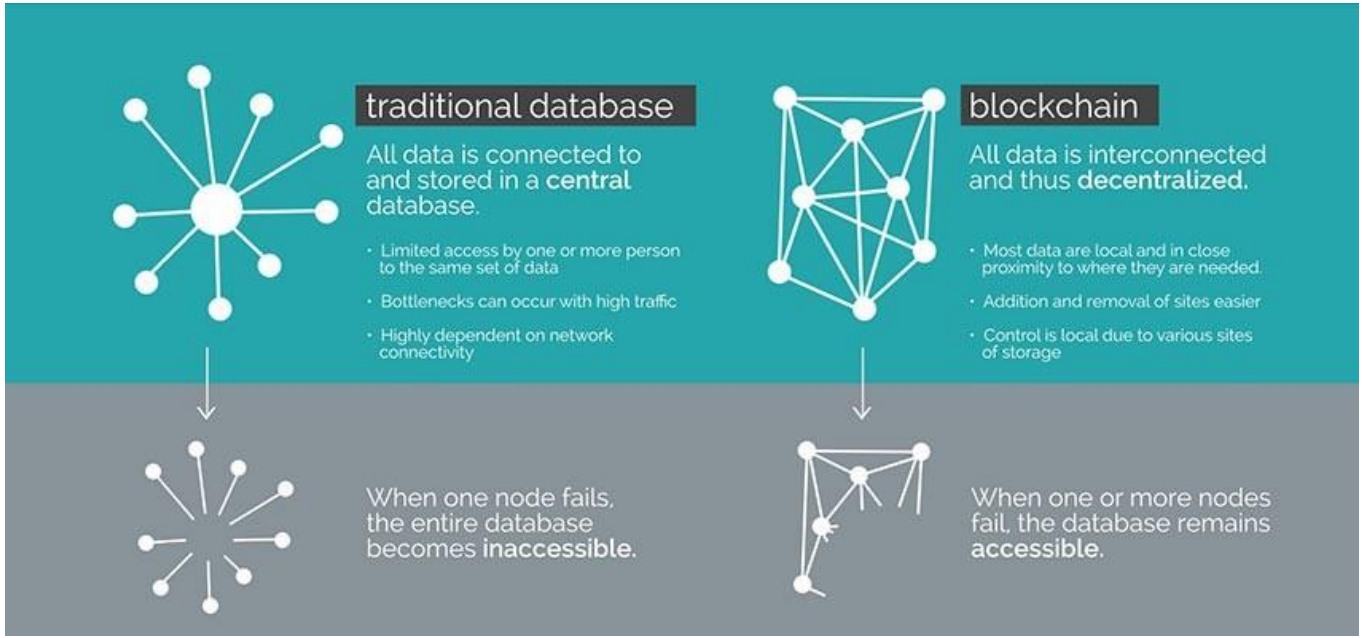


CENTRALIZED

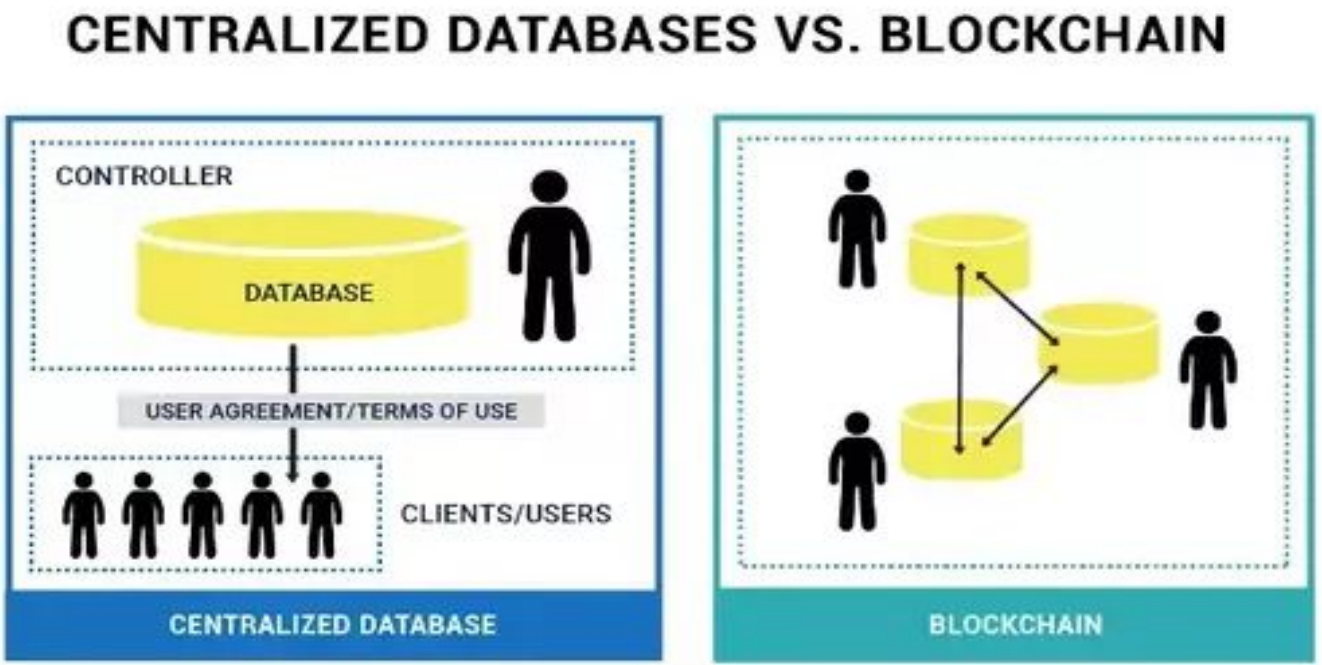


DECENTRALIZED

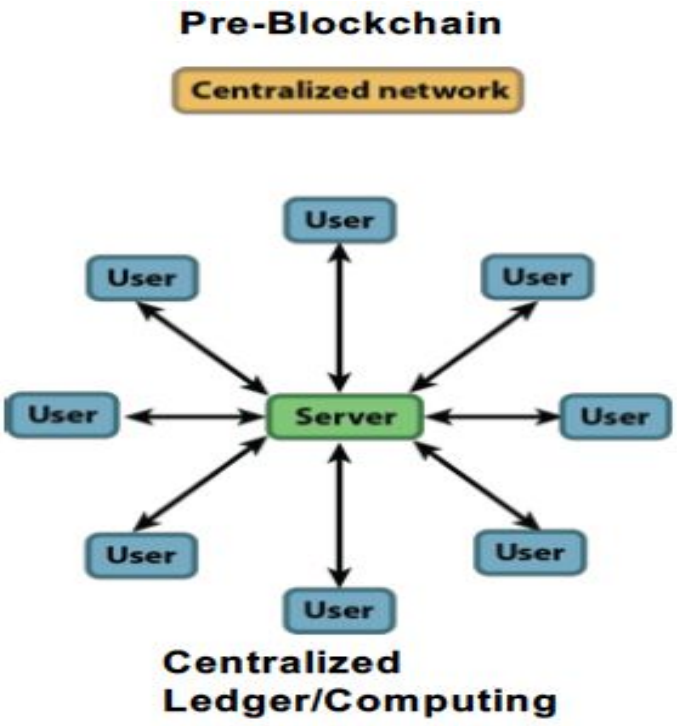
CENTRALISED VS DECENTRALISED

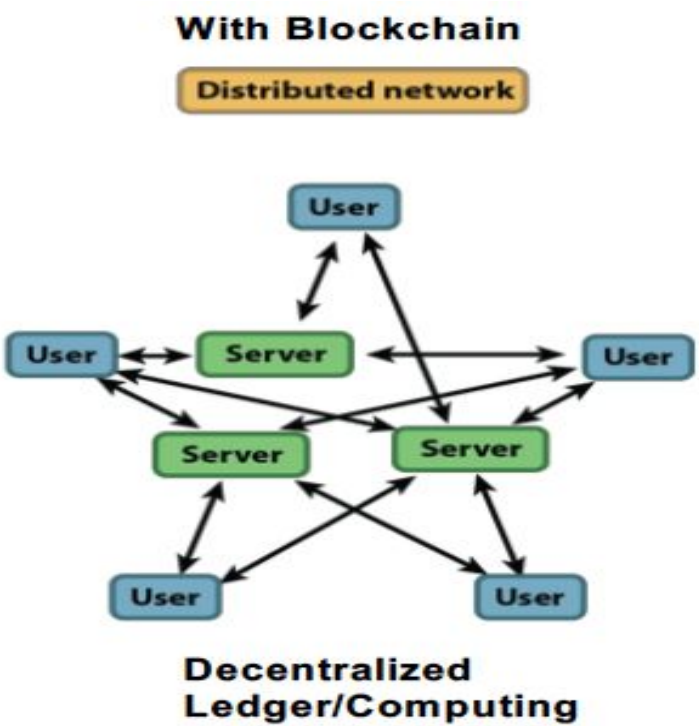


Centralized Vs Decentralized



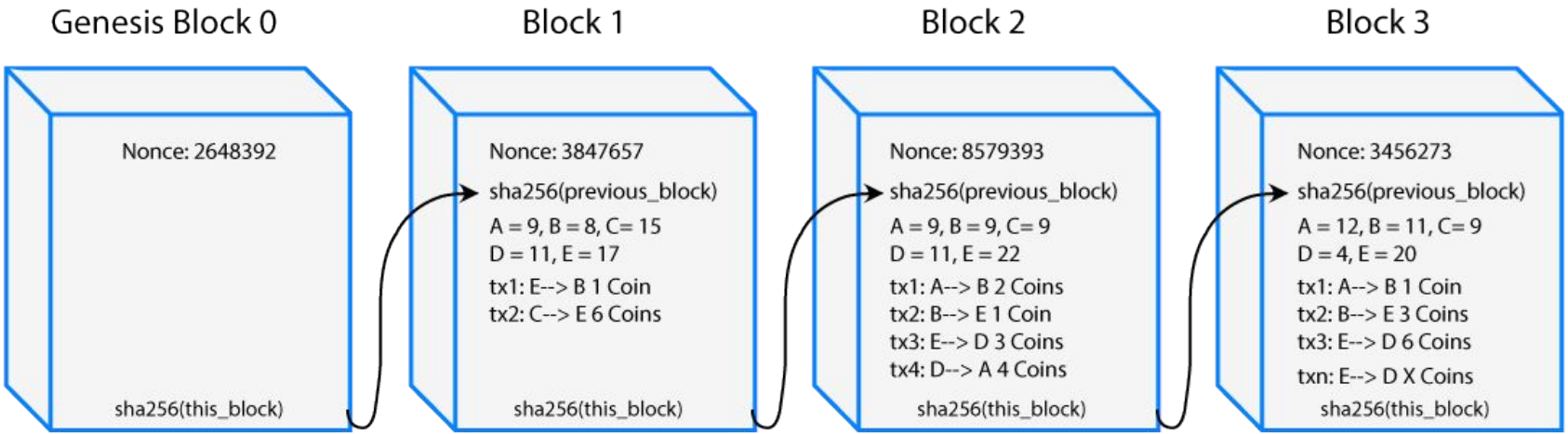
Centralized Vs Decentralized



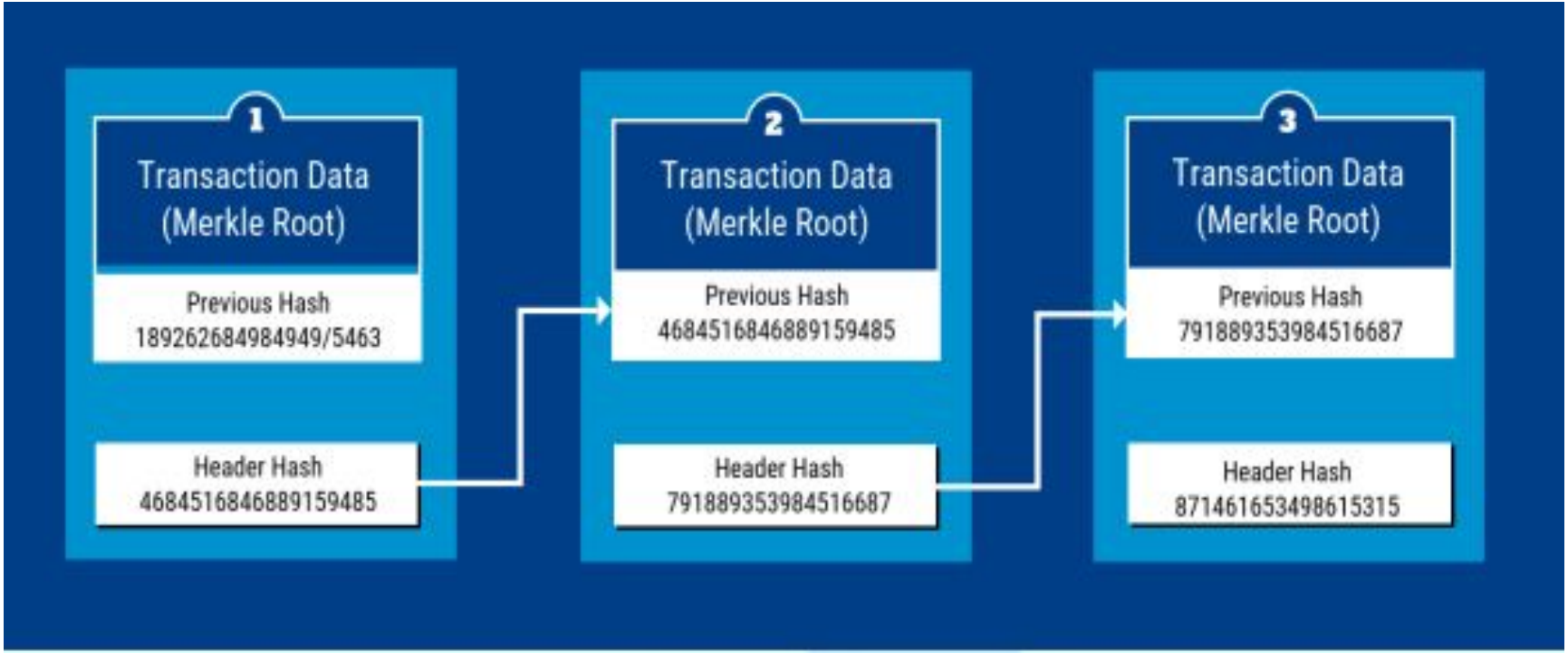


Edversity.

Blockchain Transactions



Blockchain Transactions



CONSENSUS

Introduction to Consensus

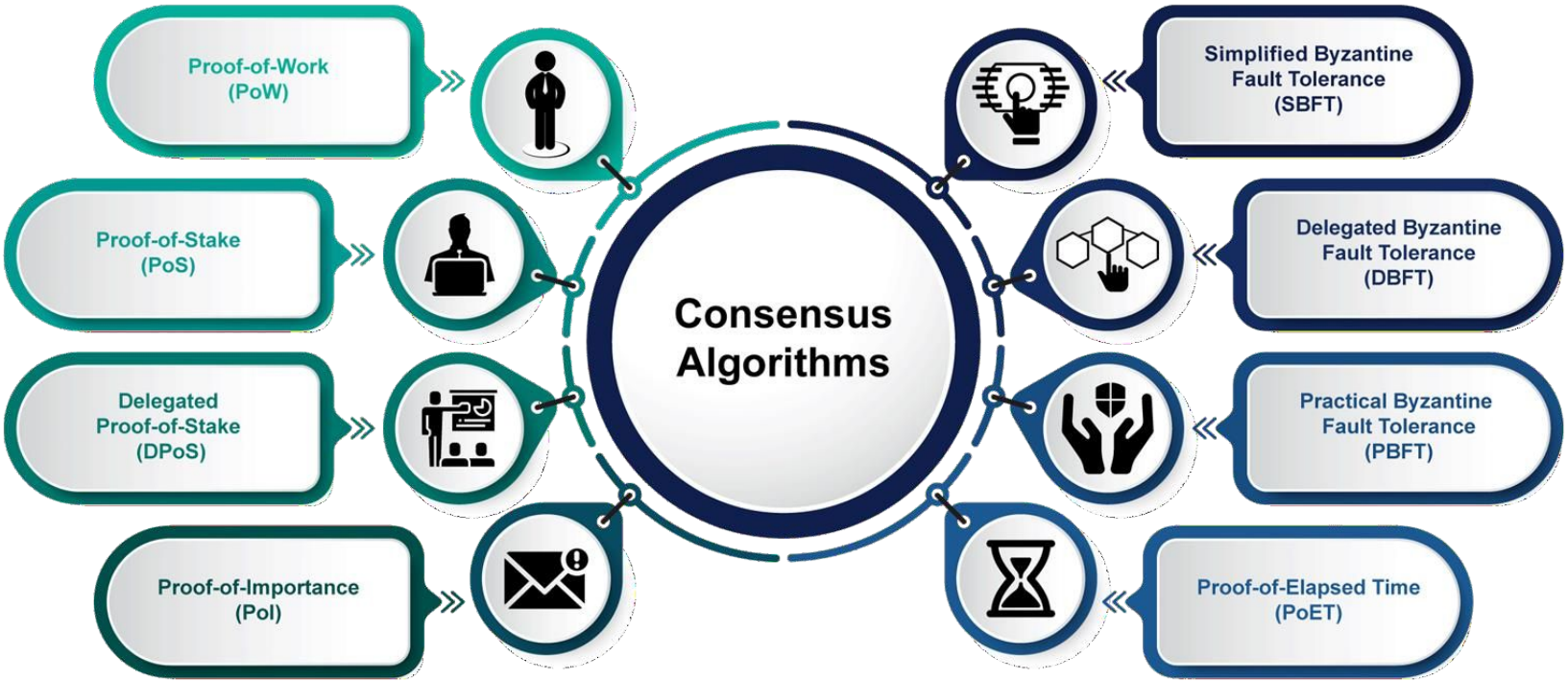
1. The decentralized blockchain needs a way for users to agree on the current state of the blockchain

2. Consensus in the blockchain is based on scarcity. Controlling more of a scarce resource gives more control over the blockchain's operation

3. Several different consensus mechanisms have been proposed for blockchain. The most common are:
   - Proof of Work
   - Proof of Stake

   Other consensus mechanisms:
   - Delegated Proof of Stake
   - Practical Byzantine Fault Tolerance
   - Directed Acyclic Graph

Consensus Mechanisms



Proof of Work

- Proof of work (PoW) is a decentralized consensus mechanism that requires members of a network to expend effort solving an arbitrary mathematical puzzle to prevent anybody from gaming the system.
- Proof of work is used widely in cryptocurrency mining, for validating transactions and mining new tokens.
- Due to proof of work, Bitcoin and other cryptocurrency transactions can be processed peer-to-peer in a secure manner without the need for a trusted third party.
- Proof of work at scale requires huge amounts of energy, which only increases as more miners join the network.
- Proof of Stake (POS) was one of several novel consensus mechanisms created as an alternative to proof of work.

Proof of Stake

- With proof-of-stake (POS), cryptocurrency owners validate block transactions based on the number of coins a validator stakes.
- Proof-of-stake (POS) was created as an alternative to Proof-of-work (POW), the original consensus mechanism used to validate a blockchain and add new blocks.
- Proof-of-stake (POS) is seen as less risky in terms of the potential for an attack on the network, as it structures compensation in a way that makes an attack less advantageous

Proof of Work VS Proof of Stake

Mining capacity depends on computational power

Validating capacity depends on the stake in the network

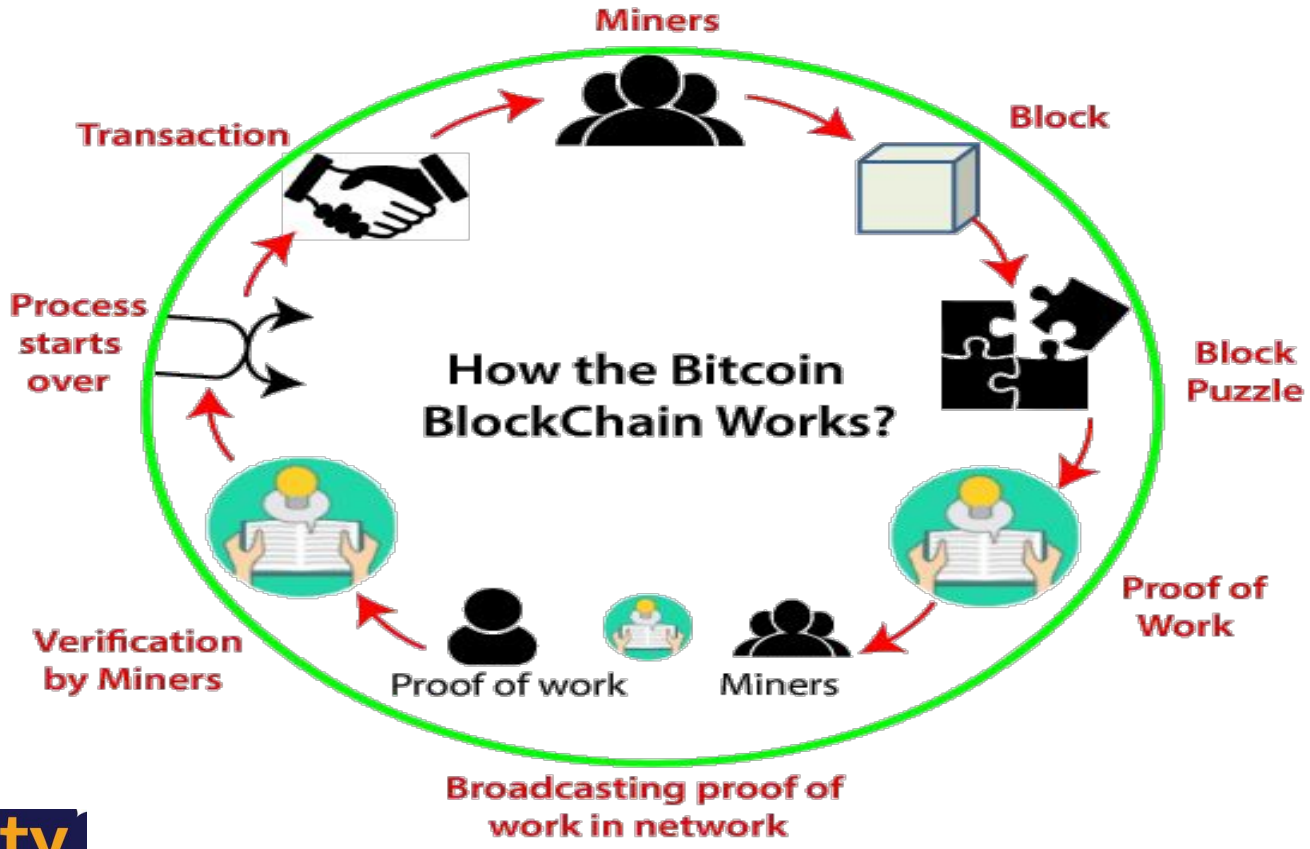
Miners receive block rewards to solve a cryptographic puzzle

Validators do not receive a block reward, instead, they collect transaction fees as reward

Hackers would need to have a computer powerful than 51% of the network to add a malicious block, leading to 51% attack

Hacker would need to own 51% of all the cryptocurrency on the network, which is practically impossible and therefore, making 51% attacks impossible.

How Does Blockchain Works



BLOCKCHAIN FUNCTIONALITY

When listening to descriptions of blockchain it is not uncommon to hear that blockchain constitutes a "globally shared database". This is not a bad analogy, as long as one bears in mind several key differences. Databases have four primary operations or functions, commonly referred to as the CRUD functions. In a classical database, those functions are:

- **CREATE**
  - New records can be created and added to the database.
- **READ**
  - Existing records can be read from the database.
- **UPDATE**
  - Existing records can be updated in-place.
- **DELETE**
  - Existing records can be removed or purged from the database.

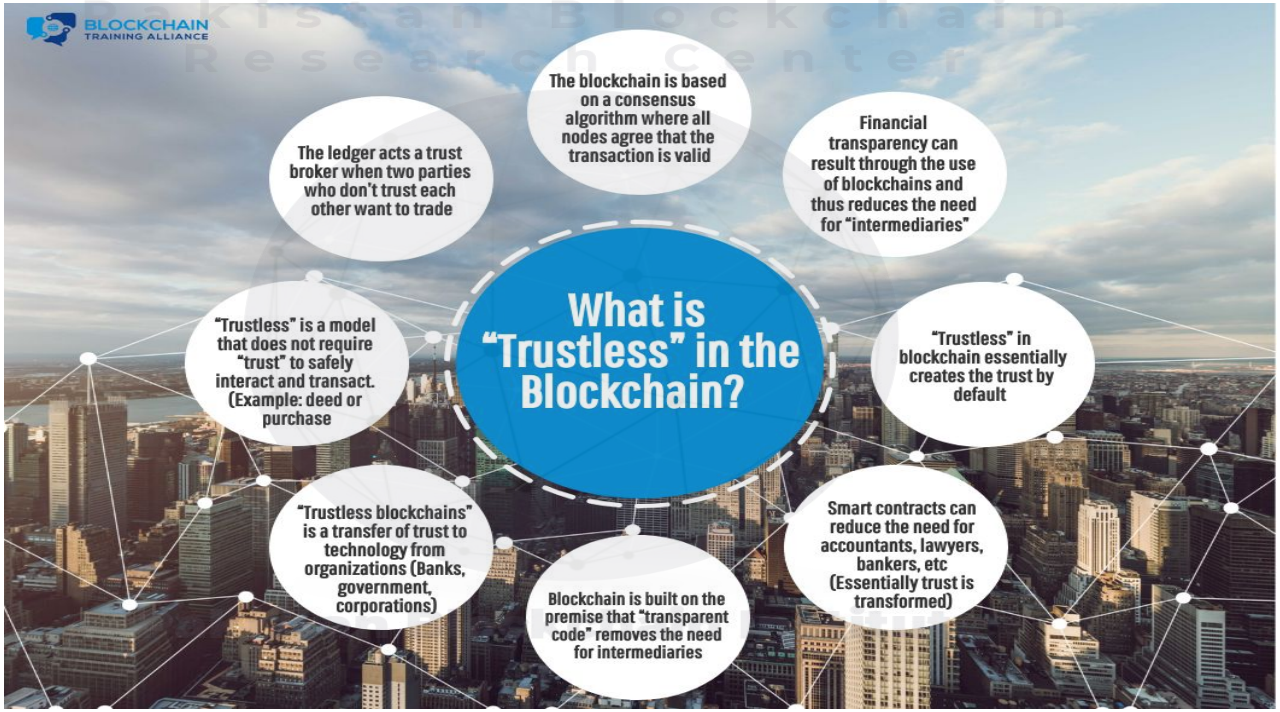
In blockchain, the last two of these functions have been intentionally removed. The only possible operations on a blockchain are:

- **CREATE**
  - New records can be created and added to the ledger.
- **READ**
  - Existing records can be read from the ledger.

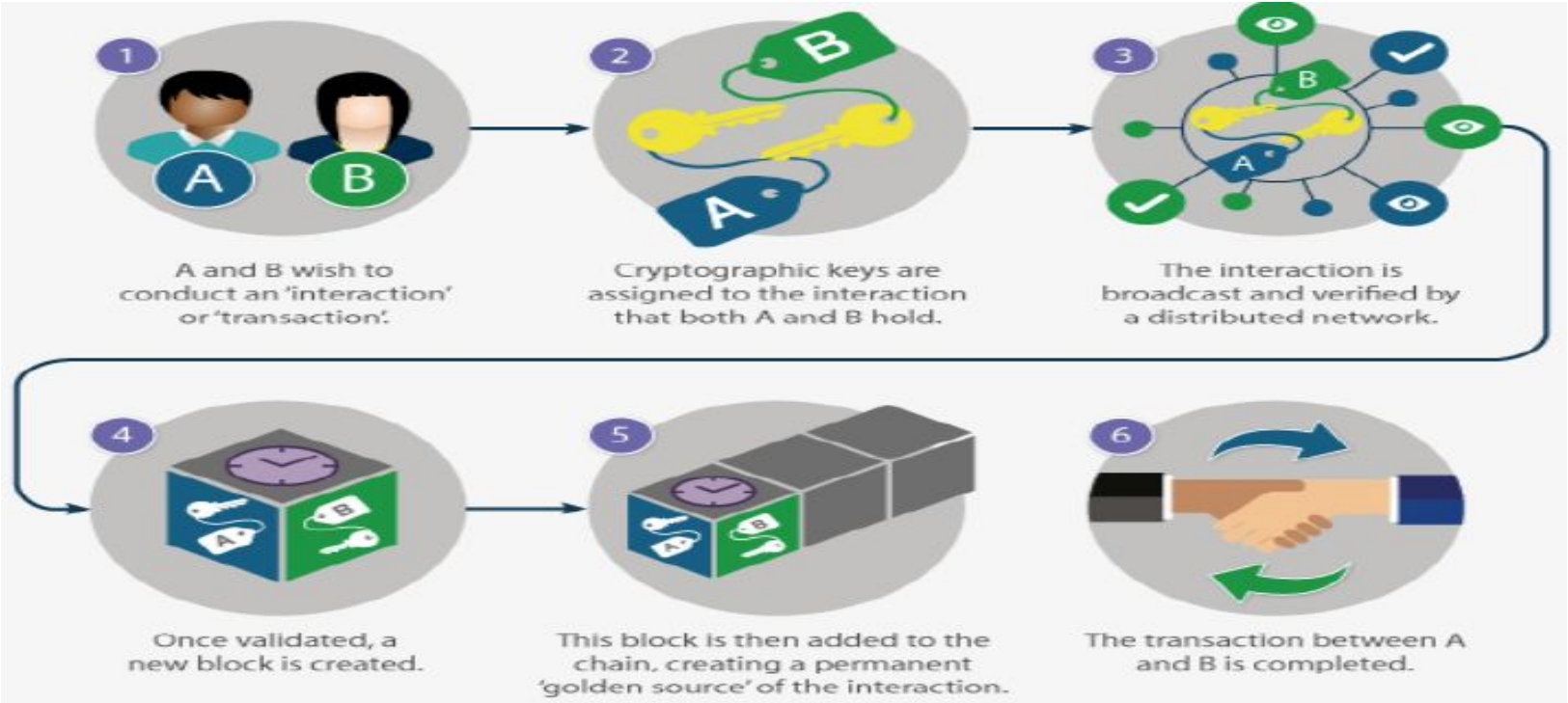
BLOCKCHAIN FUNCTIONALITY

Edversity.

TRUSTLESS



LIFECYCLE OF BLOCKCHAIN



Benefits of blockchain

Benefits of Blockchain

- Publicly verifiable
- Accountability to customers and end-users
- Secure
- Control who sees what data when
- Quality assurance
- Track origin of all supply chain components
- Lower transactions costs
- Removing middlemen reduces cost
- Resilient Network
- Always available

Benefits of Blockchain

- Decentralization
- Peer-to-peer (P2P) network
- Security/Immutability
- Open Source
- Trust
- Ease-of-use
- Transparency
- Improved traceability
- Permanent ledger
- Cost reduction

Properties of blockchain

Properties of Blockchain

- Blockchain has properties of both decentralized and distributed networks.
- Using those types of networks along with cryptography adds more properties.
- We are covering here in this course properties related to the Ethereum blockchain rather than other blockchain implementation properties.
- The other blockchain implementations might have different properties.

1-Distributed Ledger

- Multiple nodes make up a distributed blockchain network. All nodes share a common ledger, where records of transactions are kept.

2-Fault Tolerance

- A blockchain network is distributed and each node maintains the same record of the ledger.
- Even if some nodes in the network are corrupted or go down, it can continue operating
- safely up to a certain limit, as well as processing transactions with running nodes.

3-Attack Resistance

- A blockchain network does not have centralized control.
- The network's resistance to attacks is maintained by the miners who are putting their processing power (using nodes) into use to guard against malicious attacks.
- These miners earn some incentives to keep the network

safe by behaving honestly.

This is done by using the distributed network and cryptographic techniques.

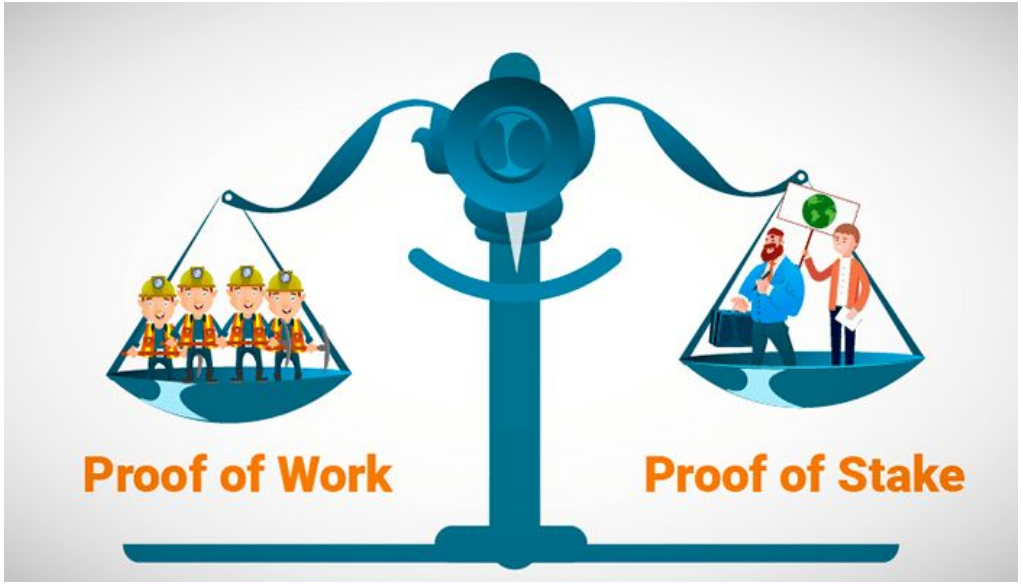
4-Remove Intermediaries

- Blockchain technology removes the dependence on TTP/middle parties/intermediaries.
- Using blockchain technology, a transaction can be done directly between two
- entities/systems. In place of intermediaries, we can place blockchain systems.

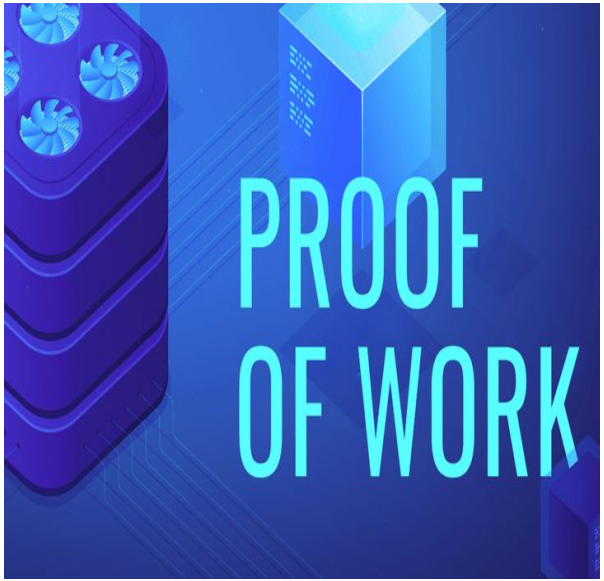
5-Consensus Protocol

- This is a protocol that ensures that all nodes participating in the network ensure the safety of the network.
- All nodes use a consensus protocol (a specific algorithm) to reach a consensus and discard the blocks generated by the attacker/bad node, to avoid catastrophic system failure.

5-Consensus Protocol

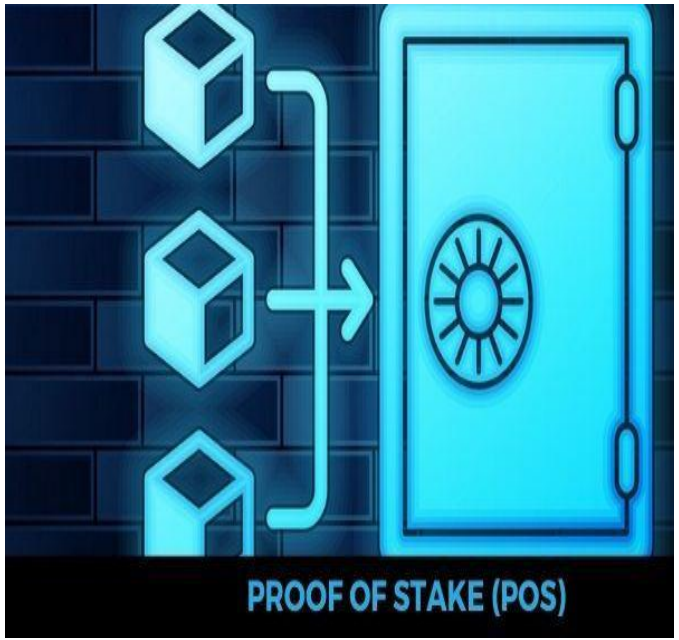


5-Consensus Protocol



The PoW protocol is a consensus algorithm in which nodes compete with other nodes to solve a cryptographic puzzle. The node that solves the puzzle first adds a new block to the blockchain (called mining). By doing this, they also earn some block reward in the lockchain's native coin.

5-Consensus Protocol



The PoS protocol is a consensus algorithm in which a person has to put the native blockchain coin up for stake (lock).The protocol selects a miner randomly or according to coinage. The miner is rewarded when the block added is valid, otherwise they may lose their stake.

6-Faster Settlement

- Traditional banking systems can be slow in some cases, as they need additional time for processing a transaction; for example, cross-border payments..
- However, with blockchain technology, there are no intermediaries; therefore, the transaction happens directly between entities and the settlement is much faster, compared to traditional systems.

7-Low Transaction Fee

- TUsing the traditional banking system, doing a cross-border payments is costly.
- The intermediaries take their commission to process the transaction between two parties.
- But by using blockchain technology, the cost of doing transactions is significantly lower because we can remove the intermediaries and perform the transactions directly.

8-Transparency

- Some blockchain systems maintain transparency. Ethereum is a public blockchain network.
- All the transactions of the Ethereum blockchain are public and transparent. Anyone can see the balance and transaction history of any wallet at any time, just by accessing the Ethereum public blockchain via a block explorer.

9-Immutability

- Every transaction that happens on the Ethereum blockchain is immutable. Smart contracts on the Ethereum blockchain are also immutable.
- Once the smart contract code is deployed, it cannot be changed. Smart contract code will remain on the blockchain forever.
- Anyone can see any deployed smart contract any time in the future as well, just by putting its contract address on the block explorers.
- Data that is being stored in smart contract variables is also immutable, unless there are data removal techniques that have not been exposed by the contract code.

10-Irreversible transactions

- Once a transaction is executed on a blockchain and it receives sufficient confirmation, the transaction becomes irreversible.
- The irreversible transaction ensures the safety of the value transfer.
- The higher the number of confirmations received for a transaction, the harder it becomes to reverse the transaction from the attacker.

11-Trustless Systems

- Two people, without knowing each other, can do transactions using blockchain technology.
- They do not have to trust each other, they only have to trust blockchain technology. For both persons, it is a trustless system.

12-Availability

- Centralized systems sometimes have to go through regular maintenance and downtime, resulting in inconvenience to the users.
- The blockchain is decentralized, so even if some nodes go down/are corrupted, the network will continue to function and will be available to process transactions 24/7.

13-Empower Individuals

- Each individual entity/person has their own wallet's public and private keys on the blockchain network. Using those wallets, they are in full control of their assets and the privileges available for those wallets.
- Blockchain assures that the ownership of a person's data is in their hands.
- However, an individual can only maintain full control over their cryptocurrency or data when they own the private keys of their wallet. When the private keys of their wallet is maintained by another entity, such as centralized exchanges, they may not have full control.

14-Chronological order of transactions

- Blockchains keep their transactions in blocks.
- Multiple transactions are coupled together and stored in a new block. Next, that new block is appended to the chain of previous blocks.
- This keeps all the blockchain transactions maintained in chronological order.

15-Timestamped

- Every transaction on the blockchain is stamped with the current time.
- This enables the blockchain to maintain all the transaction histories of an account.
- Also, this can be used to prove whether or not a transaction happened on a certain date and at a certain time.

16-Sealed with cryptography

- Asymmetric cryptography is used for wallet generation and transaction signing using the Elliptic Curve Digital Signature Algorithm (ECDSA).
- All transactions are packed together using the Merkle tree and SHA-256 cryptographic algorithms.
- This makes blockchains secure and reliable to use.

Thanks

End of Module-2 (Class-1)