Blockchain Core Concepts

What is blockchain?

Blockchain is a decentralized data structure, composed of fixed-length blocks, forming a secure and transparent digital ledger.

The blocks in a blockchain include a number of transactions.

A whitepaper was released in 2008 by bitcoin founder satoshi nakamoto. Nakamoto's white paper referred to blockchain as a`chain of blocks` over time, chain of blocks came to be referred as blockchain.

How Does It Work?

The goal of blockchain is to allow digital information to be recorded and distributed, but not edited. In this way, a blockchain is the foundation for immutable ledgers, or records of transactions that cannot be altered, deleted, or destroyed. This is why blockchains are also known as a distributed ledger technology (DLT).

A block consists of two major parts: Header and Body.

Cryptography

Transforming plaintext into ciphertext.

Cryptography provides protection by transforming data into and unreadable form.

Plantext can be converted into ciphertext by using two ways:

- **substitution**: a method that changes or swaps one character for another.

e.g if every letter is shifted right by three letters.

- **Transposition**: A method that changes the order of characters of a word by using some

predetermined method.

Symmetric key cryptography

- The same key is used to perform encryption and decryption
- The key is shared between the two parties over a secure channel.
- Confidentiality of data is provided.
- Authentication and non-repudiation are not provided.
- Origin of the message cannot be determined.

Asymmetric key cryptography

in asymmetric key cryptography:

- a pair of keys is used.
- a public key is created from a private key.
- it was developed due to problems in symmetric key cryptography.

Cryptographic Hashing

Hashing transforms data or a string of characters into a short and fixed length value.

This value is unique and called hash or hash value or message digest this value is unique hashing algorithm or cryptographic hash function are used to perform hashing.

Hashing Algorithms

- Hashing is an important cryptographic technique that ensures the integrity of data.
- Hashing algorithms are categorized on the basis of their implementations, digest size and other things.

Digital signatures

- digital signature is based on asymmetric key cryptography.
- it provides a high level of security.
- it uses a hash value which is encrypted through the private key of the sender.
- it provides authentication, integrity, and nonrepudiation.

Difference between hashing and encryption

- Hashing is a one-way process.
- Encryption is a two-way or reversible process.
- Hashing will always return a fixed length output regardless of the input size.
- In encryption, the size of the output depends on the size of input.

Consensus Algorithms

Consensus mechanism is implemented in decentralized networks.

Consensus algorithms ensure that nodes agree on a consistent global state of the blockchain.

Some common consensus algorithms in a networks.

- Proof of work
- proof of stake
- proof of elapsed time
- crash fault tolerant

Programmable Blockchains(smart contracts)

- A programmable blockchain implements smart contracts to execute logic programs.
- Ethereum Is the most popular programmable blockchain.

Smart Contracts:

Smart contracts are self-executing, decentralized agreements with predefined rules written in code. They automatically execute when conditions are met.

- it includes a set of predefined conditions.

Characteristics:

- They are self-verifying in nature.
- Decentralized.
- Immutable.

What is a Dapp

- applications that are executed on a peer-to-peer network of computers are known as Dapps. Dapps lack a central authority for decision-making.

To be Dapp:

- Applications source code must be open source.
- Applications data and records must be stored in a public blockchain.
- Application must use cryptographic tokens.

IPFS stands for inter-planetary file system.

It is a distributed file system that aims to replace http.

What is a DAO

Is an organization which:

- Functions without any conventional management structure
- Manages and sustains itself using smart contracts.
- DAOs are implemented using smart contracts.

In a decentralized organization, there is no central decision-making authority.

Thank you for your attention!