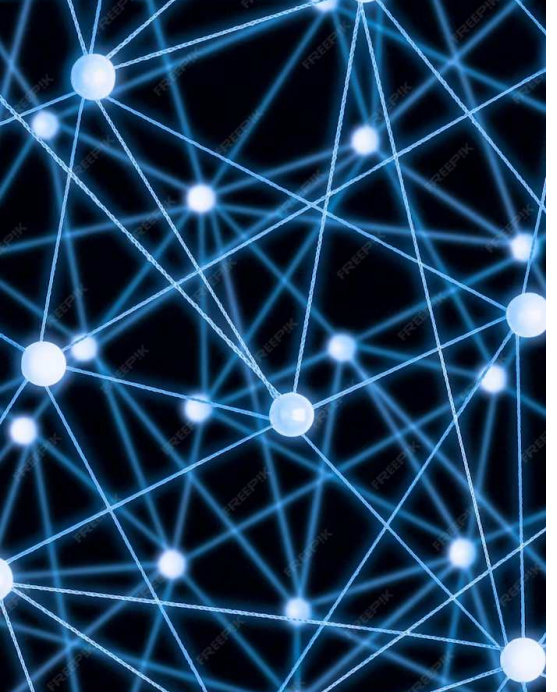
Web 3.0: Decentralized Web



Decentralized systems?

If a central entity crashes or misuses information, the whole system is compromised. Decentralization distributes decision making power across entities instead of a single authority. Consensus algorithms are the way those decisions are reached, it provides a way for d/t components in a system to achieve agreement on a single data value without the need for a central authority.

Network Definition

Is a system of linked nodes or computers that share resources such as storage, processing units, and communication channel bandwidth.

Network Types:

Centralized, decentralized, and distributed.

- BitTorrent is a great example of a distributed protocol for file-sharing.
- Evolution of the Internet - Web 1.0, 2.0, and 3.0

What is block-chain?

It allows users to send and receive data securely and transparently without needing a central authority or intermediary, by having a copy of all transactions distributed across the network using consensus mechanism, storing data in blocks, where each block is tied to the previous, resulting in a chain of block or block-chain.

Blockchain Types

1) Public,permissionless
2) Public, permissioned
3) Private, permissionless
4) Private, permissioned

Cryptography

Encryption Algorithm and **Decryption** Algorithm

There are two types of algorithms for encrypting messages: **symmetric encryption** and **asymmetric encryption**. In **symmetric**, the **same key** is used to encrypt and decrypt the data, making it fast and simple but less secure. **Asymmetric**, also known as public key cryptography,
uses **two keys**: a **public key** and **private key**. What one key can encrypt, the other can decrypt.

Hash Functions

It takes an input and returns a fixed-size output called a hash digest and the original input can't be derived from the hash. Any change to the original input will be reflected in completely different hash output.

Use cases:

- Linking blocks in a chain
- In mining
- In digital signatures

Digital Signatures

Can be used to authenticate the identity of the sender of a transaction and verify that a transaction has not been tampered with or altered in any way.

How does this work? The sender uses their own private key to sign the message creating a unique digital signature. This signature can be verified by anyone with access to the sender's public key. Two algorithms are needed in a digital signature scheme: the signing algorithm(to create a signature) and the verifying algorithm(to verify the signature).

Smart Contracts

- Is a program stored on a blockchain, Deployed smart contracts cannot be deleted by default, and interactions with them are irreversible. - Ethereum implemented Solidity and Cardano implemented Plutus programming language to develop smart contracts.Follows “if this, then that” logic.

Decentralized Applications

Decentralized applications (*DApps*) are at the core of Web3, offering **censorship-resistant** and *immutable* functionalities. These applications are built on blockchain and smart contracts, enabling new possibilities in finance, governance, and more.

Embracing the Future

Web3 is poised to reshape the internet and empower individuals with **sovereignty** over their digital lives. Embracing this future requires collaboration, innovation, and a commitment to building a more *decentralized*, equitable, and secure digital world.

Thanks!