Introduction to Blockchain & Cryptocurrencies

HA-3

Q① Explain types of Blockchain briefly with example

A) There are several types of blockchain, mainly.

i) Public Blockchain:

Public Blockchain are open, and permissionless meaning anyone can participate validate transactions, and become a part of network.

Ex: Ethereum is well known public blockchain, which allows publicly to all.

ii) Private Blockchain:

Private Blockchains are restricted to a specific group of particular or organizations.

Ex: Hyperledger fabric, witi, is a popular private blockchain.

iii) Consortium Blockchain:

Consortium blockchains are semi-decentralized and are governed by a consortium or group of organizations.

Ex: R3 Corda is a consortium blockchain platform.

(2) Explain 3-phase commit protocol with an example?

A) The three-phase commit protocol is a distributed algorithm used to achieve consensus in a distributed system.

i) Prepare phase:

In this phase, the coordinator sends a message to all participating nodes asking if they are ready to commit the transaction.

ii) Commit phase:

If all cohort nodes respond with "yes" during the prepare phase, the coordinator sends a "commit" message to all cohort nodes.

iii) Abort phase:

If any nodes responds "No" during prepare phase or it send an "Abort" message to all cohort nodes.

Example: participants: There are 3 nodes in system:

Coordinator(C), Node A, Node B

i) Prepare phase:

- Node A: "Yes"
- Node B: "Yes"

ii) Commit phase: Coordinator(C) sends a "Commit" message to Node A & Node B.

- Node A, B perform commit operations on their databases.

iii) Result: If all nodes successfully commit, the transaction is considered successful.

(3) Explain transaction life cycle. Mention how double spending can be avoided in Blockchain network.

A) The transaction life cycle in a blockchain network involves several stages from the initiation of a transaction to its final confirmation.

1) Initiation: A transaction begins when a user initiates it.

2) Creation: Once initiated, the transaction is created in a digital format.

3) Signing: In public blockchain networks, the transaction must be signed by sender using their private key.

4) Broad casting: The signed transaction is broadcasted in network.

5) Validation: Miners or validators in network receive the transaction & verify its validity.

6) Inclusion in Block:

Valid transactions are grouped together into a block.

7) Confirmation: After the block containing the transaction is added to blockchain.

(4) Explain Bitcoin anonymity and appropriately discuss Bitcoin properties.

A) Bitcoin offers a degree of pseudonymity rather than full anonymity.

i) pseudonymous Address:

Bitcoin users interact with ~~key~~network using (database) addresses, of their public keys.

ii) Transaction privacy:

Bitcoin transactions reveal the sender's address, receipts address, and the amount transferred.

iii) Anonymizing techniques:

Various techniques exist to enhance Bitcoin's privacy, such as coinjoin and coinswap.

iv) Mixing service:

It allows users to mix their bitcoins with those of other users, making it difficult to trace origin of coins.

v) Third-party data:

Some level of de-anonymization can occur when users interact with Bitcoin through centralized exchanges, which are often required to follow Know Your Customer (KYC) regulations.

(5) Explain Ethereum briefly with example?

A) • Ethereum is a blockchain platform and cryptocurrency that extends the capabilities of Bitcoin by enabling the development of de-centralized applications and smart contracts.

Example:

i) Smart Contract Creation:

You write a smart contract code specifying the rule of your crowdfunding campaign.

ii) Deployment: You deploy your smart contract onto the Ethereum blockchain.

iii) Crowdfunding campaign:

people interested in your project send Ether to the contract's address.

iv) Funding Goal Met:

If the campaign reaches its funding goal within a specified timeframe, the smart contract.

automatically releases the funds to your project.

v) Refunds or partial funding:

If the funding goal is not met, the smart contract may automatically refund the contributed ether to the backers.

vi) Transparency and trust:

All interactions with the smart contract are recorded on the Ethereum blockchain, providing transparency and trust to backers who can verify the contract's code and the movement of funds.

(6) Explain key differences between Bitcoin & Ethereum.

A) Bitcoin and Ethereum are both cryptocurrencies but they serve different purpose and have their key differences.

i) Primary purpose:

- Bitcoin: created as digital currency with the primary goal of providing a decentralized censorship of digital money.
- Ethereum: was designed as a platform of decentralized applications & smart

contracts.

ii) Smart Contracts:

- Bitcoin: does not natively support smart contracts.
- Ethereum: built with a turing-complete scripting language.

iii) Scripting Language:

- Bitcoin: uses a stack based scripting language for simple transaction scripts.
- Ethereum: uses high-level turing-complete language called solidity for creating smart contracts.

iv) Supply Cap:

- Bitcoin: has a capped supply of 21 million coins.

Ethereum: did not have a capped supply.

v) Consensus Mechanism:

Bitcoin: uses a proof of work Consensus mechanism.

Ethereum: uses PoW but in process of to a Proof of stake Consensus mechanism with Ethereum 2.0.