Advanced Cryptocurrency Concepts

Cryptocurrency · Answer Key · 15 Questions

1. What is the primary mechanism by which Bitcoin's proof-of-work consensus algorithm prevents double-spending and ensures network integrity?

A) A. Sharding and parallel processing

B) B. Cryptographic hashing and computational puzzles

C) C. Delegated proof-of-stake validation

D) D. Centralized ledger management by a consortium

2. Which cryptographic primitive is fundamental to the operation of public-key cryptography used in most cryptocurrencies, enabling secure transactions and digital signatures?

A) A. Symmetric-key encryption (e.g., AES)

B) B. Hashing algorithms (e.g., SHA-256)

C) C. Asymmetric-key encryption (e.g., RSA, ECC)

D) D. Homomorphic encryption

3. In Ethereum, what role does the 'gas' concept play within the Ethereum Virtual Machine (EVM)?

A) A. It represents the native token used for staking to secure the network.

B) B. It is a measure of computational effort required to execute smart contract functions and transactions.

C) C. It is a reward given to miners for validating blocks.

D) D. It acts as a governance token for voting on network upgrades.

4. What is the main purpose of a Merkle tree (or hash tree) in blockchain technology, as utilized in Bitcoin?

A) A. To encrypt individual transaction data for privacy.

B) B. To efficiently summarize and verify the integrity of a large set of transactions within a block.

C) C. To facilitate peer-to-peer network discovery.

D) D. To manage the distribution of newly minted coins.

5. Which of the following best describes the concept of 'smart contracts' on platforms like Ethereum?

A) A. Legal agreements enforced by traditional court systems.

B) B. Self-executing contracts with the terms of the agreement directly written into code.

C) C. Cryptographic algorithms that secure communication between users.

D) D. Decentralized autonomous organizations (DAOs) for corporate governance.

6. What is the fundamental difference between a public blockchain (like Bitcoin) and a private blockchain in terms of access and participation?

A) A. Public blockchains are permissionless, while private blockchains are permissioned.

B) B. Public blockchains use proof-of-stake, while private blockchains use proof-of-work.

C) C. Public blockchains have faster transaction speeds than private blockchains.

D) D. Private blockchains are more decentralized than public blockchains.

7. In the context of cryptocurrencies, what does the term 'fork' primarily refer to?

A) A. The process of mining new blocks.

B) B. A change in the blockchain's protocol that creates two diverging paths, one or both of which may continue to operate.

C) C. The cryptographic hashing of transaction data.

D) D. The transfer of cryptocurrency from one wallet to another.

8. Which consensus mechanism is known for its energy efficiency compared to proof-of-work, and involves validators 'staking' their cryptocurrency to secure the network?

A) A. Proof-of-Authority (PoA)

B) B. Proof-of-Stake (PoS)

C) C. Proof-of-Burn (PoB)

D) D. Byzantine Fault Tolerance (BFT)

9. What is the primary role of a 'seed phrase' (or recovery phrase) in cryptocurrency wallet management?

A) A. To encrypt individual transactions for enhanced privacy.

B) B. To generate the private key, allowing access to the user's funds if the wallet is lost or corrupted.

C) C. To verify the authenticity of a cryptocurrency exchange.

D) D. To determine the transaction fee for sending crypto.

10. What is the purpose of a 'zero-knowledge proof' in certain advanced cryptocurrency applications?

A) A. To publicly reveal all transaction details to enhance transparency.

B) B. To allow one party to prove that a statement is true to another party, without revealing any information beyond the validity of the statement itself.

C) C. To increase the block size limit for higher transaction throughput.

D) D. To facilitate the mining of new blocks through brute-force computation.

11. Which of the following is NOT a common characteristic of decentralization in blockchain networks?

A) A. No single point of control or failure.
B) B. Distributed ledger across multiple nodes.
C) C. Reliance on a central authority for transaction validation.
D) D. Censorship resistance.

12. What is the fundamental difference between a Bitcoin transaction and a typical fiat currency transaction facilitated by a bank?

A) A. Fiat transactions are typically irreversible, while Bitcoin transactions can be reversed by the sender.
B) B. Bitcoin transactions are pseudonymous and recorded on a public ledger, while fiat transactions are often private and managed by intermediaries.
C) C. Fiat transactions require private keys to authorize, while Bitcoin transactions use passwords.
D) D. Fiat transactions are always processed in real-time, while Bitcoin transactions can take days to confirm.

13. The concept of 'immutability' in blockchain refers to:

A) A. The ability to easily modify or delete past transactions.
B) B. The inherent resistance of recorded data to alteration or deletion.
C) C. The process of creating new digital coins.
D) D. The anonymity of transaction participants.

14. What is an 'ICO' (Initial Coin Offering) in the cryptocurrency space?

A) A. A traditional stock market initial public offering.
B) B. A fundraising method used by some cryptocurrency projects, often involving the sale of new tokens.
C) C. A security protocol for blockchain networks.
D) D. A type of decentralized exchange.

15. Which of these best describes a 'hard fork' in a blockchain, as opposed to a soft fork?

A) A. A soft fork is backward compatible with the old protocol, while a hard fork is not.
B) B. A hard fork requires consensus from all miners, while a soft fork does not.
C) C. A soft fork can create new coins, while a hard fork cannot.
D) D. Hard forks only occur on private blockchains, while soft forks occur on public ones.