Advanced Cryptocurrency Fundamentals

Computer Science And Economics · Answer Key · 20 Questions

1. Which specific cryptographic primitive is utilized in Bitcoin's proof-of-work consensus mechanism to ensure block integrity?

A) SHA-256
B) AES-256
C) RSA-4096
D) ECDSA

2. In the context of the Bitcoin protocol, what does a 'UTXO' represent?

A) Unspent Transaction Output
B) Universal Token Exchange Order
C) Unique Transaction Verification Object
D) Unified Transfer X-chain Operation

3. What is the primary function of a Merkle Tree within a blockchain data structure?

A) To facilitate rapid searching of transaction data
B) To reduce the energy consumption of mining
C) To provide anonymity for network participants
D) To enable cross-chain compatibility

4. What is the 'halving' event in the Bitcoin protocol?

A) The reduction of the block reward by 50%
B) The splitting of the blockchain into two separate chains
C) The decrease of transaction fees by half
D) The process of doubling the circulating supply

5. Which Byzantine Fault Tolerance mechanism is utilized by Ethereum following 'The Merge'?

A) Proof-of-Stake
B) Proof-of-Work
C) Proof-of-Authority
D) Proof-of-Burn

6. What does the 'nonce' field specifically control in a block header?

A) The variable input for the hashing algorithm
B) The timestamp of the transaction
C) The public key of the miner
D) The fee structure of the block

7. Which term describes the process of sending cryptocurrency to an address from which it cannot be retrieved?

A) Burning
B) Minting
C) Forking
D) Staking

8. In a Proof-of-Stake system, what does 'slashing' refer to?

A) The penalty for validators who act maliciously
B) The process of creating new coins
C) The reduction of transaction speed
D) The removal of old blocks from the ledger

9. What is the primary purpose of a 'Hard Fork' in a blockchain protocol?

A) To implement non-backward-compatible protocol changes
B) To increase the number of wallets
C) To lower the market volatility
D) To enable private transactions

10. Which layer of the blockchain stack handles the execution of smart contracts?

A) Application Layer
B) Network Layer
C) Consensus Layer
D) Data Layer

11. What does 'EIP-1559' specifically introduce to the Ethereum network?

A) A mechanism for burning a portion of transaction fees
B) A shift to quantum-resistant encryption
C) A reduction in node requirements
D) An increase in block size limits

12. What is the definition of a '51% attack' on a blockchain network?

A) A miner gaining control of a majority of the hash power
B) An attack on the user's private keys
C) A vulnerability in the wallet software
D) A failure in the P2P connection protocol

13. What is the primary function of a 'zero-knowledge proof' in privacy-focused blockchains?

A) To prove a statement is true without revealing the data
B) To compress transaction size
C) To increase mining rewards
D) To encrypt the entire blockchain ledger

14. In decentralized finance (DeFi), what is an 'Automated Market Maker' (AMM)?

A) A protocol that uses algorithms to price assets
B) A physical kiosk for crypto exchange
C) A government regulatory body
D) A type of high-frequency trading bot

15. What characterizes an 'ERC-20' token on the Ethereum network?

A) It is a fungible token standard
B) It is a non-fungible asset
C) It is a governance-only token
D) It is a side-chain specific currency

16. What is the 'Genesis Block' in any blockchain?

A) The first block of the chain
B) The block where a fork occurs
C) The largest block ever mined
D) The block with the highest transaction volume

17. Which problem does the 'Lightning Network' aim to solve for Bitcoin?

A) Scalability and transaction speed
B) Mining energy consumption
C) Decentralization of nodes
D) Anonymity of users

18. What is the main role of an 'Oracle' in smart contract development?

A) Providing real-world data to the blockchain
B) Executing code on the mainnet
C) Storing private user information
D) Calculating complex cryptographic hashes

19. What distinguishes 'Cold Storage' from 'Hot Wallets'?

A) It is stored offline
B) It is stored on a mobile device
C) It is backed by gold
D) It requires an internet connection

20. What is the 'Difficulty Adjustment' algorithm in Bitcoin designed to maintain?

A) Average block generation time

B) The price of Bitcoin

C) The number of active miners

D) The total circulating supply