Blockchain Fundamentals – Quiz

Cryptoeconomics

Question 1

What cryptographic function links blocks in a blockchain?

A. Symmetric encryption
B. Hash function
C. RSA encryption
D. Base64 encoding

Question 1

What cryptographic function links blocks in a blockchain?

A. Symmetric encryption
B. Hash function
C. RSA encryption
D. Base64 encoding

Answer: B
Each block contains the hash of the previous block's header, creating a cryptographic chain.

Question 2

What is a Merkle tree used for in blockchain?

A. Mining coins
B. Efficiently verifying transaction inclusion
C. Storing wallet addresses
D. Managing network nodes

Question 2

What is a Merkle tree used for in blockchain?

A. Mining coins
B. Efficiently verifying transaction inclusion
C. Storing wallet addresses
D. Managing network nodes

Answer: B
Merkle trees allow efficient verification that a transaction is included in a block without downloading the entire block.

Question 3

What is the Merkle root?

A. The first transaction in a block
B. The single hash at the top of a Merkle tree representing all transactions
C. The block reward
D. The genesis block

Question 3

What is the Merkle root?

A. The first transaction in a block
B. The single hash at the top of a Merkle tree representing all transactions
C. The block reward
D. The genesis block

Answer: B
The Merkle root is the single hash that summarizes all transactions in a block through recursive hashing.

Question 4

What happens if someone tries to alter a transaction in an old block?

A. Nothing, changes are allowed
B. Only the changed block is affected
C. All subsequent block hashes become invalid
D. The network automatically accepts the change

Question 4

What happens if someone tries to alter a transaction in an old block?

A. Nothing, changes are allowed
B. Only the changed block is affected
C. All subsequent block hashes become invalid
D. The network automatically accepts the change

Answer: C
Changing any data changes the block's hash, which invalidates all subsequent blocks that reference it.

Question 5

What is a 'nonce' in blockchain?

A. A type of cryptocurrency
B. A random number miners adjust to find a valid block hash
C. A transaction fee
D. A wallet address

Question 5

What is a 'nonce' in blockchain?

A. A type of cryptocurrency
B. A random number miners adjust to find a valid block hash
C. A transaction fee
D. A wallet address

Answer: B
The nonce (number used once) is incremented by miners until the block hash meets the difficulty target.

Question 6

What is 'immutability' in blockchain context?

A. Transactions can be reversed easily
B. Once recorded, data cannot be altered without consensus
C. The blockchain can grow indefinitely
D. Blocks are created instantly

Question 6

What is 'immutability' in blockchain context?

A. Transactions can be reversed easily
B. Once recorded, data cannot be altered without consensus
C. The blockchain can grow indefinitely
D. Blocks are created instantly

Answer: B
Immutability means past records cannot be changed without redoing all subsequent proof-of-work and gaining network consensus.

Question 7

What does a block header typically contain?

A. Only transaction data
B. Previous block hash, Merkle root, timestamp, nonce, difficulty
C. User passwords
D. Mining software version only

Question 7

What does a block header typically contain?

A. Only transaction data

B. Previous block hash, Merkle root, timestamp, nonce, difficulty

C. User passwords

D. Mining software version only

Answer: B

The block header contains metadata including the previous block hash, Merkle root, timestamp, nonce, and difficulty target.

Question 8

What is a 'full node' in blockchain?

A. A node that only stores recent blocks
B. A node that stores and validates the entire blockchain
C. A mining-only node
D. A node run by exchanges

Question 8

What is a 'full node' in blockchain?

A. A node that only stores recent blocks
B. A node that stores and validates the entire blockchain
C. A mining-only node
D. A node run by exchanges

Answer: B
A full node downloads, stores, and validates the entire blockchain history, enforcing all consensus rules.

Question 9

What is the purpose of the difficulty adjustment?

A. To increase transaction fees
B. To maintain consistent block time despite changing hashpower
C. To reduce energy consumption
D. To limit the number of miners

Question 9

What is the purpose of the difficulty adjustment?

A. To increase transaction fees
B. To maintain consistent block time despite changing hashpower
C. To reduce energy consumption
D. To limit the number of miners

Answer: B
Difficulty adjusts to maintain target block time (10 minutes for Bitcoin) as network hashrate changes.

Question 10

What is a 'light client' or SPV node?

A. A node with high processing power
B. A node that only downloads block headers and verifies specific transactions
C. A mining pool
D. An exchange wallet

Question 10

What is a 'light client' or SPV node?

A. A node with high processing power

B. A node that only downloads block headers and verifies specific transactions

C. A mining pool

D. An exchange wallet

Answer: B

SPV (Simplified Payment Verification) nodes store only headers and use Merkle proofs to verify transactions.

Question 11

What is a 'fork' in blockchain?

A. A type of transaction
B. When the chain splits into two or more paths
C. A mining technique
D. A wallet feature

Question 11

What is a 'fork' in blockchain?

A. A type of transaction
B. When the chain splits into two or more paths
C. A mining technique
D. A wallet feature

Answer: B
A fork occurs when the blockchain diverges. Temporary forks happen naturally during propagation (resolved by longest chain rule). Protocol forks are intentional changes: soft forks (backward-compatible) or hard forks (not backward-compatible).

Question 12

What is the 'longest chain rule'?

A. The oldest chain is always valid
B. The chain with most accumulated proof-of-work is considered valid
C. The chain with most transactions wins
D. The chain with highest fees wins

Question 12

What is the 'longest chain rule'?

A. The oldest chain is always valid
B. The chain with most accumulated proof-of-work is considered valid
C. The chain with most transactions wins
D. The chain with highest fees wins

Answer: B
Bitcoin follows the chain with the most cumulative proof-of-work, which typically is the longest chain.

Question 13

What is a UTXO?

A. A type of smart contract
B. Unspent Transaction Output - spendable Bitcoin amounts
C. A consensus algorithm
D. A wallet backup

Question 13

What is a UTXO?

A. A type of smart contract

B. Unspent Transaction Output - spendable Bitcoin amounts

C. A consensus algorithm

D. A wallet backup

Answer: B

UTXO (Unspent Transaction Output) represents spendable Bitcoin. Transactions consume UTXOs and create new ones.

Question 14

How does Bitcoin prevent double-spending?

A. By limiting transaction amounts
B. Through consensus on transaction ordering in the blockchain
C. By requiring KYC verification
D. Through central bank approval

Question 14

How does Bitcoin prevent double-spending?

A. By limiting transaction amounts
B. Through consensus on transaction ordering in the blockchain
C. By requiring KYC verification
D. Through central bank approval

Answer: B
The blockchain provides a single, agreed-upon ordering of transactions, preventing the same coins from being spent twice.

Question 15

What is the typical Bitcoin block size limit?

A. 4 MB
B. 1 MB (with SegWit allowing up to ˜4 MB weight)
C. 10 MB
D. Unlimited

Question 15

What is the typical Bitcoin block size limit?

A. 4 MB

B. 1 MB (with SegWit allowing up to ~4 MB weight)

C. 10 MB

D. Unlimited

Answer: B

Bitcoin has a 1 MB base block size limit. SegWit (2017) introduced a 4 million weight unit limit, where witness data counts as 0.25 units/byte. This allows actual blocks up to ~3.3-3.5 MB.

Question 16

What is 'propagation delay' in blockchain networks?

A. Time for mining
B. Time for new blocks to spread across the network
C. Transaction confirmation time
D. Wallet sync time

Question 16

What is 'propagation delay' in blockchain networks?

A. Time for mining
B. Time for new blocks to spread across the network
C. Transaction confirmation time
D. Wallet sync time

Answer: B
Propagation delay is the time it takes for a new block to be transmitted to all nodes in the network.

Question 17

What is a 'stale block' or 'orphan block'?

A. A block with no transactions
B. A valid block that is not part of the main chain
C. An invalid block
D. The genesis block

Question 17

What is a 'stale block' or 'orphan block'?

A. A block with no transactions
B. A valid block that is not part of the main chain
C. An invalid block
D. The genesis block

Answer: B
Stale blocks are valid blocks that were mined but not included in the main chain due to another block being accepted first.

Question 18

What is the coinbase transaction?

A. A transaction on the Coinbase exchange
B. The first transaction in a block that creates new coins as mining reward
C. A refund transaction
D. A fee payment

Question 18

What is the coinbase transaction?

A. A transaction on the Coinbase exchange
B. The first transaction in a block that creates new coins as mining reward
C. A refund transaction
D. A fee payment

Answer: B
The coinbase transaction is the first transaction in each block, creating new bitcoins as the block reward for miners.

Question 19

Why is blockchain considered tamper-evident?

A. Because of encryption
B. Because changing any block changes all subsequent hashes
C. Because of user authentication
D. Because of backup systems

Question 19

Why is blockchain considered tamper-evident?

A. Because of encryption
B. Because changing any block changes all subsequent hashes
C. Because of user authentication
D. Because of backup systems

Answer: B
The hash chain structure means any tampering is immediately detectable as it breaks the hash linkage.

Question 20

What is 'finality' in blockchain?

A. The end of mining
B. The assurance (probabilistic or absolute) that a transaction will not be reversed
C. The last block in the chain
D. The maximum transaction limit

Question 20

What is 'finality' in blockchain?

A. The end of mining
B. The assurance (probabilistic or absolute) that a transaction will not be reversed
C. The last block in the chain
D. The maximum transaction limit

Answer: B
Finality refers to the assurance that a transaction will not be reversed. Bitcoin provides probabilistic finality that increases with confirmations. BFT-based systems can provide absolute finality.

Question 21

Two miners find valid blocks at almost the same time (block height 700,000). Miner A's block reaches 60% of nodes first, while Miner B's block reaches 40% of nodes first. What will likely happen?

A. Both blocks are permanently added, creating two parallel chains

B. The block that reached more nodes (Miner A's) is automatically chosen

C. A temporary fork occurs; the next block mined will determine which chain becomes the main chain

D. The network votes to decide which block to keep

Question 21

Two miners find valid blocks at almost the same time (block height 700,000). Miner A's block reaches 60% of nodes first, while Miner B's block reaches 40% of nodes first. What will likely happen?

A. Both blocks are permanently added, creating two parallel chains

B. The block that reached more nodes (Miner A's) is automatically chosen

C. A temporary fork occurs; the next block mined will determine which chain becomes the main chain

D. The network votes to decide which block to keep

Answer: C

When two valid blocks are found simultaneously, a temporary fork occurs. Nodes work on whichever block they received first. When the next block is mined on one of the chains, that chain becomes longer and nodes switch to it (longest chain rule). The other block becomes a stale/orphan block.

Question 22

A Layer 2 solution like the Lightning Network enables Bitcoin transactions to occur off-chain. What is the main security trade-off?

A. Layer 2 transactions are not secured by cryptography
B. Participants must monitor the network to detect fraud; security depends on liveness assumptions
C. Layer 2 transactions can be double-spent without consequences
D. Layer 2 solutions require trust in a central authority

Question 22

A Layer 2 solution like the Lightning Network enables Bitcoin transactions to occur off-chain. What is the main security trade-off?

A. Layer 2 transactions are not secured by cryptography

B. Participants must monitor the network to detect fraud; security depends on liveness assumptions

C. Layer 2 transactions can be double-spent without consequences

D. Layer 2 solutions require trust in a central authority

Answer: B

Layer 2 solutions like Lightning Network maintain security through cryptographic proofs and the ability to settle on-chain. However, users must monitor the network (or use watchtowers) to detect and respond to fraudulent channel closure attempts within a timelock period. This introduces a liveness assumption that isn't required for on-chain transactions.

Question 23

MEV (Maximal Extractable Value) refers to profit miners/validators can extract by reordering, including, or censoring transactions. Which scenario demonstrates MEV?

A. A miner prioritizes transactions with higher fees

B. A miner sees a large pending DEX trade, inserts their own trade before it (front-running), and another after it (back-running) to profit from price movement

C. A miner includes more transactions to earn more fees

D. A validator stakes more tokens to increase block production chances

Question 23

MEV (Maximal Extractable Value) refers to profit miners/validators can extract by reordering, including, or censoring transactions. Which scenario demonstrates MEV?

A. A miner prioritizes transactions with higher fees

B. A miner sees a large pending DEX trade, inserts their own trade before it (front-running), and another after it (back-running) to profit from price movement

C. A miner includes more transactions to earn more fees

D. A validator stakes more tokens to increase block production chances

Answer: B

MEV extraction involves exploiting knowledge of pending transactions to profit beyond normal fees. Front-running and back-running (sandwich attacks) are classic examples where the block producer manipulates transaction ordering to extract value from users. Simple fee prioritization is normal behavior, not MEV extraction.

Question 24

A merchant accepts a Bitcoin payment after 1 confirmation (one block). An attacker with 35% of network hashrate wants to double-spend. What is the merchant's risk?

A. Zero risk - one confirmation makes the transaction irreversible
B. High risk - the attacker has a significant probability (˜35%) of creating a longer chain
C. Moderate risk - the attacker has some probability of success that decreases with each additional confirmation
D. Complete certainty of double-spend attack success

Question 24

A merchant accepts a Bitcoin payment after 1 confirmation (one block). An attacker with 35% of network hashrate wants to double-spend. What is the merchant's risk?

A. Zero risk - one confirmation makes the transaction irreversible

B. High risk - the attacker has a significant probability (˜35%) of creating a longer chain

C. Moderate risk - the attacker has some probability of success that decreases with each additional confirmation

D. Complete certainty of double-spend attack success

Answer: C

With 35% hashrate, the attacker has a realistic chance of mining a longer chain, especially with few confirmations. The probability of a successful double-spend decreases exponentially with each confirmation. One confirmation provides weak security against a well-resourced attacker. Most merchants wait for 3-6 confirmations for large amounts.

Question 25

Bitcoin's UTXO model differs from Ethereum's account model. If Alice has received 5 separate Bitcoin payments (0.5 BTC each) and wants to send Bob 2 BTC, what happens?

A. Alice's wallet balance of 2.5 BTC is reduced by 2 BTC

B. At least 4 UTXOs (totaling 2 BTC) are consumed as inputs, 1 output goes to Bob, and change returns to Alice as a new UTXO

C. The largest UTXO is split to send 2 BTC to Bob

D. All 5 UTXOs are automatically merged, then 2 BTC is sent

Question 25

Bitcoin's UTXO model differs from Ethereum's account model. If Alice has received 5 separate Bitcoin payments (0.5 BTC each) and wants to send Bob 2 BTC, what happens?

A. Alice's wallet balance of 2.5 BTC is reduced by 2 BTC

B. At least 4 UTXOs (totaling 2 BTC) are consumed as inputs, 1 output goes to Bob, and change returns to Alice as a new UTXO

C. The largest UTXO is split to send 2 BTC to Bob

D. All 5 UTXOs are automatically merged, then 2 BTC is sent

Answer: B

Bitcoin's UTXO model requires transactions to consume entire UTXOs as inputs and create new UTXOs as outputs. To send 2 BTC, Alice's wallet must select at least 4 of her 0.5 BTC UTXOs (totaling 2+ BTC), consume them entirely, create a 2 BTC output for Bob, and create a change output back to herself. This differs fundamentally from account-based systems where balances are simply debited.

Question 26 (True/False)

Each block in a blockchain contains exactly one transaction.

A. True
B. False

Question 26 (True/False)

Each block in a blockchain contains exactly one transaction.

A. True

B. False

Answer: False

Blocks typically contain many transactions bundled together. Bitcoin blocks can contain thousands of transactions, limited by block size.

Question 27 (True/False)

Merkle trees enable efficient verification of transaction inclusion.

A. True
B. False

Question 27 (True/False)

Merkle trees enable efficient verification of transaction inclusion.

A. True

B. False

Answer: True

Merkle trees allow verifying that a transaction is included in a block without downloading all transactions, using only the Merkle proof path.

Question 28 (True/False)

The genesis block has a previous hash pointing to an earlier block.

A. True
B. False

Question 28 (True/False)

The genesis block has a previous hash pointing to an earlier block.

A. True

B. False

Answer: False

The genesis block is the first block in the blockchain and has no previous block, so its previous hash field is typically set to all zeros.

Question 29 (True/False)

Blocks can be easily modified after they are added to the blockchain.

A. True
B. False

Question 29 (True/False)

Blocks can be easily modified after they are added to the blockchain.

A. True

B. False

Answer: False

Blockchain immutability means once a block is added and confirmed, changing it would require recalculating all subsequent blocks, which is computationally infeasible.

Question 30 (True/False)

A full node stores the entire blockchain history.

A. True
B. False

Question 30 (True/False)

A full node stores the entire blockchain history.

A. True

B. False

Answer: True
Full nodes download, store, and validate the complete blockchain from the genesis block to the most recent block.

Question 31 (True/False)

The nonce is a value that miners adjust to find a valid block hash.

A. True
B. False

Question 31 (True/False)

The nonce is a value that miners adjust to find a valid block hash.

A. True

B. False

Answer: True

The nonce (number used once) is incremented by miners until they find a hash that meets the difficulty target for proof-of-work.

Question 32 (True/False)

Changing data in an old block will not affect subsequent blocks.

A. True
B. False

Question 32 (True/False)

Changing data in an old block will not affect subsequent blocks.

A. True

B. False

Answer: False

Changing any data in a block changes its hash, which invalidates all subsequent blocks that reference it, as each block contains the hash of the previous block.

Question 33 (Fill in the Blank)

The first block is called the ___ block. *Hint: Think about the beginning...*

Question 33 (Fill in the Blank)

The first block is called the ___ block. *Hint: Think about the beginning...* **Answer: genesis**

The genesis block is the first block in any blockchain.

Question 34 (Fill in the Blank)

A ___ tree allows efficient verification of transactions. *Hint: Named after a cryptographer...*

Question 34 (Fill in the Blank)

A ___ tree allows efficient verification of transactions. *Hint: Named after a cryptographer...* **Answer: Merkle**

Merkle trees allow efficient verification that a transaction is included in a block without downloading all transactions.

Question 35 (Fill in the Blank)

Each block contains a hash of the ___ block. *Hint: What comes before?*

Question 35 (Fill in the Blank)

Each block contains a hash of the ___ block. *Hint: What comes before?* **Answer: previous**

Each block contains the hash of the previous block's header, creating the chain structure.