

Consensus Mechanisms – Quiz

Cryptoeconomics

Question 1

What is Proof of Work (PoW)?

- A. Proving you own tokens
- B. A consensus mechanism requiring computational work to validate blocks
- C. A type of wallet
- D. A transaction verification method

Question 1

What is Proof of Work (PoW)?

- A. Proving you own tokens
- B. A consensus mechanism requiring computational work to validate blocks
- C. A type of wallet
- D. A transaction verification method

Answer: B

PoW requires miners to expend computational resources solving cryptographic puzzles to add blocks.

Question 2

What is Proof of Stake (PoS)?

- A. Proving physical ownership
- B. A consensus mechanism where validators are selected based on staked tokens
- C. A mining technique
- D. A wallet security feature

Question 2

What is Proof of Stake (PoS)?

- A. Proving physical ownership
- B. A consensus mechanism where validators are selected based on staked tokens
- C. A mining technique
- D. A wallet security feature

Answer: B

PoS selects validators proportionally to their staked tokens, replacing energy-intensive mining.

Question 3

What is a '51% attack'?

- A. When 51% of nodes go offline
- B. When an entity controls majority hashpower and can manipulate the chain
- C. When 51% of transactions fail
- D. A wallet hack

Question 3

What is a '51% attack'?

- A. When 51% of nodes go offline
- B. When an entity controls majority hashpower and can manipulate the chain
- C. When 51% of transactions fail
- D. A wallet hack

Answer: B

A 51% attack occurs when a single entity controls majority computational power, enabling double-spends and chain reorganization. In PoW, $\geq 50\%$ guarantees success. However, selfish mining attacks can be profitable at $\sim 33\%$. PoS systems have different thresholds (often 33% or 67% based on BFT assumptions).

Question 4

What is 'slashing' in Proof of Stake?

- A. Reducing transaction fees
- B. Penalizing validators who act maliciously by destroying their stake
- C. Cutting block rewards
- D. Reducing network traffic

Question 4

What is 'slashing' in Proof of Stake?

- A. Reducing transaction fees
- B. Penalizing validators who act maliciously by destroying their stake
- C. Cutting block rewards
- D. Reducing network traffic

Answer: B

Slashing destroys a portion of a validator's staked tokens if they behave dishonestly or negligently.

Question 5

What is the main criticism of Proof of Work?

- A. It's too fast
- B. High energy consumption
- C. Too decentralized
- D. Too many validators

Question 5

What is the main criticism of Proof of Work?

- A. It's too fast
- B. High energy consumption
- C. Too decentralized
- D. Too many validators

Answer: B

PoW is criticized for massive energy consumption, as miners compete with increasingly powerful hardware.

Question 6

What is Byzantine Fault Tolerance (BFT)?

- A. Tolerance for slow transactions
- B. Ability to reach consensus despite some nodes being faulty or malicious
- C. Resistance to hardware failures
- D. Network speed optimization

Question 6

What is Byzantine Fault Tolerance (BFT)?

- A. Tolerance for slow transactions
- B. Ability to reach consensus despite some nodes being faulty or malicious
- C. Resistance to hardware failures
- D. Network speed optimization

Answer: B

BFT systems can maintain correct operation even when some participants are dishonest or faulty.

Question 7

What is 'finality' in consensus?

- A. The end of mining
- B. The guarantee that confirmed blocks cannot be reverted
- C. Maximum block size
- D. Transaction speed

Question 7

What is 'finality' in consensus?

- A. The end of mining
- B. The guarantee that confirmed blocks cannot be reverted
- C. Maximum block size
- D. Transaction speed

Answer: B

Finality means once a block is confirmed, it cannot be reversed. PoW has probabilistic finality; BFT has absolute finality.

Question 8

What is Delegated Proof of Stake (DPoS)?

- A. A mining technique
- B. Token holders vote to elect a limited set of block producers
- C. A wallet feature
- D. A type of token

Question 8

What is Delegated Proof of Stake (DPoS)?

- A. A mining technique
- B. Token holders vote to elect a limited set of block producers
- C. A wallet feature
- D. A type of token

Answer: B

In DPoS, token holders vote for delegates who validate transactions, creating a representative democracy model.

Question 9

What is the 'nothing at stake' problem?

- A. Low mining rewards
- B. In PoS, validators can vote on multiple forks at no cost
- C. Empty wallets
- D. Network congestion

Question 9

What is the 'nothing at stake' problem?

- A. Low mining rewards
- B. In PoS, validators can vote on multiple forks at no cost
- C. Empty wallets
- D. Network congestion

Answer: B

Unlike PoW, early PoS systems allowed validators to support multiple competing chains without penalty. Modern protocols like Ethereum solve this via slashing conditions that penalize equivocation.

How does Ethereum's PoS select validators?

- A. First-come-first-served
- B. Randomly weighted by staked ETH
- C. By transaction count
- D. By node age

Question 10

How does Ethereum's PoS select validators?

- A. First-come-first-served
- B. Randomly weighted by staked ETH
- C. By transaction count
- D. By node age

Answer: B

Ethereum uses RANDAO to randomly select validators, weighted by their staked ETH amount.

Question 11

What is a 'validator' in PoS?

- A. A miner
- B. A participant who stakes tokens to propose and attest to blocks
- C. An exchange
- D. A wallet provider

What is a 'validator' in PoS?

- A. A miner
- B. A participant who stakes tokens to propose and attest to blocks
- C. An exchange
- D. A wallet provider

Answer: B

Validators lock up stake as collateral and are responsible for proposing and validating blocks.

Question 12

What is the minimum stake to become an Ethereum validator?

- A. 1 ETH
- B. 32 ETH
- C. 100 ETH
- D. 10 ETH

Question 12

What is the minimum stake to become an Ethereum validator?

- A. 1 ETH
- B. 32 ETH
- C. 100 ETH
- D. 10 ETH

Answer: B

Ethereum requires 32 ETH to run a validator node, ensuring meaningful economic commitment.

What is Practical Byzantine Fault Tolerance (PBFT)?

- A. A mining algorithm
- B. A consensus algorithm tolerating up to $1/3$ faulty nodes
- C. A wallet security feature
- D. A transaction type

What is Practical Byzantine Fault Tolerance (PBFT)?

- A. A mining algorithm
- B. A consensus algorithm tolerating up to $1/3$ faulty nodes
- C. A wallet security feature
- D. A transaction type

Answer: B

PBFT achieves consensus as long as fewer than $1/3$ of participants are Byzantine (faulty/malicious).

What advantage does PoS have over PoW?

- A. Faster block times
- B. Much lower energy consumption
- C. Higher decentralization
- D. Simpler implementation

What advantage does PoS have over PoW?

- A. Faster block times
- B. Much lower energy consumption
- C. Higher decentralization
- D. Simpler implementation

Answer: B

PoS eliminates competitive mining, reducing energy consumption significantly. Ethereum reported ~99.95% energy reduction post-Merge, though actual savings vary by implementation.

What is a 'long-range attack' in PoS?

- A. Attacking from far away
- B. Rewriting history using old private keys
- C. High-frequency trading attack
- D. DDoS attack

What is a 'long-range attack' in PoS?

- A. Attacking from far away
- B. Rewriting history using old private keys
- C. High-frequency trading attack
- D. DDoS attack

Answer: B

In long-range attacks, adversaries with old keys try to create an alternative chain from far in the past.

Question 16

What is 'economic finality'?

- A. Financial completion
- B. Reverting blocks would cost more than potential gain
- C. Transaction fees
- D. Market cap limit

Question 16

What is 'economic finality'?

- A. Financial completion
- B. Reverting blocks would cost more than potential gain
- C. Transaction fees
- D. Market cap limit

Answer: B

Economic finality means the cost to reverse transactions exceeds any possible profit from doing so.

What is the CAP theorem?

- A. A mining optimization
- B. Distributed systems can only guarantee 2 of 3: Consistency, Availability, Partition tolerance
- C. A token limit
- D. A fee structure

Question 17

What is the CAP theorem?

- A. A mining optimization
- B. Distributed systems can only guarantee 2 of 3: Consistency, Availability, Partition tolerance
- C. A token limit
- D. A fee structure

Answer: B

CAP theorem states distributed systems must trade off between consistency, availability, and partition tolerance.

What is Proof of Authority (PoA)?

- A. Government-backed consensus
- B. Consensus based on approved validators with known identities
- C. Mining with authority
- D. A wallet type

What is Proof of Authority (PoA)?

- A. Government-backed consensus
- B. Consensus based on approved validators with known identities
- C. Mining with authority
- D. A wallet type

Answer: B

PoA uses pre-approved validators with known identities, trading decentralization for speed and efficiency.

What is 'liveness' in consensus?

- A. Network uptime
- B. The guarantee that the system continues to make progress
- C. Transaction speed
- D. Node count

What is 'liveness' in consensus?

- A. Network uptime
- B. The guarantee that the system continues to make progress
- C. Transaction speed
- D. Node count

Answer: B

Liveness ensures the system keeps producing new blocks and processing transactions, not getting stuck.

What is the main trade-off in the blockchain trilemma?

- A. Speed vs cost vs privacy
- B. Decentralization vs security vs scalability
- C. Mining vs staking vs validation
- D. Tokens vs coins vs NFTs

What is the main trade-off in the blockchain trilemma?

- A. Speed vs cost vs privacy
- B. Decentralization vs security vs scalability
- C. Mining vs staking vs validation
- D. Tokens vs coins vs NFTs

Answer: B

The blockchain trilemma suggests it's difficult to achieve all three: decentralization, security, and scalability simultaneously.

Question 21

A startup wants to launch a supply chain tracking blockchain. They need fast finality (confirmed in ≤ 5 seconds), low energy consumption, and can rely on pre-vetted partners. Which consensus mechanism best fits these requirements?

- A. Proof of Work (PoW)
- B. Proof of Authority (PoA)
- C. Delegated Proof of Stake (DPoS)
- D. Practical Byzantine Fault Tolerance (PBFT)

Question 21

A startup wants to launch a supply chain tracking blockchain. They need fast finality (confirmed in ≤ 5 seconds), low energy consumption, and can rely on pre-vetted partners. Which consensus mechanism best fits these requirements?

- A. Proof of Work (PoW)
- B. Proof of Authority (PoA)
- C. Delegated Proof of Stake (DPoS)
- D. Practical Byzantine Fault Tolerance (PBFT)

Answer: B

PoA is ideal for permissioned environments with known, trusted validators. It offers absolute finality within seconds, minimal energy use, and high throughput. PBFT could also work but requires more complex coordination. PoW lacks fast finality, and DPoS introduces unnecessary governance overhead for a pre-vetted network.

Question 22

You run an Ethereum validator with 32 ETH staked. ETH price is \$2,000. Your annual staking reward is 4% APR. If you are slashed for downtime with a 1 ETH penalty, how many days of rewards would it take to recover this loss?

- A. Approximately 285 days
- B. Approximately 180 days
- C. Approximately 365 days
- D. Approximately 90 days

Question 22

You run an Ethereum validator with 32 ETH staked. ETH price is \$2,000. Your annual staking reward is 4% APR. If you are slashed for downtime with a 1 ETH penalty, how many days of rewards would it take to recover this loss?

- A. Approximately 285 days
- B. Approximately 180 days
- C. Approximately 365 days
- D. Approximately 90 days

Answer: A

$32 \text{ ETH} \times 4\% \text{ APR} = 1.28 \text{ ETH}$ annual rewards. Daily rewards = $1.28 \text{ ETH} / 365 = 0.0035 \text{ ETH/day}$. To recover 1 ETH loss: $1 \text{ ETH} / 0.0035 \text{ ETH/day} = 285 \text{ days}$. This illustrates the significant economic penalty of slashing and importance of validator reliability.

Question 23

A new PoW blockchain has total network hashrate of 100 PH/s. An attacker wants to execute a 51% attack. Mining hardware costs \$50/TH/s and consumes \$0.05/TH/s/day in electricity. What is the MINIMUM upfront cost to acquire attack capability (ignoring ongoing electricity)?

- A. \$2.5 million
- B. \$5 million
- C. \$2.55 million
- D. \$10 million

Question 23

A new PoW blockchain has total network hashrate of 100 PH/s. An attacker wants to execute a 51% attack. Mining hardware costs \$50/TH/s and consumes \$0.05/TH/s/day in electricity. What is the MINIMUM upfront cost to acquire attack capability (ignoring ongoing electricity)?

- A. \$2.5 million
- B. \$5 million
- C. \$2.55 million
- D. \$10 million

Answer: C

To control $\geq 50\%$ hashrate, attacker needs ≥ 50 PH/s = 51,000 TH/s (rounding up). Hardware cost = 51,000 TH/s \times \$50/TH/s = \$2,550,000. This doesn't include electricity (\$2,550/day) or the fact that purchasing this much hardware would raise difficulty and alert the network. Real attacks often rent hashrate or use botnets.

Question 24

A DPoS network has 21 elected validators. An adversary controls 7 validators through various accounts. The protocol requires 2/3 supermajority (14 votes) to finalize blocks. Can the adversary halt the network by refusing to participate?

- A. Yes, because $7/21 = 33\%$ exceeds the $1/3$ threshold needed to prevent consensus
- B. No, because 14 honest validators can still reach $2/3$ majority without the adversary
- C. Yes, but only if the adversary also controls network routing
- D. No, the protocol will automatically replace non-participating validators

Question 24

A DPoS network has 21 elected validators. An adversary controls 7 validators through various accounts. The protocol requires 2/3 supermajority (14 votes) to finalize blocks. Can the adversary halt the network by refusing to participate?

- A. Yes, because $7/21 = 33\%$ exceeds the $1/3$ threshold needed to prevent consensus
- B. No, because 14 honest validators can still reach $2/3$ majority without the adversary
- C. Yes, but only if the adversary also controls network routing
- D. No, the protocol will automatically replace non-participating validators

Answer: A

With 7 malicious validators refusing to participate, only 14 validators remain active. While $14/14 = 100\%$ among active validators, the protocol requires $14/21 = 67\%$ of ALL validators. The adversary with 33% can prevent liveness by denying the $2/3$ supermajority. This is a classic BFT safety vs liveness tradeoff.

Question 25

You're designing a consensus mechanism for a decentralized scientific computing network where nodes contribute CPU cycles. Which property should you prioritize to prevent Sybil attacks where one entity creates many fake identities?

- A. Proof of Work with high computational difficulty
- B. Proof of Stake requiring locked tokens
- C. Delegated Proof of Stake with reputation voting
- D. Proof of Authority with academic institution verification

Question 25

You're designing a consensus mechanism for a decentralized scientific computing network where nodes contribute CPU cycles. Which property should you prioritize to prevent Sybil attacks where one entity creates many fake identities?

- A. Proof of Work with high computational difficulty
- B. Proof of Stake requiring locked tokens
- C. Delegated Proof of Stake with reputation voting
- D. Proof of Authority with academic institution verification

Answer: B

PoS with meaningful stake requirements creates economic cost to Sybil attacks: each fake identity needs real capital locked. PoW doesn't prevent Sybils (attackers with more hardware create more identities). DPoS still allows Sybils in voting. PoA works but contradicts 'decentralized' in the question. The stake requirement makes each identity costly while allowing permissionless participation.

Question 26 (True/False)

Proof of Work requires miners to expend computational resources to validate blocks.

- A. True
- B. False

Question 26 (True/False)

Proof of Work requires miners to expend computational resources to validate blocks.

- A. True
- B. False

Answer: True

PoW consensus requires miners to solve computationally difficult cryptographic puzzles, expending energy and computational resources to secure the network.

Question 27 (True/False)

Proof of Stake consumes more energy than Proof of Work.

- A. True
- B. False

Question 27 (True/False)

Proof of Stake consumes more energy than Proof of Work.

- A. True
- B. False

Answer: False

PoS consumes significantly less energy than PoW because it doesn't require competitive mining. Ethereum's switch to PoS reduced energy consumption by approximately 99.95%.

Question 28 (True/False)

A 51% attack occurs when someone controls the majority of network hashpower.

- A. True
- B. False

Question 28 (True/False)

A 51% attack occurs when someone controls the majority of network hashpower.

- A. True
- B. False

Answer: True

A 51% attack happens when an entity controls more than 50% of mining/ hashing power, enabling them to manipulate the blockchain and potentially double-spend.

Question 29 (True/False)

Slashing in Proof of Stake penalizes validators who act maliciously or negligently.

- A. True
- B. False

Question 29 (True/False)

Slashing in Proof of Stake penalizes validators who act maliciously or negligently.

- A. True
- B. False

Answer: True

Slashing is a penalty mechanism in PoS that destroys a portion of a validator's staked tokens if they violate protocol rules or act dishonestly.

Question 30 (True/False)

Byzantine Fault Tolerance allows systems to function correctly even with some malicious nodes.

- A. True
- B. False

Question 30 (True/False)

Byzantine Fault Tolerance allows systems to function correctly even with some malicious nodes.

- A. True
- B. False

Answer: True

BFT systems can maintain correct operation and reach consensus even when some nodes are faulty, malicious, or behaving unpredictably.

Question 31 (True/False)

Proof of Work provides instant transaction finality.

- A. True
- B. False

Question 31 (True/False)

Proof of Work provides instant transaction finality.

- A. True
- B. False

Answer: False

PoW provides probabilistic finality that increases with confirmations. Transactions become more secure with each additional block, but theoretically could be reversed.

Question 32 (True/False)

The blockchain trilemma states it's difficult to achieve decentralization, security, and scalability simultaneously.

- A. True
- B. False

Question 32 (True/False)

The blockchain trilemma states it's difficult to achieve decentralization, security, and scalability simultaneously.

- A. True
- B. False

Answer: True

The blockchain trilemma suggests that blockchain systems must make trade-offs between these three properties, finding it challenging to optimize all three at once.

Question 33 (True/False)

Delegated Proof of Stake allows token holders to elect validators through voting.

- A. True
- B. False

Question 33 (True/False)

Delegated Proof of Stake allows token holders to elect validators through voting.

- A. True
- B. False

Answer: True

DPoS is a democratic consensus model where token holders vote to elect a limited set of delegates who validate transactions and produce blocks.

Question 34 (Fill in the Blank)

Bitcoin uses Proof of ____. *Hint: It requires computational effort...*

Question 34 (Fill in the Blank)

Bitcoin uses Proof of ____. *Hint: It requires computational effort...* **Answer: Work**

Bitcoin uses Proof of Work, requiring miners to expend computational resources to validate blocks.

Question 35 (Fill in the Blank)

A ___ attack requires controlling 51% of hash power. *Hint: More than half...*

Question 35 (Fill in the Blank)

A ___ attack requires controlling 51% of hash power. Hint: More than half... Answer: 51%

A 51% attack occurs when an entity controls majority hashpower, enabling chain reorganization and double-spends.

Question 36 (Fill in the Blank)

Ethereum switched from PoW to Proof of ____. *Hint: Validators lock tokens...*

Question 36 (Fill in the Blank)

Ethereum switched from PoW to Proof of ____. *Hint: Validators lock tokens...* **Answer: Stake**

Ethereum transitioned from Proof of Work to Proof of Stake in September 2022 (The Merge), reducing energy consumption by ~99.95%.