Lesson 3.2 Quiz: Consensus Mechanisms and Blockchain Architecture

Module 3: The Trust Problem

Prof. Dr. Joerg Osterrieder

Digital Finance — BSc Course (v2026.05)

Question 1

A junior developer asks: "Why can't blockchain nodes simply vote on which transactions to include, with the majority winning?" Which answer **best** explains the fundamental problem with naive majority voting in an open network?

- (A) Voting is too slow because nodes are geographically distributed
- (B) An attacker can create millions of fake identities (nodes) to win any vote — this is the Sybil attack
- (C) Voting requires all nodes to be online simultaneously, which is impractical
- (D) Majority voting does not work if the number of nodes is even

Question 1

A junior developer asks: "Why can't blockchain nodes simply vote on which transactions to include, with the majority winning?" Which answer **best** explains the fundamental problem with naive majority voting in an open network?

- (A) Voting is too slow because nodes are geographically distributed
- (B) An attacker can create millions of fake identities (nodes) to win any vote — this is the Sybil attack
- (C) Voting requires all nodes to be online simultaneously, which is impractical
- (D) Majority voting does not work if the number of nodes is even

[Answer hidden – compile with \solutionstrue to reveal]

Question 2

The Byzantine Generals Problem requires that $n > 3f$ for agreement, where f is the number of faulty nodes. A blockchain network has 12 validator nodes. What is the **maximum** number of Byzantine (malicious) nodes the network can tolerate while still reaching consensus?

A. 4
B. 2
C. 6
D. 3

Question 2

The Byzantine Generals Problem requires that $n > 3f$ for agreement, where f is the number of faulty nodes. A blockchain network has 12 validator nodes. What is the **maximum** number of Byzantine (malicious) nodes the network can tolerate while still reaching consensus?

- A 4
- B 2
- C 6
- D 3

[Answer hidden – compile with \solutionstrue to reveal]

Question 3

A blockchain uses Proof of Work. A financial analyst claims: "PoW is secure because solving the puzzle requires enormous computation, but verifying the solution is trivial." Which cryptographic property makes this asymmetry possible?

- A The fixed output size of hash functions
- B The one-way nature (pre-image resistance) of hash functions
- C The deterministic output of hash functions
- D The collision resistance of hash functions

Question 3

A blockchain uses Proof of Work. A financial analyst claims: "PoW is secure because solving the puzzle requires enormous computation, but verifying the solution is trivial." Which cryptographic property makes this asymmetry possible?

- A The fixed output size of hash functions
- B The one-way nature (pre-image resistance) of hash functions
- C The deterministic output of hash functions
- D The collision resistance of hash functions

[Answer hidden – compile with \solutionstrue to reveal]

Question 4

An investor reads that Ethereum "achieved finality after The Merge" and interprets this as "transactions can never be reversed on Ethereum." Which clarification is **most accurate**?

- (A) Finality simply means that Ethereum no longer uses Proof of Work
- (B) Finality on Ethereum is deterministic after two epochs (≈12.8 minutes): reversal would require $\frac{1}{3}$ of all staked ETH to be slashed
- (C) Finality means that Ethereum transactions are confirmed in under one second
- (D) Finality guarantees that no hard fork can ever change Ethereum's history

Question 4

An investor reads that Ethereum "achieved finality after The Merge" and interprets this as "transactions can never be reversed on Ethereum." Which clarification is **most accurate**?

- **A** Finality simply means that Ethereum no longer uses Proof of Work
- **B** Finality on Ethereum is deterministic after two epochs ($\approx$12.8 minutes): reversal would require $\frac{1}{3}$ of all staked ETH to be slashed
- **C** Finality means that Ethereum transactions are confirmed in under one second
- **D** Finality guarantees that no hard fork can ever change Ethereum's history

[Answer hidden – compile with \solutionstrue to reveal]

Question 5

A Bitcoin miner constructs a candidate block with 2,000 transactions. The current difficulty target requires the block hash to start with 19 leading zeros (in binary). The miner starts with nonce $= 0$ and increments by 1. After 500 million attempts, no valid hash has been found. What should the miner do?

- **A** Increase the difficulty target to make the puzzle easier
- **B** Switch to a different hash algorithm that is more likely to produce leading zeros
- **C** Continue incrementing the nonce — finding a valid hash is statistically expected to take billions of attempts
- **D** Restart from nonce $= 0$ with the same block, since the random process resets

Question 5

A Bitcoin miner constructs a candidate block with 2,000 transactions. The current difficulty target requires the block hash to start with 19 leading zeros (in binary). The miner starts with nonce $= 0$ and increments by 1. After 500 million attempts, no valid hash has been found. What should the miner do?

- **A** Increase the difficulty target to make the puzzle easier
- **B** Switch to a different hash algorithm that is more likely to produce leading zeros
- **C** Continue incrementing the nonce — finding a valid hash is statistically expected to take billions of attempts
- **D** Restart from nonce $= 0$ with the same block, since the random process resets

[Answer hidden – compile with \solutionstrue to reveal]

Question 6

Bitcoin's difficulty adjusts every 2,016 blocks to target a 10-minute average block time. Over the last 2,016 blocks, the average block time was 8 minutes (total: 11.2 days instead of 14 days). How will the difficulty change?

- A Difficulty increases by 20% because $\frac{10-8}{10} = 20\%$
- B Difficulty remains unchanged until the next halving event
- C Difficulty decreases by 20% to slow block production
- D Difficulty increases by 25% because blocks were produced 25% faster than target

Question 6

Bitcoin's difficulty adjusts every 2,016 blocks to target a 10-minute average block time. Over the last 2,016 blocks, the average block time was 8 minutes (total: 11.2 days instead of 14 days). How will the difficulty change?

- (A) Difficulty increases by 20% because $\frac{10-8}{10} = 20\%$
- (B) Difficulty remains unchanged until the next halving event
- (C) Difficulty decreases by 20% to slow block production
- (D) Difficulty increases by 25% because blocks were produced 25% faster than target

[Answer hidden – compile with \solutionstrue to reveal]

Question 7

An Ethereum validator stakes 32 ETH (worth $64,000 at current prices). The validator's software has a bug that causes it to sign two conflicting blocks at the same slot height. What is the **immediate** consequence under Ethereum's PoS protocol?

- The validator receives a warning and must restart their node
- The validator loses their next block proposal opportunity but keeps their stake
- The validator is slashed: a minimum of $\frac{1}{32}$ of their stake (1 ETH, $\approx$\$2,000) is burned and they are queued for ejection
- The network ignores both blocks and selects a different validator

Question 7

An Ethereum validator stakes 32 ETH (worth $64,000 at current prices). The validator's software has a bug that causes it to sign two conflicting blocks at the same slot height. What is the **immediate** consequence under Ethereum's PoS protocol?

- The validator receives a warning and must restart their node
- The validator loses their next block proposal opportunity but keeps their stake
- The validator is slashed: a minimum of $\frac{1}{32}$ of their stake (1 ETH, $\approx$\$2,000) is burned and they are queued for ejection
- The network ignores both blocks and selects a different validator

[Answer hidden – compile with \solutionstrue to reveal]

Question 8

Two Bitcoin miners, Miner A and Miner B, simultaneously find valid blocks at height 700,001. Miner A's block is received by 60% of the network first; Miner B's block reaches the other 40%. What determines which block becomes part of the permanent chain?

- **A** Whichever chain gets the next block (700,002) built on top of it first becomes the longest chain, and the other is orphaned
- **B** The network holds a vote among all nodes to decide
- **C** The block that was timestamped first wins
- **D** The block with the lower hash value (smaller number) wins

Question 8

Two Bitcoin miners, Miner A and Miner B, simultaneously find valid blocks at height 700,001. Miner A's block is received by 60% of the network first; Miner B's block reaches the other 40%. What determines which block becomes part of the permanent chain?

- **A** Whichever chain gets the next block (700,002) built on top of it first becomes the longest chain, and the other is orphaned
- **B** The network holds a vote among all nodes to decide
- **C** The block that was timestamped first wins
- **D** The block with the lower hash value (smaller number) wins

[Answer hidden – compile with \solutionstrue to reveal]

Question 9

A consortium of banks wants to build a private blockchain for interbank settlements. They need instant finality (no probabilistic waiting) and have exactly 10 pre-approved validator nodes. Which consensus mechanism is **most appropriate**?

- **A** PBFT (Practical Byzantine Fault Tolerance) — deterministic finality with a known validator set
- **B** Proof of Stake — energy efficient and modern
- **C** Proof of Work — proven security from Bitcoin
- **D** No consensus needed — with only 10 trusted banks, a shared database suffices

Question 9

A consortium of banks wants to build a private blockchain for interbank settlements. They need instant finality (no probabilistic waiting) and have exactly 10 pre-approved validator nodes. Which consensus mechanism is **most appropriate**?

- **A** PBFT (Practical Byzantine Fault Tolerance) — deterministic finality with a known validator set
- **B** Proof of Stake — energy efficient and modern
- **C** Proof of Work — proven security from Bitcoin
- **D** No consensus needed — with only 10 trusted banks, a shared database suffices

[Answer hidden – compile with \solutionstrue to reveal]

Question 10

After Bitcoin's 2024 halving, the block reward dropped from 6.25 BTC to 3.125 BTC. A mining company's revenue falls accordingly. Assuming transaction fees remain constant, how must the company adapt to remain profitable?

- A. Increase the difficulty target to mine blocks faster
- B. Switch to mining Ethereum instead (higher rewards)
- C. Invest in more energy-efficient mining hardware and/or relocate to regions with cheaper electricity
- D. Wait for the next halving, which will restore the previous reward

Question 10

After Bitcoin's 2024 halving, the block reward dropped from 6.25 BTC to 3.125 BTC. A mining company's revenue falls accordingly. Assuming transaction fees remain constant, how must the company adapt to remain profitable?

- Increase the difficulty target to mine blocks faster
- Switch to mining Ethereum instead (higher rewards)
- Invest in more energy-efficient mining hardware and/or relocate to regions with cheaper electricity
- Wait for the next halving, which will restore the previous reward

[Answer hidden – compile with \solutionstrue to reveal]

Question 11

A blockchain startup claims their new "Proof of Reputation" mechanism selects block producers based on their social media following. An advisor warns this is vulnerable to Sybil attacks. Why?

A. Social media APIs are too slow for real-time consensus

B. Social media followers can be purchased cheaply, making the "scarce resource" easy to fake

C. Proof of Reputation has already been patented by another company

D. Social media platforms are centralized, creating a single point of failure

Question 11

A blockchain startup claims their new "Proof of Reputation" mechanism selects block producers based on their social media following. An advisor warns this is vulnerable to Sybil attacks. Why?

- (A) Social media APIs are too slow for real-time consensus
- (B) Social media followers can be purchased cheaply, making the "scarce resource" easy to fake
- (C) Proof of Reputation has already been patented by another company
- (D) Social media platforms are centralized, creating a single point of failure

[Answer hidden – compile with \solutionstrue to reveal]

Question 12

A payment company considers using blockchain and compares finality times. Their requirement is that transactions must be irrevocable within 10 seconds. Which consensus mechanism(s) can meet this requirement?

- A Bitcoin PoW (6 confirmations)
- B All of the above
- C Ethereum PoS (2 epochs)
- D Tendermint BFT (∼6 second finality)

Question 12

A payment company considers using blockchain and compares finality times. Their requirement is that transactions must be irrevocable within 10 seconds. Which consensus mechanism(s) can meet this requirement?

- Bitcoin PoW (6 confirmations)
- All of the above
- Ethereum PoS (2 epochs)
- Tendermint BFT (∼6 second finality)

[Answer hidden – compile with \solutionstrue to reveal]

Question 13

Consider the blockchain trilemma. Solana achieves high throughput (65,000 TPS) by requiring validators to run on high-specification hardware (128 GB RAM, high-bandwidth connections). Which trilemma trade-off does this represent?

- A Sacrificing security for scalability
- B Sacrificing decentralization for scalability — high hardware requirements reduce the number of entities that can run validators
- C No trade-off — Solana has solved the trilemma
- D Sacrificing scalability for decentralization

Question 13

Consider the blockchain trilemma. Solana achieves high throughput (65,000 TPS) by requiring validators to run on high-specification hardware (128 GB RAM, high-bandwidth connections). Which trilemma trade-off does this represent?

- A Sacrificing security for scalability
- B Sacrificing decentralization for scalability — high hardware requirements reduce the number of entities that can run validators
- C No trade-off — Solana has solved the trilemma
- D Sacrificing scalability for decentralization

[Answer hidden – compile with \solutionstrue to reveal]

Question 14

In Proof of Stake, wealthy validators have a higher probability of being selected to propose blocks and earn rewards. A critic argues this creates a "rich get richer" dynamic. Compare this to Proof of Work. Is the same dynamic present in PoW?

- (A) Yes — but only because electricity costs are higher for small miners
- (B) No — in PoW, anyone with a laptop can mine profitably, so wealth does not concentrate
- (C) No — PoW is purely random, so hash power does not correlate with wealth
- (D) Yes — in PoW, wealthier miners buy more hardware, earning more blocks and more revenue, creating the same concentration dynamic

Question 14

In Proof of Stake, wealthy validators have a higher probability of being selected to propose blocks and earn rewards. A critic argues this creates a "rich get richer" dynamic. Compare this to Proof of Work. Is the same dynamic present in PoW?

- (A) Yes — but only because electricity costs are higher for small miners
- (B) No — in PoW, anyone with a laptop can mine profitably, so wealth does not concentrate
- (C) No — PoW is purely random, so hash power does not correlate with wealth
- (D) Yes — in PoW, wealthier miners buy more hardware, earning more blocks and more revenue, creating the same concentration dynamic

[Answer hidden – compile with \solutionstrue to reveal]

Question 15

An attacker controls 40% of a PoW network's hash power. They attempt to execute a double-spend by mining a private chain. Analyze the probability of success. Is this attack likely to succeed?

- **A** No — with 40% hash power, the attacker's chain grows slower on average and falls further behind with each block; success probability decreases exponentially with depth
- **B** Yes — the attacker only needs to get lucky once
- **C** Yes — 40% is close enough to 50% that the attacker will occasionally outpace the honest chain
- **D** No — the network automatically detects and blocks miners with more than 30% hash power

Question 15

An attacker controls 40% of a PoW network's hash power. They attempt to execute a double-spend by mining a private chain. Analyze the probability of success. Is this attack likely to succeed?

- **A** No — with 40% hash power, the attacker's chain grows slower on average and falls further behind with each block; success probability decreases exponentially with depth
- **B** Yes — the attacker only needs to get lucky once
- **C** Yes — 40% is close enough to 50% that the attacker will occasionally outpace the honest chain
- **D** No — the network automatically detects and blocks miners with more than 30% hash power

[Answer hidden – compile with \solutionstrue to reveal]

Question 16

Ethereum's Proof of Stake uses "inactivity leaks" that gradually drain the stake of validators who go offline during a finality crisis. Why is this mechanism necessary?

- **A** To ensure the network can recover finality even if a large fraction of validators go offline — by reducing their stake, the remaining online validators eventually constitute the required $\frac{2}{3}$ supermajority
- **B** To reduce the total supply of ETH and increase its price
- **C** To incentivize validators to upgrade their hardware regularly
- **D** To punish validators who use too much bandwidth

Question 16

Ethereum's Proof of Stake uses "inactivity leaks" that gradually drain the stake of validators who go offline during a finality crisis. Why is this mechanism necessary?

- **A** To ensure the network can recover finality even if a large fraction of validators go offline — by reducing their stake, the remaining online validators eventually constitute the required $\frac{2}{3}$ supermajority
- **B** To reduce the total supply of ETH and increase its price
- **C** To incentivize validators to upgrade their hardware regularly
- **D** To punish validators who use too much bandwidth

[Answer hidden – compile with \solutionstrue to reveal]

Question 17

A financial regulator examines two blockchain networks: Network A uses PoW with 10,000 anonymous miners worldwide; Network B uses PBFT with 20 identified bank validators. Which network is **more censorship-resistant**, and why?

- Neither — both networks process all valid transactions equally
- Network B — fewer validators means faster processing, leaving less time for censorship
- Network B — the banks are regulated and audited, so they cannot censor
- Network A — with 10,000 anonymous miners across jurisdictions, no single authority can compel all miners to exclude specific transactions

Question 17

A financial regulator examines two blockchain networks: Network A uses PoW with 10,000 anonymous miners worldwide; Network B uses PBFT with 20 identified bank validators. Which network is **more censorship-resistant**, and why?

- (A) Neither — both networks process all valid transactions equally
- (B) Network B — fewer validators means faster processing, leaving less time for censorship
- (C) Network B — the banks are regulated and audited, so they cannot censor
- (D) Network A — with 10,000 anonymous miners across jurisdictions, no single authority can compel all miners to exclude specific transactions

[Answer hidden – compile with \solutionstrue to reveal]

Question 18

Bitcoin processes approximately 7 transactions per second (TPS), while Visa handles approximately 65,000 TPS at peak. A blockchain advocate claims "Layer 2 solutions solve this." Which is the **most accurate** description of how Layer 2 addresses the throughput gap?

- Layer 2 replaces Bitcoin's consensus mechanism with a faster one
- Layer 2 increases Bitcoin's block size to fit more transactions
- Layer 2 processes transactions off the main chain and periodically settles aggregated results on Layer 1, inheriting its security while avoiding its throughput limits
- Layer 2 simply compresses transaction data so more fit in each block

Question 18

Bitcoin processes approximately 7 transactions per second (TPS), while Visa handles approximately 65,000 TPS at peak. A blockchain advocate claims "Layer 2 solutions solve this." Which is the **most accurate** description of how Layer 2 addresses the throughput gap?

- Layer 2 replaces Bitcoin's consensus mechanism with a faster one
- Layer 2 increases Bitcoin's block size to fit more transactions
- Layer 2 processes transactions off the main chain and periodically settles aggregated results on Layer 1, inheriting its security while avoiding its throughput limits
- Layer 2 simply compresses transaction data so more fit in each block

[Answer hidden – compile with \solutionstrue to reveal]

Question 19

A government proposes banning Proof of Work mining within its borders due to environmental concerns (as the EU considered in 2022). Evaluate the **most likely** impact on the Bitcoin network.

- (A) The ban forces Bitcoin to switch to Proof of Stake
- (B) Bitcoin's price permanently crashes because the network is perceived as insecure
- (C) Mining moves to other jurisdictions; after the next difficulty adjustment, the network continues operating normally at a slightly lower hash rate
- (D) Bitcoin stops working because it loses too many miners

Question 19

A government proposes banning Proof of Work mining within its borders due to environmental concerns (as the EU considered in 2022). Evaluate the **most likely** impact on the Bitcoin network.

- **A** The ban forces Bitcoin to switch to Proof of Stake
- **B** Bitcoin's price permanently crashes because the network is perceived as insecure
- **C** Mining moves to other jurisdictions; after the next difficulty adjustment, the network continues operating normally at a slightly lower hash rate
- **D** Bitcoin stops working because it loses too many miners

[Answer hidden – compile with \solutionstrue to reveal]

Question 20

A startup asks you to recommend a consensus mechanism for a decentralized stock exchange processing 1,000 trades per second with full public auditability. Trades must be irrevocable within 3 seconds. The exchange should be permissionless (anyone can run a node). Evaluate the options and identify the **best fit**.

- (A) Avalanche consensus — sub-second finality, permissionless, high throughput with probabilistic sampling
- (B) Bitcoin-style PoW — proven security track record
- (C) Ethereum PoS — large validator set and smart contract support
- (D) PBFT — deterministic finality in under 3 seconds

Question 20

A startup asks you to recommend a consensus mechanism for a decentralized stock exchange processing 1,000 trades per second with full public auditability. Trades must be irrevocable within 3 seconds. The exchange should be permissionless (anyone can run a node). Evaluate the options and identify the **best fit**.

- (A) Avalanche consensus — sub-second finality, permissionless, high throughput with probabilistic sampling
- (B) Bitcoin-style PoW — proven security track record
- (C) Ethereum PoS — large validator set and smart contract support
- (D) PBFT — deterministic finality in under 3 seconds

[Answer hidden – compile with \solutionstrue to reveal]