Lesson 3.2 Quiz: Consensus Mechanisms and Blockchain Architecture

Module 3: The Trust Problem

Prof. Dr. Joerg Osterrieder

Digital Finance — BSc Course

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: (B) In an open, permissionless network, there is no identity verification. An attacker can spin up unlimited fake nodes to control the vote. Consensus mechanisms like PoW and PoS prevent Sybil attacks by tying voting power to a scarce resource (electricity or capital).

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. 2
B. 3
C. 4
D. 6

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) 2
- (B) 3
- (C) 4
- (D) 6

Answer: (B) The requirement is $n > 3f$, so $12 > 3f$, meaning $f < 4$. The maximum integer value is $f = 3$. With 3 Byzantine nodes out of 12, the network has 9 honest nodes, satisfying $12 > 3 \times 3 = 9$.

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

Answer: (B) Pre-image resistance means you cannot reverse a hash to find the input. Miners must brute-force search for a nonce that produces a hash below the target. But once found, any node computes a single hash to verify it matches — exploiting the one-way asymmetry.

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

Answer: (A) Ethereum's PoS provides economic finality: once a block is finalized (after 2 epochs), reversing it would require at least $\frac{1}{3}$ of validators to submit conflicting attestations, triggering slashing of their staked ETH. This makes reversal economically catastrophic, not physically impossible.

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

Answer: (B) Mining is a brute-force probabilistic search. With 19 leading zeros required, the expected number of attempts is $2^{19} \approx 524{,}288$, but in practice Bitcoin's difficulty is much higher (80+ leading binary zeros), requiring $\sim 10^{20}$ attempts globally. The miner must keep trying.

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

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

Answer: (B) The adjustment formula is: $\text{new\_difficulty} = \text{old\_difficulty} \times \frac{\text{target\_time}}{\text{actual\_time}} = \text{old} \times \frac{14 \text{ days}}{11.2 \text{ days}} = \text{old} \times 1.25$. Difficulty increases by 25% to compensate for blocks arriving faster than the 10-minute target.

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 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 validator loses their next block proposal opportunity but keeps their stake
- 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?

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

Answer: (B) Double-voting (signing two blocks at the same height) is a slashable offense. The protocol automatically detects conflicting signatures, burns a portion of the validator's stake, and initiates forced exit. This economic punishment is what gives PoS its security guarantee.

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

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

Answer: (C) Under the longest chain rule, a temporary fork exists until one chain grows longer. The next miner to find block 700,002 will build on whichever version of 700,001 they received first. The extended chain becomes canonical; the shorter chain is orphaned.

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

Answer: (C) PBFT is designed for permissioned networks with a known set of participants. It provides deterministic finality (no waiting for confirmations), tolerates up to 3 Byzantine nodes out of 10, and does not waste energy on mining. A shared database (D) sacrifices auditability and fault tolerance.

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. Invest in more energy-efficient mining hardware and/or relocate to regions with cheaper electricity
- C. Switch to mining Ethereum instead (higher rewards)
- 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?

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

Answer: (B) Miners cannot change the difficulty target (it is set by the protocol). The halving permanently reduces the reward; it never reverts. Ethereum no longer has mining (post-Merge PoS). The only option is reducing costs: more efficient hardware (lower J/TH) and cheaper electricity.

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 platforms are centralized, creating a single point of failure

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

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

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

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

Answer: (B) A consensus mechanism's Sybil resistance depends on tying voting power to a genuinely scarce resource. PoW uses electricity (expensive); PoS uses capital (expensive). Social media followers can be bought cheaply by the thousands, allowing an attacker to accumulate disproportionate influence at low cost.

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 Ethereum PoS (2 epochs)
- C Tendermint BFT (∼6 second finality)
- D All of the above

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) Ethereum PoS (2 epochs)
- (C) Tendermint BFT (∼6 second finality)
- (D) All of the above

Answer: (C) Bitcoin requires ∼60 minutes for 6 confirmations. Ethereum PoS requires ∼12.8 minutes for finality. Only Tendermint (and similar BFT protocols like Avalanche) achieve sub-10-second deterministic finality, making them suitable for real-time payment applications.

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 Sacrificing scalability for decentralization
- D No trade-off — Solana has solved the trilemma

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) Sacrificing scalability for decentralization
- (D) No trade-off — Solana has solved the trilemma

Answer: (B) High hardware requirements create a barrier to entry: fewer individuals and organizations can afford to run validator nodes. This concentrates validation power among well-funded entities, reducing decentralization. Solana achieves scalability by accepting this centralization trade-off.

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. No — in PoW, anyone with a laptop can mine profitably, so wealth does not concentrate

B. Yes — in PoW, wealthier miners buy more hardware, earning more blocks and more revenue, creating the same concentration dynamic

C. No — PoW is purely random, so hash power does not correlate with wealth

D. Yes — but only because electricity costs are higher for small miners

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) No — in PoW, anyone with a laptop can mine profitably, so wealth does not concentrate

(B) Yes — in PoW, wealthier miners buy more hardware, earning more blocks and more revenue, creating the same concentration dynamic

(C) No — PoW is purely random, so hash power does not correlate with wealth

(D) Yes — but only because electricity costs are higher for small miners

Answer: (B) Both PoW and PoS exhibit economies of scale. In PoW, wealthier entities buy more ASICs and secure bulk electricity deals. In PoS, wealthier validators stake more and earn proportionally more rewards. The "rich get richer" concern applies to both mechanisms, though PoS at least avoids the environmental externality.

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. Yes — 40% is close enough to 50% that the attacker will occasionally outpace the honest chain

B. 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

C. Yes — the attacker only needs to get lucky once

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) Yes — 40% is close enough to 50% that the attacker will occasionally outpace the honest chain

(B) 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

(C) Yes — the attacker only needs to get lucky once

(D) No — the network automatically detects and blocks miners with more than 30% hash power

Answer: (B) With 40% hash power vs. 60% honest, the attacker's expected chain growth is $\frac{40}{60} \approx 0.67$ blocks per honest block. After k confirmations, the probability of catching up decreases exponentially: $P \approx (40/60)^k$. After 6 confirmations, $P \approx 0.67^6 \approx 9\%$. This is why merchants wait for confirmations.

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 punish validators who use too much bandwidth
- (B) To reduce the total supply of ETH and increase its price
- (C) 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
- (D) To incentivize validators to upgrade their hardware regularly

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 punish validators who use too much bandwidth
- (B) To reduce the total supply of ETH and increase its price
- (C) 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
- (D) To incentivize validators to upgrade their hardware regularly

Answer: (C) If more than $\frac{1}{3}$ of validators go offline, finality halts (the $\frac{2}{3}$ threshold cannot be met). Inactivity leaks gradually reduce offline validators' stakes until the online validators represent $\frac{2}{3}$ of the remaining total stake, restoring the network's ability to finalize blocks.

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. Network B — the banks are regulated and audited, so they cannot censor

B. Network A — with 10,000 anonymous miners across jurisdictions, no single authority can compel all miners to exclude specific transactions

C. Neither — both networks process all valid transactions equally

D. Network B — fewer validators means faster processing, leaving less time for censorship

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

Answer: (B) Censorship resistance comes from decentralization and anonymity. Network A's 10,000 anonymous miners span multiple jurisdictions; blocking a transaction requires convincing all of them. Network B's 20 identified banks can be ordered by a regulator or court to exclude specific transactions. This is the fundamental decentralization vs. permissioned trade-off.

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?

- (A) Layer 2 increases Bitcoin's block size to fit more transactions
- (B) Layer 2 replaces Bitcoin's consensus mechanism with a faster one
- (C) Layer 2 processes transactions off the main chain and periodically settles aggregated results on Layer 1, inheriting its security while avoiding its throughput limits
- (D) 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?

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

Answer: (C) Layer 2 solutions (Lightning Network, rollups) move transaction execution off-chain. Thousands of transactions occur on L2, and only a summary (or cryptographic proof) is posted to L1. This preserves L1's decentralization and security while dramatically increasing effective throughput.

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. Bitcoin stops working because it loses too many miners

B. Mining moves to other jurisdictions; after the next difficulty adjustment, the network continues operating normally at a slightly lower hash rate

C. The ban forces Bitcoin to switch to Proof of Stake

D. Bitcoin's price permanently crashes because the network is perceived as insecure

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. Bitcoin stops working because it loses too many miners

B. Mining moves to other jurisdictions; after the next difficulty adjustment, the network continues operating normally at a slightly lower hash rate

C. The ban forces Bitcoin to switch to Proof of Stake

D. Bitcoin's price permanently crashes because the network is perceived as insecure

Answer: (B) When China banned crypto mining in 2021, roughly 50% of global hash power went offline. The network experienced slower blocks temporarily, but difficulty adjusted downward within two weeks. Miners relocated to the US, Kazakhstan, and other countries. Bitcoin's protocol is jurisdiction-agnostic — it adapts automatically.

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

Answer: (C) PoW is eliminated by the 3-second finality requirement (Bitcoin: $\sim$60 min). Ethereum PoS is eliminated by both the 3-second requirement ($\sim$13 min finality) and 1,000 TPS ($\sim$30 TPS on L1). PBFT provides fast finality but is permissioned, violating the openness requirement. Avalanche achieves sub-second finality, thousands of TPS, and permissionless participation through its novel repeated sub-sampled voting mechanism.