Advanced Topics

Module Quiz – 20 Multiple-Choice Questions

Topics covered: L2 scaling · Rollup mechanics · Flash loans · MEV · Smart contract security · Bridge attacks · Audit tools

Select the best answer. Answers revealed after each question.

Bloom's levels: 4 Understand · 8 Apply · 6 Analyze · 2 Evaluate

Questions 1–5: Scalability & L2 Basics

Q1. [Understand] **The scalability trilemma states that a blockchain can fully optimize for at most how many of these three properties simultaneously: security, scalability, decentralization?**
A) One B) Two C) Three D) It depends on the consensus algorithm

Questions 1–5: Scalability & L2 Basics

Q1. [Understand] **The scalability trilemma states that a blockchain can fully optimize for at most how many of these three properties simultaneously: security, scalability, decentralization?**
A) One B) Two C) Three D) It depends on the consensus algorithm
Answer: B) A blockchain can optimize for at most two of the three properties; L2 solutions attempt all three by inheriting L1 security while executing off-chain.

Q2. [Understand] **What is the primary function of a sequencer in a Layer 2 rollup?**
A) Mine new blocks on L1 B) Validate zero-knowledge proofs C) Order and batch transactions before submitting them to L1 D) Store full transaction history

Questions 1–5: Scalability & L2 Basics

Q1. [Understand] **The scalability trilemma states that a blockchain can fully optimize for at most how many of these three properties simultaneously: security, scalability, decentralization?**
A) One B) Two C) Three D) It depends on the consensus algorithm
Answer: B) A blockchain can optimize for at most two of the three properties; L2 solutions attempt all three by inheriting L1 security while executing off-chain.

Q2. [Understand] **What is the primary function of a sequencer in a Layer 2 rollup?**
A) Mine new blocks on L1 B) Validate zero-knowledge proofs C) Order and batch transactions before submitting them to L1 D) Store full transaction history
Answer: C) The sequencer orders and batches transactions, then submits compressed data to L1.

Q3. [Apply] **Ethereum L1 processes approximately 15 TPS. An optimistic rollup claims 2,000 TPS. By approximately what factor does the rollup improve throughput?**
A) $\sim$13x B) $\sim$50x C) $\sim$133x D) $\sim$2,000x

Questions 1–5: Scalability & L2 Basics

Q1. [Understand] **The scalability trilemma states that a blockchain can fully optimize for at most how many of these three properties simultaneously: security, scalability, decentralization?**
A) One B) Two C) Three D) It depends on the consensus algorithm
Answer: B) A blockchain can optimize for at most two of the three properties; L2 solutions attempt all three by inheriting L1 security while executing off-chain.

Q2. [Understand] **What is the primary function of a sequencer in a Layer 2 rollup?**
A) Mine new blocks on L1 B) Validate zero-knowledge proofs C) Order and batch transactions before submitting them to L1 D) Store full transaction history
Answer: C) The sequencer orders and batches transactions, then submits compressed data to L1.

Q3. [Apply] **Ethereum L1 processes approximately 15 TPS. An optimistic rollup claims 2,000 TPS. By approximately what factor does the rollup improve throughput?**
A) $\sim$13x B) $\sim$50x C) $\sim$133x D) $\sim$2,000x
Answer: C) $\sim$133x ($2{,}000/15 \approx 133$), achieved by executing off-chain and posting only compressed calldata (or blobs post-Dencun) to L1.

Q4. [Apply] **A user submits a withdrawal from an optimistic rollup. The challenge period is 7 days. On which day at the earliest can the user access their funds on L1?**
A) Day 1 B) Day 3 C) Day 7 D) Day 8

Questions 1–5: Scalability & L2 Basics

Q1. [Understand] **The scalability trilemma states that a blockchain can fully optimize for at most how many of these three properties simultaneously: security, scalability, decentralization?**
A) One B) Two C) Three D) It depends on the consensus algorithm
Answer: B) A blockchain can optimize for at most two of the three properties; L2 solutions attempt all three by inheriting L1 security while executing off-chain.

Q2. [Understand] **What is the primary function of a sequencer in a Layer 2 rollup?**
A) Mine new blocks on L1 B) Validate zero-knowledge proofs C) Order and batch transactions before submitting them to L1 D) Store full transaction history
Answer: C) The sequencer orders and batches transactions, then submits compressed data to L1.

Q3. [Apply] **Ethereum L1 processes approximately 15 TPS. An optimistic rollup claims 2,000 TPS. By approximately what factor does the rollup improve throughput?**
A) $\sim$13x B) $\sim$50x C) $\sim$133x D) $\sim$2,000x
Answer: C) $\sim$133x ($2{,}000/15 \approx 133$), achieved by executing off-chain and posting only compressed calldata (or blobs post-Dencun) to L1.

Q4. [Apply] **A user submits a withdrawal from an optimistic rollup. The challenge period is 7 days. On which day at the earliest can the user access their funds on L1?**
A) Day 1 B) Day 3 C) Day 7 D) Day 8
Answer: D) Day 8 — the full 7-day challenge period must elapse before the withdrawal finalizes.

Q5. [Apply] **Before the Dencun upgrade, an Arbitrum swap cost approximately \$0.50. After Dencun (EIP-4844), it costs \$0.01. What is the percentage fee reduction?**
A) 50% B) 80% C) 95% D) 98%

Questions 1–5: Scalability & L2 Basics

Q1. [Understand] **The scalability trilemma states that a blockchain can fully optimize for at most how many of these three properties simultaneously: security, scalability, decentralization?**
A) One B) Two C) Three D) It depends on the consensus algorithm
Answer: B) A blockchain can optimize for at most two of the three properties; L2 solutions attempt all three by inheriting L1 security while executing off-chain.

Q2. [Understand] **What is the primary function of a sequencer in a Layer 2 rollup?**
A) Mine new blocks on L1 B) Validate zero-knowledge proofs C) Order and batch transactions before submitting them to L1 D) Store full transaction history
Answer: C) The sequencer orders and batches transactions, then submits compressed data to L1.

Q3. [Apply] **Ethereum L1 processes approximately 15 TPS. An optimistic rollup claims 2,000 TPS. By approximately what factor does the rollup improve throughput?**
A) $\sim$13x B) $\sim$50x C) $\sim$133x D) $\sim$2,000x
Answer: C) $\sim$133x ($2{,}000/15 \approx 133$), achieved by executing off-chain and posting only compressed calldata (or blobs post-Dencun) to L1.

Q4. [Apply] **A user submits a withdrawal from an optimistic rollup. The challenge period is 7 days. On which day at the earliest can the user access their funds on L1?**
A) Day 1 B) Day 3 C) Day 7 D) Day 8
Answer: D) Day 8 — the full 7-day challenge period must elapse before the withdrawal finalizes.

Q5. [Apply] **Before the Dencun upgrade, an Arbitrum swap cost approximately \$0.50. After Dencun (EIP-4844), it costs \$0.01. What is the percentage fee reduction?**
A) 50% B) 80% C) 95% D) 98%
Answer: D) 98% — EIP-4844 blob transactions dramatically cut L2 data posting costs.

Questions 6–10: Rollup Mechanics, Fees & Flash Loans

Q6. [Understand] **What type of cryptographic proof do ZK-rollups use to verify transaction validity directly on L1?**
A) Hash commitments B) Merkle proofs C) Zero-knowledge validity proofs D) Fraud proofs with challenge windows

Questions 6–10: Rollup Mechanics, Fees & Flash Loans

Q6. [Understand] **What type of cryptographic proof do ZK-rollups use to verify transaction validity directly on L1?**
A) Hash commitments B) Merkle proofs C) Zero-knowledge validity proofs D) Fraud proofs with challenge windows
Answer: C) ZK-rollups use validity proofs (SNARKs or STARKs) to mathematically prove all batched transactions are correct without revealing individual details.

Q7. [Apply] **A ZK-rollup batches 1,000 transactions into a single L1 proof. If the on-chain proof verification costs $10, what is the per-transaction L1 cost?**
A) $10.00 B) $1.00 C) $0.10 D) $0.01

Questions 6–10: Rollup Mechanics, Fees & Flash Loans

Q6. [Understand] **What type of cryptographic proof do ZK-rollups use to verify transaction validity directly on L1?**
A) Hash commitments B) Merkle proofs C) Zero-knowledge validity proofs D) Fraud proofs with challenge windows
Answer: C) ZK-rollups use validity proofs (SNARKs or STARKs) to mathematically prove all batched transactions are correct without revealing individual details.

Q7. [Apply] **A ZK-rollup batches 1,000 transactions into a single L1 proof. If the on-chain proof verification costs $10, what is the per-transaction L1 cost?**
A) $10.00 B) $1.00 C) $0.10 D) $0.01
Answer: D) $0.01 per transaction ($10 / 1,000) — cost amortization across the batch is the core economic advantage of rollups.

Q8. [Analyze] **Why do optimistic rollups have a 7-day withdrawal delay while ZK-rollups can finalize in minutes?**
A) Optimistic rollups are older technology B) ZK-rollups batch fewer transactions C) Optimistic rollups assume validity and need time for challengers to submit fraud proofs; ZK-rollups prove validity upfront D) Both have the same delay

Questions 6–10: Rollup Mechanics, Fees & Flash Loans

Q6. [Understand] **What type of cryptographic proof do ZK-rollups use to verify transaction validity directly on L1?**
A) Hash commitments B) Merkle proofs C) Zero-knowledge validity proofs D) Fraud proofs with challenge windows
Answer: C) ZK-rollups use validity proofs (SNARKs or STARKs) to mathematically prove all batched transactions are correct without revealing individual details.

Q7. [Apply] **A ZK-rollup batches 1,000 transactions into a single L1 proof. If the on-chain proof verification costs $10, what is the per-transaction L1 cost?**
A) $10.00 B) $1.00 C) $0.10 D) $0.01
Answer: D) $0.01 per transaction ($10 / 1,000) — cost amortization across the batch is the core economic advantage of rollups.

Q8. [Analyze] **Why do optimistic rollups have a 7-day withdrawal delay while ZK-rollups can finalize in minutes?**
A) Optimistic rollups are older technology B) ZK-rollups batch fewer transactions C) Optimistic rollups assume validity and need time for challengers to submit fraud proofs; ZK-rollups prove validity upfront D) Both have the same delay
Answer: C) Optimistic rollups need the 7-day window for fraud proofs; ZK-rollups submit a validity proof with each batch, allowing L1 to finalize immediately.

Q9. [Understand] **What makes flash loans "atomic" and distinguishes them from traditional uncollateralized loans?**
A) Secured by on-chain NFTs B) The borrow and repay must occur within the same transaction; if repayment fails the entire transaction reverts C) They require KYC D) Interest rates are fixed by governance

Questions 6–10: Rollup Mechanics, Fees & Flash Loans

Q6. [Understand] **What type of cryptographic proof do ZK-rollups use to verify transaction validity directly on L1?**
A) Hash commitments B) Merkle proofs C) Zero-knowledge validity proofs D) Fraud proofs with challenge windows
Answer: C) ZK-rollups use validity proofs (SNARKs or STARKs) to mathematically prove all batched transactions are correct without revealing individual details.

Q7. [Apply] **A ZK-rollup batches 1,000 transactions into a single L1 proof. If the on-chain proof verification costs $10, what is the per-transaction L1 cost?**
A) $10.00 B) $1.00 C) $0.10 D) $0.01
Answer: D) $0.01 per transaction ($10 / 1,000) — cost amortization across the batch is the core economic advantage of rollups.

Q8. [Analyze] **Why do optimistic rollups have a 7-day withdrawal delay while ZK-rollups can finalize in minutes?**
A) Optimistic rollups are older technology B) ZK-rollups batch fewer transactions C) Optimistic rollups assume validity and need time for challengers to submit fraud proofs; ZK-rollups prove validity upfront D) Both have the same delay
Answer: C) Optimistic rollups need the 7-day window for fraud proofs; ZK-rollups submit a validity proof with each batch, allowing L1 to finalize immediately.

Q9. [Understand] **What makes flash loans "atomic" and distinguishes them from traditional uncollateralized loans?**
A) Secured by on-chain NFTs B) The borrow and repay must occur within the same transaction; if repayment fails the entire transaction reverts C) They require KYC D) Interest rates are fixed by governance
Answer: B) The entire sequence — borrow, use, repay — executes in one transaction; if repayment fails the EVM reverts all state changes.

Q10. [Analyze] **In the Beanstalk attack ($182M), the attacker used a flash loan to acquire governance tokens and immediately pass a malicious proposal. Why couldn't the protocol simply "undo" the governance vote?**
A) The attacker destroyed the governance contract B) The vote was executed atomically — the proposal passed and drained funds in the same transaction C) The protocol had no admin keys D) Legal protection

Questions 6–10: Rollup Mechanics, Fees & Flash Loans

Q6. [Understand] **What type of cryptographic proof do ZK-rollups use to verify transaction validity directly on L1?**
A) Hash commitments B) Merkle proofs C) Zero-knowledge validity proofs D) Fraud proofs with challenge windows
Answer: C) ZK-rollups use validity proofs (SNARKs or STARKs) to mathematically prove all batched transactions are correct without revealing individual details.

Q7. [Apply] **A ZK-rollup batches 1,000 transactions into a single L1 proof. If the on-chain proof verification costs $10, what is the per-transaction L1 cost?**
A) $10.00 B) $1.00 C) $0.10 D) $0.01
Answer: D) $0.01 per transaction ($10 / 1,000) — cost amortization across the batch is the core economic advantage of rollups.

Q8. [Analyze] **Why do optimistic rollups have a 7-day withdrawal delay while ZK-rollups can finalize in minutes?**
A) Optimistic rollups are older technology B) ZK-rollups batch fewer transactions C) Optimistic rollups assume validity and need time for challengers to submit fraud proofs; ZK-rollups prove validity upfront D) Both have the same delay
Answer: C) Optimistic rollups need the 7-day window for fraud proofs; ZK-rollups submit a validity proof with each batch, allowing L1 to finalize immediately.

Q9. [Understand] **What makes flash loans "atomic" and distinguishes them from traditional uncollateralized loans?**
A) Secured by on-chain NFTs B) The borrow and repay must occur within the same transaction; if repayment fails the entire transaction reverts C) They require KYC D) Interest rates are fixed by governance
Answer: B) The entire sequence — borrow, use, repay — executes in one transaction; if repayment fails the EVM reverts all state changes.

Q10. [Analyze] **In the Beanstalk attack ($182M), the attacker used a flash loan to acquire governance tokens and immediately pass a malicious proposal. Why couldn't the protocol simply "undo" the governance vote?**
A) The attacker destroyed the governance contract B) The vote was executed atomically — the proposal passed and drained funds in the same transaction C) The protocol had no admin keys D) Legal protection
Answer: B) Governance execution happened within the same atomic transaction as the flash loan — by confirmation, the funds were already drained.

Questions 11–15: MEV & Smart Contract Security

Q11. [Analyze] **A sandwich attack involves a MEV bot trading immediately before AND after a user's swap. Which participant ultimately bears the economic cost?**
A) The liquidity providers B) The MEV bot C) The user whose swap is sandwiched D) The block validator

Questions 11–15: MEV & Smart Contract Security

Q11. [Analyze] **A sandwich attack involves a MEV bot trading immediately before AND after a user's swap. Which participant ultimately bears the economic cost?**
A) The liquidity providers B) The MEV bot C) The user whose swap is sandwiched D) The block validator
Answer: C) The user — the bot front-runs to push the price up, then back-runs to capture the spread, so the user receives fewer tokens than expected.

Q12. [Apply] **A user swaps 10 ETH for USDC on a DEX. A MEV bot front-runs the trade, pushing the effective USDC price from $2,500 to $2,510 per ETH. How much value did the user lose to the sandwich?**
A) $10 B) $100 C) $250 D) $2,500

Questions 11–15: MEV & Smart Contract Security

Q11. [Analyze] **A sandwich attack involves a MEV bot trading immediately before AND after a user's swap. Which participant ultimately bears the economic cost?**
A) The liquidity providers B) The MEV bot C) The user whose swap is sandwiched D) The block validator
Answer: C) The user — the bot front-runs to push the price up, then back-runs to capture the spread, so the user receives fewer tokens than expected.

Q12. [Apply] **A user swaps 10 ETH for USDC on a DEX. A MEV bot front-runs the trade, pushing the effective USDC price from $2,500 to $2,510 per ETH. How much value did the user lose to the sandwich?**
A) $10 B) $100 C) $250 D) $2,500
Answer: B) $100 (10 ETH $\times$ \$10 price impact = \$100) — the "invisible tax" of MEV on every poorly protected swap.

Q13. [Apply] **A smart contract sends ETH to an external address before updating the sender's internal balance. Which vulnerability does this pattern create?**
A) Integer overflow B) Front-running C) Reentrancy D) Oracle manipulation

Questions 11–15: MEV & Smart Contract Security

Q11. [Analyze] **A sandwich attack involves a MEV bot trading immediately before AND after a user's swap. Which participant ultimately bears the economic cost?**
A) The liquidity providers B) The MEV bot C) The user whose swap is sandwiched D) The block validator
Answer: C) The user — the bot front-runs to push the price up, then back-runs to capture the spread, so the user receives fewer tokens than expected.

Q12. [Apply] **A user swaps 10 ETH for USDC on a DEX. A MEV bot front-runs the trade, pushing the effective USDC price from $2,500 to $2,510 per ETH. How much value did the user lose to the sandwich?**
A) $10 B) $100 C) $250 D) $2,500
Answer: B) $100 (10 ETH $\times$ \$10 price impact = \$100) — the "invisible tax" of MEV on every poorly protected swap.

Q13. [Apply] **A smart contract sends ETH to an external address before updating the sender's internal balance. Which vulnerability does this pattern create?**
A) Integer overflow B) Front-running C) Reentrancy D) Oracle manipulation
Answer: C) Reentrancy — the receiving contract's `fallback()` re-calls `withdraw()` before the balance is zeroed, draining funds repeatedly (The DAO, 2016, $60M).

Q14. [Analyze] **The Checks-Effects-Interactions (CEI) pattern defends against reentrancy. In what order should a secure `withdraw()` function execute its three steps?**
A) Interaction $\rightarrow$ Check $\rightarrow$ Effect B) Check $\rightarrow$ Interaction $\rightarrow$ Effect C) Effect $\rightarrow$ Interaction $\rightarrow$ Check D) Check $\rightarrow$ Effect $\rightarrow$ Interaction

Questions 11–15: MEV & Smart Contract Security

Q11. [Analyze] **A sandwich attack involves a MEV bot trading immediately before AND after a user's swap. Which participant ultimately bears the economic cost?**
A) The liquidity providers B) The MEV bot C) The user whose swap is sandwiched D) The block validator
Answer: C) The user — the bot front-runs to push the price up, then back-runs to capture the spread, so the user receives fewer tokens than expected.

Q12. [Apply] **A user swaps 10 ETH for USDC on a DEX. A MEV bot front-runs the trade, pushing the effective USDC price from $2,500 to $2,510 per ETH. How much value did the user lose to the sandwich?**
A) $10 B) $100 C) $250 D) $2,500
Answer: B) $100 (10 ETH $\times$ \$10 price impact = \$100) — the "invisible tax" of MEV on every poorly protected swap.

Q13. [Apply] **A smart contract sends ETH to an external address before updating the sender's internal balance. Which vulnerability does this pattern create?**
A) Integer overflow B) Front-running C) Reentrancy D) Oracle manipulation
Answer: C) Reentrancy — the receiving contract's `fallback()` re-calls `withdraw()` before the balance is zeroed, draining funds repeatedly (The DAO, 2016, $60M).

Q14. [Analyze] **The Checks-Effects-Interactions (CEI) pattern defends against reentrancy. In what order should a secure `withdraw()` function execute its three steps?**
A) Interaction $\rightarrow$ Check $\rightarrow$ Effect B) Check $\rightarrow$ Interaction $\rightarrow$ Effect C) Effect $\rightarrow$ Interaction $\rightarrow$ Check D) Check $\rightarrow$ Effect $\rightarrow$ Interaction
Answer: D) Check, then Effect (zero the balance), then Interaction (send ETH) — balance is zeroed before the external call, so reentrant calls find nothing to withdraw.

Q15. [Apply] **A lending protocol uses a single DEX's spot price as its price oracle. An attacker uses a flash loan to manipulate the pool reserves within one block. Which defense would most effectively prevent this attack?**
A) Add a 1% withdrawal fee B) Require KYC C) Use a TWAP oracle D) Increase collateral ratio to 200%

Questions 11–15: MEV & Smart Contract Security

Q11. [Analyze] **A sandwich attack involves a MEV bot trading immediately before AND after a user's swap. Which participant ultimately bears the economic cost?**
A) The liquidity providers B) The MEV bot C) The user whose swap is sandwiched D) The block validator
Answer: C) The user — the bot front-runs to push the price up, then back-runs to capture the spread, so the user receives fewer tokens than expected.

Q12. [Apply] **A user swaps 10 ETH for USDC on a DEX. A MEV bot front-runs the trade, pushing the effective USDC price from $2,500 to $2,510 per ETH. How much value did the user lose to the sandwich?**
A) $10 B) $100 C) $250 D) $2,500
Answer: B) $100 (10 ETH $\times$ \$10 price impact = \$100) — the "invisible tax" of MEV on every poorly protected swap.

Q13. [Apply] **A smart contract sends ETH to an external address before updating the sender's internal balance. Which vulnerability does this pattern create?**
A) Integer overflow B) Front-running C) Reentrancy D) Oracle manipulation
Answer: C) Reentrancy — the receiving contract's `fallback()` re-calls `withdraw()` before the balance is zeroed, draining funds repeatedly (The DAO, 2016, $60M).

Q14. [Analyze] **The Checks-Effects-Interactions (CEI) pattern defends against reentrancy. In what order should a secure `withdraw()` function execute its three steps?**
A) Interaction $\rightarrow$ Check $\rightarrow$ Effect B) Check $\rightarrow$ Interaction $\rightarrow$ Effect C) Effect $\rightarrow$ Interaction $\rightarrow$ Check D) Check $\rightarrow$ Effect $\rightarrow$ Interaction
Answer: D) Check, then Effect (zero the balance), then Interaction (send ETH) — balance is zeroed before the external call, so reentrant calls find nothing to withdraw.

Q15. [Apply] **A lending protocol uses a single DEX's spot price as its price oracle. An attacker uses a flash loan to manipulate the pool reserves within one block. Which defense would most effectively prevent this attack?**
A) Add a 1% withdrawal fee B) Require KYC C) Use a TWAP oracle D) Increase collateral ratio to 200%
Answer: C) A TWAP (Time-Weighted Average Price) averages price over many blocks, making single-block flash loan manipulation economically infeasible.

Questions 16–20: Bridges, Audits & Risk Assessment

Q16. [Analyze] **The Ronin Bridge used a 9-validator multisig, and the attacker compromised 5 validators to authorize a $625M drain. What percentage of validators did the attacker need to control?**
A) 33% B) 44% C) 56% D) 67%

Questions 16–20: Bridges, Audits & Risk Assessment

Q16. [Analyze] **The Ronin Bridge used a 9-validator multisig, and the attacker compromised 5 validators to authorize a $625M drain. What percentage of validators did the attacker need to control?**
A) 33% B) 44% C) 56% D) 67%
Answer: C) 56% ($5/9 \approx 55.6\%$) — a simple majority threshold made it vulnerable to social engineering of just 5 individuals.
Q17. [Apply] **A security team runs Slither on a contract and finds zero issues. Should the team deploy to mainnet immediately?**
A) Yes – zero findings means secure B) Yes – static analysis is the gold standard C) No – Slither has limited coverage; a full audit requires fuzzing, formal verification, and manual review
D) No – only formal verification can certify safety

Questions 16–20: Bridges, Audits & Risk Assessment

Q16. [Analyze] **The Ronin Bridge used a 9-validator multisig, and the attacker compromised 5 validators to authorize a $625M drain. What percentage of validators did the attacker need to control?**
A) 33% B) 44% C) 56% D) 67%
Answer: C) 56% ($5/9 \approx 55.6\%$) — a simple majority threshold made it vulnerable to social engineering of just 5 individuals.

Q17. [Apply] **A security team runs Slither on a contract and finds zero issues. Should the team deploy to mainnet immediately?**
A) Yes – zero findings means secure B) Yes – static analysis is the gold standard C) No – Slither has limited coverage; a full audit requires fuzzing, formal verification, and manual review
D) No – only formal verification can certify safety
Answer: C) Slither catches known patterns quickly but misses logic bugs and economic design flaws — defense-in-depth requires multiple complementary tools.

Q18. [Analyze] **Why are cross-chain bridge exploits typically larger in dollar terms than single-protocol exploits?**
A) Bridges charge higher fees B) Bridges are newer and less audited C) Bridges hold pooled assets from multiple chains; a single vulnerability can drain all connected networks simultaneously D) Bridge contracts cannot be upgraded

Questions 16–20: Bridges, Audits & Risk Assessment

Q16. [Analyze] **The Ronin Bridge used a 9-validator multisig, and the attacker compromised 5 validators to authorize a $625M drain. What percentage of validators did the attacker need to control?**
A) 33% B) 44% C) 56% D) 67%
Answer: C) 56% ($5/9 \approx 55.6\%$) — a simple majority threshold made it vulnerable to social engineering of just 5 individuals.

Q17. [Apply] **A security team runs Slither on a contract and finds zero issues. Should the team deploy to mainnet immediately?**
A) Yes – zero findings means secure B) Yes – static analysis is the gold standard C) No – Slither has limited coverage; a full audit requires fuzzing, formal verification, and manual review D) No – only formal verification can certify safety
Answer: C) Slither catches known patterns quickly but misses logic bugs and economic design flaws — defense-in-depth requires multiple complementary tools.

Q18. [Analyze] **Why are cross-chain bridge exploits typically larger in dollar terms than single-protocol exploits?**
A) Bridges charge higher fees B) Bridges are newer and less audited C) Bridges hold pooled assets from multiple chains; a single vulnerability can drain all connected networks simultaneously D) Bridge contracts cannot be upgraded
Answer: C) Bridges concentrate cross-chain liquidity into one target — Ronin ($625M), Wormhole ($320M), and Nomad ($190M) all followed this pattern.

Q19. [Evaluate] **Protocol A has 3 audits, a $5M bug bounty, formal verification, and a 48-hour timelock. Protocol B has 1 audit and $500M TVL. Which has a stronger security posture?**
A) Protocol B – TVL proves trust B) They are equal C) Protocol A – multiple audits, formal verification, bug bounty, and timelocks represent defense in depth D) Protocol B – one reputable audit is sufficient

Questions 16–20: Bridges, Audits & Risk Assessment

Q16. [Analyze] **The Ronin Bridge used a 9-validator multisig, and the attacker compromised 5 validators to authorize a $625M drain. What percentage of validators did the attacker need to control?**
A) 33% B) 44% C) 56% D) 67%
Answer: C) 56% (5/9 $\approx$ 55.6%) — a simple majority threshold made it vulnerable to social engineering of just 5 individuals.

Q17. [Apply] **A security team runs Slither on a contract and finds zero issues. Should the team deploy to mainnet immediately?**
A) Yes – zero findings means secure B) Yes – static analysis is the gold standard C) No – Slither has limited coverage; a full audit requires fuzzing, formal verification, and manual review D) No – only formal verification can certify safety
Answer: C) Slither catches known patterns quickly but misses logic bugs and economic design flaws — defense-in-depth requires multiple complementary tools.

Q18. [Analyze] **Why are cross-chain bridge exploits typically larger in dollar terms than single-protocol exploits?**
A) Bridges charge higher fees B) Bridges are newer and less audited C) Bridges hold pooled assets from multiple chains; a single vulnerability can drain all connected networks simultaneously D) Bridge contracts cannot be upgraded
Answer: C) Bridges concentrate cross-chain liquidity into one target — Ronin ($625M), Wormhole ($320M), and Nomad ($190M) all followed this pattern.

Q19. [Evaluate] **Protocol A has 3 audits, a $5M bug bounty, formal verification, and a 48-hour timelock. Protocol B has 1 audit and $500M TVL. Which has a stronger security posture?**
A) Protocol B – TVL proves trust B) They are equal C) Protocol A – multiple audits, formal verification, bug bounty, and timelocks represent defense in depth D) Protocol B – one reputable audit is sufficient
Answer: C) Protocol A demonstrates defense in depth; Protocol B's high TVL is a target, not a security property, and a single audit is insufficient assurance.

Q20. [Evaluate] **An L2 protocol uses a single centralized sequencer, has no fraud proof mechanism deployed, and holds $2B in TVL. What is your risk assessment?**
A) Low risk – L2s are safer than L1 B) Medium risk – centralization is acceptable early C) High risk – centralized sequencer, absent fraud proofs, and $2B TVL combine into critical unmitigated risk D) Low risk – $2B TVL shows market confidence

Questions 16–20: Bridges, Audits & Risk Assessment

Q16. [Analyze] **The Ronin Bridge used a 9-validator multisig, and the attacker compromised 5 validators to authorize a $625M drain. What percentage of validators did the attacker need to control?**
A) 33% B) 44% C) 56% D) 67%
Answer: C) 56% (5/9 ≈ 55.6%) — a simple majority threshold made it vulnerable to social engineering of just 5 individuals.

Q17. [Apply] **A security team runs Slither on a contract and finds zero issues. Should the team deploy to mainnet immediately?**
A) Yes – zero findings means secure B) Yes – static analysis is the gold standard C) No – Slither has limited coverage; a full audit requires fuzzing, formal verification, and manual review D) No – only formal verification can certify safety
Answer: C) Slither catches known patterns quickly but misses logic bugs and economic design flaws — defense-in-depth requires multiple complementary tools.

Q18. [Analyze] **Why are cross-chain bridge exploits typically larger in dollar terms than single-protocol exploits?**
A) Bridges charge higher fees B) Bridges are newer and less audited C) Bridges hold pooled assets from multiple chains; a single vulnerability can drain all connected networks simultaneously D) Bridge contracts cannot be upgraded
Answer: C) Bridges concentrate cross-chain liquidity into one target — Ronin ($625M), Wormhole ($320M), and Nomad ($190M) all followed this pattern.

Q19. [Evaluate] **Protocol A has 3 audits, a $5M bug bounty, formal verification, and a 48-hour timelock. Protocol B has 1 audit and $500M TVL. Which has a stronger security posture?**
A) Protocol B – TVL proves trust B) They are equal C) Protocol A – multiple audits, formal verification, bug bounty, and timelocks represent defense in depth D) Protocol B – one reputable audit is sufficient
Answer: C) Protocol A demonstrates defense in depth; Protocol B's high TVL is a target, not a security property, and a single audit is insufficient assurance.

Q20. [Evaluate] **An L2 protocol uses a single centralized sequencer, has no fraud proof mechanism deployed, and holds $2B in TVL. What is your risk assessment?**
A) Low risk – L2s are safer than L1 B) Medium risk – centralization is acceptable early C) High risk – centralized sequencer, absent fraud proofs, and $2B TVL combine into critical unmitigated risk D) Low risk – $2B TVL shows market confidence
Answer: C) A centralized sequencer is a single point of failure, absent fraud proofs leave users unable to verify validity, and $2B TVL makes it a prime target — security theater, not genuine guarantees.