Quiz: Smart Contract Security

Instructions: 20 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the primary reason smart contract security is critical?
A) Contracts can be easily patched after deployment B) Code is immutable and self-executing with high-value assets at stake C) Blockchain networks prevent all security vulnerabilities D) Smart contracts are not subject to financial risk

Quiz (1–5)

Q1. What is the primary reason smart contract security is critical?
A) Contracts can be easily patched after deployment B) Code is immutable and self-executing with high-value assets at stake C) Blockchain networks prevent all security vulnerabilities D) Smart contracts are not subject to financial risk
Answer: B – Smart contracts are immutable (code is law) and often hold billions in assets, making vulnerabilities catastrophic.

Q2. How much was lost to crypto hacks in 2024?
A) $500M B) $1.1B C) $2.2B D) $3.8B

Quiz (1–5)

Q1. What is the primary reason smart contract security is critical?
A) Contracts can be easily patched after deployment B) Code is immutable and self-executing with high-value assets at stake C) Blockchain networks prevent all security vulnerabilities D) Smart contracts are not subject to financial risk
Answer: B – Smart contracts are immutable (code is law) and often hold billions in assets, making vulnerabilities catastrophic.

Q2. How much was lost to crypto hacks in 2024?
A) $500M B) $1.1B C) $2.2B D) $3.8B
Answer: C – $2.2B was stolen across 303 incidents in 2024 (per Chainalysis); $3.8B was the 2022 peak.

Q3. What is the leading cause of DeFi exploits?
A) Reentrancy attacks B) Oracle manipulation C) Access control failures D) Integer overflow

Quiz (1–5)

Q1. What is the primary reason smart contract security is critical?
A) Contracts can be easily patched after deployment B) Code is immutable and self-executing with high-value assets at stake C) Blockchain networks prevent all security vulnerabilities D) Smart contracts are not subject to financial risk
Answer: B – Smart contracts are immutable (code is law) and often hold billions in assets, making vulnerabilities catastrophic.

Q2. How much was lost to crypto hacks in 2024?
A) $500M B) $1.1B C) $2.2B D) $3.8B
Answer: C – $2.2B was stolen across 303 incidents in 2024 (per Chainalysis); $3.8B was the 2022 peak.

Q3. What is the leading cause of DeFi exploits?
A) Reentrancy attacks B) Oracle manipulation C) Access control failures D) Integer overflow
Answer: C – Access control failures (44% of losses) have become the leading vulnerability type.

Q4. What was the outcome of The DAO hack in 2016?
A) Ethereum shut down permanently B) $60M drained, leading to Ethereum hard fork (ETH/ETC split) C) Only $10M was stolen and later recovered D) No significant impact on Ethereum

Quiz (1–5)

Q1. What is the primary reason smart contract security is critical?
A) Contracts can be easily patched after deployment B) Code is immutable and self-executing with high-value assets at stake C) Blockchain networks prevent all security vulnerabilities D) Smart contracts are not subject to financial risk
Answer: B – Smart contracts are immutable (code is law) and often hold billions in assets, making vulnerabilities catastrophic.

Q2. How much was lost to crypto hacks in 2024?
A) $500M B) $1.1B C) $2.2B D) $3.8B
Answer: C – $2.2B was stolen across 303 incidents in 2024 (per Chainalysis); $3.8B was the 2022 peak.

Q3. What is the leading cause of DeFi exploits?
A) Reentrancy attacks B) Oracle manipulation C) Access control failures D) Integer overflow
Answer: C – Access control failures (44% of losses) have become the leading vulnerability type.

Q4. What was the outcome of The DAO hack in 2016?
A) Ethereum shut down permanently B) $60M drained, leading to Ethereum hard fork (ETH/ETC split) C) Only $10M was stolen and later recovered D) No significant impact on Ethereum
Answer: B – $60M was drained via reentrancy, leading to controversial hard fork creating ETH and ETC.

Q5. What is the Checks-Effects-Interactions pattern?
A) Check oracles, effect prices, interact with users B) Verify conditions, update state FIRST, then make external calls LAST C) Check balances, calculate effects, interact with DEXs D) Validate inputs, log events, send transactions

Quiz (1–5)

Q1. What is the primary reason smart contract security is critical?
A) Contracts can be easily patched after deployment B) Code is immutable and self-executing with high-value assets at stake C) Blockchain networks prevent all security vulnerabilities D) Smart contracts are not subject to financial risk
Answer: B – Smart contracts are immutable (code is law) and often hold billions in assets, making vulnerabilities catastrophic.

Q2. How much was lost to crypto hacks in 2024?
A) $500M B) $1.1B C) $2.2B D) $3.8B
Answer: C – $2.2B was stolen across 303 incidents in 2024 (per Chainalysis); $3.8B was the 2022 peak.

Q3. What is the leading cause of DeFi exploits?
A) Reentrancy attacks B) Oracle manipulation C) Access control failures D) Integer overflow
Answer: C – Access control failures (44% of losses) have become the leading vulnerability type.

Q4. What was the outcome of The DAO hack in 2016?
A) Ethereum shut down permanently B) $60M drained, leading to Ethereum hard fork (ETH/ETC split) C) Only $10M was stolen and later recovered D) No significant impact on Ethereum
Answer: B – $60M was drained via reentrancy, leading to controversial hard fork creating ETH and ETC.

Q5. What is the Checks-Effects-Interactions pattern?
A) Check oracles, effect prices, interact with users B) Verify conditions, update state FIRST, then make external calls LAST C) Check balances, calculate effects, interact with DEXs D) Validate inputs, log events, send transactions
Answer: B – This pattern prevents reentrancy by updating state before external calls.

Quiz (6–10)

Q6. How does a reentrancy attack work?
A) Attacker calls withdraw() recursively before balance is updated B) Attacker overflows integer variables C) Attacker manipulates oracle price feeds D) Attacker guesses private keys

Quiz (6–10)

Q6. How does a reentrancy attack work?
A) Attacker calls withdraw() recursively before balance is updated B) Attacker overflows integer variables C) Attacker manipulates oracle price feeds D) Attacker guesses private keys
Answer: A – External call triggers fallback that recursively calls withdraw().

Q7. What caused the Parity Wallet hack (2017)?
A) Reentrancy B) Unprotected initWallet() function C) Oracle manipulation D) Integer overflow

Quiz (6–10)

Q6. How does a reentrancy attack work?
A) Attacker calls withdraw() recursively before balance is updated B) Attacker overflows integer variables C) Attacker manipulates oracle price feeds D) Attacker guesses private keys
Answer: A – External call triggers fallback that recursively calls withdraw().

Q7. What caused the Parity Wallet hack (2017)?
A) Reentrancy B) Unprotected initWallet() function C) Oracle manipulation D) Integer overflow
Answer: B – Attacker called unprotected initWallet(), became owner, called selfdestruct.

Q8. What percentage of 2024 hacks involved private key compromises?
A) 10% B) 25% C) 44% D) 75%

Quiz (6–10)

Q6. How does a reentrancy attack work?
A) Attacker calls withdraw() recursively before balance is updated B) Attacker overflows integer variables C) Attacker manipulates oracle price feeds D) Attacker guesses private keys
Answer: A – External call triggers fallback that recursively calls withdraw().

Q7. What caused the Parity Wallet hack (2017)?
A) Reentrancy B) Unprotected initWallet() function C) Oracle manipulation D) Integer overflow
Answer: B – Attacker called unprotected initWallet(), became owner, called selfdestruct.

Q8. What percentage of 2024 hacks involved private key compromises?
A) 10% B) 25% C) 44% D) 75%
Answer: C – 44% of 2024 losses from key theft.

Q9. How do oracle manipulation attacks exploit DeFi protocols?
A) Hacking Chainlink nodes B) Flash loan manipulates DEX price, protocol reads false price C) Stealing API keys D) DDoS attacks on oracle networks

Quiz (6–10)

Q6. How does a reentrancy attack work?
A) Attacker calls withdraw() recursively before balance is updated B) Attacker overflows integer variables C) Attacker manipulates oracle price feeds D) Attacker guesses private keys
Answer: A – External call triggers fallback that recursively calls withdraw().

Q7. What caused the Parity Wallet hack (2017)?
A) Reentrancy B) Unprotected initWallet() function C) Oracle manipulation D) Integer overflow
Answer: B – Attacker called unprotected initWallet(), became owner, called selfdestruct.

Q8. What percentage of 2024 hacks involved private key compromises?
A) 10% B) 25% C) 44% D) 75%
Answer: C – 44% of 2024 losses from key theft.

Q9. How do oracle manipulation attacks exploit DeFi protocols?
A) Hacking Chainlink nodes B) Flash loan manipulates DEX price, protocol reads false price C) Stealing API keys D) DDoS attacks on oracle networks
Answer: B – Flash loan manipulates DEX pool price used as oracle.

Q10. What is the best defense against oracle manipulation?
A) Single DEX price B) Decentralized oracles (Chainlink), TWAP, multiple sources C) Disable price updates D) Manual price entry

Quiz (6–10)

Q6. How does a reentrancy attack work?
A) Attacker calls withdraw() recursively before balance is updated B) Attacker overflows integer variables C) Attacker manipulates oracle price feeds D) Attacker guesses private keys
Answer: A – External call triggers fallback that recursively calls withdraw().

Q7. What caused the Parity Wallet hack (2017)?
A) Reentrancy B) Unprotected initWallet() function C) Oracle manipulation D) Integer overflow
Answer: B – Attacker called unprotected initWallet(), became owner, called selfdestruct.

Q8. What percentage of 2024 hacks involved private key compromises?
A) 10% B) 25% C) 44% D) 75%
Answer: C – 44% of 2024 losses from key theft.

Q9. How do oracle manipulation attacks exploit DeFi protocols?
A) Hacking Chainlink nodes B) Flash loan manipulates DEX price, protocol reads false price C) Stealing API keys D) DDoS attacks on oracle networks
Answer: B – Flash loan manipulates DEX pool price used as oracle.

Q10. What is the best defense against oracle manipulation?
A) Single DEX price B) Decentralized oracles (Chainlink), TWAP, multiple sources C) Disable price updates D) Manual price entry
Answer: B – Multiple decentralized sources and TWAP prevent manipulation.

Quiz (11–15)

Q11. What was the largest bridge exploit?
A) Wormhole ($320M) B) Nomad ($190M) C) Ronin Bridge ($625M) D) Poly Network ($600M)

Quiz (11–15)

Q11. What was the largest bridge exploit?
A) Wormhole ($320M) B) Nomad ($190M) C) Ronin Bridge ($625M) D) Poly Network ($600M)
Answer: C – Ronin Bridge (2022) lost $625M via validator key compromise.

Q12. Why are bridges particularly vulnerable?
A) They use outdated Solidity versions B) Complex multi-chain logic, centralized validators, high-value targets C) They lack smart contract functionality D) Bridges are not vulnerable

Quiz (11–15)

Q11. What was the largest bridge exploit?
A) Wormhole ($320M) B) Nomad ($190M) C) Ronin Bridge ($625M) D) Poly Network ($600M)
Answer: C – Ronin Bridge (2022) lost $625M via validator key compromise.

Q12. Why are bridges particularly vulnerable?
A) They use outdated Solidity versions B) Complex multi-chain logic, centralized validators, high-value targets C) They lack smart contract functionality D) Bridges are not vulnerable
Answer: B – Large attack surface and billions in locked assets.

Q13. What type of analysis does Slither perform?
A) Formal verification B) Fuzzing C) Static analysis D) Runtime monitoring

Quiz (11–15)

Q11. What was the largest bridge exploit?
A) Wormhole ($320M) B) Nomad ($190M) C) Ronin Bridge ($625M) D) Poly Network ($600M)
Answer: C – Ronin Bridge (2022) lost $625M via validator key compromise.

Q12. Why are bridges particularly vulnerable?
A) They use outdated Solidity versions B) Complex multi-chain logic, centralized validators, high-value targets C) They lack smart contract functionality D) Bridges are not vulnerable
Answer: B – Large attack surface and billions in locked assets.

Q13. What type of analysis does Slither perform?
A) Formal verification B) Fuzzing C) Static analysis D) Runtime monitoring
Answer: C – Slither is a fast static analyzer.

Q14. Which tool provides mathematical proofs of contract correctness?
A) Slither B) Mythril C) Echidna D) Certora

Quiz (11–15)

Q11. What was the largest bridge exploit?
A) Wormhole ($320M) B) Nomad ($190M) C) Ronin Bridge ($625M) D) Poly Network ($600M)
Answer: C – Ronin Bridge (2022) lost $625M via validator key compromise.

Q12. Why are bridges particularly vulnerable?
A) They use outdated Solidity versions B) Complex multi-chain logic, centralized validators, high-value targets C) They lack smart contract functionality D) Bridges are not vulnerable
Answer: B – Large attack surface and billions in locked assets.

Q13. What type of analysis does Slither perform?
A) Formal verification B) Fuzzing C) Static analysis D) Runtime monitoring
Answer: C – Slither is a fast static analyzer.

Q14. Which tool provides mathematical proofs of contract correctness?
A) Slither B) Mythril C) Echidna D) Certora
Answer: D – Certora is a formal verifier.

Q15. What does Echidna do?
A) Static code analysis B) Symbolic execution C) Property-based fuzzing D) Runtime monitoring

Quiz (11–15)

Q11. What was the largest bridge exploit?
A) Wormhole ($320M) B) Nomad ($190M) C) Ronin Bridge ($625M) D) Poly Network ($600M)
Answer: C – Ronin Bridge (2022) lost $625M via validator key compromise.

Q12. Why are bridges particularly vulnerable?
A) They use outdated Solidity versions B) Complex multi-chain logic, centralized validators, high-value targets C) They lack smart contract functionality D) Bridges are not vulnerable
Answer: B – Large attack surface and billions in locked assets.

Q13. What type of analysis does Slither perform?
A) Formal verification B) Fuzzing C) Static analysis D) Runtime monitoring
Answer: C – Slither is a fast static analyzer.

Q14. Which tool provides mathematical proofs of contract correctness?
A) Slither B) Mythril C) Echidna D) Certora
Answer: D – Certora is a formal verifier.

Q15. What does Echidna do?
A) Static code analysis B) Symbolic execution C) Property-based fuzzing D) Runtime monitoring
Answer: C – Echidna fuzzes to find invariant violations.

Quiz (16–20)

Q16. What is the typical cost range for a professional smart contract audit?
A) $1k–$5k B) $10k–$25k C) $50k–$500k D) $1M+

Quiz (16–20)

Q16. What is the typical cost range for a professional smart contract audit?
A) $1k–$5k B) $10k–$25k C) $50k–$500k D) $1M+
Answer: C – Manual audits by firms like Trail of Bits or OpenZeppelin cost $50k–$500k for 2-4 weeks.

Q17. What was the record bug bounty payout?
A) $1M B) $5M C) $10M D) $25M

Quiz (16–20)

Q16. What is the typical cost range for a professional smart contract audit?
A) $1k–$5k B) $10k–$25k C) $50k–$500k D) $1M+
Answer: C – Manual audits by firms like Trail of Bits or OpenZeppelin cost $50k–$500k for 2-4 weeks.

Q17. What was the record bug bounty payout?
A) $1M B) $5M C) $10M D) $25M
Answer: C – Wormhole paid $10M bounty in 2022 (highest on record).

Q18. How do upgradeable contracts work?
A) Code is rewritten on-chain B) Proxy pattern: proxy holds storage, delegates to upgradeable implementation C) Contracts are deleted and redeployed D) Upgrades happen automatically via AI

Quiz (16–20)

Q16. What is the typical cost range for a professional smart contract audit?
A) $1k–$5k B) $10k–$25k C) $50k–$500k D) $1M+
Answer: C – Manual audits by firms like Trail of Bits or OpenZeppelin cost $50k–$500k for 2-4 weeks.

Q17. What was the record bug bounty payout?
A) $1M B) $5M C) $10M D) $25M
Answer: C – Wormhole paid $10M bounty in 2022 (highest on record).

Q18. How do upgradeable contracts work?
A) Code is rewritten on-chain B) Proxy pattern: proxy holds storage, delegates to upgradeable implementation C) Contracts are deleted and redeployed D) Upgrades happen automatically via AI
Answer: B – Proxy separates storage (in proxy) from logic (in implementation), allowing logic upgrades.

Q19. What is the main risk of upgradeable contracts?
A) Gas costs are higher B) Admin key compromise allows malicious upgrade C) Storage is lost during upgrade D) They cannot be used with ERC-20 tokens

Quiz (16–20)

Q16. What is the typical cost range for a professional smart contract audit?
A) $1k–$5k B) $10k–$25k C) $50k–$500k D) $1M+
Answer: C – Manual audits by firms like Trail of Bits or OpenZeppelin cost $50k–$500k for 2-4 weeks.

Q17. What was the record bug bounty payout?
A) $1M B) $5M C) $10M D) $25M
Answer: C – Wormhole paid $10M bounty in 2022 (highest on record).

Q18. How do upgradeable contracts work?
A) Code is rewritten on-chain B) Proxy pattern: proxy holds storage, delegates to upgradeable implementation C) Contracts are deleted and redeployed D) Upgrades happen automatically via AI
Answer: B – Proxy separates storage (in proxy) from logic (in implementation), allowing logic upgrades.

Q19. What is the main risk of upgradeable contracts?
A) Gas costs are higher B) Admin key compromise allows malicious upgrade C) Storage is lost during upgrade D) They cannot be used with ERC-20 tokens
Answer: B – If admin key is compromised, attacker can upgrade to malicious implementation.

Q20. What does "defense in depth" mean for smart contract security?
A) Using only one security tool thoroughly B) Layered approach: automated tools + audits + formal verification + bounties + monitoring C) Focusing only on the most common vulnerability D) Relying solely on audits

Quiz (16–20)

Q16. What is the typical cost range for a professional smart contract audit?
A) $1k–$5k B) $10k–$25k C) $50k–$500k D) $1M+
Answer: C – Manual audits by firms like Trail of Bits or OpenZeppelin cost $50k–$500k for 2-4 weeks.

Q17. What was the record bug bounty payout?
A) $1M B) $5M C) $10M D) $25M
Answer: C – Wormhole paid $10M bounty in 2022 (highest on record).

Q18. How do upgradeable contracts work?
A) Code is rewritten on-chain B) Proxy pattern: proxy holds storage, delegates to upgradeable implementation C) Contracts are deleted and redeployed D) Upgrades happen automatically via AI
Answer: B – Proxy separates storage (in proxy) from logic (in implementation), allowing logic upgrades.

Q19. What is the main risk of upgradeable contracts?
A) Gas costs are higher B) Admin key compromise allows malicious upgrade C) Storage is lost during upgrade D) They cannot be used with ERC-20 tokens
Answer: B – If admin key is compromised, attacker can upgrade to malicious implementation.

Q20. What does "defense in depth" mean for smart contract security?
A) Using only one security tool thoroughly B) Layered approach: automated tools + audits + formal verification + bounties + monitoring C) Focusing only on the most common vulnerability D) Relying solely on audits
Answer: B – Multiple security layers catch bugs that previous layers missed; no single tool is sufficient.