Lesson 3.3 Quiz: Smart Contracts and Programmable Finance

Module 3: The Trust Problem

Prof. Dr. Joerg Osterrieder

Digital Finance — BSc Course (v2026.05)

Q1: Smart Contract Definition

Which statement **best** describes a smart contract?

A. A database query that retrieves financial data from a centralized server
B. A legal agreement signed electronically via DocuSign
C. A self-executing program stored on a blockchain that runs when predetermined conditions are met
D. An AI system that negotiates contract terms between two parties

Q1: Smart Contract Definition

Which statement **best** describes a smart contract?

- **A** A database query that retrieves financial data from a centralized server
- **B** A legal agreement signed electronically via DocuSign
- **C** A self-executing program stored on a blockchain that runs when predetermined conditions are met
- **D** An AI system that negotiates contract terms between two parties

[Answer hidden – compile with \solutionstrue to reveal]

Q2: EVM Purpose

What is the primary purpose of the Ethereum Virtual Machine (EVM)?

A. To store user passwords and private keys securely
B. To provide a deterministic execution environment for smart contract bytecode on every node
C. To convert Solidity code into JavaScript for web browsers
D. To mine new Ethereum tokens using Proof of Work

Q2: EVM Purpose

What is the primary purpose of the Ethereum Virtual Machine (EVM)?

- (A) To store user passwords and private keys securely
- (B) To provide a deterministic execution environment for smart contract bytecode on every node
- (C) To convert Solidity code into JavaScript for web browsers
- (D) To mine new Ethereum tokens using Proof of Work

[Answer hidden – compile with \solutionstrue to reveal]

Q3: Gas Purpose

Why does Ethereum require users to pay gas fees?

A. To fund the Ethereum Foundation's research budget
B. To compensate users who hold ETH in their wallets
C. To pay software developers who write smart contracts
D. To prevent spam and infinite loops by making computation cost money

Q3: Gas Purpose

Why does Ethereum require users to pay gas fees?

- A To fund the Ethereum Foundation's research budget
- B To compensate users who hold ETH in their wallets
- C To pay software developers who write smart contracts
- D To prevent spam and infinite loops by making computation cost money

[Answer hidden – compile with \solutionstrue to reveal]

Q4: Immutability Trade-off

A deployed smart contract contains a bug. What can the developer do?

A. Roll back the blockchain to before the contract was deployed
B. Deploy a new corrected contract and migrate users, but the buggy contract remains on-chain forever
C. Contact Ethereum customer support to remove the contract
D. Edit the contract code on-chain to fix the bug

Q4: Immutability Trade-off

A deployed smart contract contains a bug. What can the developer do?

- **A** Roll back the blockchain to before the contract was deployed
- **B** Deploy a new corrected contract and migrate users, but the buggy contract remains on-chain forever
- **C** Contact Ethereum customer support to remove the contract
- **D** Edit the contract code on-chain to fix the bug

[Answer hidden – compile with \solutionstrue to reveal]

Q5: Token Standard Purpose

Why do token standards like ERC-20 exist?

A. To allow the Ethereum Foundation to control token supply
B. To ensure interoperability so any wallet or exchange can handle any compliant token
C. To guarantee that all tokens will increase in value
D. To prevent new tokens from being created on Ethereum

Q5: Token Standard Purpose

Why do token standards like ERC-20 exist?

- **A** To allow the Ethereum Foundation to control token supply
- **B** To ensure interoperability so any wallet or exchange can handle any compliant token
- **C** To guarantee that all tokens will increase in value
- **D** To prevent new tokens from being created on Ethereum

[Answer hidden – compile with \solutionstrue to reveal]

Q6: Gas Cost Calculation

A simple ETH transfer costs 21,000 gas. If the gas price is 30 gwei and 1 ETH = \$3,000, what is the transaction fee in USD?

- (A) \$18.90
- (B) \$0.63
- (C) \$1.89
- (D) \$6.30

Q6: Gas Cost Calculation

A simple ETH transfer costs 21,000 gas. If the gas price is 30 gwei and 1 ETH = $3,000, what is the transaction fee in USD?

- (A) $18.90
- (B) $0.63
- (C) $1.89
- (D) $6.30

[Answer hidden – compile with \solutionstrue to reveal]

Q7: ERC-20 vs. ERC-721

A company wants to tokenize 1,000 identical loyalty points. Which standard should it use?

A. ERC-721, because each loyalty point is a unique asset
B. ERC-1155, because the company might add NFTs later
C. ERC-20, because the points are interchangeable (fungible)
D. No standard is needed — just use a database

Q7: ERC-20 vs. ERC-721

A company wants to tokenize 1,000 identical loyalty points. Which standard should it use?

- **A** ERC-721, because each loyalty point is a unique asset
- **B** ERC-1155, because the company might add NFTs later
- **C** ERC-20, because the points are interchangeable (fungible)
- **D** No standard is needed — just use a database

[Answer hidden – compile with \solutionstrue to reveal]

Q8: EIP-1559 Fee Calculation

Under EIP-1559, the base fee is 20 gwei and you set a priority tip of 2 gwei. Your transaction uses 50,000 gas. How much ETH do you pay, and what happens to it?

- A. 0.001 ETH: all burned
- B. 0.0011 ETH: 0.001 ETH burned, 0.0001 ETH to the validator
- C. 0.0011 ETH: all goes to the validator
- D. 0.0022 ETH: half burned, half to the validator

Q8: EIP-1559 Fee Calculation

Under EIP-1559, the base fee is 20 gwei and you set a priority tip of 2 gwei. Your transaction uses 50,000 gas. How much ETH do you pay, and what happens to it?

A. 0.001 ETH: all burned

B. 0.0011 ETH: 0.001 ETH burned, 0.0001 ETH to the validator

C. 0.0011 ETH: all goes to the validator

D. 0.0022 ETH: half burned, half to the validator

[Answer hidden – compile with \solutionstrue to reveal]

Q9: DAO Voting Mechanics

A DAO has 1,000,000 governance tokens. A proposal requires >50% of *votes cast* to pass. Only 80,000 tokens are used to vote: 50,000 vote YES, 30,000 vote NO. Does the proposal pass?

- **A** Yes — 50,000 / 80,000 = 62.5% of votes cast exceeds 50%
- **B** No — a quorum of at least 50% of total supply must participate
- **C** Cannot be determined without knowing the gas price
- **D** No — 50,000 is only 5% of total supply

Q9: DAO Voting Mechanics

A DAO has 1,000,000 governance tokens. A proposal requires >50% of *votes cast* to pass. Only 80,000 tokens are used to vote: 50,000 vote YES, 30,000 vote NO. Does the proposal pass?

A. Yes — 50,000 / 80,000 = 62.5% of votes cast exceeds 50%
B. No — a quorum of at least 50% of total supply must participate
C. Cannot be determined without knowing the gas price
D. No — 50,000 is only 5% of total supply

[Answer hidden – compile with \solutionstrue to reveal]

Q10: Rollup Cost Savings

Ethereum Layer-1 charges $5.00 per transaction. An optimistic rollup batches 500 transactions into a single Layer-1 proof that costs $250. What is the per-transaction cost on the rollup?

- (A) $2.50
- (B) $0.05
- (C) $5.00
- (D) $0.50

Q10: Rollup Cost Savings

Ethereum Layer-1 charges $5.00 per transaction. An optimistic rollup batches 500 transactions into a single Layer-1 proof that costs $250. What is the per-transaction cost on the rollup?

- (A) $2.50
- (B) $0.05
- (C) $5.00
- (D) $0.50

[Answer hidden – compile with \solutionstrue to reveal]

Q11: Reentrancy Attack

In the 2016 DAO hack, the attacker exploited a **reentrancy** vulnerability. What does this mean?

A. The attacker submitted more transactions than the network could handle
B. The attacker guessed the contract's private key
C. The attacker modified the contract's source code after deployment
D. The attacker called a withdrawal function repeatedly before the contract updated its balance, draining funds

Q11: Reentrancy Attack

In the 2016 DAO hack, the attacker exploited a **reentrancy** vulnerability. What does this mean?

- (A) The attacker submitted more transactions than the network could handle
- (B) The attacker guessed the contract's private key
- (C) The attacker modified the contract's source code after deployment
- (D) The attacker called a withdrawal function repeatedly before the contract updated its balance, draining funds

[Answer hidden – compile with \solutionstrue to reveal]

Q12: Optimistic vs. ZK Rollup

What is the **key difference** between optimistic rollups and ZK-rollups?

- (A) ZK-rollups require a 7-day dispute window; optimistic rollups do not
- (B) Optimistic rollups are faster and cheaper in all cases
- (C) Optimistic rollups assume validity and use fraud proofs; ZK-rollups provide cryptographic validity proofs
- (D) Optimistic rollups only work with ERC-20 tokens

Q12: Optimistic vs. ZK Rollup

What is the **key difference** between optimistic rollups and ZK-rollups?

A. ZK-rollups require a 7-day dispute window; optimistic rollups do not
B. Optimistic rollups are faster and cheaper in all cases
C. Optimistic rollups assume validity and use fraud proofs; ZK-rollups provide cryptographic validity proofs
D. Optimistic rollups only work with ERC-20 tokens

[Answer hidden – compile with \solutionstrue to reveal]

Q13: Bridge Vulnerability

Why are cross-chain bridges particularly attractive targets for attackers?

A. Bridges hold large pools of locked assets and concentrate trust in their validation mechanism
B. Bridges only operate on private blockchains
C. Bridges use outdated encryption algorithms
D. Bridges are unregulated and therefore have no security measures

Q13: Bridge Vulnerability

Why are cross-chain bridges particularly attractive targets for attackers?

- **A** Bridges hold large pools of locked assets and concentrate trust in their validation mechanism
- **B** Bridges only operate on private blockchains
- **C** Bridges use outdated encryption algorithms
- **D** Bridges are unregulated and therefore have no security measures

[Answer hidden – compile with \solutionstrue to reveal]

Q14: MEV Sandwich Attack

In a sandwich attack, a searcher observes a pending large buy order on a DEX. What does the searcher do?

A. Shorts the token on a centralized exchange

B. Reports the victim's transaction to regulators

C. Cancels the victim's transaction by paying higher gas

D. Places a buy order *before* the victim (frontrun) and a sell order *after* the victim (backrun), capturing the price impact

Q14: MEV Sandwich Attack

In a sandwich attack, a searcher observes a pending large buy order on a DEX. What does the searcher do?

- (A) Shorts the token on a centralized exchange
- (B) Reports the victim's transaction to regulators
- (C) Cancels the victim's transaction by paying higher gas
- (D) Places a buy order *before* the victim (frontrun) and a sell order *after* the victim (backrun), capturing the price impact

[Answer hidden – compile with \solutionstrue to reveal]

Q15: Governance Token Risk

A single wallet holds 51% of a DAO's governance tokens. What is the primary risk?

- **A** The DAO will run out of gas for voting transactions
- **B** The majority holder can unilaterally pass any proposal, making governance effectively centralized
- **C** The Ethereum Foundation will revoke the DAO's smart contract
- **D** Other token holders will automatically lose their tokens

Q15: Governance Token Risk

A single wallet holds 51% of a DAO's governance tokens. What is the primary risk?

- **A** The DAO will run out of gas for voting transactions
- **B** The majority holder can unilaterally pass any proposal, making governance effectively centralized
- **C** The Ethereum Foundation will revoke the DAO's smart contract
- **D** Other token holders will automatically lose their tokens

[Answer hidden – compile with \solutionstrue to reveal]

Q16: Sidechain vs. Rollup Security

Why do sidechains (e.g., Polygon PoS) offer weaker security guarantees than rollups?

- (A) Sidechains have their own validator set and do not post proofs to Ethereum Layer-1
- (B) Sidechains are always slower than Layer-1
- (C) Sidechains cannot process ERC-20 tokens
- (D) Sidechains use older programming languages

Q16: Sidechain vs. Rollup Security

Why do sidechains (e.g., Polygon PoS) offer weaker security guarantees than rollups?

- **A** Sidechains have their own validator set and do not post proofs to Ethereum Layer-1
- **B** Sidechains are always slower than Layer-1
- **C** Sidechains cannot process ERC-20 tokens
- **D** Sidechains use older programming languages

[Answer hidden – compile with \solutionstrue to reveal]

Q17: Smart Contract vs. Traditional Contract

A startup considers using a smart contract instead of a traditional legal agreement for an escrow service. Which argument **against** smart contracts is most valid?

- (A) Smart contracts cannot handle ambiguity, edge cases, or unforeseen circumstances that a court could resolve
- (B) Smart contracts require the Ethereum Foundation's approval
- (C) Smart contracts execute too slowly for financial transactions
- (D) Smart contracts are too expensive to deploy compared to hiring a lawyer

Q17: Smart Contract vs. Traditional Contract

A startup considers using a smart contract instead of a traditional legal agreement for an escrow service. Which argument **against** smart contracts is most valid?

- (A) Smart contracts cannot handle ambiguity, edge cases, or unforeseen circumstances that a court could resolve
- (B) Smart contracts require the Ethereum Foundation's approval
- (C) Smart contracts execute too slowly for financial transactions
- (D) Smart contracts are too expensive to deploy compared to hiring a lawyer

[Answer hidden – compile with \solutionstrue to reveal]

Q18: L2 Selection

A DeFi protocol needs fast finality (under 10 minutes) and strong security guarantees. It handles high-value trades. Which Layer-2 solution is **most appropriate**?

- A ZK-rollup (cryptographic validity proof, no dispute window)
- A state channel (near-instant, but only for two-party interactions)
- An optimistic rollup (7-day fraud proof window)
- A sidechain (own validators, fast finality)

Q18: L2 Selection

A DeFi protocol needs fast finality (under 10 minutes) and strong security guarantees. It handles high-value trades. Which Layer-2 solution is **most appropriate**?

- A ZK-rollup (cryptographic validity proof, no dispute window)
- A state channel (near-instant, but only for two-party interactions)
- An optimistic rollup (7-day fraud proof window)
- A sidechain (own validators, fast finality)

[Answer hidden – compile with \solutionstrue to reveal]

Q19: DAO Governance Design

You are designing a DAO governance system. Which mechanism **best** mitigates flash loan governance attacks?

- (A) Increasing the gas cost of voting transactions
- (B) Reducing the total supply of governance tokens
- (C) Allowing only the contract deployer to vote
- (D) Requiring voters to hold tokens for a minimum period (e.g., 7 days) before their votes count

Q19: DAO Governance Design

You are designing a DAO governance system. Which mechanism **best** mitigates flash loan governance attacks?

- (A) Increasing the gas cost of voting transactions
- (B) Reducing the total supply of governance tokens
- (C) Allowing only the contract deployer to vote
- (D) Requiring voters to hold tokens for a minimum period (e.g., 7 days) before their votes count

[Answer hidden – compile with \solutionstrue to reveal]

Q20: LLM Smart Contract Auditing

A team uses an LLM to audit their Solidity code. The LLM reports "no vulnerabilities found." How should the team proceed?

A. Deploy immediately — LLMs are more thorough than human auditors
B. Deploy to a testnet only and never use real funds
C. Treat the LLM report as a useful first pass but commission a professional security audit and consider formal verification before deploying
D. Ignore the LLM report entirely — AI cannot understand code

Q20: LLM Smart Contract Auditing

A team uses an LLM to audit their Solidity code. The LLM reports "no vulnerabilities found." How should the team proceed?

- (A) Deploy immediately — LLMs are more thorough than human auditors
- (B) Deploy to a testnet only and never use real funds
- (C) Treat the LLM report as a useful first pass but commission a professional security audit and consider formal verification before deploying
- (D) Ignore the LLM report entirely — AI cannot understand code

[Answer hidden – compile with \solutionstrue to reveal]