Lesson 3.3 Quiz: Smart Contracts and Programmable Finance

Module 3: The Trust Problem

Prof. Dr. Joerg Osterrieder

Digital Finance — BSc Course

Q1: Smart Contract Definition

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

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

Q1: Smart Contract Definition

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

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

Answer: (B) A smart contract is code deployed on a blockchain that automatically executes when its conditions are triggered, without intermediaries.

Q2: EVM Purpose

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

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

Q2: EVM Purpose

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

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

Answer: (B) The EVM executes smart contract bytecode identically on every node, ensuring deterministic and verifiable computation across the network.

Q3: Gas Purpose

Why does Ethereum require users to pay gas fees?

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

Q3: Gas Purpose

Why does Ethereum require users to pay gas fees?

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

Answer: (B) Gas fees prevent abuse (e.g., infinite loops) by requiring users to pay for every unit of computation. This also compensates validators for processing transactions.

Q4: Immutability Trade-off

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

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

Q4: Immutability Trade-off

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

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

Answer: (C) Smart contracts are immutable once deployed. The original buggy contract cannot be modified or deleted. The developer must deploy a new version and convince users to migrate.

Q5: Token Standard Purpose

Why do token standards like ERC-20 exist?

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

Q5: Token Standard Purpose

Why do token standards like ERC-20 exist?

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

Answer: (B) Token standards define a common interface (function names, events) so that wallets, DEXs, and dApps can interact with any compliant token without custom integration.

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

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

Answer: (B) Fee = 21,000 × 30 gwei = 630,000 gwei = 0.00063 ETH. In USD: 0.00063 × \$3,000 = \$1.89.

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-20, because the points are interchangeable (fungible)
C. ERC-1155, because the company might add NFTs later
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-20, because the points are interchangeable (fungible)
- (C) ERC-1155, because the company might add NFTs later
- (D) No standard is needed — just use a database

Answer: (B) Identical, interchangeable loyalty points are fungible by definition. ERC-20 is the correct standard for fungible tokens.

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

Answer: (B) Total $= 50{,}000 \times (20 + 2)$ gwei $= 1{,}100{,}000$ gwei $= 0.0011$ ETH. Base fee portion ($50{,}000 \times 20 = 1{,}000{,}000$ gwei $= 0.001$ ETH) is burned. Tip portion ($50{,}000 \times 2 = 100{,}000$ gwei $= 0.0001$ ETH) goes to the validator.

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

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

Answer: (B) 50,000 / 80,000 = 62.5% of votes cast. Since the rule requires >50% of votes cast, the proposal passes. (Note: many DAOs also have quorum requirements, but the question only states a majority-of-votes-cast rule.)

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

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

Answer: (B) Per-transaction cost = $250 / 500 = $0.50. This is a 10× cost reduction compared to Layer-1.

Q11: Reentrancy Attack

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

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

Q11: Reentrancy Attack

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

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

Answer: (B) Reentrancy occurs when a contract sends ETH before updating its internal state. The attacker's contract re-enters the withdrawal function before the balance is decremented, withdrawing the same funds multiple times.

Q12: Optimistic vs. ZK Rollup

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

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

Answer: (B) Optimistic rollups assume transactions are correct unless someone submits a fraud proof (7-day window). ZK-rollups generate a mathematical proof (ZK-SNARK/STARK) that guarantees correctness without a dispute period.

Q13: Bridge Vulnerability

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

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

Q13: Bridge Vulnerability

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

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

Answer: (B) Bridges lock assets on one chain and mint wrapped tokens on another, creating large "honey pots." A flaw in the bridge's validator set or smart contract logic can drain the entire pool.

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

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

Answer: (B) The searcher buys before the victim (pushing the price up), lets the victim's trade push it higher, then sells immediately after at the inflated price — profiting from the victim's price impact.

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 Other token holders will automatically lose their tokens
- D The Ethereum Foundation will revoke the DAO's smart contract

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) Other token holders will automatically lose their tokens
- (D) The Ethereum Foundation will revoke the DAO's smart contract

Answer: (B) With >50% of tokens, the whale can pass any proposal alone, defeating the purpose of decentralized governance. This is the "plutocracy" problem inherent in token-weighted voting.

Q16: Sidechain vs. Rollup Security

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

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

Q16: Sidechain vs. Rollup Security

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

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

Answer: (B) Sidechains rely on their own consensus mechanism and validator set. If those validators collude or are compromised, funds can be stolen. Rollups post data and proofs to Ethereum Layer-1, inheriting its security.

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

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

Answer: (B) Smart contracts execute rigid "if-then" logic. Real-world agreements often involve ambiguity, force majeure, and disputes that require human judgment. A smart contract cannot say "it depends" — a court can.

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

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

Answer: (C) ZK-rollups provide fast finality (minutes, not 7 days) with cryptographic proofs of correctness, and inherit Ethereum's security. For high-value trades, the stronger security guarantee makes ZK-rollups the best fit.

Q19: DAO Governance Design

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

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

Q19: DAO Governance Design

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

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

Answer: (A) A time-lock or snapshot-based voting system requires voters to hold tokens before a snapshot block, preventing attackers from borrowing tokens via flash loan and voting in the same transaction.

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** Treat the LLM report as a useful first pass but commission a professional security audit and consider formal verification before deploying
- **C** Ignore the LLM report entirely — AI cannot understand code
- **D** Deploy to a testnet only and never use real funds

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) Treat the LLM report as a useful first pass but commission a professional security audit and consider formal verification before deploying

(C) Ignore the LLM report entirely — AI cannot understand code

(D) Deploy to a testnet only and never use real funds

Answer: (B) LLMs can catch common patterns but may miss novel attack vectors and can produce false negatives. A professional audit (and ideally formal verification) remains essential for any contract handling real value.