Lesson 3.3 Exercises: Smart Contracts and Programmable Finance

Module 3: The Trust Problem

Prof. Dr. Joerg Osterrieder

Digital Finance — BSc Course

Exercise 1: Smart Contract Properties

Scenario: A traditional insurance company processes claims manually: a customer files a claim, an adjuster reviews it, and the company decides whether to pay. Average processing time: 14 days.

A smart contract version works as follows: a weather oracle reports rainfall data on-chain. If rainfall at the insured location exceeds 200mm in 24 hours, the contract automatically pays the policyholder.

Tasks:

a) Identify three properties of smart contracts (from the lecture) that make this automatic payout possible.

b) Describe one scenario where the smart contract approach **fails** but the traditional approach succeeds (i.e., a legitimate claim that the smart contract would reject).

c) Explain what an **oracle** is in this context and why it introduces a trust assumption.

Difficulty: Introductory — tests understanding of smart contract properties and limitations.

Exercise 2: Gas Cost Computation

Scenario: A user wants to execute two transactions on Ethereum:

Transaction	Gas Used	Gas Price (gwei)
Simple ETH transfer	21,000	25
Uniswap token swap	184,000	25

Assume 1 ETH = \$3,200 and 1 gwei = 10^{-9} ETH.

Tasks:

a. Calculate the fee for each transaction in gwei, ETH, and USD.

b. The gas price rises to 150 gwei during a popular NFT mint. Recalculate both fees in USD.

c. Explain why the Uniswap swap costs 8.76× more gas than a simple transfer.

d. Under EIP-1559, the base fee is 22 gwei and the user sets a 3 gwei tip. Calculate the total fee for the Uniswap swap and state how much is burned vs. paid to the validator.

Difficulty: Intermediate — requires arithmetic and EIP-1559 understanding.

Exercise 3: Choosing the Right Token Standard

Scenario: Three companies want to tokenize assets on Ethereum:

1. **Company A:** A stablecoin pegged to the Swiss franc (1 token = 1 CHF). All tokens are identical and divisible to 18 decimals.
2. **Company B:** A luxury watch manufacturer. Each watch has a unique serial number, production history, and ownership chain. No two watches are alike.
3. **Company C:** A gaming company. Players earn both generic "gold coins" (fungible, used as in-game currency) and unique "legendary swords" (non-fungible, each with different stats).

Tasks:

a. For each company, recommend the appropriate token standard (ERC-20, ERC-721, or ERC-1155) and justify your choice in one sentence.

b. Company B considers making its tokens "soulbound" (non-transferable). Explain what this means and identify one advantage and one disadvantage.

c. Explain why Company C would *not* want to deploy two separate contracts (one ERC-20 and one ERC-721) instead of using ERC-1155.

Difficulty: Intermediate — requires analysis of token properties.

Exercise 4: DAO Governance Analysis

Scenario: A DeFi lending protocol is governed by a DAO with 10,000,000 governance tokens (GOV). The current token distribution is:

Holder	GOV Tokens
Founding team	3,000,000
Venture capital fund	2,500,000
Community treasury	2,000,000
Retail holders (5,000 wallets)	2,500,000

Proposals require $>50\%$ of votes cast to pass. There is no quorum requirement.

Tasks:

a) Can the founding team alone pass a proposal if they are the only voters? Show your calculation.

b) If the founding team and VC fund vote together, can any combination of retail holders outvote them? (Assume the community treasury does not vote.)

c) Propose a governance mechanism that would reduce the founding team's dominance.

d) Describe how a flash loan governance attack could work against this DAO and propose a defense.

Difficulty: Advanced — requires quantitative reasoning and governance design.

Exercise 5: Layer-2 Scaling Comparison

Scenario: A payment company processes 10,000 transactions per day on Ethereum Layer-1 at a cost of $4.00 per transaction. It is evaluating three Layer-2 solutions:

	Optimistic Rollup	**ZK-Rollup**	**Sidechain**
Cost per tx	$0.25	$0.10	$0.02
Finality time	7 days (dispute window)	∼10 minutes	∼2 seconds
Security model	Inherits L1 (fraud proof)	Inherits L1 (validity proof)	Own validator set
EVM compatibility	Full	Partial (improving)	Full

Tasks:

a. Calculate the daily and annual cost savings for each Layer-2 option vs. Layer-1.

b. The company processes high-value cross-border payments. Which L2 would you recommend and why?

c. Explain why the sidechain is cheapest but may not be appropriate for a regulated financial institution.

d. What does "inherits L1 security" mean in practice? How is it different from the sidechain model?

Difficulty: Advanced — requires quantitative comparison and qualitative evaluation.

Exercise 6: MEV Sandwich Attack

Scenario: A user submits a Uniswap trade to buy 10,000 USDC worth of Token X. The current price is 1 Token X = 2.00 USDC. The user's slippage tolerance is 1%.

A MEV searcher observes this pending transaction in the mempool and executes a sandwich attack:

1. **Frontrun:** Buys 5,000 USDC worth of Token X, pushing the price to 2.04 USDC
2. **Victim's trade:** Executes at 2.04 USDC (within 1% slippage)
3. **Backrun:** Sells Token X at the now-higher price of 2.06 USDC

Tasks:

a) How many Token X does the victim receive compared to the expected amount (at 2.00 USDC)?

b) Calculate the searcher's approximate profit from the sandwich (ignore gas costs).

c) If the user had set slippage tolerance to 0.3%, would the attack still succeed? Explain.

d) Propose two mechanisms that could protect users from sandwich attacks.

Difficulty: Advanced — requires quantitative analysis and MEV reasoning.

Exercise 7: Cross-Chain Bridge Risk Assessment

Scenario: A DeFi user wants to move $50,000 in USDC from Ethereum to an EVM-compatible sidechain. Two bridge options are available:

	Bridge Alpha	**Bridge Beta**
Validator set	5-of-9 multisig	200 independent validators
TVL (locked value)	$2 billion	$80 million
Audit status	3 audits (Tier-1 firms)	1 audit (boutique firm)
History	18 months, no exploits	6 months, no exploits
Fee	0.05%	0.30%

Tasks:

a. Calculate the bridge fee for each option.

b. Identify the primary security risk for each bridge and explain which attack vector is most likely.

c. Explain why a bridge with $2 billion TVL is a bigger target than one with $80 million, despite having better audits.

d. Recommend one bridge and justify your choice, considering both cost and risk.

Difficulty: Advanced — requires risk assessment and decision-making.

Exercise 8: Comprehensive Case – Decentralized Crowdfunding

Scenario: You are designing a smart-contract-based crowdfunding platform (like Kickstarter, but decentralized). Requirements:

- Creators set a funding goal (e.g., 100 ETH) and a deadline (e.g., 30 days)
- Backers send ETH to the contract
- If the goal is met by the deadline, the creator receives the funds
- If the goal is **not** met, backers can withdraw their contributions (refund)

Tasks:

a. List the key state variables the smart contract needs (at least 5).

b. Write pseudocode for the `contribute()`, `withdraw()`, and `claimFunds()` functions.

c. Identify two potential vulnerabilities in this design and propose mitigations.

d. The platform wants to charge a 2% fee. Where in the contract logic should this fee be deducted, and to which address should it be sent?

e. Should this contract be upgradeable? Argue both sides and state your recommendation.

Difficulty: Advanced–Integrative — combines Solidity design, security, and governance concepts.

Answer Key

Exercise 2:

(a) Transfer: 21,000 $\times$ 25 = 525,000 gwei = 0.000525 ETH = $1.68. Swap: 184,000 $\times$ 25 = 4,600,000 gwei = 0.0046 ETH = $14.72.

(b) At 150 gwei: Transfer: 21,000 $\times$ 150 = 0.00315 ETH = $10.08. Swap: 184,000 $\times$ 150 = 0.0276 ETH = $88.32.

(c) A Uniswap swap involves multiple storage reads/writes, price calculations, token transfers (two ERC-20 contracts), and liquidity pool updates — each operation has a gas cost.

(d) Total: 184,000 $\times$ (22+3) = 4,600,000 gwei = 0.0046 ETH. Burned: 184,000 $\times$ 22 = 4,048,000 gwei = 0.004048 ETH. Validator: 184,000 $\times$ 3 = 552,000 gwei = 0.000552 ETH.

Exercise 3:

(a) A: ERC-20 (fungible, identical units). B: ERC-721 (each watch is unique). C: ERC-1155 (manages both fungible gold and unique swords in one contract).

(b) Soulbound = non-transferable. Advantage: prevents fraud/resale of ownership certificates. Disadvantage: owner cannot resell or transfer the watch without deploying new logic.

(c) Two contracts double deployment cost, require separate approvals, and complicate in-game atomic trades (e.g., swapping gold for a sword in one transaction).

Answer Key (continued)

Exercise 4:

(a) Yes. If only the founding team votes: 3,000,000 / 3,000,000 = 100% $>$ 50%. They pass any proposal unopposed.

(b) Team + VC = 5,500,000. All retail = 2,500,000. Total votes cast = 8,000,000. Team+VC share = 68.75%. Retail cannot outvote them even with 100% turnout.

(c) Options: quadratic voting ($\sqrt{\text{tokens}}$ = vote weight), timelocked voting (must hold tokens for n days), delegate-based voting, quorum requirements ($\geq$40% of supply must vote).

(d) Attacker borrows governance tokens via flash loan, votes to drain treasury, returns tokens — all in one block. Defense: snapshot voting (votes count based on holdings at a past block, not the current one).

Exercise 5:

(a) L1 daily: 10,000 $\times$ \$4 = \$40,000. Optimistic: 10,000 $\times$ \$0.25 = \$2,500, saving \$37,500/day (\$13.7M/yr). ZK: \$1,000/day, saving \$39,000/day (\$14.2M/yr). Sidechain: \$200/day, saving \$39,800/day (\$14.5M/yr).

(b) ZK-rollup: fast finality ($\sim$10 min) + L1 security guarantees are critical for high-value regulated payments. Optimistic rollup's 7-day dispute window is unacceptable for time-sensitive settlements.

(c) A sidechain has its own validator set; if validators collude, funds can be stolen. Regulated institutions require the security guarantees of L1 (Ethereum) backing.

(d) "Inherits L1 security" means the rollup posts data/proofs to Ethereum. Even if the rollup operator disappears, users can reconstruct their state and withdraw from L1. A sidechain has no such fallback.

Answer Key (continued)

Exercise 6:

(a) Expected: 10,000 / 2.00 = 5,000 Token X. Actual: 10,000 / 2.04 $\approx$ 4,902 Token X. Victim receives $\sim$98 fewer tokens (a 1.96% loss).

(b) Searcher buys at 2.00: 5,000 / 2.00 = 2,500 tokens. Sells at 2.06: 2,500 $\times$ 2.06 = \$5,150. Profit $\approx$ \$150 (before gas).

(c) At 0.3% slippage: max acceptable price = 2.00 $\times$ 1.003 = 2.006. The frontrun pushes price to 2.04, which exceeds 2.006. The victim's trade would **revert**, so the sandwich fails.

(d) (1) Use private mempools (e.g., Flashbots Protect) so searchers cannot see pending transactions. (2) Set tight slippage tolerance. (3) Use DEX aggregators with MEV protection (e.g., CowSwap batch auctions).

Exercise 7:

(a) Alpha: \$50,000 $\times$ 0.05% = \$25. Beta: \$50,000 $\times$ 0.30% = \$150.

(b) Alpha: 5-of-9 multisig means compromising 5 signers unlocks \$2B. Beta: requires corrupting a majority of 200 validators, which is harder but the system is less battle-tested.

(c) Attacker ROI scales with TVL. A \$2B bridge offers 25$\times$ the reward of an \$80M bridge, justifying more sophisticated attacks despite stronger audits.

(d) Alpha is recommended for \$50,000: lower fee (\$25 vs. \$150), longer track record (18 months), and multiple Tier-1 audits. The multisig risk is real but manageable for this transfer size.