Exercises: Lesson 3.4 – DeFi, Stablecoins, and Tokenomics

Module 3: The Trust Problem

Prof. Dr. Joerg Osterrieder

Exercise 1: AMM Price Calculations

A constant product AMM pool holds 5,000 ETH and 10,000,000 USDC.

Tasks:

a) What is the constant k? What is the current implied price of 1 ETH?

b) A trader buys 200 ETH from the pool. Calculate the new USDC reserve, the amount of USDC the trader pays, and the effective price per ETH.

c) After the trade in (b), a second trader buys another 200 ETH. Calculate the effective price per ETH for this second trade. Why is it higher than the first trade?

d) Both traders together bought 400 ETH. If instead a single trader bought all 400 ETH in one transaction, what would the effective price per ETH be? Compare with the average of the two sequential trades.

e) A pool charges a 0.3% fee on each trade (deducted from the input token before the swap). Recalculate part (b) with the fee included. How much goes to liquidity providers?

Exercise 2: Impermanent Loss Calculation

A liquidity provider deposits 10 ETH and 20,000 USDC into an AMM pool when ETH = \$2,000.

Impermanent loss formula: $\text{IL} = \frac{2\sqrt{r}}{1+r} - 1$ where $r = P_{\text{new}}/P_{\text{old}}$.

Tasks:

a. What is the initial total value of the LP's position?

b. ETH rises to \$3,000 ($r = 1.5$). Calculate the impermanent loss as a percentage.

c. Convert the percentage from (b) to a dollar loss. What is the LP's pool value vs. the HODL value?

d. The pool earned 1.2% in trading fees during this period. Was providing liquidity profitable compared to holding?

e. ETH drops to \$1,000 ($r = 0.5$). Calculate IL. Is the impermanent loss symmetric for equal-magnitude price moves up and down?

f. At what annual fee yield does the LP break even if ETH price doubles over one year ($r = 2.0$)?

Exercise 3: DeFi Lending and Liquidation

A borrower deposits 20 ETH at \$2,500/ETH as collateral and borrows 25,000 USDC from a lending protocol. The protocol's parameters are:

- Minimum collateralization ratio: 150%
- Liquidation threshold: 130%
- Liquidation bonus: 5%
- Borrow APR: 4%

Tasks:

a. What is the initial collateralization ratio?

b. At what ETH price does the position reach the 150% minimum ratio? At what price is it liquidated (130%)?

c. ETH drops to \$1,700. A liquidator repays 12,500 USDC of the debt. How much ETH does the liquidator receive (including the 5% bonus)?

d. After the partial liquidation in (c), what is the borrower's remaining collateral (in ETH), remaining debt, and new collateralization ratio at \$1,700/ETH?

e. If the borrower had also accumulated 6 months of interest at 4% APR before liquidation, how does the outstanding debt change? Recalculate the liquidation price.

Exercise 4: Flash Loan Arbitrage

An arbitrageur observes that Token X trades at $9.80 on DEX A and $10.20 on DEX B. They execute a flash loan to exploit the spread.

Parameters:

- Flash loan amount: 1,000,000 USDC
- Flash loan fee: 0.09%
- DEX A trading fee: 0.3%
- DEX B trading fee: 0.3%
- Gas cost: $50 per transaction (3 transactions total: borrow, buy, sell/repay)

Tasks:

a. Calculate the flash loan fee in USDC.

b. The trader buys Token X on DEX A. After the 0.3% trading fee, how much USDC actually goes toward purchasing tokens? How many Token X units are acquired?

c. The trader sells all Token X on DEX B. After the 0.3% trading fee, how much USDC is received?

d. Calculate total costs (flash loan fee + gas). What is the net profit or loss?

e. What is the **minimum** price spread between DEX A and DEX B for this arbitrage to be profitable, given these fee parameters?

Exercise 5: Stablecoin Mechanism Comparison

Consider three stablecoins:

- **Coin F:** Fiat-backed, claims 100% reserves in cash and US Treasuries
- **Coin C:** Crypto-backed, requires 150% ETH collateral, liquidation at 130%
- **Coin A:** Algorithmic, uses a mint/burn mechanism with governance token GOV

Tasks:

a) Fill in the comparison table:

Dimension	Coin F	Coin C	Coin A
Decentralization			
Capital efficiency			
Primary de-peg risk			
Regulatory risk			

b) Coin F's quarterly audit reveals only 85% of reserves are in cash/Treasuries; 15% is in commercial paper. Explain the de-peg risk this creates.

c) ETH crashes 50% in one day. Walk through the chain of events for Coin C. Does it survive?

d) During a market panic, Coin A drops to \$0.95. The algorithm mints GOV tokens to buy back Coin A. If GOV is also falling, explain the death spiral mathematically.

Exercise 6: Tokenomics Analysis

A new DeFi protocol launches with the following tokenomics:

- Total supply: 1,000,000,000 tokens
- Distribution: Team 20%, Investors 15%, Community rewards 40%, Treasury 15%, Public sale 10%
- Team vesting: 1-year cliff, then linear over 3 years
- Investor vesting: 6-month cliff, then linear over 2 years
- Community rewards: emitted over 5 years with annual halving

Tasks:

a. How many tokens are in circulation at launch (day 0)? Assume only the public sale tokens are immediately liquid.

b. Calculate the circulating supply at month 6, month 12, and month 24. (Hint: handle each vesting schedule separately.)

c. If the token price at launch is \$0.50, what is the fully diluted valuation (FDV)? What is the market cap based on circulating supply?

d. At month 12, the team cliff unlocks. If 50% of team tokens are sold immediately, what sell pressure (in dollars at \$0.50/token) hits the market?

e. The protocol burns 1% of all trading fees. If daily volume is \$10M and the fee is 0.3%, how many tokens are burned annually (at \$0.50/token)?

Exercise 7: DeFi Attack Analysis

Classify each of the following exploits by attack type (reentrancy, oracle manipulation, flash loan, governance). Then propose one defense for each.

a. An attacker calls a `withdraw()` function that sends ETH before updating the balance. The attacker's contract calls `withdraw()` again in the fallback function, draining $3.6M.

b. An attacker borrows $50M via flash loan, buys a large amount of Token Y on a DEX (moving the price from $5 to $12), then uses Token Y as collateral on a lending protocol (which reads the DEX spot price) to borrow $30M in stablecoins.

c. An attacker flash-borrows 1M governance tokens, creates and votes on a proposal to transfer the protocol's $8M treasury to their address, and returns the tokens — all in one transaction.

d. An attacker monitors the mempool, sees a large buy order on a DEX, and submits a buy order with higher gas to get executed first (sandwich attack). After the victim's trade moves the price up, the attacker sells at the higher price.

Exercise 8: DeFi Risk Assessment

You are advising a university endowment fund considering allocating 2% of its portfolio to DeFi yield farming. The proposed strategy is to provide liquidity to an ETH/USDC AMM pool earning 12% APY in fees plus 8% APY in governance token rewards.

Tasks:

a. List the **five** distinct risk categories the endowment faces (beyond standard market risk). For each, provide a one-sentence description.

b. If ETH moves $\pm 30\%$ over the year, calculate the impermanent loss using the IL formula. Does the 12% fee yield cover it?

c. The 8% reward is paid in the protocol's governance token. If the governance token drops 60% over the year, what is the effective reward in dollar terms?

d. Assuming all risks materialize at moderate severity (ETH -30%, governance token -60%, smart contract exploit probability 5% causing 100% loss), calculate the expected annual return.

e. Would you recommend this allocation? Justify your answer in 3–4 sentences, considering the endowment's risk tolerance and fiduciary duty.

Answer Key (1/3)

Exercise 1:

(a) $k = 5{,}000 \times 10{,}000{,}000 = 5 \times 10^{10}$. Price $= 10{,}000{,}000/5{,}000 = \$2{,}000$/ETH.

(b) New ETH: 4,800. New USDC: $5 \times 10^{10}/4{,}800 = 10{,}416{,}667$. Trader pays: 416,667 USDC. Effective price: $416{,}667/200 = \$2{,}083.33$/ETH.

(c) New ETH: 4,600. New USDC: $5 \times 10^{10}/4{,}600 = 10{,}869{,}565$. Trader pays: $10{,}869{,}565 - 10{,}416{,}667 = 452{,}899$. Effective: \$2,264.49/ETH. Higher because reserves are more depleted (larger slippage).

(d) Single trade of 400: ETH to 4,600, USDC to 10,869,565. Total paid: 869,565. Effective: \$2,173.91/ETH. Average sequential: $(2{,}083.33 + 2{,}264.49)/2 = \$2{,}173.91$. Same total cost (path independent for constant product).

(e) With 0.3% fee: Input after fee $= 416{,}667 \times 0.997 = 415{,}417$ USDC. The fee $= 416{,}667 \times 0.003 = \$1{,}250$ goes to LPs. Actual swap uses 415,417 USDC (LP gets slightly less ETH).

Exercise 2:

(a) $10 \times 2{,}000 + 20{,}000 = \$40{,}000$.

(b) IL $= 2\sqrt{1.5}/(1 + 1.5) - 1 = 2(1.2247)/2.5 - 1 = 0.9798 - 1 = -2.02\%$.

(c) HODL: $10 \times 3{,}000 + 20{,}000 = \$50{,}000$. Pool value: $50{,}000 \times (1 - 0.0202) = \$48{,}990$. Dollar IL: \$1,010.

(d) Fee yield: $40{,}000 \times 0.012 = \$480$. Net: $480 - 1{,}010 = -\$530$. No, not profitable.

(e) $r = 0.5$: IL $= 2\sqrt{0.5}/(1 + 0.5) - 1 = 2(0.7071)/1.5 - 1 = 0.9428 - 1 = -5.72\%$. Not symmetric: $r = 1.5$ gives -2.0% but $r = 0.5$ gives -5.7%.

(f) $r = 2$: IL $= -5.72\%$. Breakeven fee yield $= 5.72\%$ annually.

Answer Key (2/3)

Exercise 3:

(a) Collateral: $20 \times 2{,}500 = \$50{,}000$. Ratio: $50{,}000/25{,}000 = 200\%$.

(b) At 150%: $20P/25{,}000 = 1.5 \Rightarrow P = \$1{,}875$. At 130%: $20P/25{,}000 = 1.3 \Rightarrow P = \$1{,}625$.

(c) Liquidator repays 12,500 USDC. Collateral received $= 12{,}500 \times 1.05/1{,}700 = 7.72$ ETH.

(d) Remaining ETH: $20 - 7.72 = 12.28$ ETH ($= \$20{,}876$). Debt: $25{,}000 - 12{,}500 = \$12{,}500$. Ratio: $20{,}876/12{,}500 = 167\%$.

(e) Interest: $25{,}000 \times 0.04 \times 0.5 = \$500$. New debt: \$25,500. Liquidation: $20P/25{,}500 = 1.3 \Rightarrow P = \$1{,}657.50$.

Exercise 4:

(a) Fee: $1{,}000{,}000 \times 0.0009 = \$900$.

(b) Net buy amount: $1{,}000{,}000 \times 0.997 = 997{,}000$ USDC. Tokens: $997{,}000/9.80 = 101{,}735$ units.

(c) Gross sale: $101{,}735 \times 10.20 = 1{,}037{,}697$. After fee: $1{,}037{,}697 \times 0.997 = 1{,}034{,}586$ USDC.

(d) Costs: $900 + 150 = \$1{,}050$. Gross: $1{,}034{,}586 - 1{,}000{,}000 = 34{,}586$. Net: $34{,}586 - 1{,}050 = \$33{,}536$.

(e) Need gross $>$ costs. Min spread must cover $\approx$0.7% (two $\times$ 0.3% DEX fees + 0.09% flash loan + gas). With $\$1$M, approx spread $> 0.70\%$.

Exercise 5:

(a) Coin F: Low decentralization, high capital eff., reserve fraud risk, high regulatory risk. Coin C: High decentr., low capital eff. (150% locked), collateral crash risk, moderate regulatory risk. Coin A: High decentr., high capital eff., death spiral risk, highest regulatory risk (no reserves).

(b) Holders may doubt redemption at $\$1.00 \rightarrow$ sell below peg $\rightarrow$ arbitrage may not restore confidence if reserves are genuinely insufficient.

(c) 50% ETH crash $\rightarrow$ collateral ratios plunge below 130% $\rightarrow$ mass liquidations sell ETH $\rightarrow$ further price drop $\rightarrow$ cascade. If liquidation mechanisms function and reserves are deep, it survives but with significant bad debt.

(d) At $\$0.95$, protocol mints X GOV tokens worth $\$0.05 \times S$ to buy S stablecoins. If GOV drops 50%, need $2X$ tokens. If GOV drops further, need $4X$, etc. Exponential minting $\rightarrow$ hyperinflation $\rightarrow$ GOV $\rightarrow \$0 \rightarrow$ stablecoin $\rightarrow \$0$.

Answer Key (3/3)

Exercise 6:

(a) Day 0: 10% public sale = 100,000,000 tokens.

(b) Month 6: Public 100M + investor cliff unlocks (15% = 150M, 0 months of linear vesting yet) + community (400M × year-1 emission). Year 1 halving: 50% in Y1 = 200M, so 6/12 = 100M. Total ≈ 350M. Month 12: + team cliff (200M, 0 linear yet) + investor 6 months linear (75M) + community another 100M = 350 + 200 + 75 + 100 = 725M. Month 24: team 12 months of 3-yr linear = 66.7M more, investor fully vested = 75M more, community Y2 = 100M (halved) =≈ 967M.

(c) FDV: $1{,}000{,}000{,}000 \times 0.50 = \$500$M. Market cap: $100{,}000{,}000 \times 0.50 = \$50$M.

(d) Team cliff: $200{,}000{,}000 \times 0.50 \times 0.50 = \$50{,}000{,}000$ sell pressure.

(e) Daily burn: $10{,}000{,}000 \times 0.003 \times 0.01 = \$300$/day. Annual: \$109,500. Tokens: $109{,}500/0.50 = 219{,}000$ tokens/year.

Exercise 7:

(a) **Reentrancy.** Defense: Checks-Effects-Interactions pattern (update balance before sending ETH) or reentrancy guard mutex.

(b) **Oracle manipulation** (flash loan-assisted). Defense: Use TWAP oracle (time-weighted average) instead of spot price.

(c) **Governance attack** (flash loan-assisted). Defense: Snapshot-based voting (use token balances from a past block) and time-locked proposal execution.

(d) **Front-running / sandwich attack.** Defense: Private mempools (Flashbots), maximum slippage settings, commit-reveal order schemes.

Exercise 8:

(a) Smart contract risk, impermanent loss, oracle risk, governance/regulatory risk, liquidity/exit risk.

(b) $r = 0.7$: IL $= 2\sqrt{0.7}/1.7 - 1 = -1.46\%$. $r = 1.3$: IL $= 2\sqrt{1.3}/2.3 - 1 = -0.63\%$. Both covered by 12% fee yield.

(c) Effective reward: $8\% \times (1 - 0.60) = 3.2\%$.

(d) Expected return: $0.95 \times (12\% - 1.5\% + 3.2\%) + 0.05 \times (-100\%) = 0.95 \times 13.7\% - 5\% = 13.0\% - 5.0\% = 8.0\%$.

(e) Not recommended. Despite positive expected return, the 5% probability of total loss is unacceptable for a fiduciary. Endowments prioritize capital preservation; a 5% chance of losing the entire allocation violates prudent investor standards regardless of expected value.