Lesson 3.4 Quiz: DeFi, Stablecoins, and Tokenomics

Module 3: The Trust Problem

Prof. Dr. Joerg Osterrieder

Digital Finance — BSc Course

Question 1

A decentralized exchange uses a constant product AMM with the formula $x \cdot y = k$. A student asks: "What does k represent?" Which answer is **most accurate**?

- (A) The total dollar value of the pool
- (B) The number of liquidity providers in the pool
- (C) A constant that constrains the reserve ratio — the product of the two token reserves must remain unchanged after every trade
- (D) The maximum amount of tokens that can be traded in one transaction

Question 1

A decentralized exchange uses a constant product AMM with the formula $x \cdot y = k$. A student asks: "What does k represent?" Which answer is **most accurate**?

- (A) The total dollar value of the pool
- (B) The number of liquidity providers in the pool
- (C) A constant that constrains the reserve ratio — the product of the two token reserves must remain unchanged after every trade
- (D) The maximum amount of tokens that can be traded in one transaction

Answer: (C) The constant k enforces the invariant that the product of the two reserves (x for token X and y for token Y) remains fixed. Trades increase one reserve and decrease the other while preserving k.

Question 2

An AMM pool holds 500 ETH and 1,000,000 USDC. What is the current implied price of 1 ETH in this pool?

A. $500
B. $1,000
C. $2,000
D. $1,500,000

Question 2

An AMM pool holds 500 ETH and 1,000,000 USDC. What is the current implied price of 1 ETH in this pool?

- (A) $500
- (B) $1,000
- (C) $2,000
- (D) $1,500,000

Answer: (C) The implied price in a constant product AMM is $P = y/x = 1{,}000{,}000/500 = 2{,}000$ USDC per ETH.

Question 3

A liquidity provider deposits equal-value amounts of ETH and USDC into a pool. After one month, ETH has doubled in price. The LP withdraws their position and discovers they have **less value** than if they had simply held the original tokens. What is this phenomenon called?

- A Slippage
- B Impermanent loss
- C Gas fee erosion
- D Front-running

Question 3

A liquidity provider deposits equal-value amounts of ETH and USDC into a pool. After one month, ETH has doubled in price. The LP withdraws their position and discovers they have **less value** than if they had simply held the original tokens. What is this phenomenon called?

- (A) Slippage
- (B) Impermanent loss
- (C) Gas fee erosion
- (D) Front-running

Answer: (B) Impermanent loss is the difference between holding tokens in a pool (where the AMM rebalances) versus holding them in a wallet. When prices diverge, the AMM sells the appreciating token, leaving the LP with less total value.

Question 4

In DeFi lending, why must borrowers deposit **more** collateral than the loan value (overcollateralization)?

A. To pay the gas fees for the smart contract execution

B. Because there are no credit scores, legal enforcement, or identity verification — the collateral is the only guarantee of repayment

C. Because Ethereum requires a minimum deposit to interact with smart contracts

D. To ensure the protocol can afford to pay its developers

Question 4

In DeFi lending, why must borrowers deposit **more** collateral than the loan value (overcollateralization)?

- (A) To pay the gas fees for the smart contract execution
- (B) Because there are no credit scores, legal enforcement, or identity verification — the collateral is the only guarantee of repayment
- (C) Because Ethereum requires a minimum deposit to interact with smart contracts
- (D) To ensure the protocol can afford to pay its developers

Answer: (B) In permissionless, pseudonymous DeFi, there is no credit history, no legal recourse, and no identity verification. Overcollateralization ensures the protocol can seize enough value to cover the loan if the borrower defaults.

Question 5

An AMM pool starts with 2,000 ETH and 4,000,000 USDC ($k = 8 \times 10^9$). A trader buys 100 ETH. How much USDC does the trader pay?

- A 200,000 USDC
- B 210,526 USDC
- C 195,000 USDC
- D 250,000 USDC

Question 5

An AMM pool starts with 2,000 ETH and 4,000,000 USDC ($k = 8 \times 10^9$). A trader buys 100 ETH. How much USDC does the trader pay?

- (A) 200,000 USDC
- (B) 210,526 USDC
- (C) 195,000 USDC
- (D) 250,000 USDC

Answer: (B) After the trade, ETH reserves drop to $2{,}000 - 100 = 1{,}900$. New USDC reserve: $k/1{,}900 = 8 \times 10^9/1{,}900 = 4{,}210{,}526$ USDC. Trader pays: $4{,}210{,}526 - 4{,}000{,}000 = 210{,}526$ USDC. The effective price is $\approx$\$2,105/ETH (vs. the initial \$2,000), demonstrating slippage.

Question 6

Using the impermanent loss formula $\text{IL} = \frac{2\sqrt{r}}{1+r} - 1$ where r is the price ratio (new/old), calculate the impermanent loss when ETH price **triples** ($r = 3$).

- A -5.7%
- B -13.4%
- C -25.0%
- D -33.3%

Question 6

Using the impermanent loss formula $\text{IL} = \frac{2\sqrt{r}}{1+r} - 1$ where r is the price ratio (new/old), calculate the impermanent loss when ETH price **triples** ($r = 3$).

- (A) -5.7%
- (B) -13.4%
- (C) -25.0%
- (D) -33.3%

Answer: (B) $\text{IL} = \frac{2\sqrt{3}}{1+3} - 1 = \frac{2 \times 1.732}{4} - 1 = \frac{3.464}{4} - 1 = 0.866 - 1 = -0.134 = -13.4\%$. A 3x price change costs the LP 13.4% compared to simply holding.

Question 7

A borrower deposits 10 ETH at $1,800/ETH as collateral and borrows 10,000 USDC. What is the current collateralization ratio?

- (A) 100%
- (B) 120%
- (C) 150%
- (D) 180%

Question 7

A borrower deposits 10 ETH at \$1,800/ETH as collateral and borrows 10,000 USDC. What is the current collateralization ratio?

- (A) 100%
- (B) 120%
- (C) 150%
- (D) 180%

Answer: (D) Collateral value: $10 \times 1{,}800 = \$18{,}000$. Debt: \$10,000. Ratio: $18{,}000/10{,}000 = 180\%$.

Question 8

In the scenario from Question 7, the protocol liquidates positions when the ratio falls to 120%. At what ETH price is the position liquidated?

- A $1,000
- B $1,200
- C $1,500
- D $1,800

Question 8

In the scenario from Question 7, the protocol liquidates positions when the ratio falls to 120%. At what ETH price is the position liquidated?

- (A) $1,000
- (B) $1,200
- (C) $1,500
- (D) $1,800

Answer: (B) Liquidation occurs when $10 \times P/10{,}000 = 1.20$, so $P = 1.20 \times 10{,}000/10 = \$1{,}200$. When ETH drops to $1,200, the collateral is worth $12,000 against $10,000 debt — exactly the 120% threshold.

Question 9

A trader executes the following flash loan arbitrage: borrow 500,000 USDC (0.09% fee), buy ETH at $1,980 on DEX A, sell ETH at $2,000 on DEX B. What is the approximate profit?

- (A) $5,050 (loss)
- (B) $4,601
- (C) $10,000
- (D) $0 (exactly break even)

Question 9

A trader executes the following flash loan arbitrage: borrow 500,000 USDC (0.09% fee), buy ETH at $1,980 on DEX A, sell ETH at $2,000 on DEX B. What is the approximate profit?

- (A) $5,050 (loss)
- (B) $4,601
- (C) $10,000
- (D) $0 (exactly break even)

Answer: (B) ETH bought: $500{,}000/1{,}980 = 252.53$ ETH. Sold: $252.53 \times 2{,}000 = 505{,}051$ USDC. Flash loan fee: $500{,}000 \times 0.0009 = 450$ USDC. Repay: $500{,}000 + 450 = 500{,}450$. Profit: $505{,}051 - 500{,}450 = \$4{,}601$.

Question 10

A protocol uses a DEX spot price as its oracle. An attacker executes a large buy on the DEX, temporarily pushing the price of Token X from $10 to $15. The attacker then uses Token X as collateral on the victim protocol (which reads $15) to borrow assets. This is an example of:

- A reentrancy attack
- A governance attack
- Oracle manipulation
- A Sybil attack

Question 10

A protocol uses a DEX spot price as its oracle. An attacker executes a large buy on the DEX, temporarily pushing the price of Token X from \$10 to \$15. The attacker then uses Token X as collateral on the victim protocol (which reads \$15) to borrow assets. This is an example of:

- (A) A reentrancy attack
- (B) A governance attack
- (C) Oracle manipulation
- (D) A Sybil attack

Answer: (C) This is oracle manipulation: the attacker artificially moves the price on the oracle source (the DEX) to inflate the value of their collateral on the victim protocol, enabling them to borrow more than the true collateral value justifies.

Question 11

A smart contract has a `withdraw()` function with this order: (1) check balance, (2) send ETH, (3) update balance. An auditor identifies this as vulnerable. What pattern should replace it?

- A. Send ETH first, then check balance, then update balance
- B. Check balance, update balance, then send ETH (Checks-Effects-Interactions)
- C. Remove the balance check entirely and rely on the EVM's built-in protection
- D. Add a second `withdraw()` function as a backup

Question 11

A smart contract has a `withdraw()` function with this order: (1) check balance, (2) send ETH, (3) update balance. An auditor identifies this as vulnerable. What pattern should replace it?

- (A) Send ETH first, then check balance, then update balance
- (B) Check balance, update balance, then send ETH (Checks-Effects-Interactions)
- (C) Remove the balance check entirely and rely on the EVM's built-in protection
- (D) Add a second `withdraw()` function as a backup

Answer: (B) The Checks-Effects-Interactions pattern mandates: (1) check conditions, (2) update state (effects), (3) make external calls (interactions). By updating the balance *before* sending ETH, a reentrancy callback will find the balance already set to zero.

Question 12

A protocol uses a time-weighted average price (TWAP) oracle instead of a DEX spot price. Why does this make oracle manipulation **more expensive** for the attacker?

- (A) TWAP oracles are encrypted, so the attacker cannot read the price
- (B) TWAP averages the price over multiple blocks, so the attacker must sustain the price distortion over time, which requires holding a large position across blocks and paying opportunity cost
- (C) TWAP oracles only report prices once per day, making them too slow to attack
- (D) TWAP uses a different blockchain with higher security

Question 12

A protocol uses a time-weighted average price (TWAP) oracle instead of a DEX spot price. Why does this make oracle manipulation **more expensive** for the attacker?

(A) TWAP oracles are encrypted, so the attacker cannot read the price

(B) TWAP averages the price over multiple blocks, so the attacker must sustain the price distortion over time, which requires holding a large position across blocks and paying opportunity cost

(C) TWAP oracles only report prices once per day, making them too slow to attack

(D) TWAP uses a different blockchain with higher security

Answer: (B) A spot price can be manipulated within a single transaction (via flash loan). A TWAP averages prices over N blocks (e.g., 30 minutes). To distort the TWAP, the attacker must maintain the manipulated price for the entire averaging window, tying up capital and bearing price risk — far more costly than a single-transaction attack.

Question 13

Compare a fiat-backed stablecoin and a crypto-backed stablecoin. Which statement **best** characterizes their trade-off?

- (A) Fiat-backed is decentralized; crypto-backed is centralized
- (B) Fiat-backed requires trust in the issuer's reserves; crypto-backed requires trust in the collateral's price stability and the liquidation mechanism
- (C) Both types have identical risk profiles because they both target $1.00
- (D) Crypto-backed stablecoins cannot de-peg because the collateral is on-chain

Question 13

Compare a fiat-backed stablecoin and a crypto-backed stablecoin. Which statement **best** characterizes their trade-off?

(A) Fiat-backed is decentralized; crypto-backed is centralized

(B) Fiat-backed requires trust in the issuer's reserves; crypto-backed requires trust in the collateral's price stability and the liquidation mechanism

(C) Both types have identical risk profiles because they both target $1.00

(D) Crypto-backed stablecoins cannot de-peg because the collateral is on-chain

Answer: (B) Fiat-backed stablecoins depend on the issuer actually holding the claimed reserves (centralized trust). Crypto-backed stablecoins are trustless on-chain but depend on the collateral maintaining sufficient value and the liquidation mechanism functioning correctly during market stress.

Question 14

An algorithmic stablecoin maintains its peg by minting a governance token when the stablecoin trades below $1.00 and burning the governance token when it trades above $1.00. During a confidence crisis, holders sell the stablecoin *and* the governance token simultaneously. Why does this create a death spiral?

- A. The smart contract runs out of gas and cannot process transactions
- B. The algorithm mints more governance tokens to absorb selling, but the governance token is also crashing — so more tokens are needed, which accelerates the crash
- C. The blockchain network becomes congested and stops producing blocks
- D. The algorithm cannot detect that both tokens are falling simultaneously

Question 14

An algorithmic stablecoin maintains its peg by minting a governance token when the stablecoin trades below $1.00 and burning the governance token when it trades above $1.00. During a confidence crisis, holders sell the stablecoin *and* the governance token simultaneously. Why does this create a death spiral?

- (A) The smart contract runs out of gas and cannot process transactions
- (B) The algorithm mints more governance tokens to absorb selling, but the governance token is also crashing — so more tokens are needed, which accelerates the crash
- (C) The blockchain network becomes congested and stops producing blocks
- (D) The algorithm cannot detect that both tokens are falling simultaneously

Answer: (B) The stabilization mechanism depends on the governance token absorbing sell pressure. When the governance token itself loses value, the algorithm must mint exponentially more tokens to absorb the same dollar amount of selling. This hyperinflation of the governance token destroys confidence further, creating a self-reinforcing downward spiral.

Question 15

A DeFi lending protocol experiences a flash crash in ETH. Within 10 minutes, the collateralization ratio of 40% of all loans drops below the liquidation threshold. Why can this cascade cause protocol insolvency even with overcollateralization?

- **A** The protocol runs out of governance tokens to compensate liquidators
- **B** Mass liquidations sell large amounts of ETH into thin markets, driving the price further down, which triggers more liquidations — a positive feedback loop that can exhaust the collateral faster than liquidators can process
- **C** The smart contract has a hard limit on the number of liquidations per block
- **D** Liquidators are required to wait 24 hours before seizing collateral

Question 15

A DeFi lending protocol experiences a flash crash in ETH. Within 10 minutes, the collateralization ratio of 40% of all loans drops below the liquidation threshold. Why can this cascade cause protocol insolvency even with overcollateralization?

- (A) The protocol runs out of governance tokens to compensate liquidators
- (B) Mass liquidations sell large amounts of ETH into thin markets, driving the price further down, which triggers more liquidations — a positive feedback loop that can exhaust the collateral faster than liquidators can process
- (C) The smart contract has a hard limit on the number of liquidations per block
- (D) Liquidators are required to wait 24 hours before seizing collateral

Answer: (B) Liquidation cascades create a positive feedback loop: collateral is sold $\rightarrow$ price drops $\rightarrow$ more positions breach the threshold $\rightarrow$ more collateral sold. If the price drops faster than liquidators can execute, some positions become undercollateralized (debt exceeds collateral), leaving the protocol with bad debt.

Question 16

A protocol distributes 60% of its token supply to insiders (team + investors) with a 1-year cliff followed by 3-year linear vesting. At month 12, all insider tokens become eligible simultaneously. What risk does this create?

- A The protocol will run out of tokens for community incentives
- B A large supply shock: insiders may sell simultaneously, creating downward price pressure exactly at the cliff date
- C The smart contract cannot process the vesting unlock and will freeze
- D The tokens become worthless because they were locked too long

Question 16

A protocol distributes 60% of its token supply to insiders (team + investors) with a 1-year cliff followed by 3-year linear vesting. At month 12, all insider tokens become eligible simultaneously. What risk does this create?

- (A) The protocol will run out of tokens for community incentives
- (B) A large supply shock: insiders may sell simultaneously, creating downward price pressure exactly at the cliff date
- (C) The smart contract cannot process the vesting unlock and will freeze
- (D) The tokens become worthless because they were locked too long

Answer: (B) A vesting cliff creates a concentrated supply event: a large block of previously illiquid tokens becomes liquid simultaneously. If insiders sell, the sudden supply increase can overwhelm demand and crash the price. Savvy investors often sell *before* the cliff in anticipation.

Question 17

Total value locked (TVL) is the most common metric for DeFi protocol size. A critic argues that TVL is misleading. Which of the following **best** supports this critique?

- TVL does not account for the protocol's token price
- Recursive borrowing (deposit $\rightarrow$ borrow $\rightarrow$ re-deposit) inflates TVL because the same dollar of capital is counted multiple times
- TVL only measures Ethereum-based protocols, excluding other blockchains
- TVL does not include NFTs, which are a major DeFi asset class

Question 17

Total value locked (TVL) is the most common metric for DeFi protocol size. A critic argues that TVL is misleading. Which of the following **best** supports this critique?

- (A) TVL does not account for the protocol's token price
- (B) Recursive borrowing (deposit → borrow → re-deposit) inflates TVL because the same dollar of capital is counted multiple times
- (C) TVL only measures Ethereum-based protocols, excluding other blockchains
- (D) TVL does not include NFTs, which are a major DeFi asset class

Answer: (B) Recursive borrowing (also called "looping") allows the same capital to appear in TVL multiple times. For example, depositing $100M, borrowing $70M, and re-depositing creates $170M in TVL from only $100M of real capital. This double-counting inflates the apparent size of DeFi.

Question 18

An entrepreneur proposes building a "fully decentralized" lending protocol that also complies with KYC/AML regulations by requiring identity verification before depositing. Evaluate this proposal. What is the **most fundamental** contradiction?

A. KYC is too expensive for a startup

B. Requiring identity verification introduces a centralized gatekeeper, which contradicts the permissionless nature of DeFi — someone must verify identities, store data, and enforce access, recreating the intermediary that DeFi aims to eliminate

C. KYC slows down transaction speed below what blockchain can support

D. Regulators will not approve any lending protocol on a public blockchain

Question 18

An entrepreneur proposes building a "fully decentralized" lending protocol that also complies with KYC/AML regulations by requiring identity verification before depositing. Evaluate this proposal. What is the **most fundamental** contradiction?

- (A) KYC is too expensive for a startup
- (B) Requiring identity verification introduces a centralized gatekeeper, which contradicts the permissionless nature of DeFi — someone must verify identities, store data, and enforce access, recreating the intermediary that DeFi aims to eliminate
- (C) KYC slows down transaction speed below what blockchain can support
- (D) Regulators will not approve any lending protocol on a public blockchain

Answer: (B) The core value proposition of DeFi is permissionless access. KYC requires a trusted entity to verify and store identities — this is, by definition, an intermediary. The protocol may use smart contracts for execution, but it is no longer "fully decentralized" if access depends on a centralized identity provider.

Question 19

A DeFi protocol proposes allowing governance token holders to vote on increasing the liquidation bonus from 5% to 15%. Supporters argue this attracts more liquidators. Evaluate the **most significant** unintended consequence.

- A Higher bonuses make liquidation more attractive, but they also punish borrowers more severely, potentially discouraging new borrowers and reducing protocol usage
- B Higher bonuses will crash the governance token price
- C Higher bonuses make the protocol immune to liquidation cascades
- D The smart contract cannot support a bonus above 10%

Question 19

A DeFi protocol proposes allowing governance token holders to vote on increasing the liquidation bonus from 5% to 15%. Supporters argue this attracts more liquidators. Evaluate the **most significant** unintended consequence.

(A) Higher bonuses make liquidation more attractive, but they also punish borrowers more severely, potentially discouraging new borrowers and reducing protocol usage

(B) Higher bonuses will crash the governance token price

(C) Higher bonuses make the protocol immune to liquidation cascades

(D) The smart contract cannot support a bonus above 10%

Answer: (A) A higher liquidation bonus incentivizes liquidators but also means borrowers lose more in a liquidation event. This makes borrowing riskier and more punitive, potentially driving borrowers to competing protocols with lower penalties. The optimal bonus balances liquidator incentives against borrower protection.

Question 20

A regulator proposes classifying all stablecoins as securities and requiring issuers to maintain 100% reserves in government bonds. Evaluate the impact on the three stablecoin types. Which type faces the **most existential** threat from this regulation?

- (A) Fiat-backed — they would need to restructure their reserves
- (B) Crypto-backed — they would need to replace crypto collateral with government bonds
- (C) Algorithmic — they have no reserves at all, and their stabilization mechanism is incompatible with the reserve requirement, making compliance structurally impossible
- (D) All three face equal risk because the regulation applies uniformly

Question 20

A regulator proposes classifying all stablecoins as securities and requiring issuers to maintain 100% reserves in government bonds. Evaluate the impact on the three stablecoin types. Which type faces the **most existential** threat from this regulation?

- (A) Fiat-backed — they would need to restructure their reserves
- (B) Crypto-backed — they would need to replace crypto collateral with government bonds
- (C) Algorithmic — they have no reserves at all, and their stabilization mechanism is incompatible with the reserve requirement, making compliance structurally impossible
- (D) All three face equal risk because the regulation applies uniformly

Answer: (C) Fiat-backed stablecoins could adapt (they already hold similar reserves). Crypto-backed stablecoins would require fundamental redesign but could theoretically comply. Algorithmic stablecoins, by design, have no reserves — they maintain the peg through supply/demand mechanisms. A 100% reserve requirement would eliminate their entire operating model.