Lesson 3.4 Quiz: DeFi, Stablecoins, and Tokenomics

Module 3: The Trust Problem

Prof. Dr. Joerg Osterrieder

Digital Finance — BSc Course (v2026.05)

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

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

[Answer hidden – compile with \solutionstrue to reveal]

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 $1,000
- B $1,500,000
- C $2,000
- D $500

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

[Answer hidden – compile with \solutionstrue to reveal]

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

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

[Answer hidden – compile with \solutionstrue to reveal]

Question 4

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

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

Question 4

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

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

[Answer hidden – compile with \solutionstrue to reveal]

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 hidden – compile with \solutionstrue to reveal]

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

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

[Answer hidden – compile with \solutionstrue to reveal]

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 150%
- B 180%
- C 100%
- D 120%

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 150%
- B 180%
- C 100%
- D 120%

[Answer hidden – compile with \solutionstrue to reveal]

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

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

[Answer hidden – compile with \solutionstrue to reveal]

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

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

[Answer hidden – compile with \solutionstrue to reveal]

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. Oracle manipulation
- B. A Sybil attack
- C. A governance attack
- D. A reentrancy 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. Oracle manipulation
- B. A Sybil attack
- C. A governance attack
- D. A reentrancy attack

[Answer hidden – compile with \solutionstrue to reveal]

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

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

[Answer hidden – compile with \solutionstrue to reveal]

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 uses a different blockchain with higher security
- B. TWAP oracles only report prices once per day, making them too slow to attack
- C. 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
- D. TWAP oracles are encrypted, so the attacker cannot read the price

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 uses a different blockchain with higher security
- B. TWAP oracles only report prices once per day, making them too slow to attack
- C. 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
- D. TWAP oracles are encrypted, so the attacker cannot read the price

[Answer hidden – compile with \solutionstrue to reveal]

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. Crypto-backed stablecoins cannot de-peg because the collateral is on-chain
- D. Both types have identical risk profiles because they both target $1.00

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. Crypto-backed stablecoins cannot de-peg because the collateral is on-chain
- D. Both types have identical risk profiles because they both target $1.00

[Answer hidden – compile with \solutionstrue to reveal]

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

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

[Answer hidden – compile with \solutionstrue to reveal]

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 smart contract has a hard limit on the number of liquidations per block
- (B) The protocol runs out of governance tokens to compensate liquidators
- (C) Liquidators are required to wait 24 hours before seizing collateral
- (D) 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

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 smart contract has a hard limit on the number of liquidations per block
- B The protocol runs out of governance tokens to compensate liquidators
- C Liquidators are required to wait 24 hours before seizing collateral
- D 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

[Answer hidden – compile with \solutionstrue to reveal]

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

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

[Answer hidden – compile with \solutionstrue to reveal]

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

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

[Answer hidden – compile with \solutionstrue to reveal]

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. KYC slows down transaction speed below what blockchain can support
- C. Regulators will not approve any lending protocol on a public blockchain
- D. 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

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. KYC slows down transaction speed below what blockchain can support
- C. Regulators will not approve any lending protocol on a public blockchain
- D. 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

[Answer hidden – compile with \solutionstrue to reveal]

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

[Answer hidden – compile with \solutionstrue to reveal]

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

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

[Answer hidden – compile with \solutionstrue to reveal]