DeFi Course — Exam Training Exercises

There is at most 1 right answer for the multiple choice questions. There is a penalty of -1 points if an answer is incorrect, therefore, please only provide an answer if you are certain about your choice. No answer corresponds to 0 points.

1 Decentralized Exchange

a As an integral part of the decentralized finance (DeFi) ecosystem, Decentralized Exchanges (DEX) with Automated Market Maker (AMM) protocols have gained significant traction with the recently revived interest in blockchain.

i) Which of the following is NOT a property for a typical on-chain order book market?

A) Censorship resistance

B) Front-running resistance

C) No impermanent loss

D) Non-custodial settlement

ii) Which of the following is **NOT** a DeFi market manipulation activity?

A) Front-/back-running

B) Sandwich attack

C) Re-entrancy attack

D) Price oracle manipulation

iii) Which of the following statement is incorrect?

A) Expected price slippage is the anticipated rise or decrease in price depending on the amount to be exchanged and the available liquidity.

B) The expected slippage decreases as trading volume increases.

C) Unexpected price slippage is the rise or decrease in price during the time between creating a transaction and its execution.

D) The sum of the expected and unexpected slippage represents the price impact of a trade.

iv) Could you briefly describe two advantages and two disadvantages of using an AMM?

b i) Bob wants to swap dx amount of X token for dy amount of Y tokens in a liquidity pool. Suppose the current supply of token X and Y in the pool are Sx and Sy, and there is no trading fee. Please derive dy using the constant product market maker as the pricing formula.

ii) Assume Bob supplies 10 ETH and 1000 DAI to create a Sushiswap $50/50$ ETH–DAI pool and he is the only liquidity provider for this pool. Initially, ETH is worth \$100 USD (1 ETH=100 DAI). At some point, the price of ETH increases to \$200 USD (1 ETH=200 DAI). Then the arbitrageurs from outside of Sushiswap exploit this opportunity to buy all the ETH in Bob's pool until the price reaches 200 DAI and matches external exchanges. Please calculate Bob's impermanent loss based on the constant market maker pricing formula, rounding your result to 2 decimal places.

The two parts carry, respectively, 40% and 60% of the marks.

2 DeFi Security

a Security is a very important aspect in the DeFi ecosystem.

i) What system layers does DeFi security affect?

ii) Indicate whether the statement is true (T) or false (F). Each wrong answer is penalized by 0.4 points.

A) Assume that all miners in the Ethereum network order blocks by gas price and do not collaborate with relayer service. An attacker needs to pay a gas price of $p - 1$ to back-run a victim transaction with a gas price of p.

B) MEV (DeFi application layer) is a concern for blockchain consensus because miners can censor other MEV searchers and instead extract MEV themselves, which is unfair.

C) Eclipse attack can lead to double-spending.

D) An attacker can only front-run, but it is hard to back-run victim transactions.

E) A BEV relay system doesn't necessarily reduce P2P overhead.

F) A BEV relayer does not centralize the P2P Network.

G) Eclipse attack cannot lead to network-wide Denial of Service.

H) Dynamic analysis of smart contracts provides strong guarantees but many false positives.

I) When slippage tolerance is very low, sandwich attacks are more difficult to perform.

J) In the replay attack, the adversary observes transactions in the blockchain layer.

b Flash loan attack.

i) What is a flash loan?

ii) Describe the steps for performing a Pump and Arbitrage Attack using a flash loan; given two decentralized exchanges, DEX1 and DEX2, that one can trade ETH for WBTC and WBTC for ETH. A margin trade provider MTP that can be used to put short positions (i.e., profit if the value of an asset falls). A Lending protocol LPF that can provide a flash loan of ETH, and another Lending protocol that provides over collateralized loans LPO (e.g. collateralize ETH and borrow WBTC). What is the cost for the attacker? You need to describe the steps and not provide exact values.

c Sandwich attack and BEV.

i) Describe the steps of a sandwich attack, given a transaction T_v that exchanges X for Y. What could one do to minimize the risk? What knowledge does the adversary need to have to perform such an attack, and how he can get it.

ii) What is a BEV Relayer?

iii) Mention three possible anti-MEV mitigations. Would they be able also to prevent cross-chain MEV?

The three parts carry, respectively, 35%, 30%, and 35% of the marks.