DeFi Talents

Organized by

Frankfurt School Blockchain Center

Web3 Talents

Powered by

KFW

INNO LAB

Deka

DATENSERVICE

dwpbank

Supported by

DEC INSTITUTE

DCA

MAMA

ECOTA

Assignment 3

December 2, 2024

By

Manjiri Birajdar

Software Developer

Assignment

Practical: Swap tokens on Uniswap. You can use a testnet like Ethereum Sepolia or Arbitrum Sepolia, OP Sepolia.

Hints:

- What is Sepolia Testnet and How to Get Sepolia ETH From Faucets | CoinGecko
- SepoliaETH Faucet - Ethereum Sepolia Testnet | Bitbond
- Introducing the Amoy Testnet for Polygon PoS

1. **Create a categorization of DEXs with the following two dimensions**
    a. spot vs. derivatives
    b. AMM vs order-book
2. **What changes does Uniswap's Unichain aim to bring to the table?**
3. **What are the risks associated with DEXs?**
    a. For liquidity providers (LPs)
    b. For traders who engage in token swaps?
    c. What is "impermanent loss" and how is it different from (price) slippage?
    d. Explain a sandwich attack in the context of an AMM trade
    e. Read this article - What went wrong? What should the user have done?
4. **What is the significance of cross-chain DEXs and DEX aggregators?**

DEX Categorization: Spot vs. Derivatives

Spot DEXs	Derivatives DEXs
Trades actual assets at real-time prices (e.g., Uniswap)	Trades financial contracts (e.g., dYdX)
Better for regular trading	Used for leverage trading and hedging

DYOR!

DEX Categorization: AMM vs. Order-Book

AMM DEXs	Order-Book DEXs
Uses liquidity pools (e.g., Uniswap)	Matches buyers and sellers (e.g., Loopring)
Better for passive liquidity	More suited for professional traders

DYOR!

Uniswap’s Unichain: Key Innovations

- Scalability: Optimized transactions with lower costs
- Security Enhancements: Improved resilience against exploits
- Seamless Cross-Chain Interoperability: Enhancing connectivity

DYOR!

Risks for Liquidity Providers (LPs)

- Impermanent Loss: Price fluctuations affect LPs' earnings
- Smart Contract Vulnerabilities: Bugs may lead to losses
- Liquidity Drain Risks: Large withdrawals impact LP returns

DYOR!

Risks for Traders in Token Swaps

- Price Slippage: Trade execution price differs from expected
- Front-Running Attacks: Malicious bots manipulate prices
- Hidden Fees & Gas Costs: High fees reduce profitability

DYOR!

Impermanent Loss vs. Price Slippage

Impermanent Loss	Price Slippage
refers to the potential loss incurred when the price of deposited assets changes compared to holding them outside the pool.	refers to the discrepancy between the expected and executed trade prices, often due to market volatility or low liquidity.
Affects Liquidity Providers	Affects traders executing swaps
Loss due to asset fluctuation in pools	Price difference due to liquidity changes

DYOR!

Sandwich Attack in AMM Trades

- Front-run: Attacker buys before victim’s trade to raise price
- Victim's trade executes at inflated price
- Back-run: Attacker sells for profit after execution
- Impact: Victim gets unfavorable pricing

DYOR!

Case Study Analysis: USDC Investor's $2 Million Loss

What Went Wrong?

1. **Improper Trade Execution:** The user attempted to swap **$2 million USDC for USDT** but used **3CRV LP tokens**, leading to a significant loss.
2. **Slippage Oversight:** The user **did not set a slippage tolerance**, allowing the transaction to execute at an extremely unfavorable rate.
3. **Liquidity Pool Misunderstanding:** Instead of withdrawing USDC from the pool before swapping, the user **traded LP tokens directly**, leading to major inefficiencies.
4. **MEV Bot Exploitation:** Maximal Extractable Value (MEV) bots **detected the large, poorly configured trade and front-ran it**, capturing most of the value.

What Should the User Have Done?

✅ **Withdraw USDC from the Liquidity Pool First** – Instead of swapping LP tokens directly, the user should have exited the 3CRV liquidity pool to get USDC first.

✅ **Set a Reasonable Slippage Limit** – Always configure a slippage tolerance (e.g., **0.5%-1%**) to prevent massive price differences in execution.

✅ **Use Private Transactions or MEV Protection** – Platforms like **Flashbots Protect or MEV-resistant DEXs** can reduce risks from front-running attacks.

✅ **Break Up Large Trades** – Instead of executing a single **$2M swap**, the user should have **split the trade into smaller portions** to minimize price impact.

✅ **Check Market Liquidity Before Executing Large Orders** – Always ensure there's sufficient liquidity on the DEX or use **DEX aggregators** to get better pricing.

This case highlights the importance of **risk management, strategic trade execution, and understanding DeFi mechanics** to prevent costly mistakes. 🚨

Constant sum (CSMM)

Constant sum (CSMM) :

Formula: demand_x * (y_pool / x_pool)

1. USDT pool contains 10, ETH pool contains 3. Alice demands 1 ETH, how much USDT does she have to pay?
   Answer: `3.3333333333333335`

2. DAI pool contains 52501, ETH pool contains 2500. Bob demands 120 ETH, how much DAI does he have to pay?
   Answer: `2520.048`

DYOR!

Constant product (CPMM)

Constant product (CPMM) :

Formula:

k = x_pool * y_pool
new_y_pool = y_pool - demand_x
new_x_pool = k / new_y_pool
alice_usdt_payment_cpmm = new_x_pool - x_pool

1. USDT pool contains 1000, ETH pool contains 3. Alice demands 1 ETH, how much USDT does she have to pay?
   Answer: `0.0030030030030028243`

2. Bob has to pay 50 LINK to obtain 10 ETH, the ETH pool contains 40 after the transaction. How large was the LINK pool before the transaction? How large was it afterward?
   Answer:
   ```
   LINK pool before transaction: 40.0
   LINK pool after transaction: -10.0
   ```

Constant function (CFMM)

Constant function (CFMM)

Formula:

k_initial = x**2 + 5*y
x_new = x - demand_x
y_new = (k_initial - x_new**2) / 5
cfmm_price_X_eth = y - y_new

1. The function for k is k(y,x) = x^2 + 5y. What is the price for 1 ETH if the ETH pool (x) contains 250 and the USDT pool contains 2500?
   Answer: `CFMM price for 1 ETH: -99.80000000000018`

2. The function for k is k(y,x) = x^2 + 5y. What is the price for 3 ETH if the ETH pool (x) contains 250 and the USDT pool contains 2500?
   Answer: `CFMM price for 3 ETH: -298.1999999999998`

Constant product (CPMM)

Calculations based on constant product (CPMM) mechanics. What do you observe?

Initial situation: 100 ETH and 20,000 DAI → CP = 2,000,000

ETH Purchased	Cost per ETH traded DAI	Total Cost in DAI	Premium	New DAI Liquidity	New ETH liquidity	Constant Product
1	202.02	202.02	1.01%	20,202.02	99	2,000,000
5	210.53	1,052.63	5.26%	21,052.63	95	2,000,000
10	222.22	2,222.22	11.11%	22,222.22	90	2,000,000
50	400.00	20,000.00	100.00%	40,000.00	50	2,000,000
75	800.00	60,000.00	300.00%	80,000.00	25	2,000,000
99	20,000.00	1,980,000.00	9,900.00%	2,000,000.00	1	2,000,000
100					0	2,000,000

References

https://en.wikipedia.org/wiki/Constant_function_market_maker

https://www.axios.com/2024/09/04/uniswap-labs-regulators-cftc

https://en.wikipedia.org/wiki/Decentralized_finance

https://cointelegraph.com/news/usdc-investor-shells-out-2m-to-receive-0-05-usdt-trying-to-evade-crash