Blockchain (BlCh)

CEX/DEX

Thomas Bocek

17.10.2025

Learning Goals

- Lecture 8
  - Knowledge
    -
    -
  - Skills
    -
   -
  - Application
    -

OST

CEX: Exchange Rate

- Centralized (CEX): ask/bid, sell/buy, the last trade, e.g., 200 DAI for 1 ETH → price (order book)

  - Workflow: create order, publish on exchange, wait to get filled. Browse orders, start fill order.

  - Prince changes if trade happens, ask was same or lower than bid. Ask/bid submitted by users – add/remove orders

  - Slippage: you see a price, submit, and until its executed, price can change.
    - Set limits, order may stay in the orderbook

- Decentralized (DEX): ratio of pairs (automatic market making)

  - Workflow: exchange pairs

  - Example amount in pool: DAI 200, ETH 1 → price 200DAI/1ETH

- Both: large swap can change price → price impact

Price(USDT)	Amount(BTC)	Total
63239.97	0.44255	27,986.84872
63239.96	0.36276	22,940.92789
63238.74	0.07300	4,616.42802
63238.65	0.10230	6,469.31390
63237.52	0.07800	4,932.52656
63237.00	0.01493	944.12841
63236.98	0.06168	3,900.45693
63235.57	0.10038	6,347.58652
63233.64	0.04732	2,992.21584
63232.60	0.01429	903.59385
63232.40	0.10459	6,613.47672
63232.39	0.06168	3,900.17382
63231.49	0.01791	1,132.47599
63231.48	0.16768	10,602.65457
63231.47	0.15867	10,032.93734
63227.71	0.16472	10,414.86839
63227.70	0.69732	44,089.93976

63,227.69 ↓ $63,227.69   More

Price(USDT)	Amount(BTC)	Total
63227.69	0.09446	5,972.48760
63227.68	0.07903	4,996.88355
63225.08	0.00367	232.03604
63223.01	0.06710	4,242.26397
63222.59	0.02300	1,454.11957
63222.20	0.11855	7,494.99181
63222.00	0.02000	1,264.44000
63221.00	0.11908	7,528.35668
63220.88	0.00074	46.78345
63220.65	1.56572	98,985.83612
63220.15	0.00237	149.83176
63220.00	3.92240	247,974.12800
63219.84	0.00032	20.23035
63218.21	0.04054	2,562.86623
63217.98	0.10230	6,467.19935
63216.80	0.00032	20.22938
63216.60	0.08410	5,316.51606

DEX: Exchange Rate / Decentralized Swaps

- DEX uses X * Y = k, where k is constant, X and Y are asset values (if you take out X you need to provide Y)

  - DAI = 200, ETH = 1, k = 200

- Constant function market makers (CFMM)

  - "We are still very early in the evolution of constant function market makers..." [ref]

- Exchange price calculation (X * Y = k) → X * Y = (X + x) * (Y - y)

  - Swap for 0.5 ETH, if you send 0.5 ETH to pool
    - 200 * 0.5 / (1+0.5) = 66
    - 66/0.5 → 133 DAI → ~**133 DAI for 1 ETH**

  - Deduct 66 DAI from pool, add 0.5 ETH → 133/1.5 → ~ **88 DAI for 1 ETH**
    - K = 133.333 * 1.5 = 200
    - Never draining the pool
    - Trade with better price than resulting pool (huge price impact)

$$y = \frac{Yx}{X + x}$$
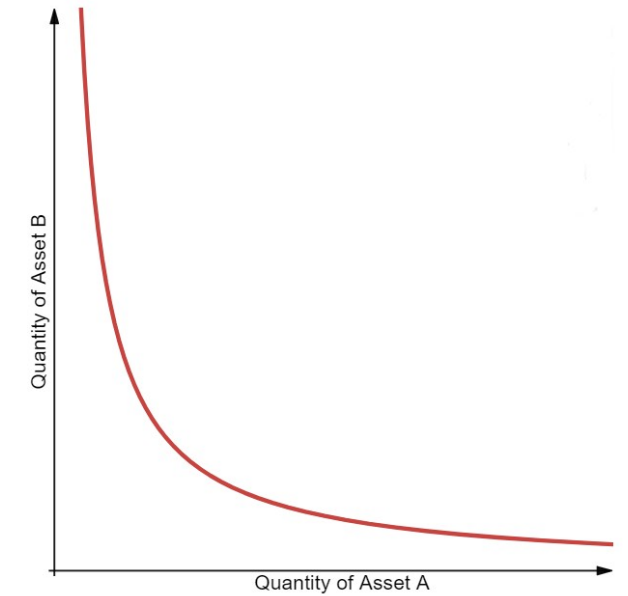
Quantity of Asset B

Quantity of Asset A

```
x is input asset amount   (ETH)
X is input asset balance  (ETH)
y is output asset amount  (DAI)
Y is output asset balance (DAI)
```

OST

Exchange Rate / Decentralized Swaps

x is input asset amount   (ETH)
X is input asset balance   (ETH)
y is output asset amount   (DAI)
Y is output asset balance (DAI)

- Reverse of 133/1.5 → I want to buy ETH with 66 DAI

  - 1.5*66/(133+66) = 0.5 $x = \dfrac{Xy}{Y+y}$

  - Swap at price 133.333 → new price 200DAI/ETH → reversible

- If swap price == the final pool price

  -

$$\frac{Y-y}{X+x} = \frac{y}{x} \qquad y = \frac{Yx}{X+2x}$$

  - Example 200 0.5/(1+2*0.5)

    - 150/1.5 = 50/0.5 (swap and final price the same)

  - However, not reversible with same numbers. To get the same price (200), need to swap 75 DAI for 0.375ETH → 225/1.125ETH

  - THORChain

$$y = \frac{xYX}{(x+X)^2}$$

OST

Decentralized Swap

- Many AMM variations

  - THORChain – punish large swaps [how its calculated]

  - Example: 0.5 * 200 * 1 / (0.5 + 1)^2 = 44.4 (price 88DAI/1ETH)

  - Resulting pool: 155.555/1.5 → price 103.7DAI/1ETH

    – Large trades gives you a worse rate than the resulting pool price. Small values, e.g., 0.1 ETH → 16.5DAI / 165DAI/ETH, pool: 166.8DAI/ETH

- More AMMs, here

- Attacks: Exploit slippage tolerance: sandwich attack (front-running) [seen in practice]

```
x is input asset amount    (ETH)
X is input asset balance   (ETH)
y is output asset amount   (DAI)
Y is output asset balance  (DAI)
```

$$y = \frac{xYX}{(x+X)^2}$$

OST

Decentralized Swap

- Swap 0.5 ETH for DAI, how much DAI? (price 200DAI/ETH)

- (price 133DAI/ETH), but DAI funds not decreased yet

- Pool: 133 DAI, 1.5 ETH, price (88DAI/ETH)

$$y = \frac{Yx}{X + x}$$

66
133 DAI

200 DAI

0.5 ETH
1 ETH

OST
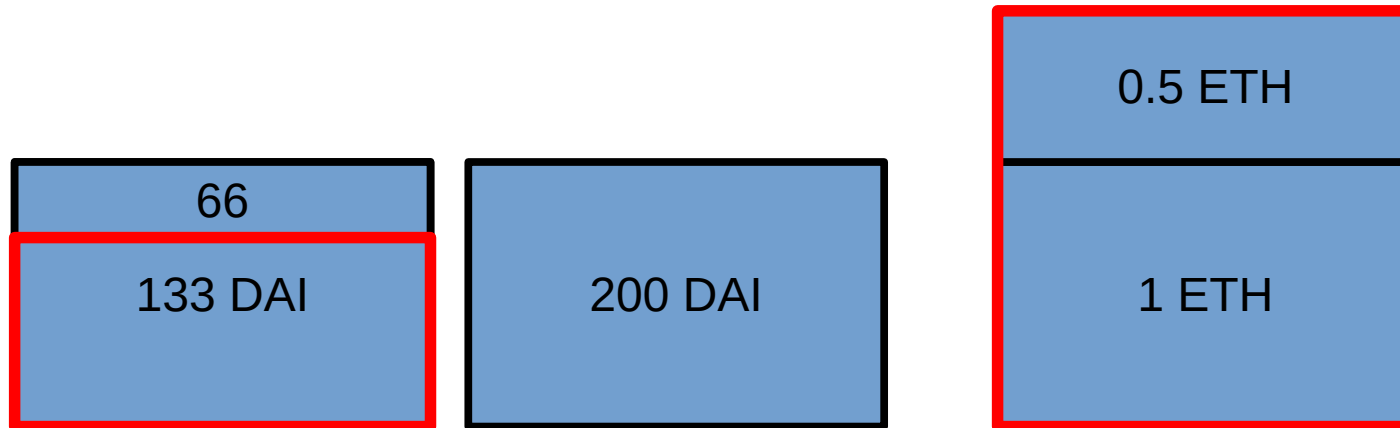
DeFi Fundamentals

- Swaps (just covered)

- Arbitrage bots

  - Swapping in multiple pools or CEX, if a boot sees e.g., a trading opportunity,

    - Example: Pool 1: 250 DAI for 1 ETH, pool 2: 200 DAI for 1 ETH

    - Arbitrage bot has 1 ETH (not considering price impact in this example)
      - Buy for 1 ETH 250 DAI in pool 1
      - Sell 250 DAI for 1.25 ETH in pool 2, profit = 0.25 ETH

  - Keep the same price across exchanges

- Flash loans

  - Same chain: arbitrage bots can use flash loans

  - Get loan and pay it back in the same transaction

    - No risk for lender, either he gets the tokens back or transaction is invalid

- Example with Aave: from 1000 to 1045, including payback of 1000.9

  - SushiSwap, Uniswap, DAI, wETH

- Without arbitrage bots, DEX does not work!

  - Essential part of the ecosystem

OST

DeFi Fundamentals

- Swaps (just covered)

- Arbitrage bots (just covered)

- Liquidity providers (LP)

  - Someone should provide liquidity - filling the pools

  - General rules for AMM-based DEX

    - Providing / removing liquidity - **no change of price**

    - LP provide 50/50 ratio of assets, example with a 200DAI/1ETH pool

    - LP can provide 100DAI/0.5ETH, or 400DAI/2ETH

    - LP_a gets liquidity units (LP token), with 100/0.5 (new pool: 300/1.5), LP_a owns 1/3 of the pool

- Why should a LP provide liquidity?

OST

Liquidity Providing

- LP token → % of the liquidity provided in the pool

  - Earn fees for providing liquidity

  - For each swap, user has to pay fees
    - Fees are distributed proportionally to the amount of LP tokens
    - Eg., fees collected are 2ETH, LP gets 10%, 0.2ETH

 - More liquidity provided by others, the 10% will be decreased → less earnings

- Why is not everyone providing liquidity?

  - Free money?

|						
BUSD 1 ibBUSD = 1.0708 BUSD	Lending APR: Staking APR : Total APR: Total APY ⓘ:	10.35% 1.38% 11.73% 12.44%	206.17M BUSD	131.73M BUSD	63.89%
USDT 1 ibUSDT = 1.0266 USDT	Lending APR: Staking APR : Total APR: Total APY ⓘ:	9.81% 1.76% 11.56% 12.26%	117.95M USDT	71.4M USDT	60.53%
TUSD 1 ibTUSD = 1.0057 TUSD	Lending APR: Staking APR : Total APR: Total APY ⓘ:	0.921% 1.98% 2.9% 2.94%	59.56M TUSD	11M TUSD	18.47%
BTCB 1 ibBTCB = 1.0043 BTCB	Lending APR: Staking APR : Total APR: Total APY ⓘ:	0.377% 1.16% 1.54% 1.55%	2.75k BTCB	325.09 BTCB	11.82%
ETH 1 ibETH = 1.0121 ETH	Lending APR: Staking APR : Total APR: Total APY ⓘ:	0.830% 0.632% 1.46% 1.47%	55.81k ETH	9.79k ETH	17.53%

Liquidity Providing

- Impermanent Loss (its mostly permanent, better name: price shift loss)

  - "Users who provide liquidity to AMMs can see their staked tokens lose value compared to simply holding the tokens on their own."

  - Example: I own 10% of the pool: 200 DAI (price 1$), 1 ETH (price 200$)

    - 20 DAI, 0.1 ETH ($20) → $40

  - ETH price goes up 300$, hodler:

    - 20 DAI, 0.1 ETH ($30) → $50

  - Pool is at 200/1, other pools are at 300/1 → arbitration
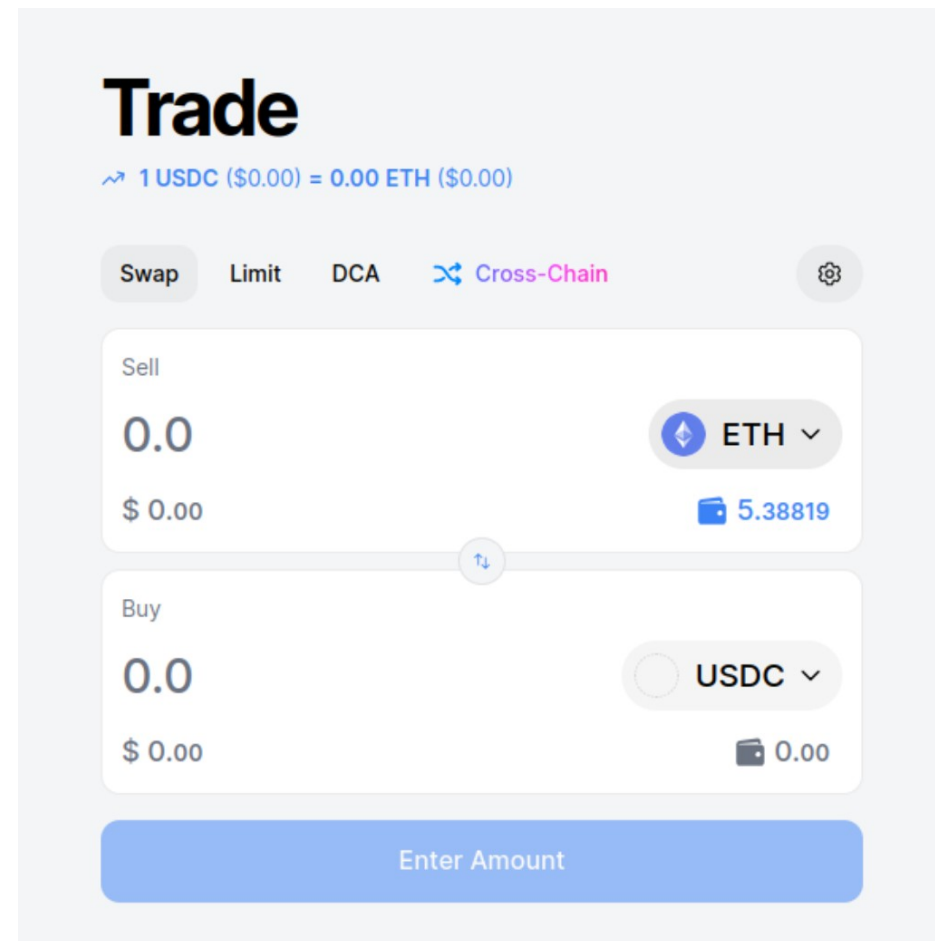
$$y = \frac{Yx}{X + x}$$

OST
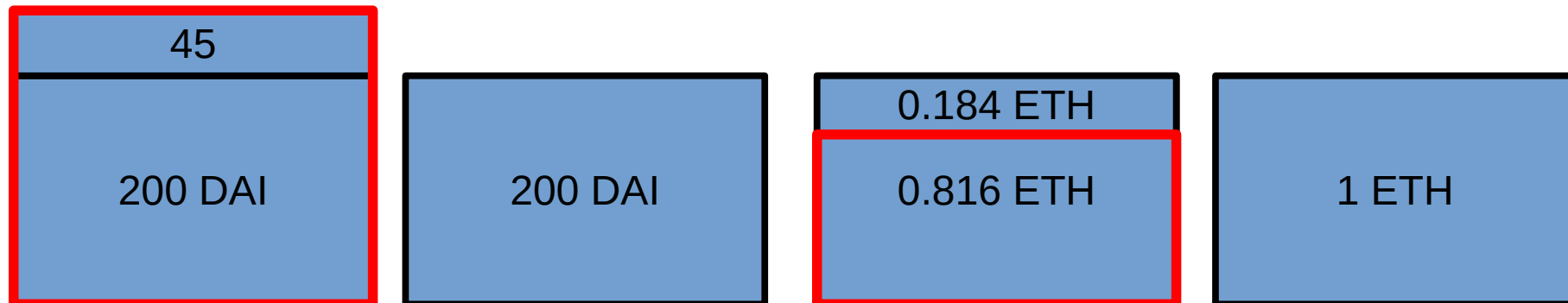
Liquidity Providing

- Uniswap formula: ~245DAI/0.8166

  - 10% of 245 DAI → $24.5

  - 10% of 0.8166 ETH → 0.08166 ETH ($24.5)

- $49 vs $50 - 1$ loss instead hodling

  - The more volatile the market is the higher the impermanent loss

- LP Token: fees + impermanent loss

  - Other incentive staking: if you place your token in a staking or yield farming contract

Impermanent Loss

source
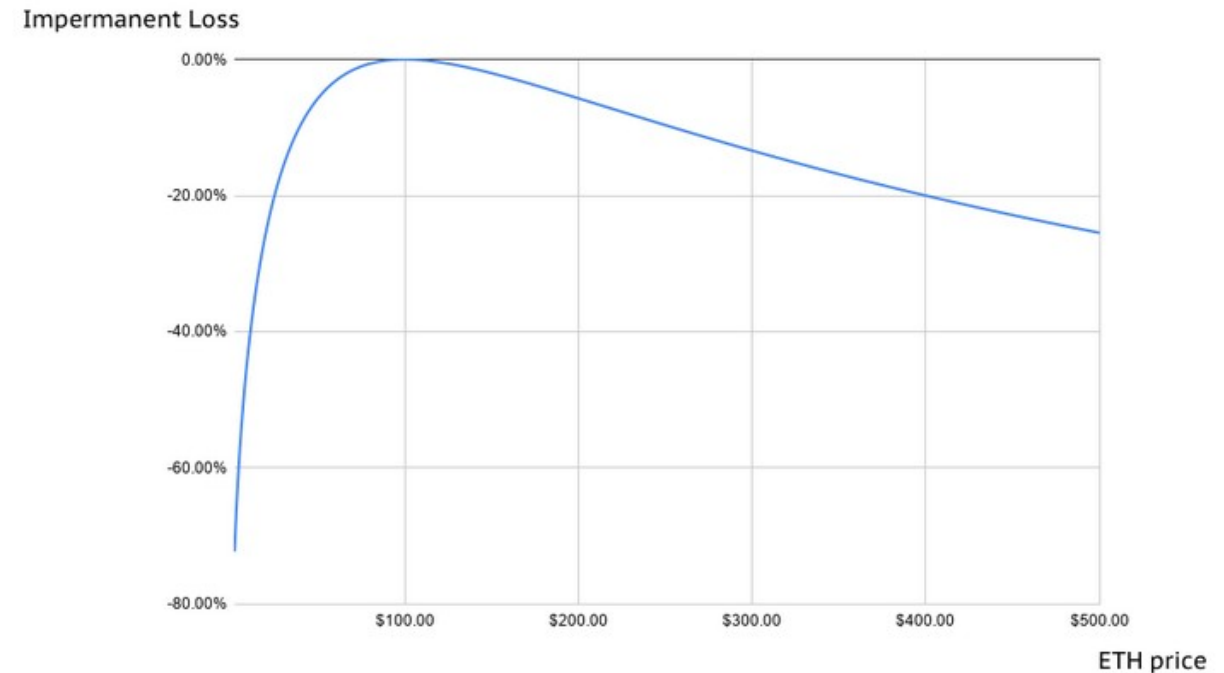
Lets use a DEX

- SushiSwap

  - ClassicAMM → v3 introduces concentrated liquidity, which makes the impermanent loss situation better, but introduces complexity

  - UniswapV2Router02.sol

  - UniswapV2Factory.sol

  - Sepolia, V2Factory

  - Sepolia, V2Router02

- https://www.sushi.com/swap?chainId=11155111