OST
Eastern Switzerland
University of Applied Sciences

Blockchain (BlCh)

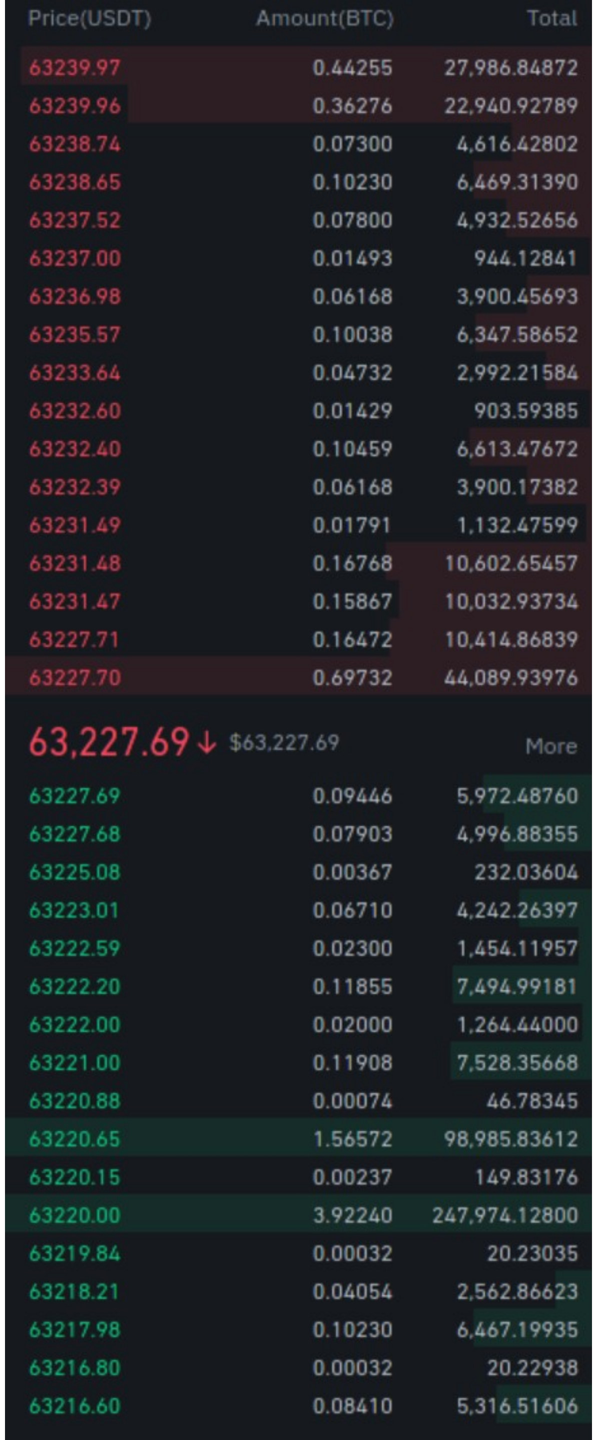
DeFi Details

Thomas Bocek

04.11.2021

Exchange Rate

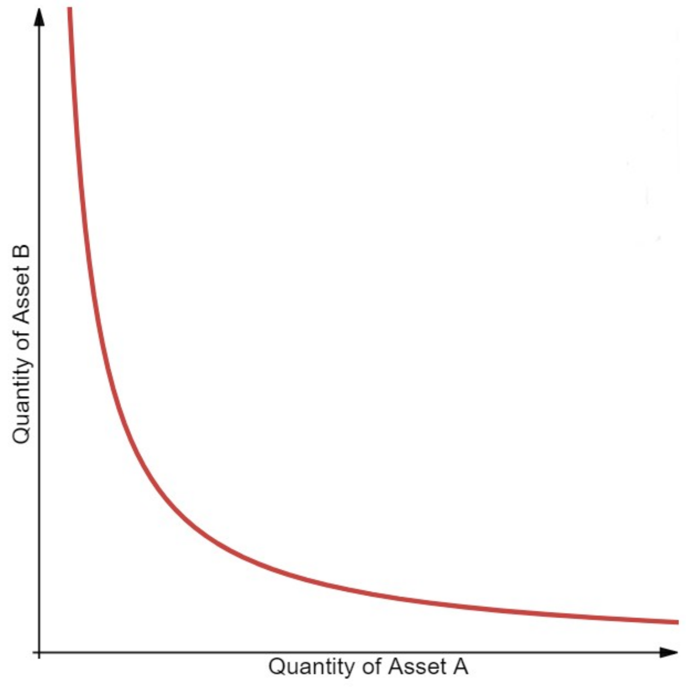
- Centralized: ask/bid, sell/buy, the last trade, e.g., 200 DAI for 1 ETH → price (order book)
  - Prince changes if trade happens, ask was same or lower than bid. Ask/bid submitted by users
  - Slippage: you see a price, submit, and until its executed, price can change.
    - Set limits, order may stay in the orderbook
- Order/time important → frontrunning, more data stored on chain
- Decentralized: ratio of pairs (automatic market making)
  - Slippage: the “same” - sometimes (mis)used as price impact
  - Example amount in pool: DAI 200, ETH 1 → price 200DAI/1ETH
- Large swap can change price (as with CEX)



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
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

Exchange Rate / Decentralized Swaps

- To not drain pool, Uniswap 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]
- Simple exchange price calculation (Uniswap)
  - Swap for 0.5 ETH, if you send 0.5 ETH to pool
    - 200/1.5 → 133 DAI → ~133 DAI for 1 ETH
  - Deduct 66 DAI from pool → 133/1.5 → ~ 88 DAI for 1 ETH
    - k=133.333 * 1.5 = 200
    - Not draining the pool, but trading with better price than resulting pool



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

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

Exchange Rate / Decentralized Swaps

- Reverse of 133/1.5 → I want to buy ETH with 66 DAI
  - 133+66/1.5 at price 133.333 → 66/133 = 0.5 ETH (new price 200DAI/ETH)
- If swap price should be == the final pool price
  - Similar to Uniswap, but the trade will happen exactly at the price of the resulting pool price
  - Example 200*0.5/(1+2*0.5) = 50
    - 150/1.5 = 50/0.5
  - However, reverse: from 150 DAI/1.5 ETH → y=0.3, results in 200 DAI/1.2ETH, new price 166DAI/ETH. To get the same price (200), need to swap 75 DAI for 0.375ETH → 225/1.125ETH

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

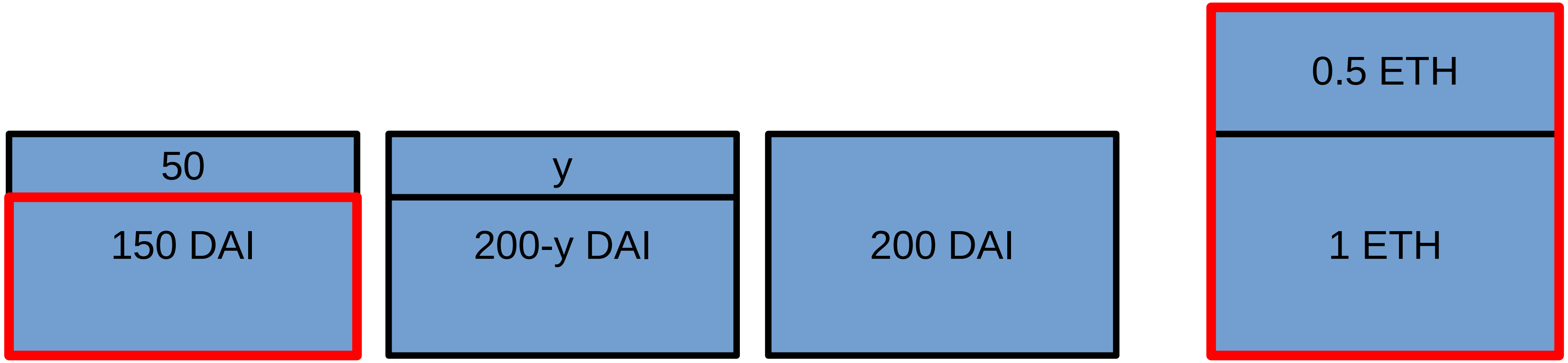
$$\frac{Y - y}{X + x} = \frac{y}{x}$$

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

Decentralized Swap

- Swap 0.5 ETH for DAI, how much DAI? (price 200DAI/ETH)
- (price 133DAI/ETH), but DAI funds not decreased yet
- How much do you get?
- Fixed formula, y=50, bought 50 DAI for 0.5ETH (price 100DAI/ETH)
- Pool: 150 DAI, 1.5 ETH, price (100DAI/ETH)

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



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)
```

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

AMM 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 1: 200 DAI for 1 ETH
    - Buy for 1 ETH 250 DAI in pool 1, go to pool 2 and sell 250 DAI for 1.25 ETH, profit = 0.25 ETH
- Liquidity providers (LP)
  - Filling the pools
  - General rules for AMM-based DEX: providing / removing liquidity does not change the price
    - LP provide 50/50 ratio of assets, example with a 200DAI/1ETH pool
    - LP can provide 100DAI/0.5ETH, or 400DAI/2ETH

Liquidity Providing

- Why should a LP provide liquidity?
  - The LP receives an LP token (ERC20) → % of the liquidity provided in the pool
    - E.g., LP provides 20DAI/0.1ETH → LP tokens says its 10% of the pool
      - Adding / removing liquidity from others affects my pool percentage. Eg., more liquidity provided, the 10% will be decreased.
  - 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
  - Earn fees for providing liquidity
- With LP token, you can back the 10% (or less if liquidity was added) of pool assets + accumulated fees

Liquidity Providing

- Why is not everybody liquidity providing?
  - Impermanent Loss (its mostly permanent)
    - “Users who provide liquidity to AMMs can see their staked tokens lose value compared to simply holding the tokens on their own.”
    - 200 DAI (price 1$), 1 ETH (price 200$) → $40 (10%)
    - ETH price goes up 300$, hodler: 50$ (10%)
    - Arbitration, 1 ETH can be bought for 200$ in this pool and sold for 300$ → provide 45 Dai, get 0.19 ETH
    - Uniswap formula: 245DAI/0.81ETH $49 (10%) - 1$ loss instead hodling
      - The more volatile the market is the higher the impermanent loss
      - Uniswap V3, to reduce the impermanent loss risk, provide liquidity within certain price ranges

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

    - My previously used formula: Pool: 250DAI/0.8333ETH 50$ (10%) ?

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

Liquidity Providing (Liquidity Mining)

- LP Token: fees + impermanent loss
  - Other incentive staking: if you place your token in a staking contract
  - Staking != staking
    - Staking on the blockchain layer: proof of funds to mine blocks (ETH 2, Cardano)
    - Staking in contracts: remove liquidity (supply) from the market to influence the price, as a reward, get more tokens (any tokens, e.g., governance tokens – token economics)
- Liquidity mining = yield farming
  - A protocol chooses e.g., the best LP with highest APY automatically (e.g., yearn)
    - Optimize crypto assets earnings through lending and trading services [ref]
    - CRV – Curve Token → Curve – AMM smart contract