

CPSC 3640/5400: Decentralized Payments, Contracts, and Finance for Humans and AI

Lecture 11: Decentralized Exchange (DEX)

Fan Zhang
Yale University
2026 Fall

Last lecture: Mixer and Tornado Cash

- Zero-knowledge proofs (ZKPs)
- Privacy Pools:
 - deposit creates a commitment to SN
 - Withdrawal proves knowledge of the opening r
 - Compliance via ASP
- Question in HoC: Grader can't link two transaction IDs; what else can you show to help?
- Answer: The opening r

Tornado Cash is not a payment system

- A mixer for you to mix your coins
- Not to pay someone else
 - E.g., one trouble is how to tell SN and r to the payee, which enables payer to track payee.
- Tornado Cash is a simplified version of Zcash, which does a lot more to support full blown private payments.
 - We provided some optional slides.

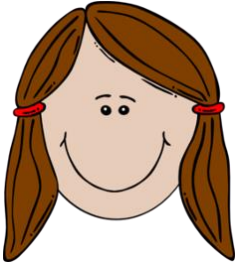
Roadmap so far

- **DeFi Primitives:** What they are, how they are implemented
 - Apps: **Tokens, Tokenization, Decentralized Exchanges [today]**, Oracles, lending/borrowing, (re-)staking
 - Infra for fast transactions
- **DeFi advantages:** things not possible in TradFi
 - **Privacy**, Interoperability, and Censorship Resistance
- **DeFi risks:** new problems unique to DeFi & mitigation
 - order manipulation, human factors, bugs

This lecture: Decentralized Exchange

- Most basic finance activity: Exchange
- E.g., Alice wants to **buy ETH** & Bob wants to **sell**.
- How do they state the **intention** to trade?
- How do they get **matched**?
- How do they **swap** their assets?

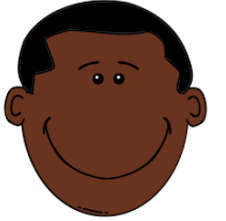
Limit orders



Alice

BUY 3 ETH
for < 3k USD

SELL 2 ETH
for > 1.9k USD

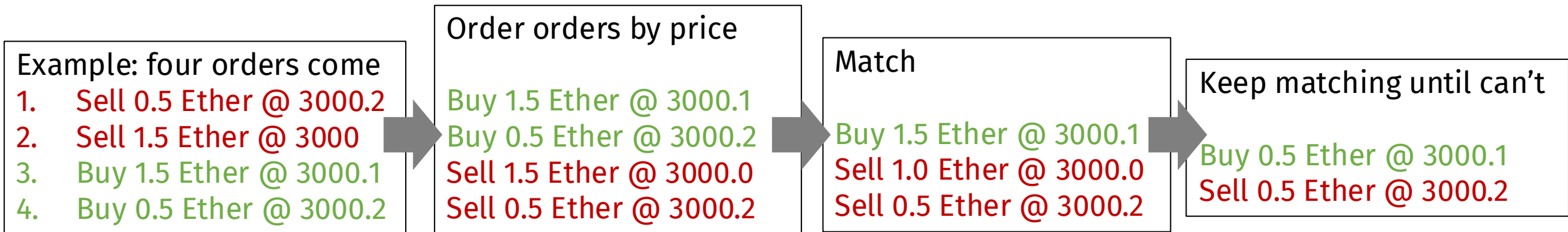


Bob

- Intention to trade takes the form of a **limit order** – order to buy or sell at a specific price or better.
- What are the conditions for opposite limit orders to match?
- Can these two orders match?

Limit Order Books (LOB)

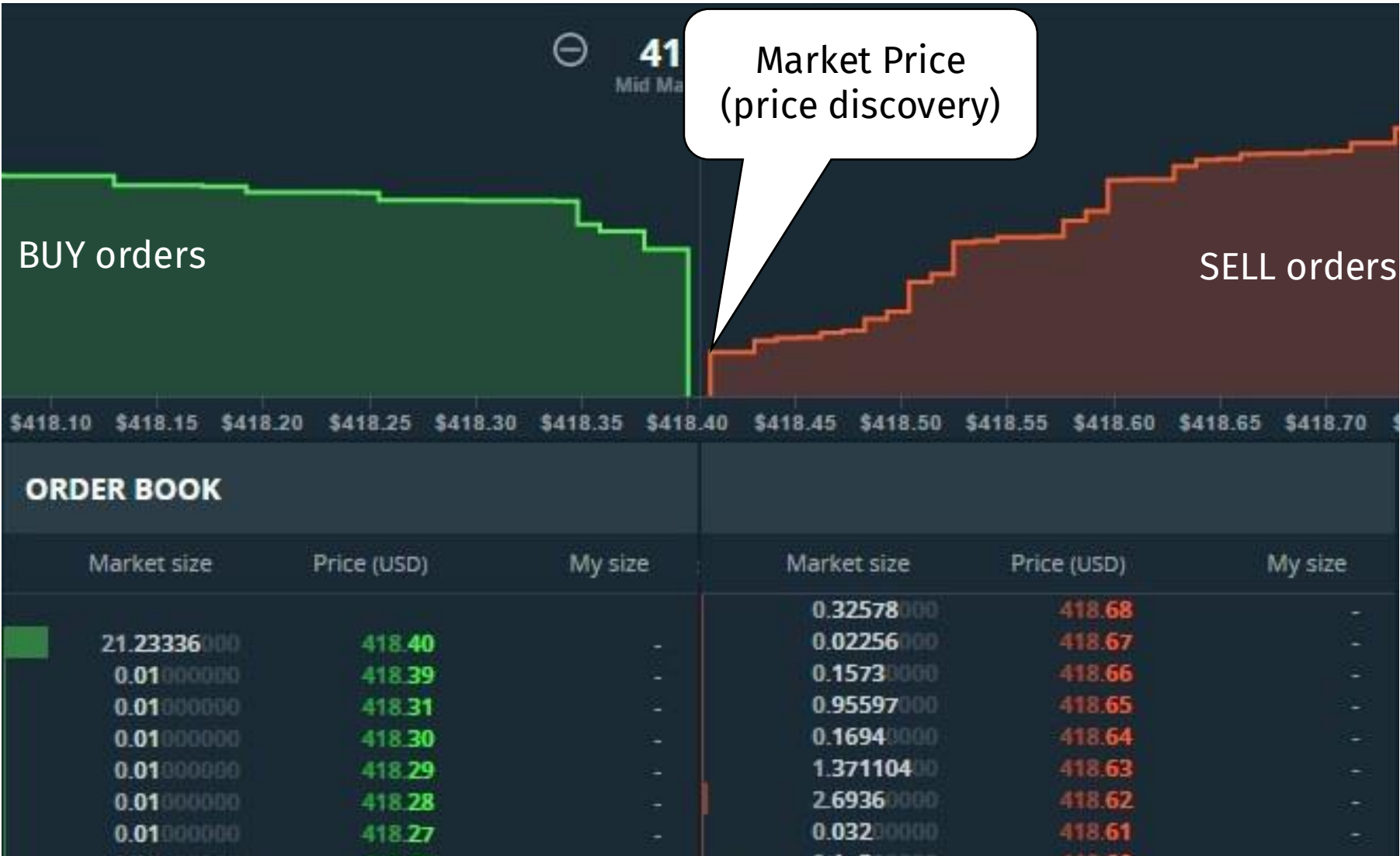
- Collection of such limit orders.
- How to match orders?



These stay on the order book.

Visualizing an order book

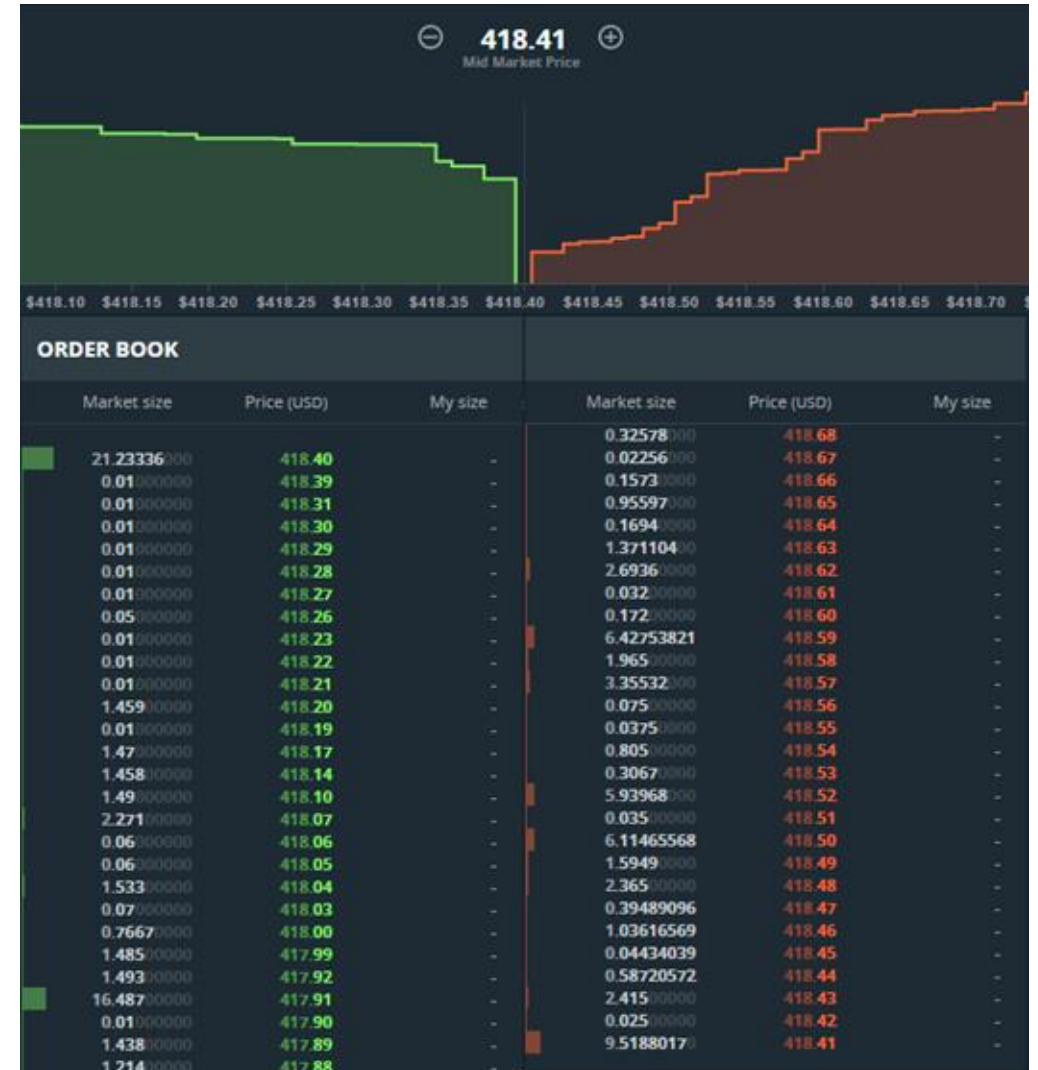
Y axis:
cumulative
order
depth



X axis: price

Limit Order Books

- **Liquidity**: volume of limit orders
- High liquidity markets have a very small **spread**, and vice-versa
- Why would a trader want a more liquid market?
- **Slippage**



Centralized Exchanges

- Centralized LOB is an efficient way to build exchanges
- Traditional exchanges - NYSE, NASDAQ
 - Each handles \$1-3 trillion in volume
 - Need to be heavily regulated to avoid insider trading
- Blockchain exchanges – Binance, Coinbase, **FTX**
 - Frequent regulatory issues leading to bans – Binance
 - Safety of customer funds not guaranteed – FTX
 - Need solutions like proof-of-reserves
 - Transfer custodianship of tokens – defeats the point of blockchains

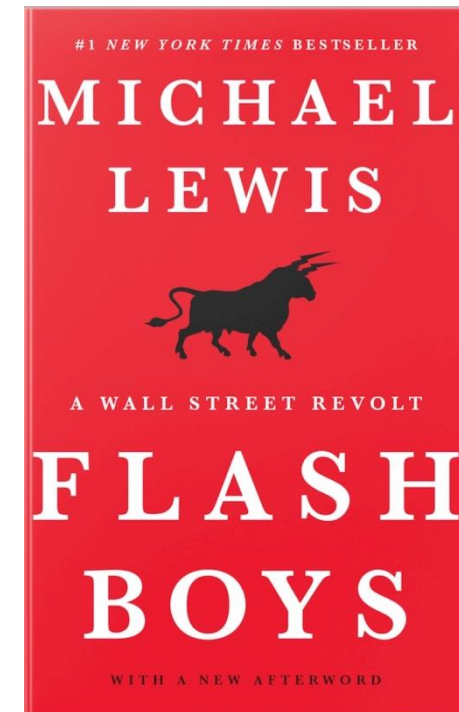
WARNING



RUGS FREQUENTLY PULLED OUT

Risks of centralized exchanges

- In addition to rug pulling there are other serious risks
- The centralized exchange knows about your order before the rest of the market – **frontrunning**

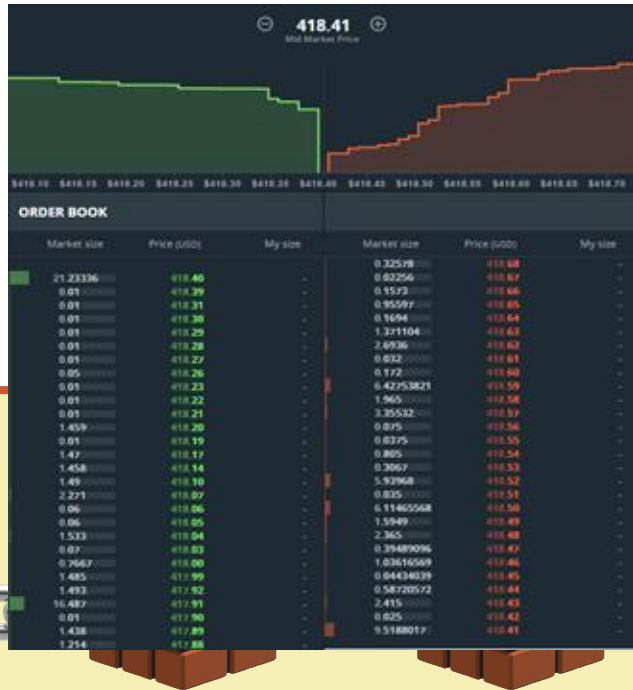
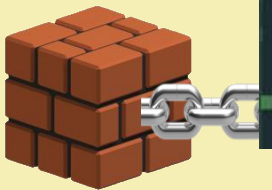


Risks of centralized exchanges

- In addition to rug pulling there are other serious risks
- The centralized exchange knows about your order before the rest of the market – frontrunning
- Exchange has the power to **censor** txns
- Removing central trust is the goal of **decentralize exchange**
- Two ways to decentralize
 - LOB (off-chain LOB or on-chain LOB)
 - Automated Market Makers (AMMs)

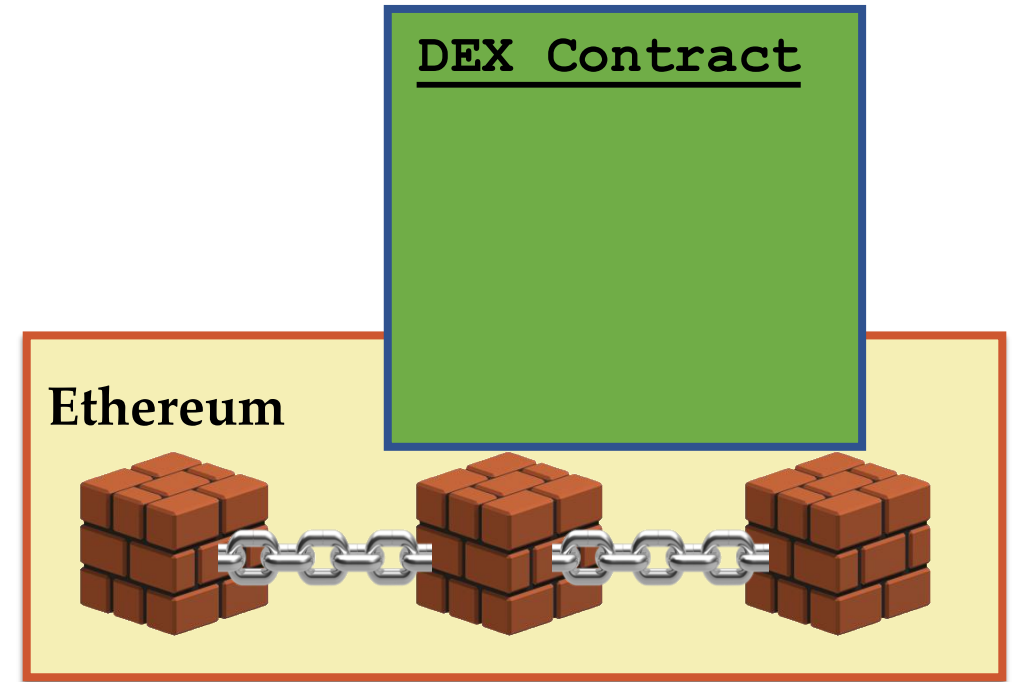
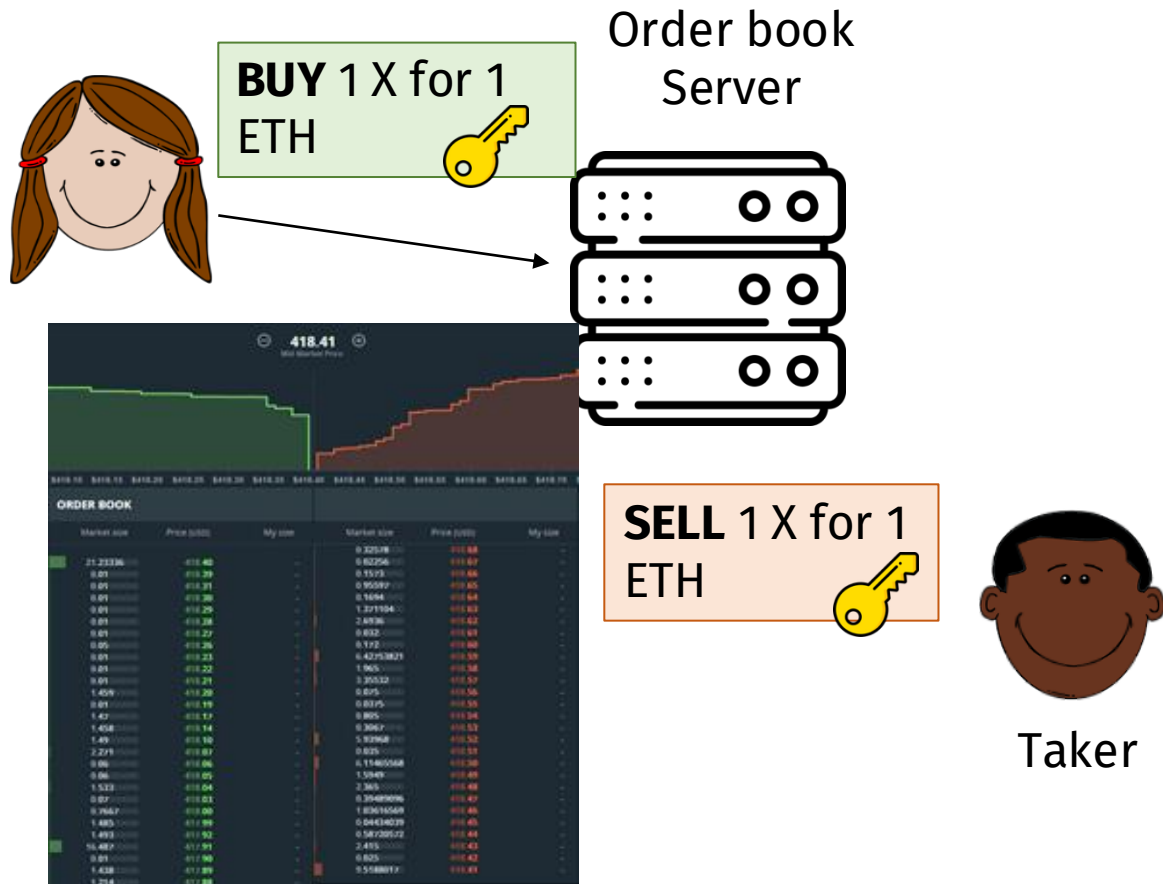
On-chain order book (hard to scale)

Ethereum

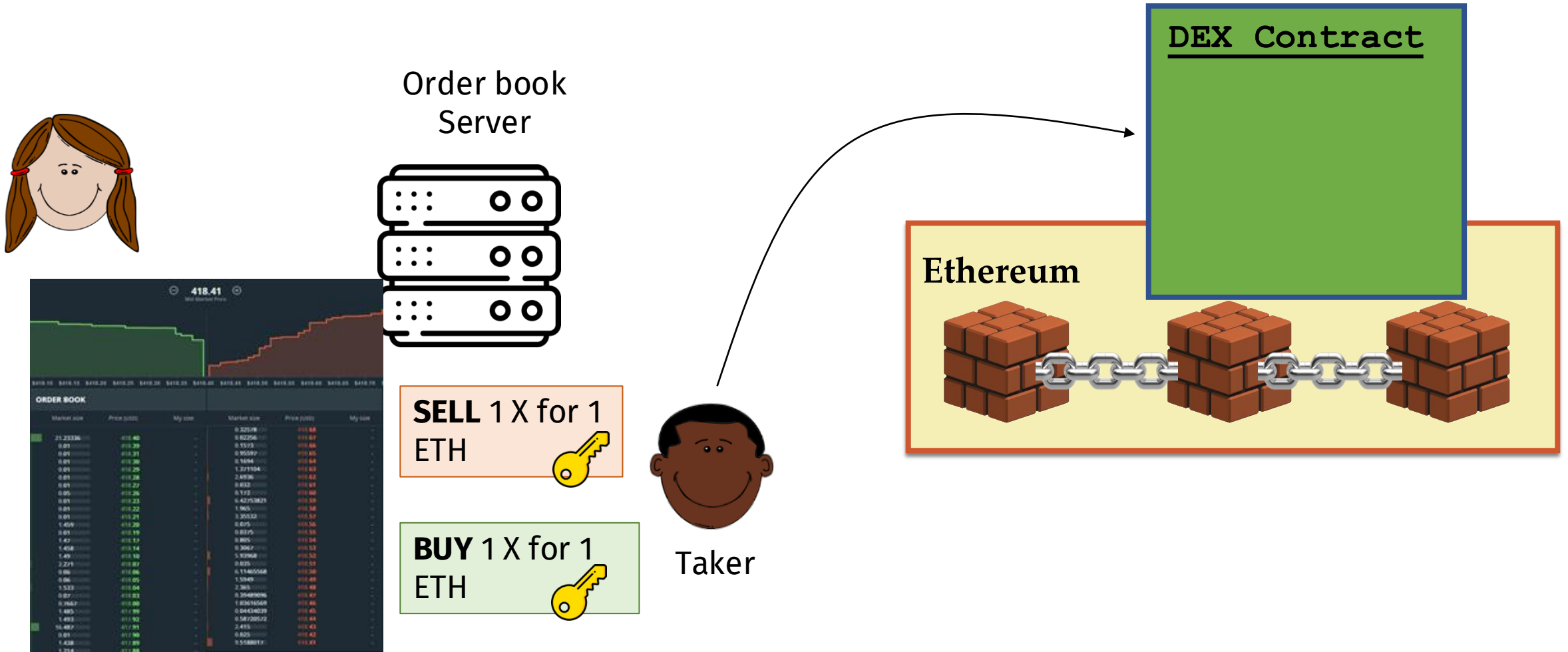


- + Censorship resistance
- + Integrated with DeFi ecosystem
- Matching algorithm is incredibly expensive to run on-chain
- Cancelled or failed orders still cost fees

Off-chain order book



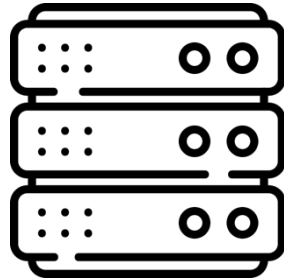
Off-chain order book



Off-chain order book



Order book
Server

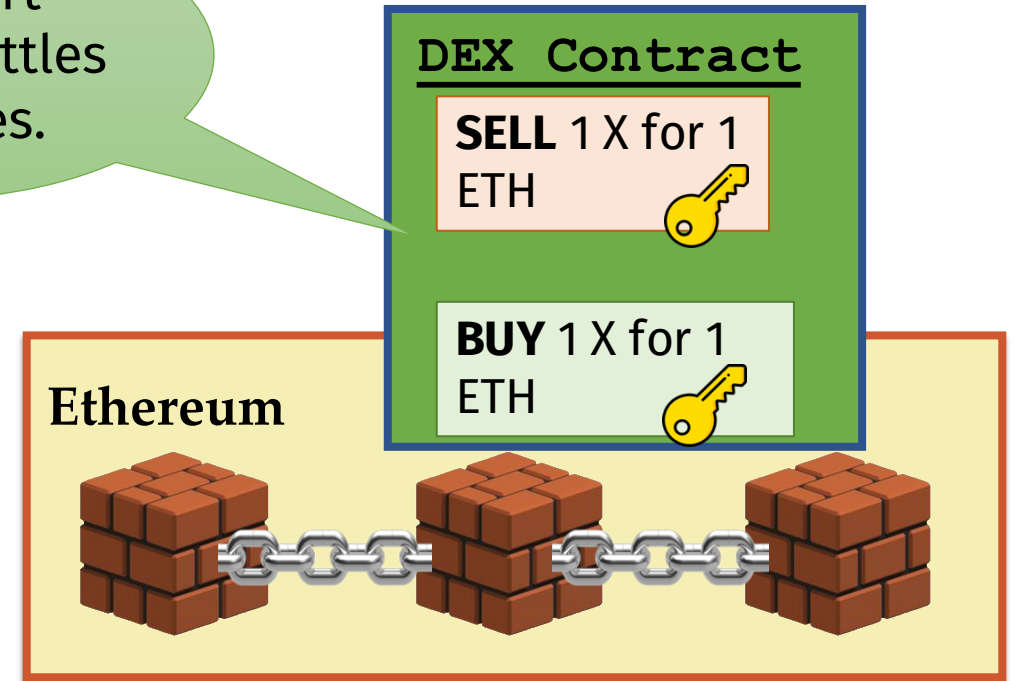


- Fast matching
- No fees for canceled orders
- **Server can censor orders**
- **Server can frontrun**



Taker

DEX Smart
Contract settles
the trades.

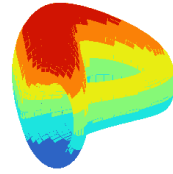


Shortcomings of Decentralized LOB

- Off-chain LOB is susceptible to **frontrunning** and **censorship**
 - On-chain LOB is **(incredibly) expensive in terms of gas**
 - **Liquidity problem**: for small markets, it can be hard to find counterparties to trade against.
-
- Now we introduce idea #2 that solves some of the problems:
Automated Market Maker (AMM)



UNISWAP



Curve

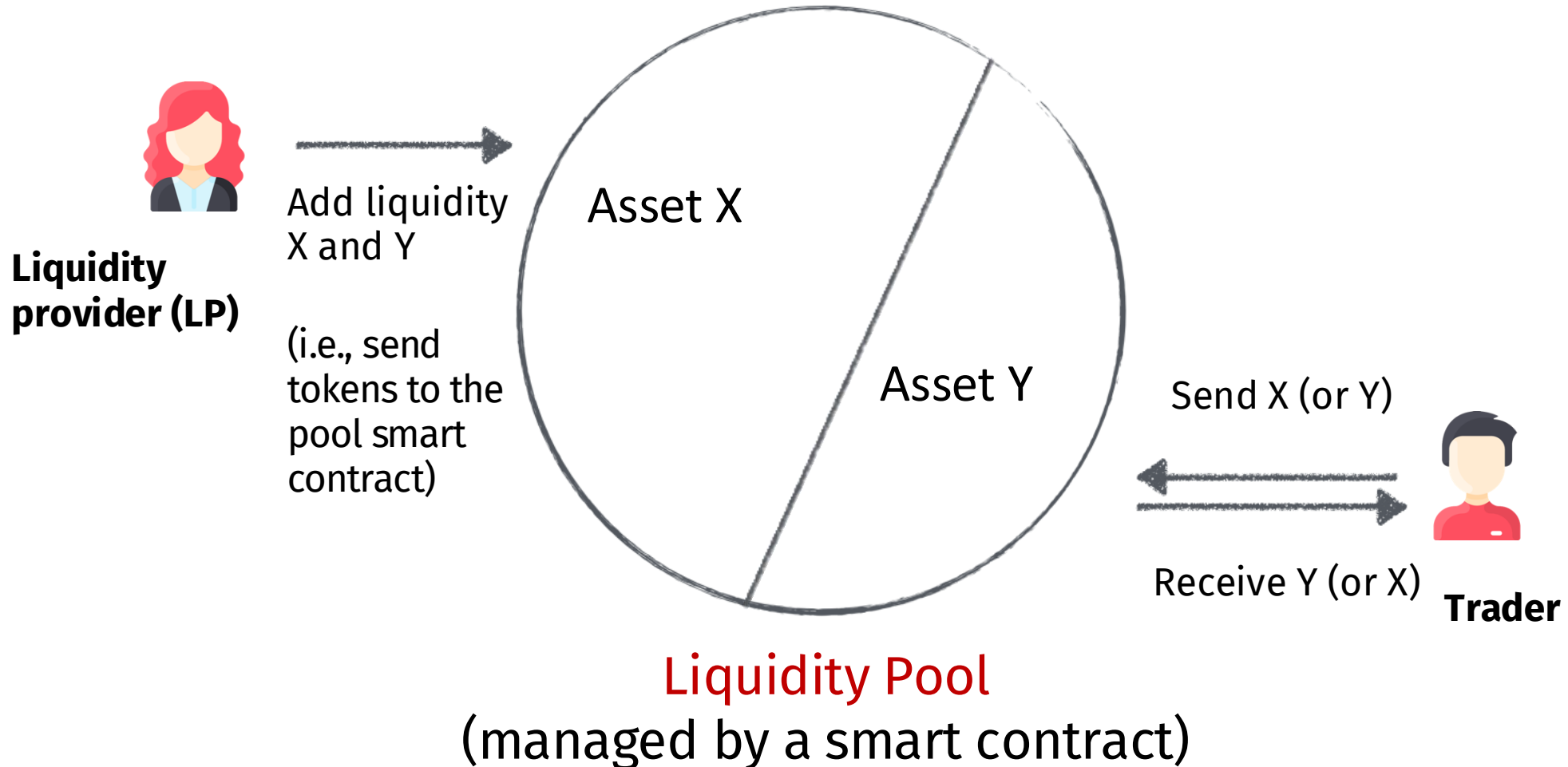


Automated Market Maker

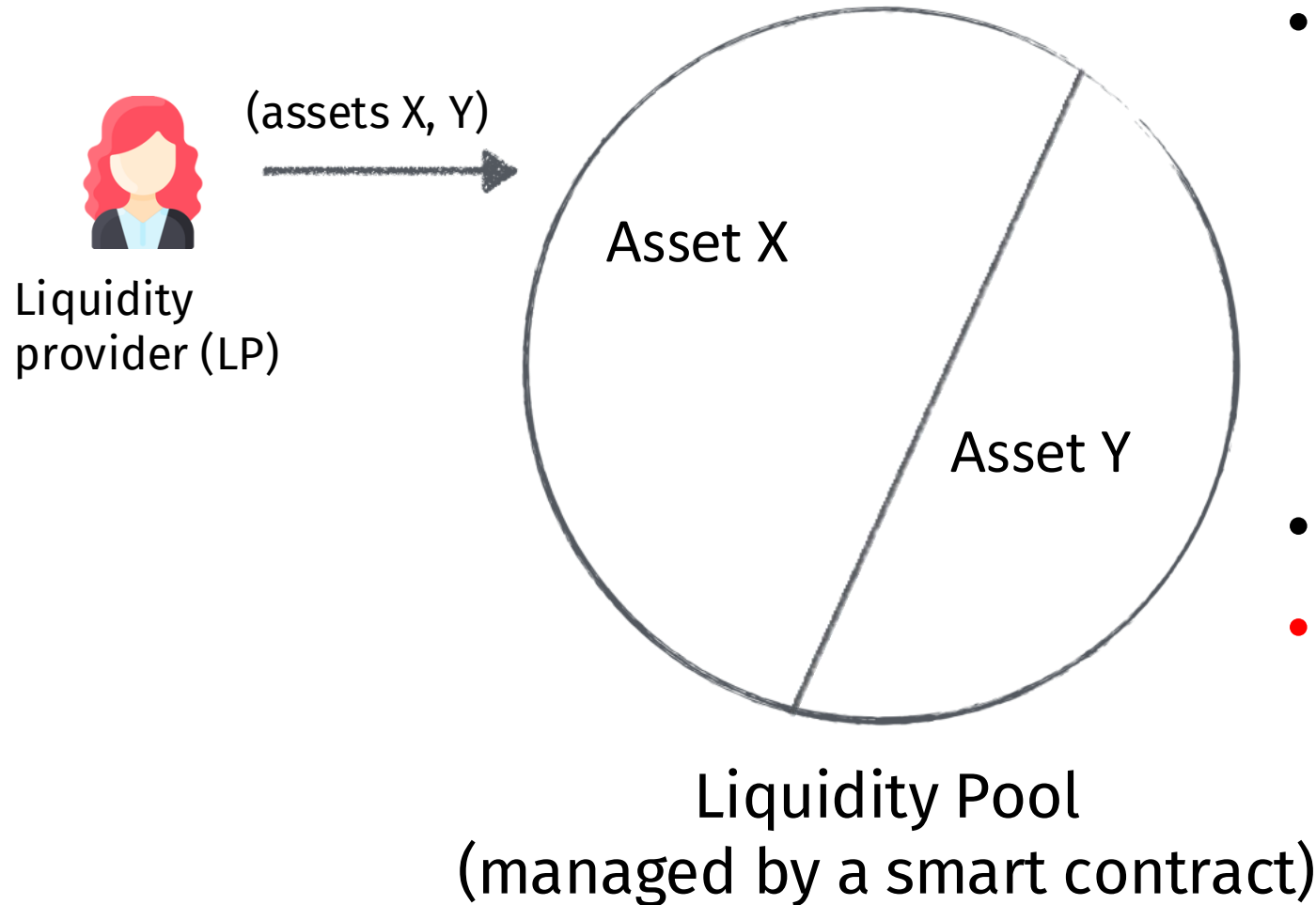
☆ 19	 Uniswap UNI
☆ 68	 Curve DAO CRV
☆ 74	 PancakeSwap CAKE
☆ 97	 1inch 1INCH
☆ 99	 Osmosis OSMO
☆ 149	 Balancer BAL
☆ 186	 Sushi SUSHI

AMM – Automated Market Maker

- Idea: **Peer-Pool-Peer** instead of Peer-Peer matching



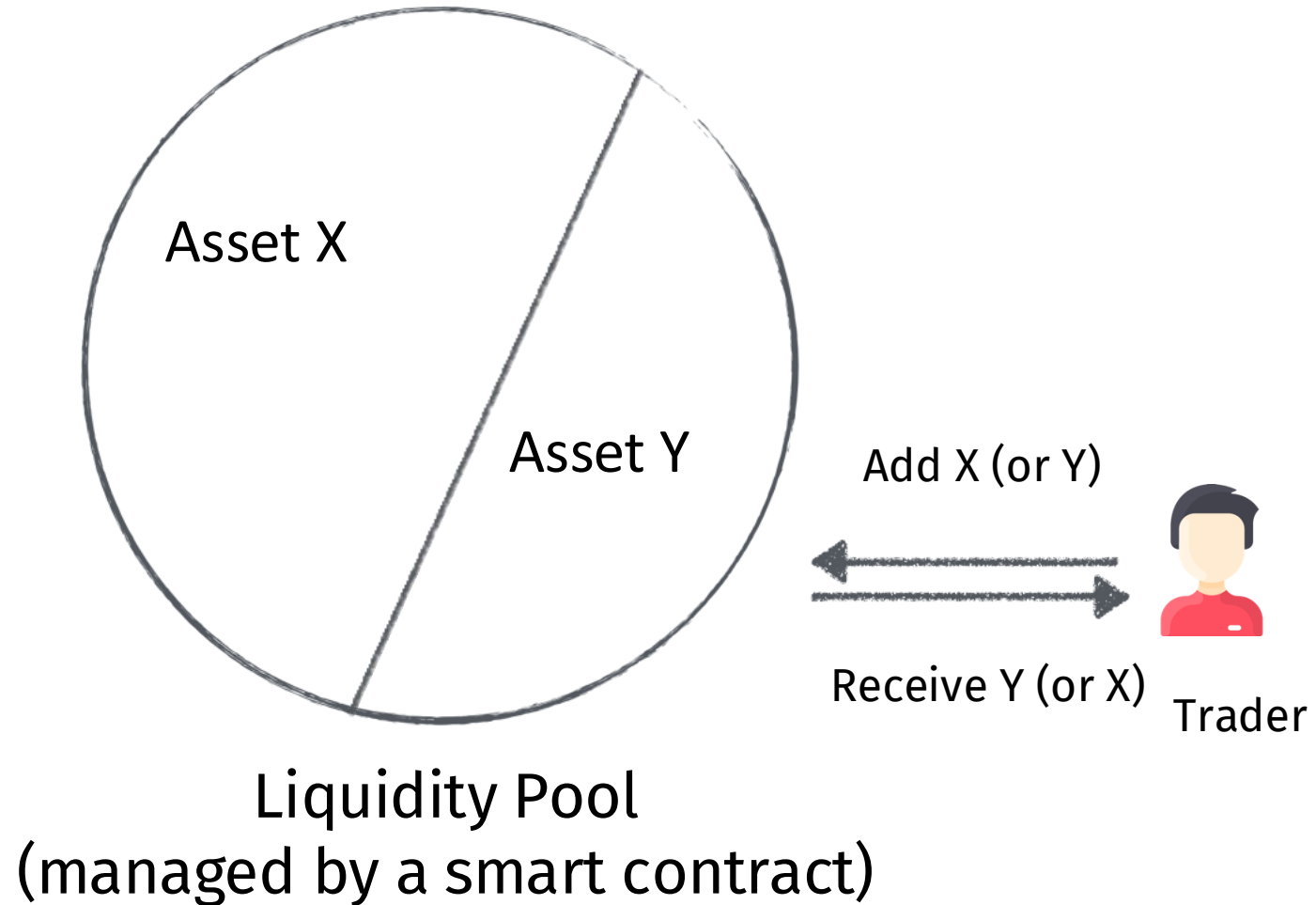
AMM – Automated Market Maker



- **liquidity providers (LPs):** Entities with large amount of idle liquidity pitch in to make the pool.
- LP's incentives?
- **Earn fees**

AMM – Automated Market Maker

- Trading against the pool
- **how to regulate price?**



A solution: CFMMs

- Price is set algorithmically as a function of asset reserve (x, y)
- General form: $\psi(x, y) = \psi(x + \Delta x, y - \Delta y)$
- A popular example: Constant Product (CP) AMM

$$x \times y = k$$

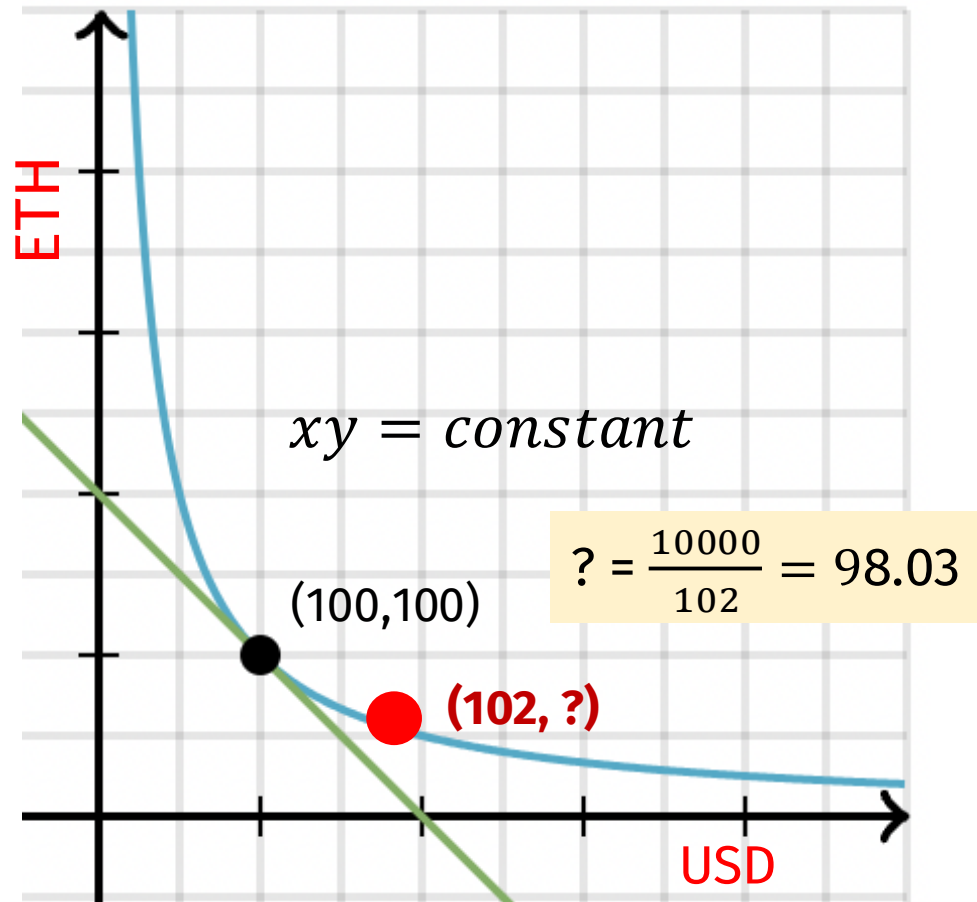
Asset X
quantity

Asset Y
quantity

constant

- Each trade $(\Delta x, \Delta y)$ must satisfy $xy = (x + \Delta x)(y - \Delta y)$

AMM Example



Sell 2 USD



Trader

Pool returns $100 - 98.03 = 1.97$ ETH

Top CFMMs

- Uniswap, Sushiswap:

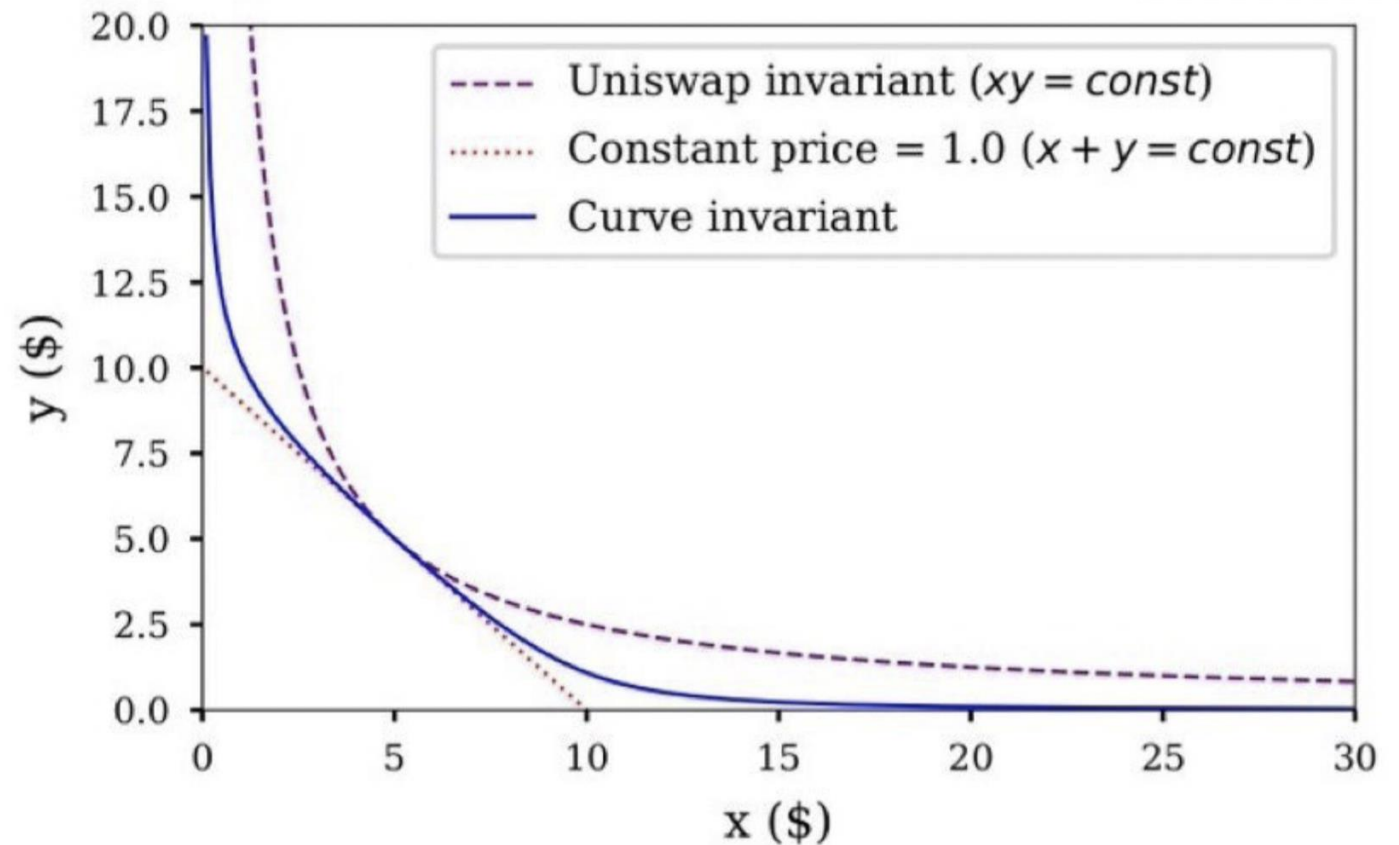
$$xy = \text{constant}$$

- Balancer:

$$x^\theta y^{1-\theta} = \text{constant}$$

- Curve:

$$x + y + \frac{\alpha}{xy} = \text{constant}$$



We care about both traders and LPs

- For traders
 - Price impact
 - slippage
 - Arbitrage
 - Sandwich attacks
- For LPs
 - Loss v.s. holding
 - Loss v.s. rebalancing

Considerations for traders

- Price impact
- slippage
- Arbitrage
- Sandwich attacks

Price

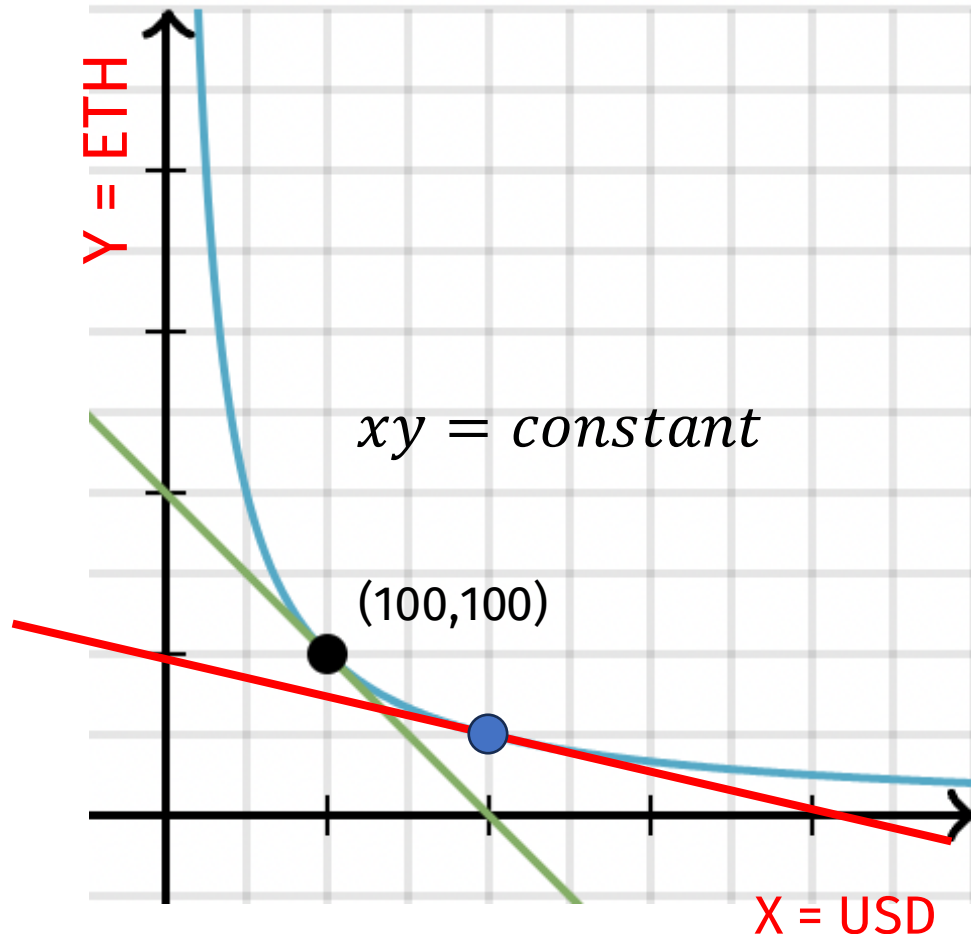
What is the price of apple in dollar?

Apple price: $\frac{1 \text{ dollar}}{3 \text{ apples}} = \frac{1}{3}$ USD per Apple



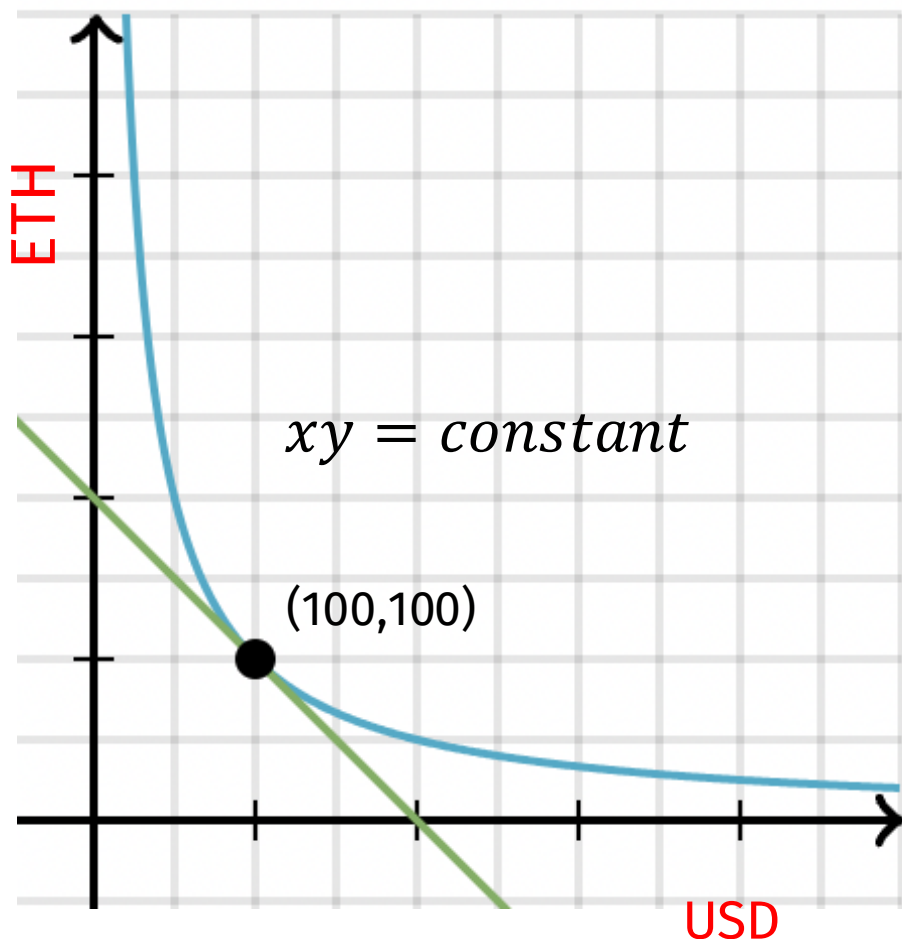
If you give X and get Y, price of Y = $\frac{X \text{ you gave}}{Y \text{ you received}}$ X per Y

Spot price at (x, y)



- **Spot price**: the price of asset at the current reserve
- **i.e.**, Consider a trader buying an infinitesimal amount of ETH and moves reserve **left** by $\Delta x \rightarrow 0$
- What is Δy ?
- Geometrically: **|slope|** times Δx
- Spot price of $Y = \frac{\Delta x}{\Delta y} = \frac{1}{\text{slope}}$
- Spot price of $X = ?$
- Which spot price (of ETH) is higher: Green or Red?

Spot price at (x, y) for CPMM



- On CPMM, slope at (x, y) is $-\frac{y}{x}$
- Spot price of Y at reserve (x, y) is $\frac{x}{y}$
- Spot price of X at reserve (x, y) is ?
- For a pool with 3000 USD and 2 ETH, spot price of ETH is 1500 USD/ETH.
- **Easy way to remember:** assets in a CPMM pool always have the same value.

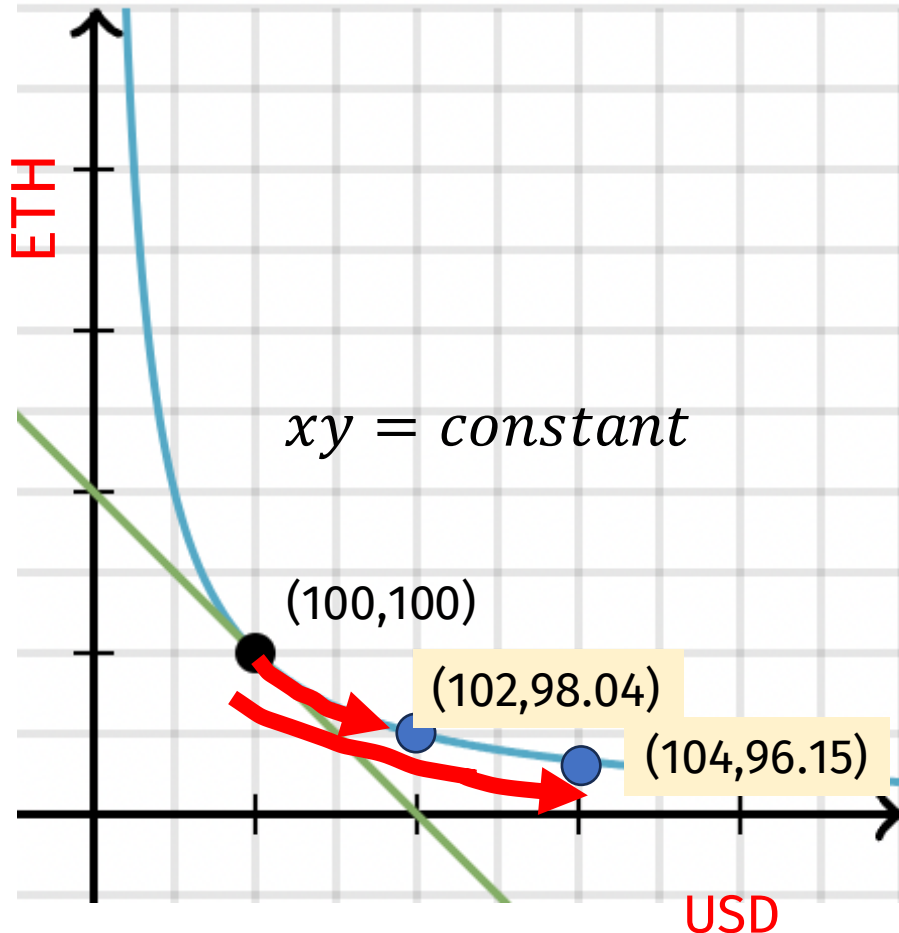
Price impact

- Any trade will move the price from the spot price
- How much does price (of X) change for a trade of size Δ ?
- Change of slope (y') is **second derivative** (y'')
- Price changes by roughly $y''\Delta$
- The more *curvy* the bonding curve, the more sensitive the price is to trade size.

Price impact for CPMM

- For CPMM $y'' = \frac{2k}{x^3} = \frac{2y}{x^2} = \frac{2(\text{spot price of X})}{x}$
- For a trade of size Δ , relative price impact on X is $\frac{2 \cdot \Delta}{x}$
- I.e., If your sell/buy 5% of the reserve X, it will drive up price by roughly **[?]**
- (Actual number is 9.30%; we ignored high order derivatives)
- Why do traders prefer high liquidity?

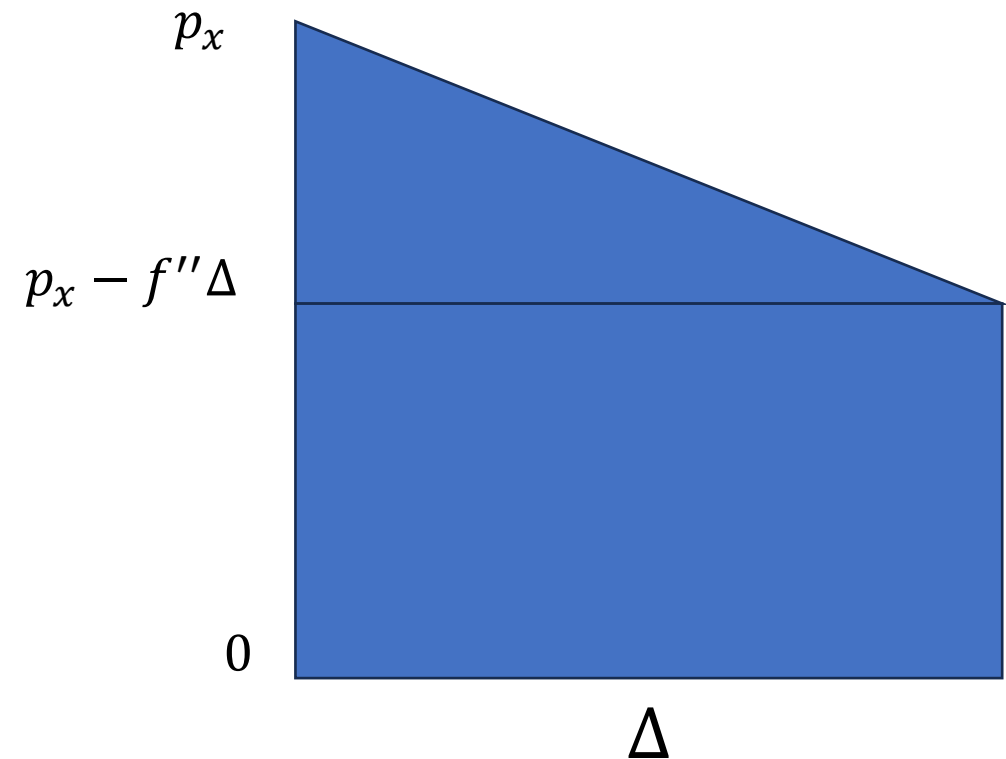
Slippage



- As a result of price impact, traders incur a loss
- ideal = what you would hypothetically get at spot price
- actual = what you actually get
- **slippage** = ideal – actual
- What is slippage of this order?
- If order size doubles, then slippage?

Why is slippage quadratic in Δ

- Consider **selling** Δ units of X
- Let spot price be p_x
- Prices drops as you sell, until $p_x - f''\Delta$ (see slides on price impact)
- Ideal = $p_x\Delta$
- Actual = blue (result of $\int_0^\Delta p_x(t)dt$)
- Slippage = the missing triangle = $\frac{1}{2}f''\Delta^2$



Why is slippage quadratic in Δ (CPMM)

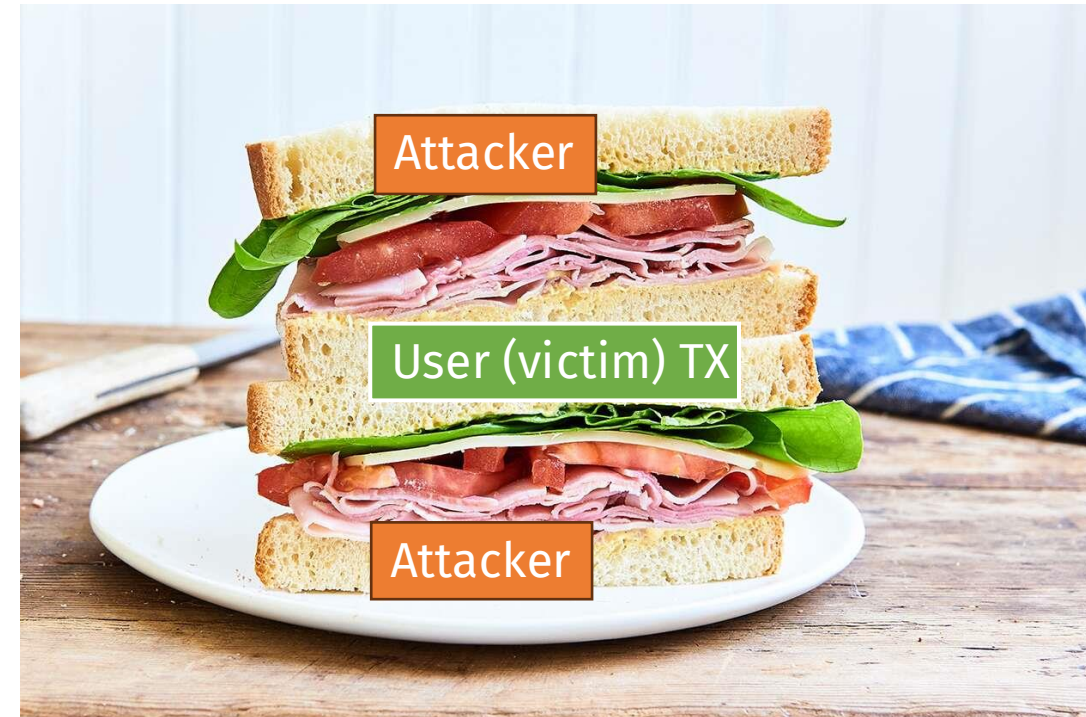
- For CPMM $f'' = \frac{2k}{x^3} = \frac{2y}{x^2} = \frac{2p_x}{x}$
- Slippage $= \frac{1}{2} f'' \Delta^2 = \frac{p_x}{x} \Delta^2$
- Relative slippage $= \frac{\text{slippage}}{\text{ideal}} = \frac{\Delta}{x}$
- I.e., a trade that's 1% of the pool's reserve costs about 1% in slippage.

Why is slippage quadratic in Δ

- Alternatively:
- Receives $y - \frac{xy}{x+\Delta} = \frac{y\Delta}{x+\Delta}$
- How much Y “should have received”: $\frac{y}{x}\Delta$
- Slippage = $\frac{y\Delta}{x} - \frac{y\Delta}{x+\Delta} = \frac{y\Delta^2}{x(x+\Delta)} \approx \frac{y\Delta^2}{x^2} = \frac{p_x\Delta^2}{x}$

Attacks leveraging slippage

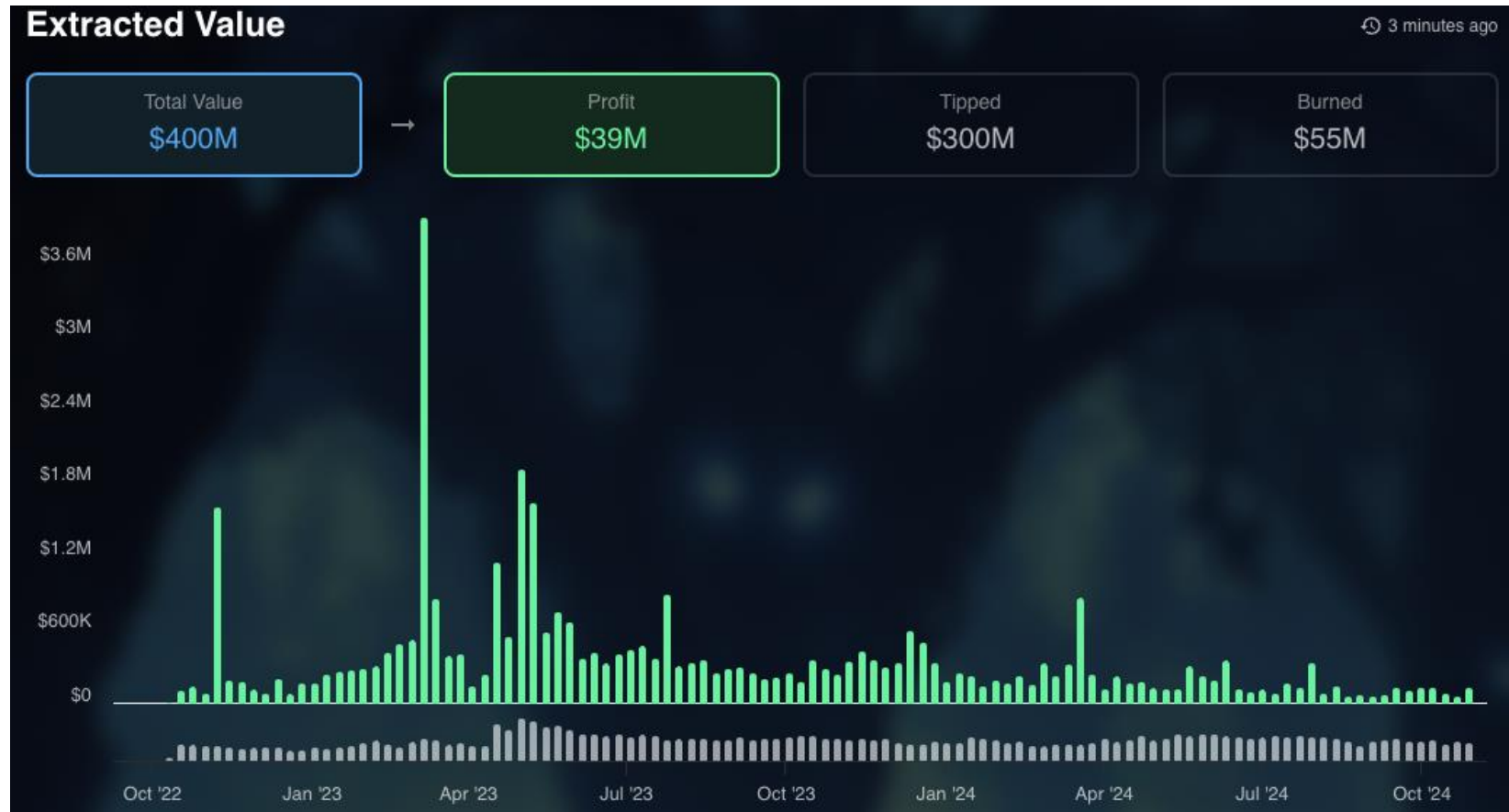
- User: **T** = Selling ETH for USD
- Will cause USD price to *rise*
- If an attacker can precisely control the ordering of transactions, how to profit from price increase?
- Buy USD before **T**. Sell USD after price increase.



Result: profit for attacker; user incurs a larger slippage.

Sandwich attacks

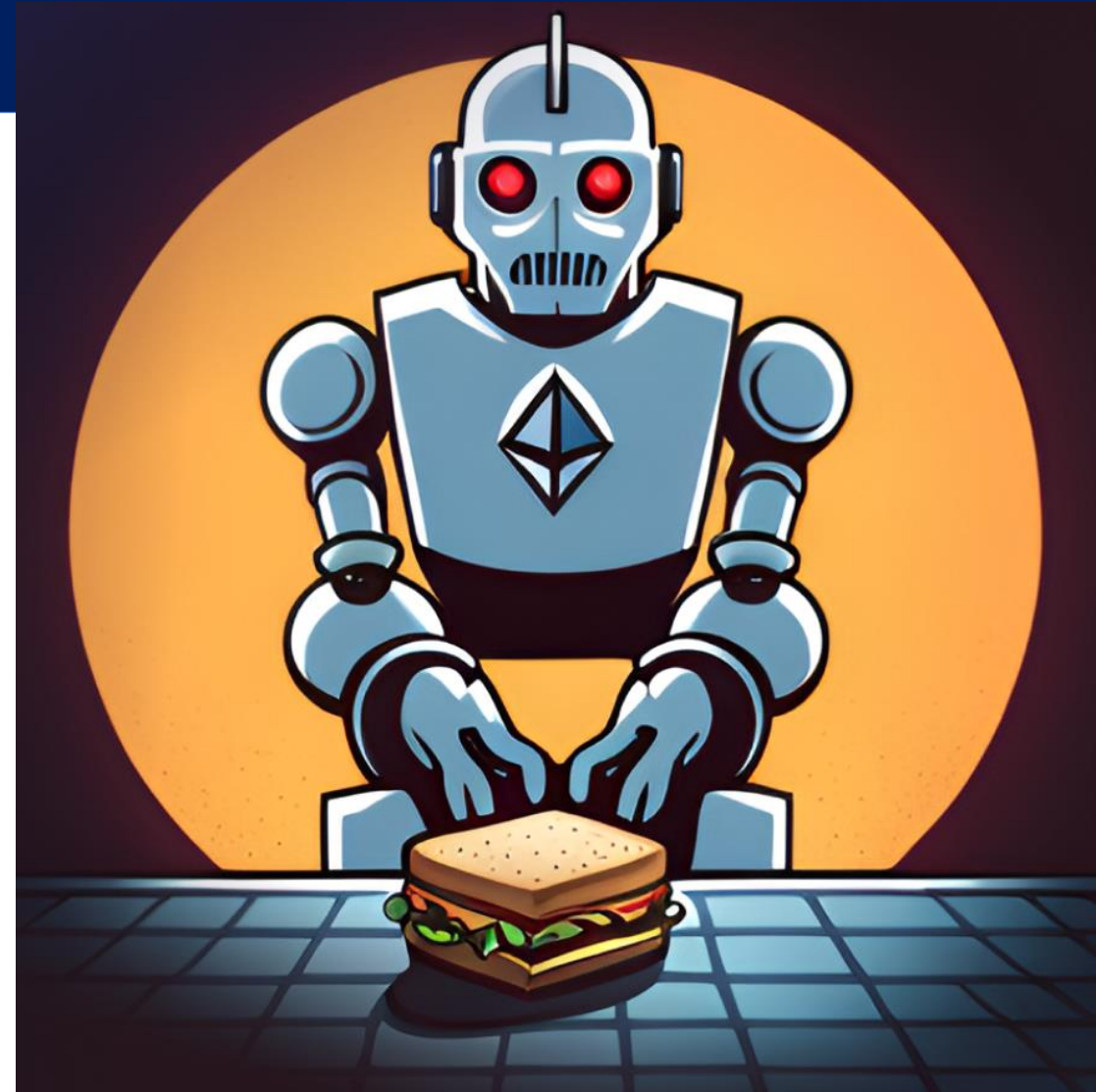
- Does this really happen in practice?
- Big time!



<https://libmev.com/?mevTypeLabels=%5B%22Sandwich%22%5D> (Nov 4, 2024)

Sandwich attacks

- Who does this?
 - Specialized “bots”
- How do they precisely manipulate the ordering of transactions?
 - They may be miners (validators)
 - Or, they can bribe validators! [If you include this three transactions in order, I will pay a high fee]
- Will discuss this in detail in a few lectures.



Slippage Protection

- One simple protection is to limit slippage (commonly to 5%)
- A transaction fails when crossing the slippage limit.

Swap

0.1

ETH

Balance: 0.1762 Max

↓

0.0064

WBTC

Balance: 0

1 WBTC = 15.6262 ETH

Expected Output

0.00639952 WBTC

Price Impact

0.00%

Minimum received after slippage (5.00%)

0.00609478 WBTC

Network Fee

~\$10.60

Auto Router

+

Swap