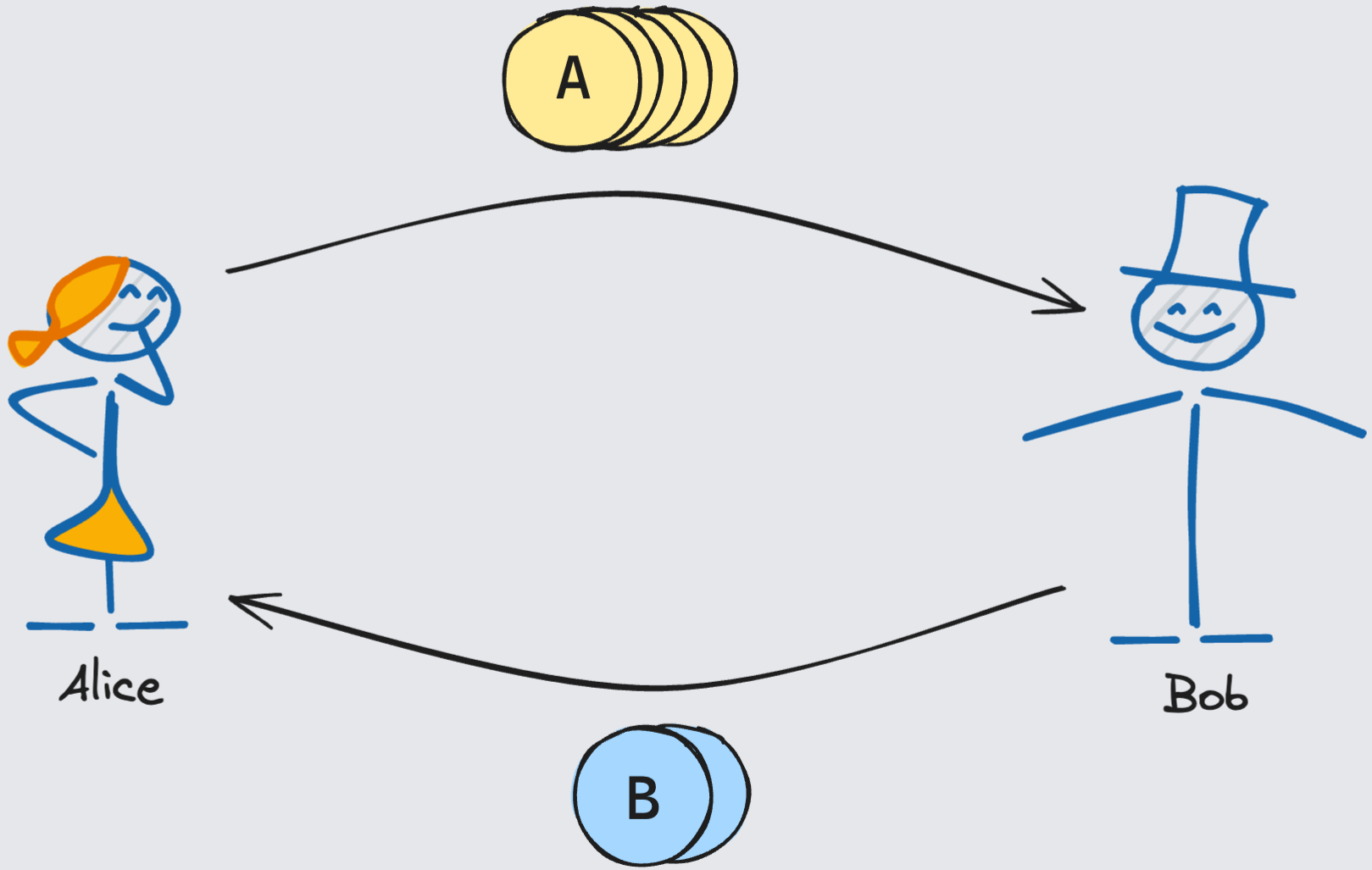
Decentralized exchanges (DEX)

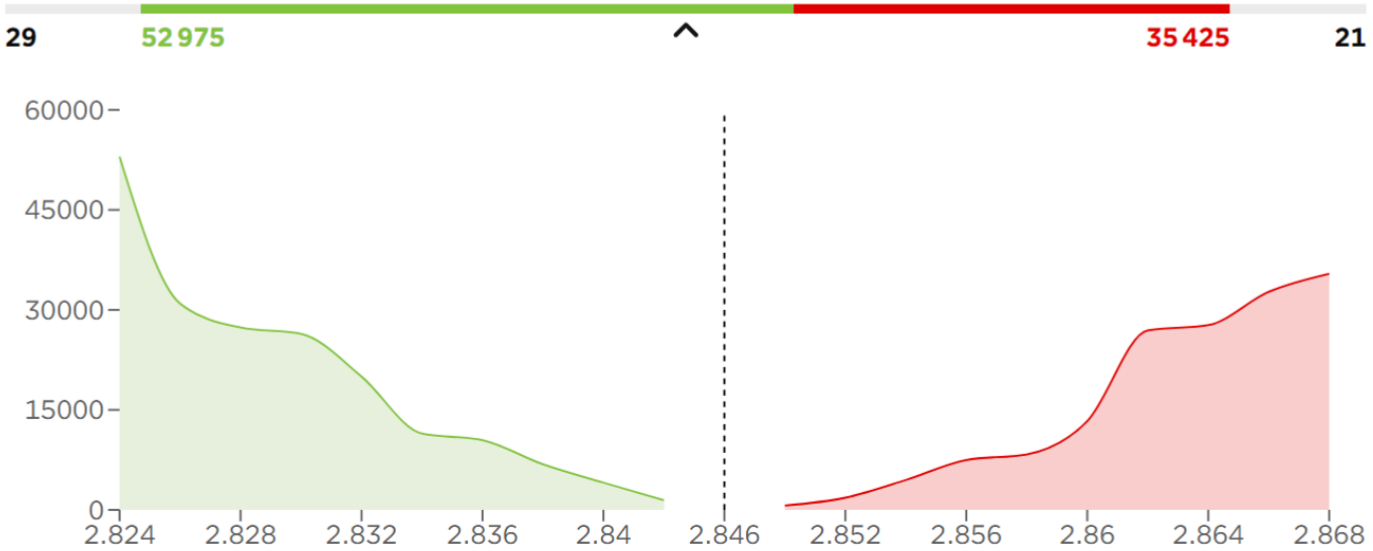
Prepared by Kirill Sizov

Financial exchange

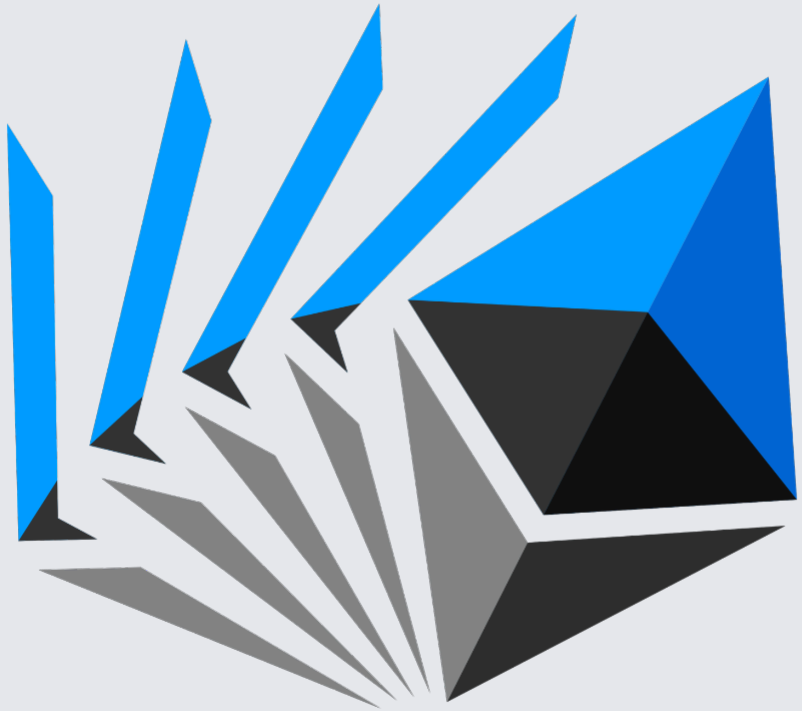


Order book

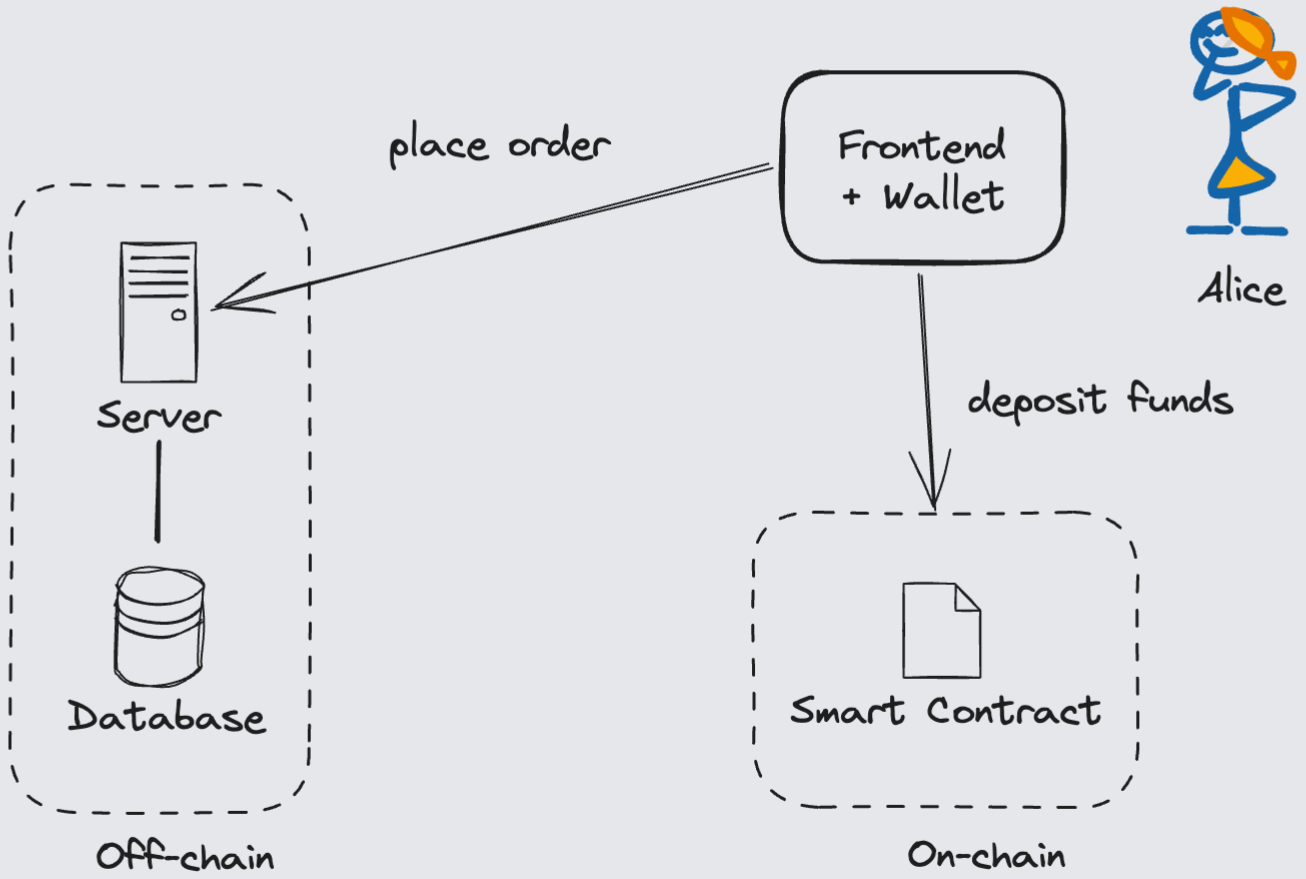
Order	Volume	Buy	Sell	Volume	Order
2	1 452	2,842	2,850	647	2
4	2 635	2,840	2,852	1 179	1
2	2 756	2,838	2,854	2 656	4
3	3 621	2,836	2,856	3 009	2
2	979	2,834	2,858	829	3
3	8 566	2,832	2,860	5 000	1
4	6 382	2,830	2,862	13 587	3
2	958	2,828	2,864	804	2
2	3 596	2,826	2,866	5 000	1
5	22 030	2,824	2,868	2 714	2



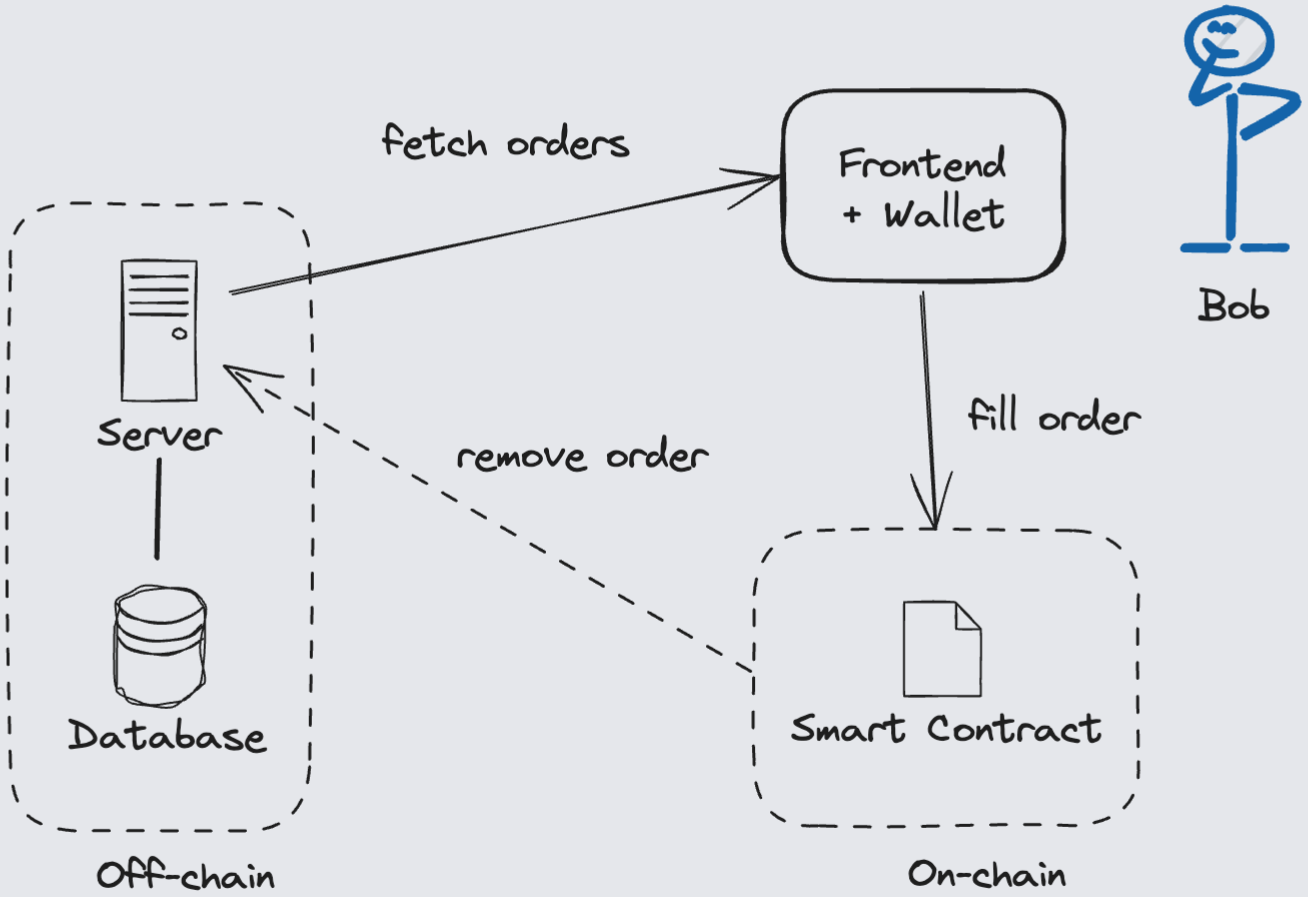
EtherDelta



Place order


place order
Frontend
+ Wallet
Alice
Server
deposit funds
Database
Smart Contract
Off-chain
On-chain

Fill order


fetch orders
Frontend
+ Wallet
Bob
Server
remove order
fill order
Database
Smart Contract
Off-chain
On-chain

DEX based on orderbook

Pros

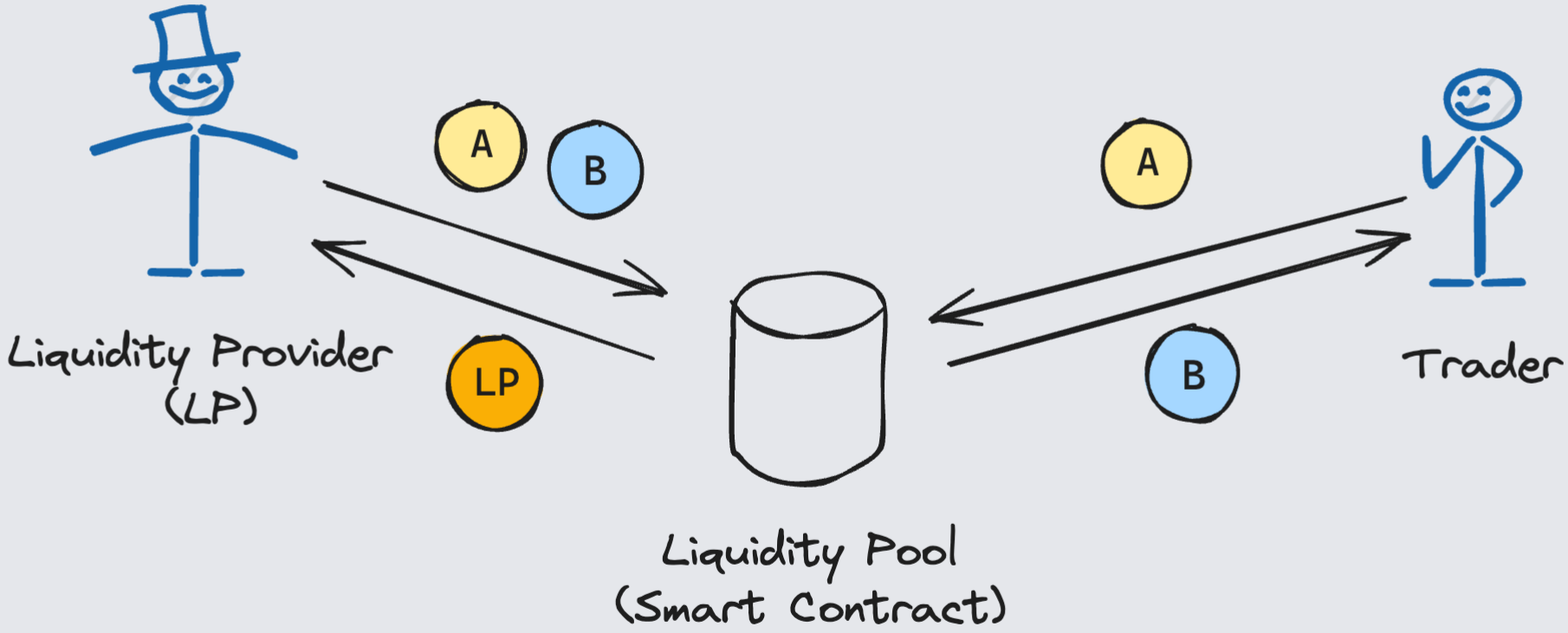
- No KYC/AML.
- No fees paid to the exchange.

Cons

- Gas fees for deposit, withdraw, trade creation/cancel
- High latency.
- Not so decentralized.

Automated Market Maker (AMM)

Liquidity pool



Why do we need DEX?

Liquidity providers

- Want to provide money to traders to earn fees.
- But have to trust someone to manage their money.

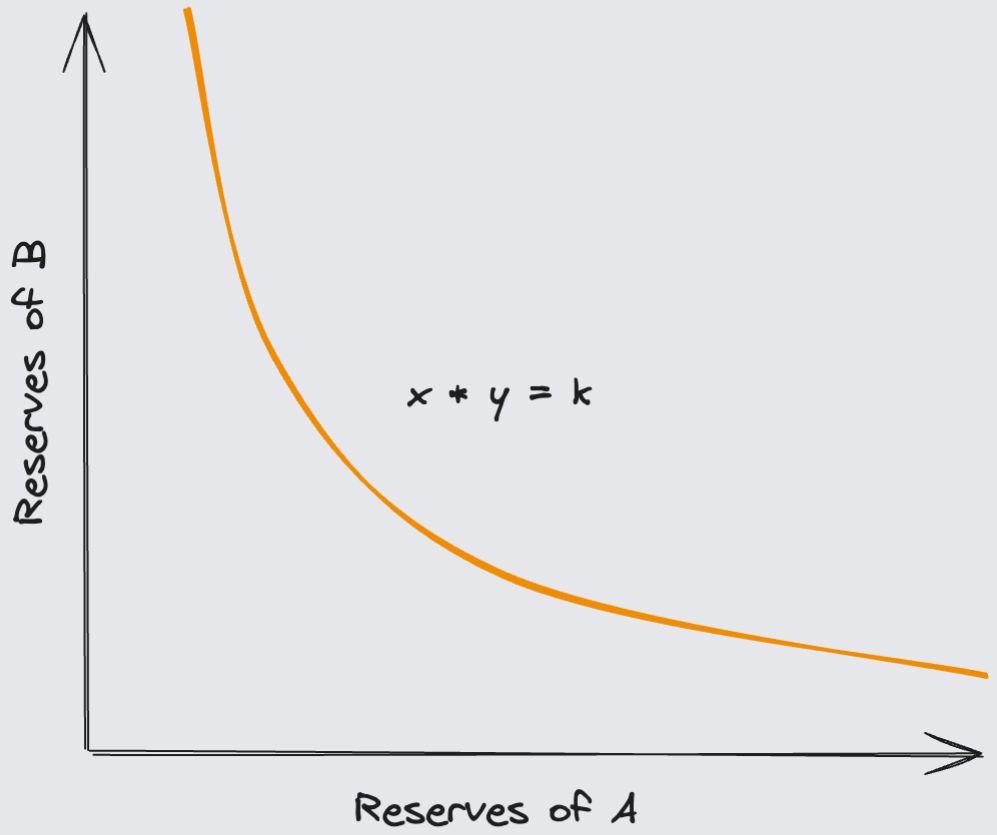
Traders

- Want to buy coins.
- But struggle to find a trusted source to buy.

Uniswap

Constant Product

- **Invariant formula**: $x \cdot y = k$
  - x – quantity of Token A.
  - y – quantity of Token B.
  - k – constant value.



Mint

When liquidity providers (LPs) supply assets to a pool, they receive LP tokens in return.

The formula for minting LP tokens is:

$$received_{LP} = \min\left(\frac{deposited_A}{total_A}, \frac{deposited_B}{total_B}\right) \cdot total_{LP}$$

Burn

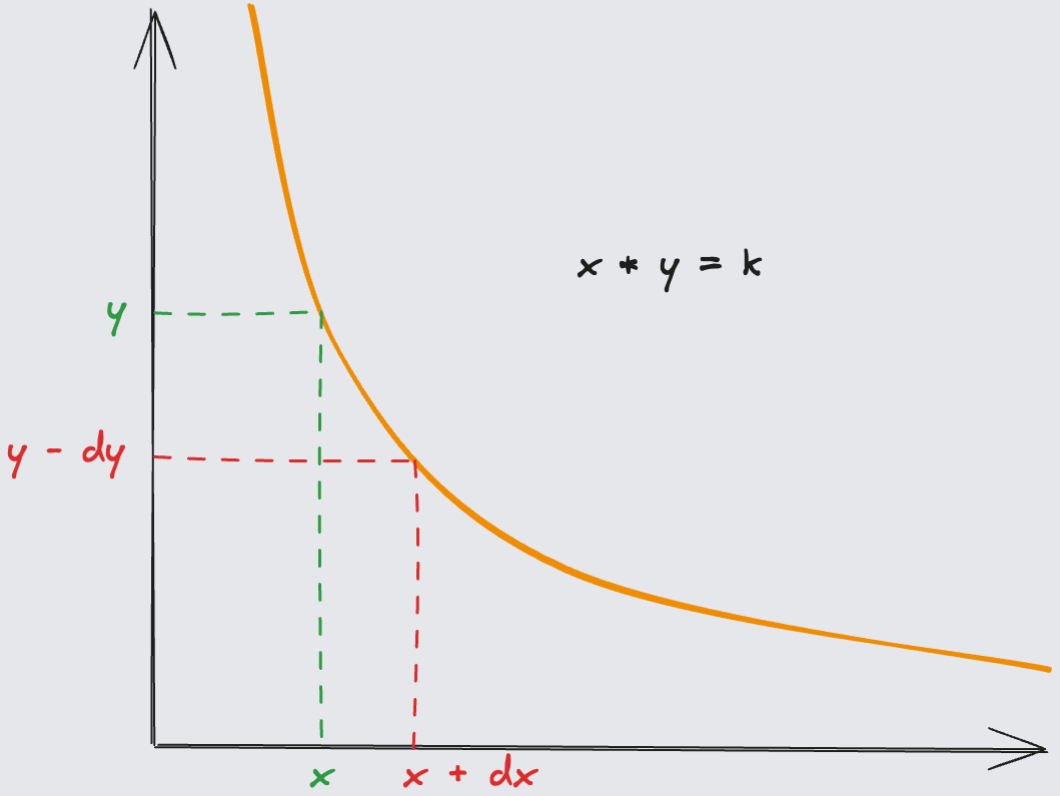
LPs can retrieve their share of the pool's assets by burning their LP tokens.

The formula for burning LP tokens and retrieving assets is:

- $received_A = \frac{burned_{LP}}{total_{LP}} \cdot total_A$
- $received_B = \frac{burned_{LP}}{total_{LP}} \cdot total_B$

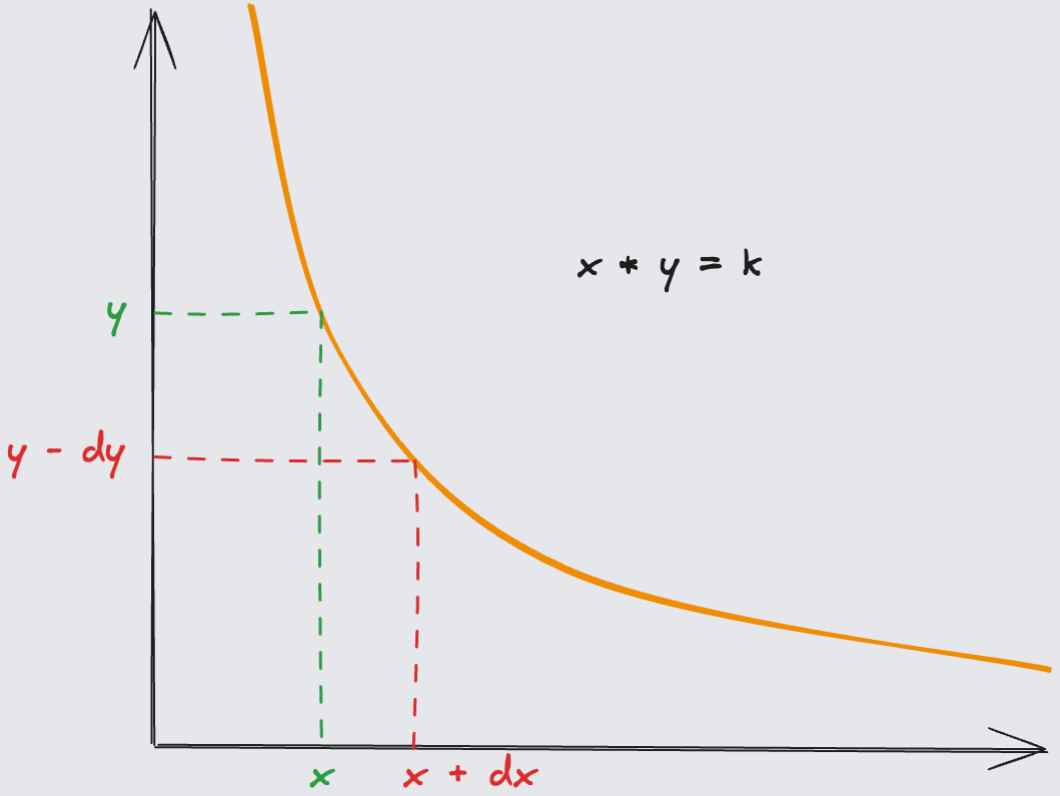
Pricing

- $(x + dx)(y - dy) = k = xy$
- $y - dy = \frac{xy}{x+dx}$
- $dy = \frac{y \cdot dx}{x+dx}$
- $\lim_{dx \to 0} \frac{dy}{dx} = \frac{y}{x}$



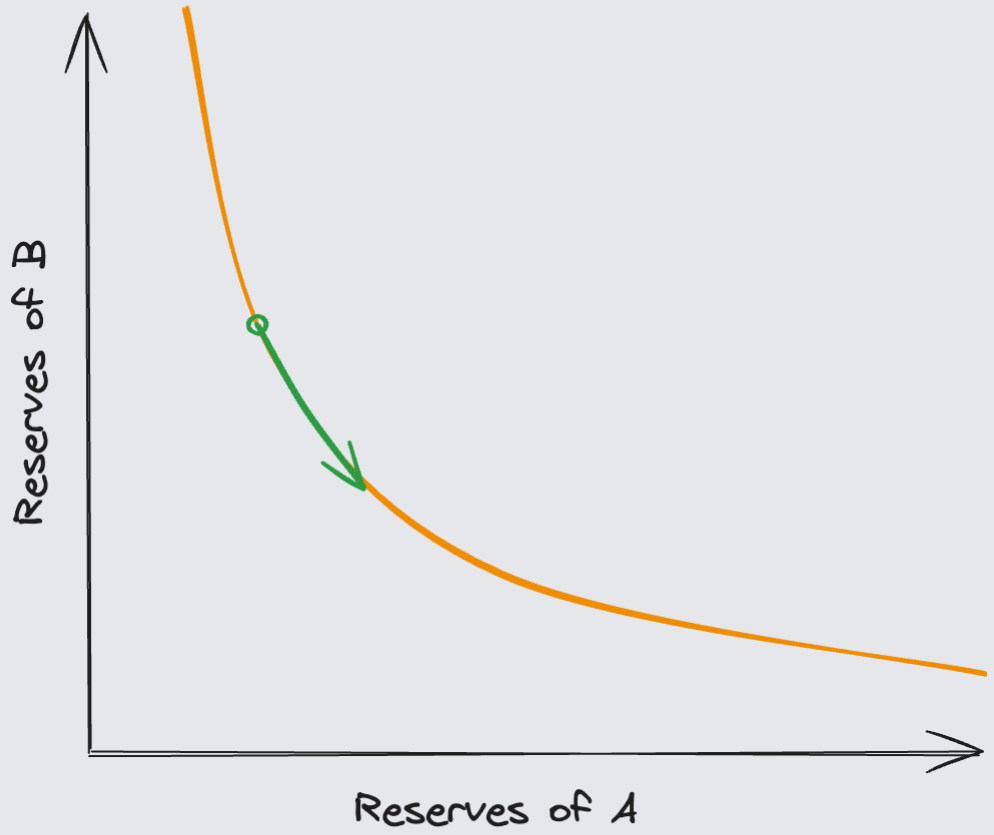
Pricing with fee

- Trading fee = 0.3%
- $(x + 0.997 \cdot dx)(y - dy) = k = xy$
- $dy = \frac{y \cdot 0.997 \cdot dx}{x + 0.997 \cdot dx}$
- $\sqrt{k} = \sqrt{xy}$ grows after each trade.
- $\sqrt{k_2} - \sqrt{k_1}$ represents growth of liquidity between two points in time.



Expected slippage

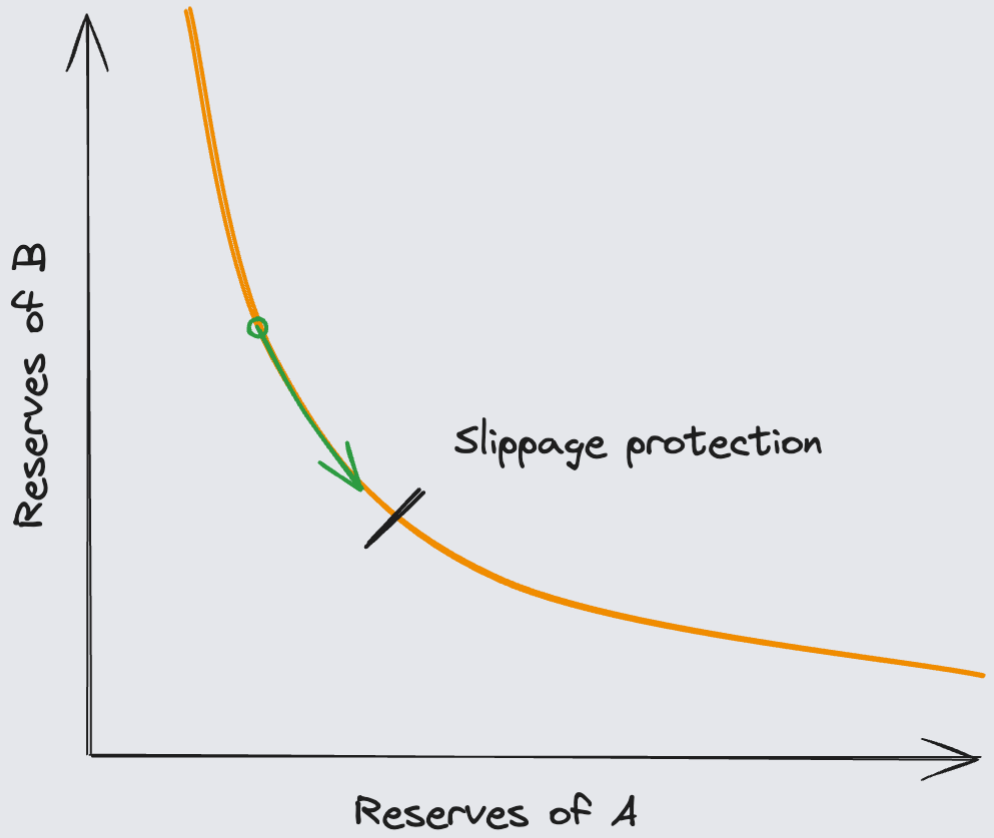
The expected increase or decrease in price based on the trading volume and available liquidity.



Unexpected slippage

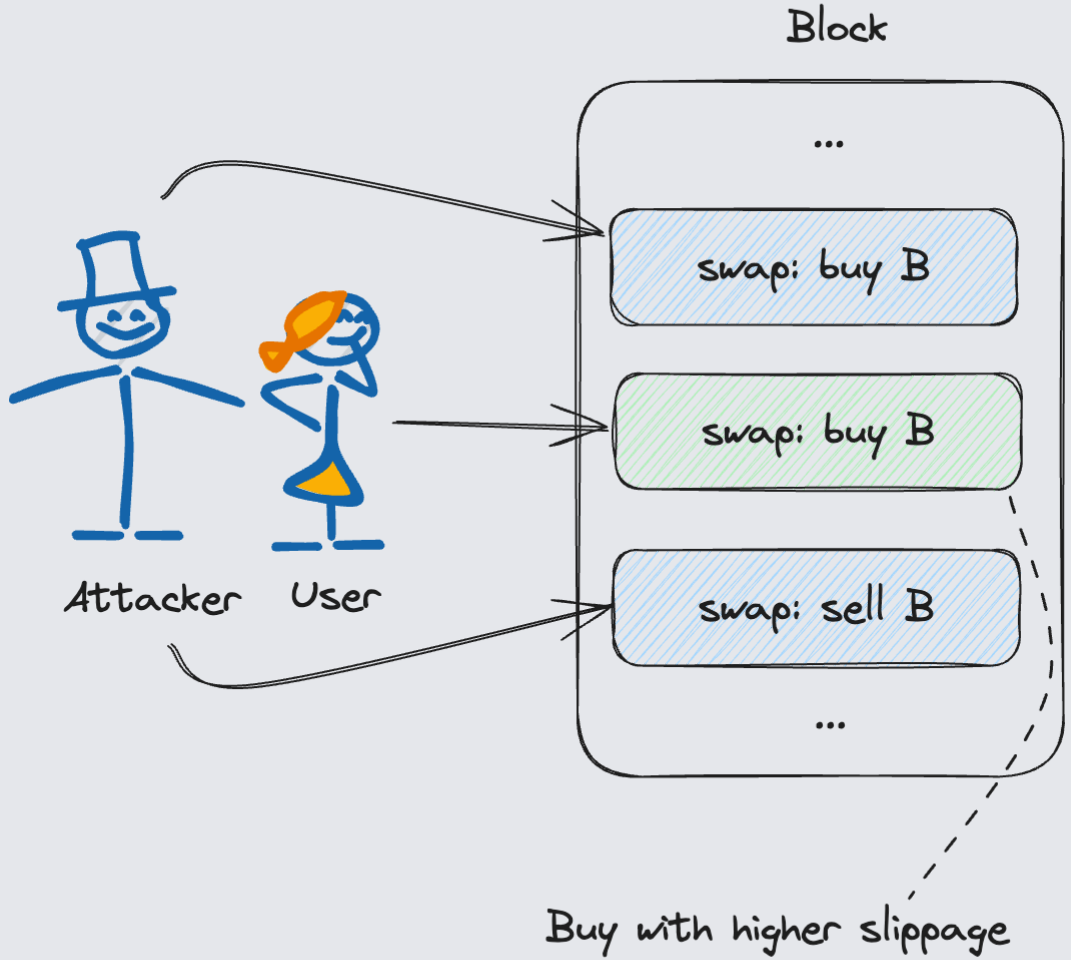
Slippage protection

Configures a slippage protection threshold to prevent unacceptable slippage.

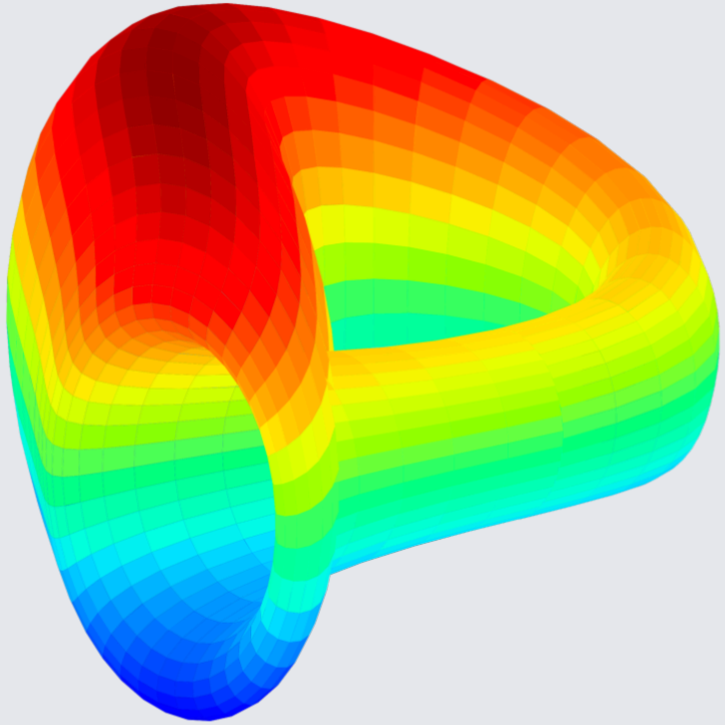


Sandwich attack

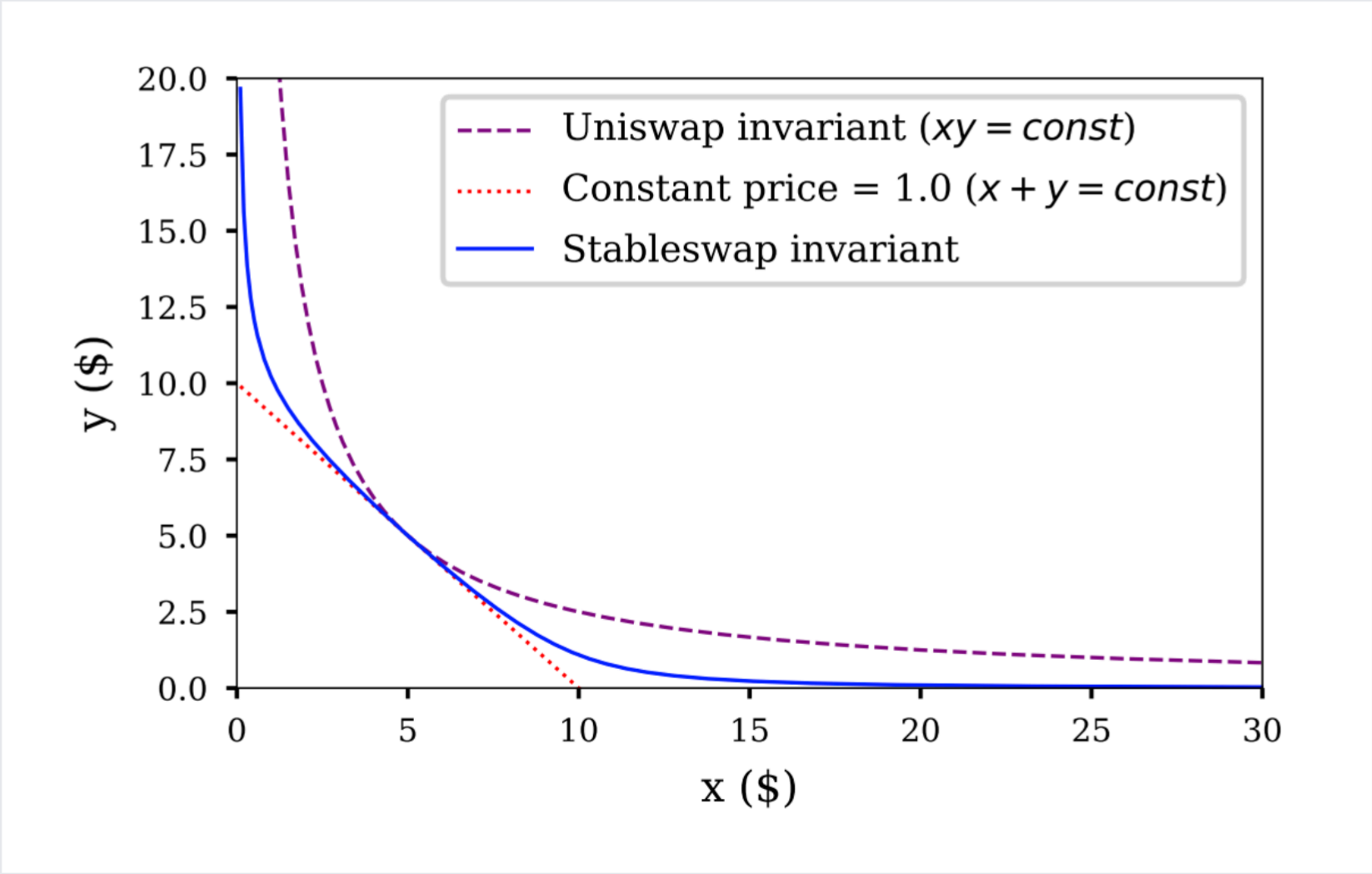
Manipulation where an attacker places buy and sell orders around a victim's transaction to artificially inflate the price and then sell at a profit.



Curve



Stableswap invariant



Stableswap invariant

- $\chi(x+y)+xy=\chi D+\frac{D^2}{4}$
- The multiplier χ will magnify the low slippage portion of the equation.
- $\chi=\frac{Axy}{(\frac{D}{2})^2}$ – ideally the the curve is linear when pools are equally balanced.
- **Final formula**: $4A(x+y)+D=4DA+\frac{D^3}{4xy}$

Uniswap V3

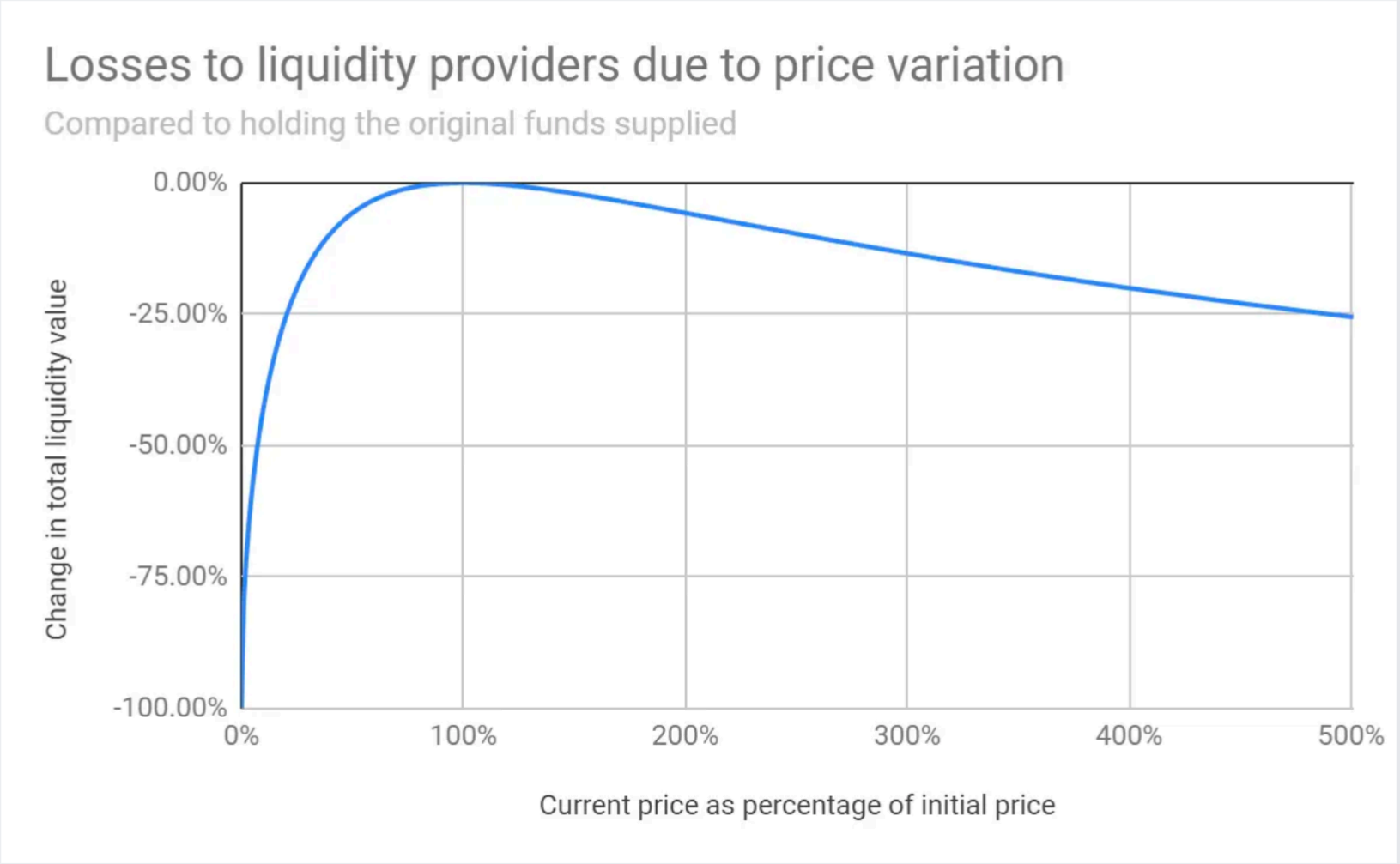
Impermanent loss

					Price		Total
Initial	2000	+	1	x	2000	=	4000
Price changed	2236	+	0.8944	x	2500	=	4472
If holded	2000	+	1	x	2500	=	4500

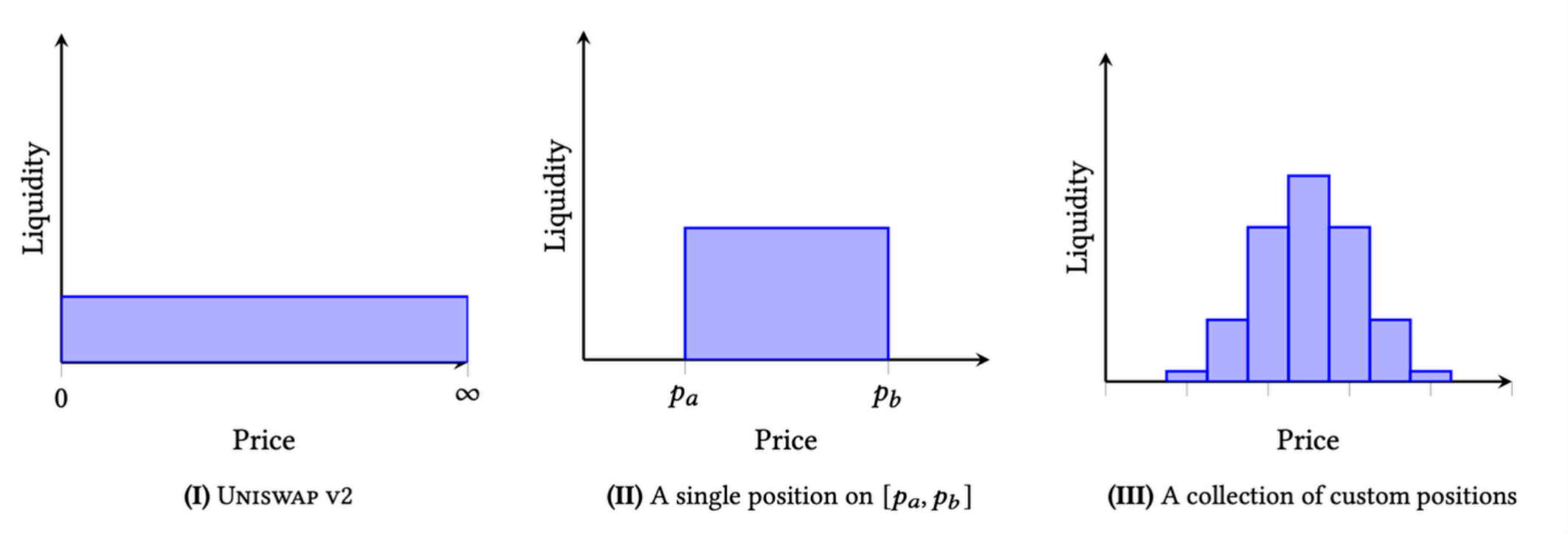
28

Impermanent loss

Impermanent loss



Concentrated liquidity



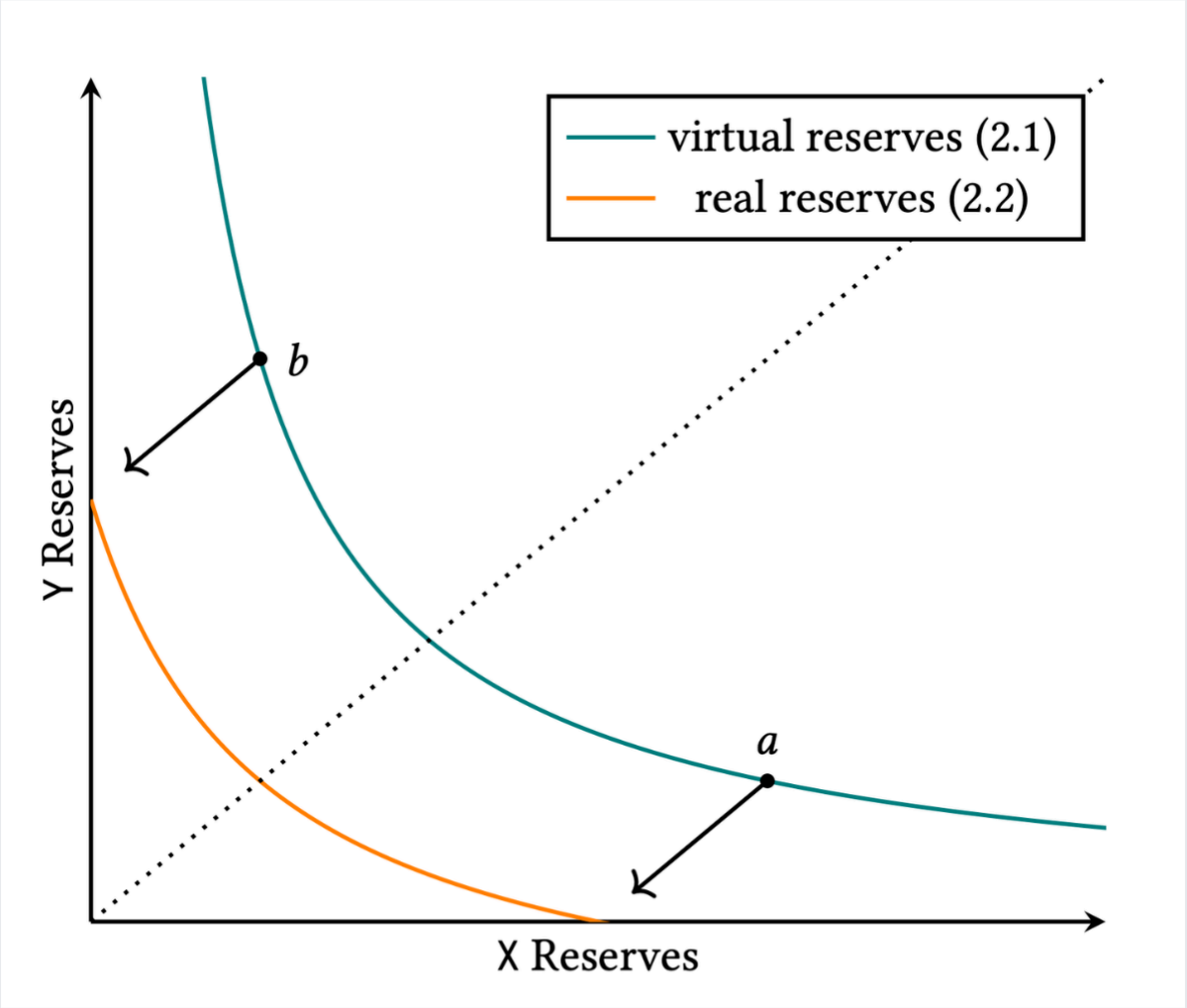
Virtual liquidity

Virtual reserves

$$x \cdot y = L^2$$

Real reserves

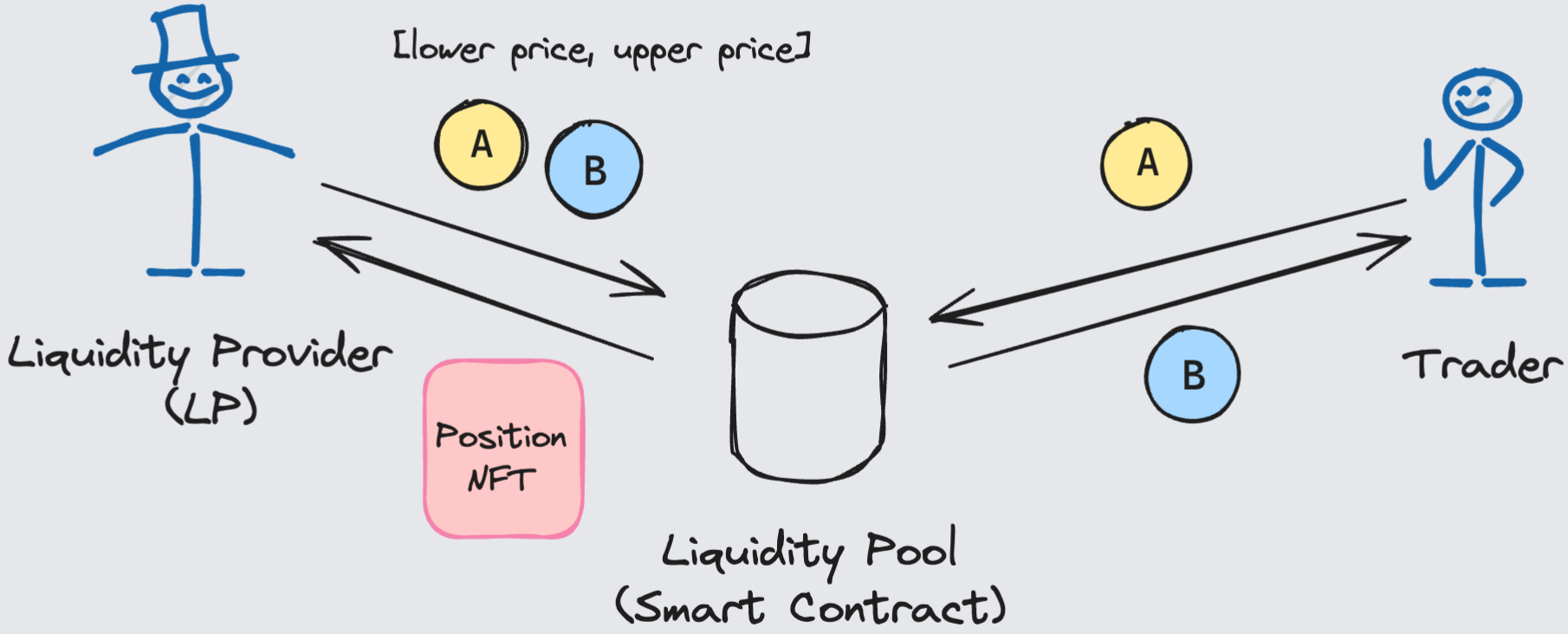
$$(x + \frac{L}{\sqrt{p_b}})(y + L\sqrt{p_a}) = L^2$$



Math behind

- $(x + \frac{L}{\sqrt{p_b}})(y + L\sqrt{p_a}) = L^2$
- $y = \frac{L^2}{x + \frac{L}{\sqrt{p_b}}} - L\sqrt{p_a}$
- $price = -\frac{dy}{dx} = \frac{L^2}{(x + \frac{L}{\sqrt{p_b}})^2} = \frac{L^2}{L^4} \cdot (y + L\sqrt{p_a})^2 = \frac{(y + L\sqrt{p_a})^2}{L^2}$
- Check cases when $x = 0$ and $y = 0$

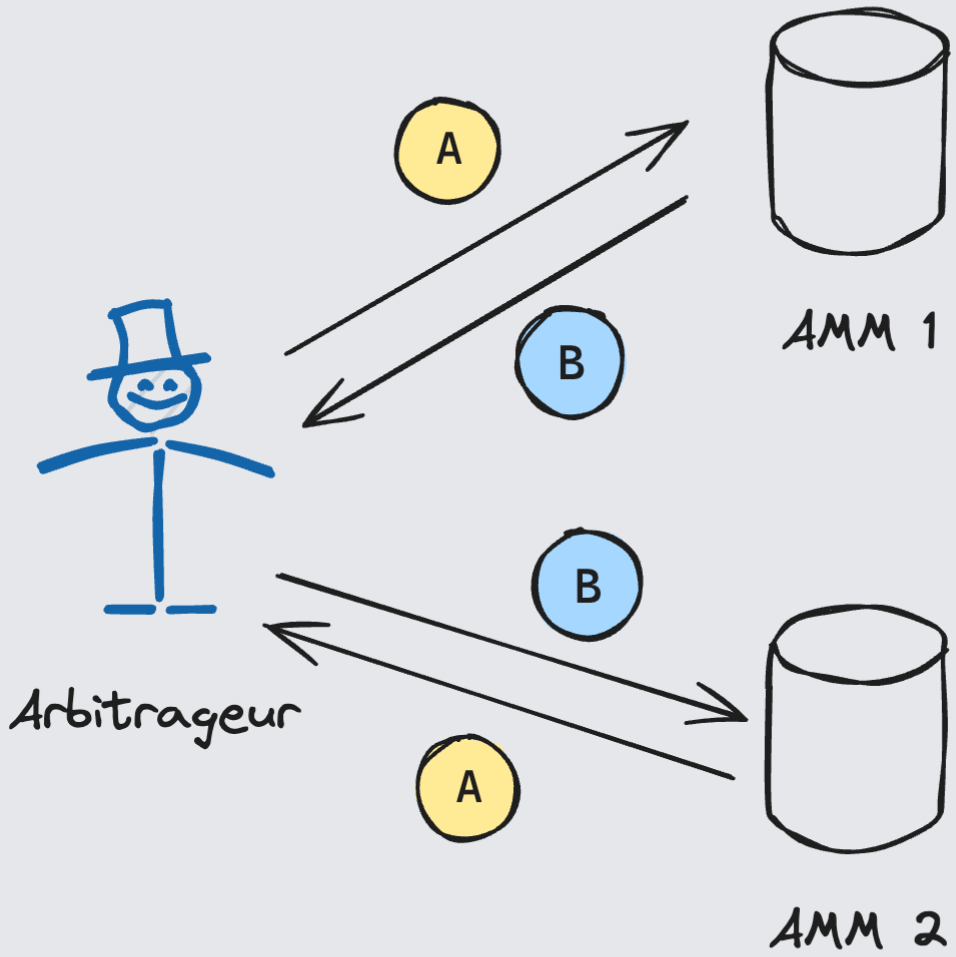
General scheme



Can AMM price deviate from "real market" price?

Arbitrage

- Prices are synchronized by arbitrageurs.
- Arbitrage is exploiting price discrepancies across different DEXes for profit.



DEX price as price oracle?