

Decentralized Finance

Decentralized Exchanges (DEX)

Instructors: Dan Boneh, Arthur Gervais, Andrew Miller, Christine Parlour, Dawn Song



 Stanford
University



Imperial College
London



 UNIVERSITY OF
ILLINOIS
URBANA-CHAMPAIGN

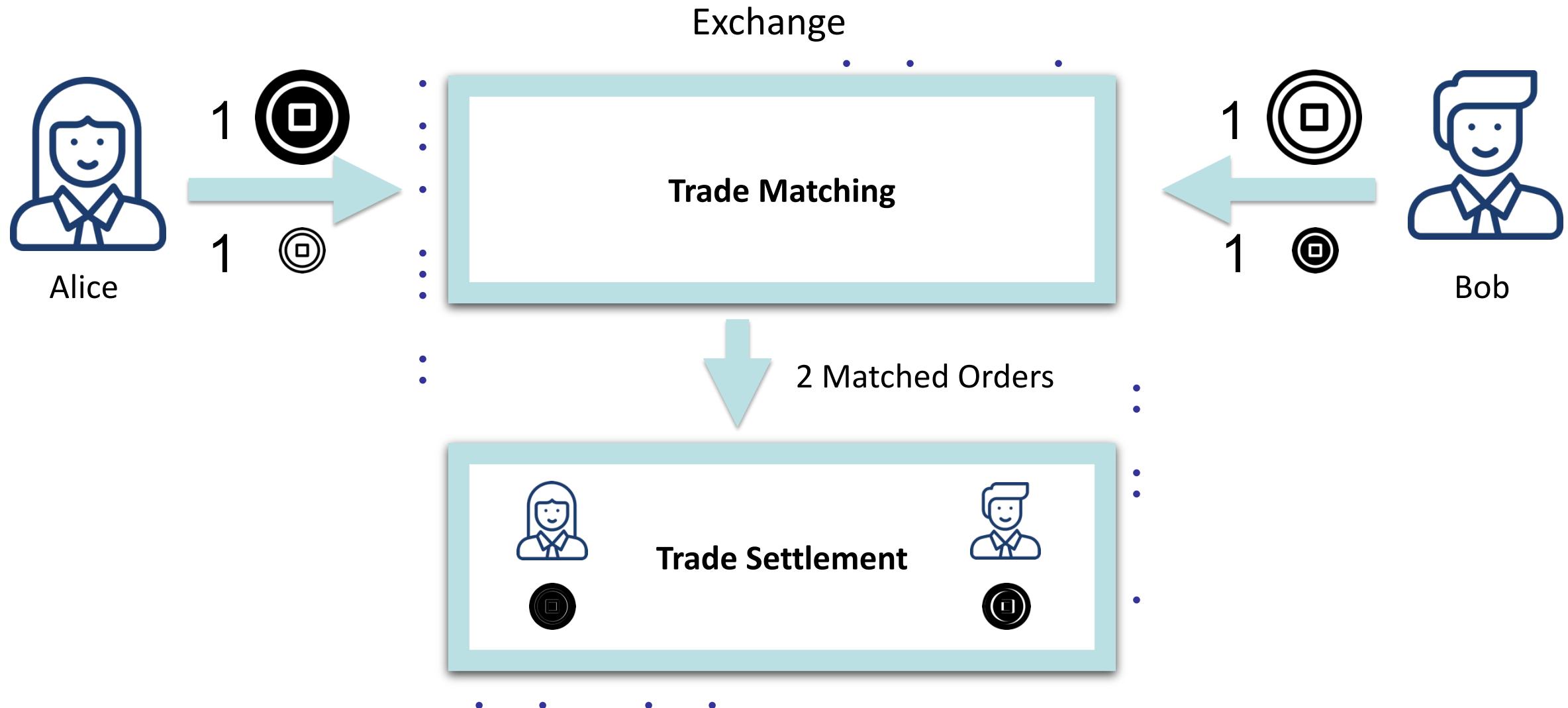


Berkeley
UNIVERSITY OF CALIFORNIA

Financial Exchanges



Financial Exchanges 101



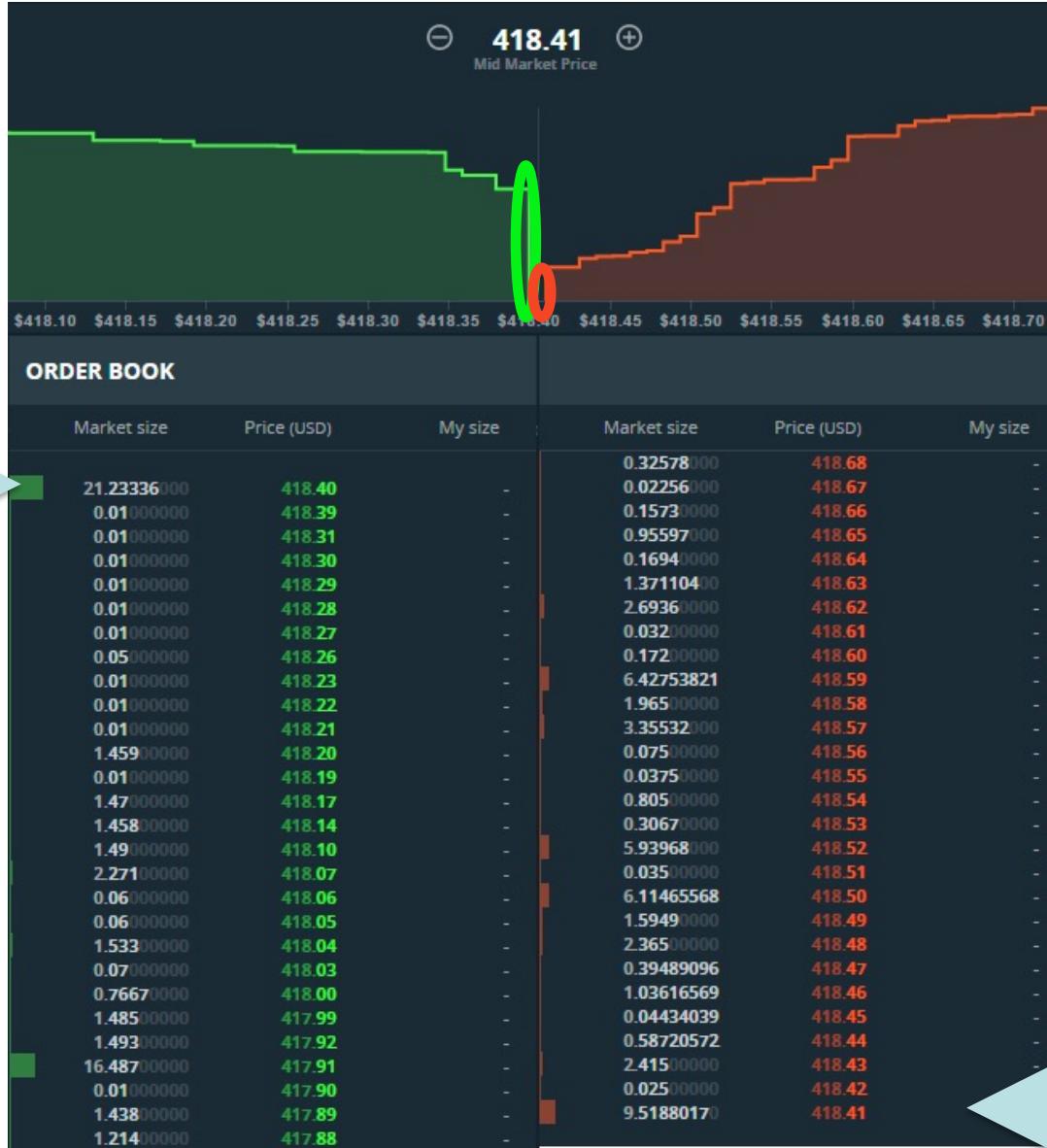
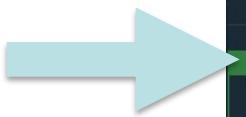
Trade Matching Models

Exchange

Trade Matching

**Non-Custodial
Trade Settlement**

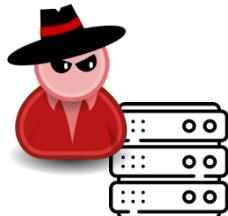
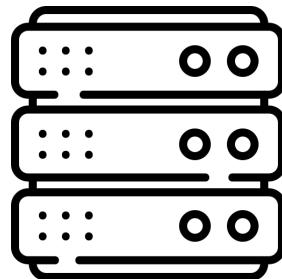
Order Book



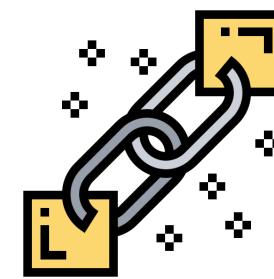
Two Order Book Models

- + Fast matching
- + No fees for canceled orders
- No censorship resistance
- Exchange front running

Server



On-Chain



- + Censorship resistance
- + Robust
- Slow matching
- Blockchain fees for orders
- Miner/trader front running



EtherDelta

EtherDelta | PPT | Chat | Help | Tokens | Contract | English | Account

Balance

Deposit Withdraw Transfer

Please select an account using the account dropdown in the upper right.

Order Book

| PPT | 0.024880000 | 0.995 |
|---------|-------------|--------|
| 40.000 | 0.024422244 | 0.077 |
| 25.000 | 0.024000000 | 0.600 |
| 2.583 | 0.023450000 | 0.061 |
| 30.000 | 0.023330000 | 0.700 |
| 7.134 | 0.022400000 | 0.160 |
| 15.000 | 0.022000000 | 0.330 |
| 20.000 | 0.021000000 | 0.420 |
| 587.500 | 0.019777777 | 11.619 |
| 5.000 | 0.019770000 | 0.099 |
| 189.000 | 0.019000000 | 3.591 |
| 400.000 | 0.018990000 | 7.596 |
| 252.898 | 0.018900000 | 4.780 |
| 200.000 | 0.017999000 | 3.600 |
| 10.000 | 0.017888880 | 0.179 |
| 1.500 | 0.017400000 | 0.026 |
| 50.006 | 0.017399999 | 0.870 |
| 50.006 | 0.017399999 | 0.870 |

Buy/Sell

Buy Order Sell Order

Amount to buy PPT

Price ETH

Total

Expires

Order Book

| PPT | PPT/ETH | ETH |
|----------|-------------|--------|
| 0.500 | 0.015175100 | 0.008 |
| 6.800 | 0.015069000 | 0.102 |
| 14.186 | 0.014605753 | 0.207 |
| 14.560 | 0.014230001 | 0.207 |
| 10.000 | 0.014230000 | 0.142 |
| 15.000 | 0.014220000 | 0.213 |
| 0.211 | 0.014210000 | 0.003 |
| 150.000 | 0.014000000 | 2.100 |
| 15.000 | 0.013330000 | 0.200 |
| 3000.000 | 0.013301000 | 39.903 |
| 500.000 | 0.013300000 | 6.650 |
| 43.527 | 0.013000000 | 0.566 |
| 5.988 | 0.011131000 | 0.067 |
| 11.111 | 0.011111111 | 0.123 |
| 5.678 | 0.011001100 | 0.062 |
| 4.234 | 0.010345678 | 0.044 |
| 25.000 | 0.010301030 | 0.258 |
| 1500.000 | 0.010200000 | 15.300 |
| 20.000 | 0.010191010 | 0.260 |

Price Chart

PPT/ETH ▲ 0.015508 +4.584%

1H 2H 6H 24H

Sep 2 Sep 9 Sep 16

Trades & Volume

| Time | PPT | PPT/ETH |
|------------------|---------|-------------|
| 6:00:32 PM 9/18 | 10.000 | 0.015507512 |
| 5:59:32 PM 9/18 | 290.000 | 0.015359271 |
| 5:17:43 PM 9/18 | 25.000 | 0.015432548 |
| 2:30:01 PM 9/18 | 13.644 | 0.015498731 |
| 12:10:40 PM 9/18 | 20.000 | 0.017399999 |
| 10:33:54 AM 9/18 | 8.765 | 0.015128456 |
| 8:24:26 AM 9/18 | 10.000 | 0.015000000 |
| 8:22:41 AM 9/18 | 10.000 | 0.015030000 |
| 8:17:02 AM 9/18 | 10.000 | 0.015166125 |
| 8:16:40 AM 9/18 | 38.731 | 0.015175101 |
| 8:16:40 AM 9/18 | 15.890 | 0.015175860 |
| 8:07:06 AM 9/18 | 11.269 | 0.015175101 |
| 6:58:17 AM 9/18 | 200.000 | 0.015565806 |
| 5:47:25 AM 9/18 | 99.500 | 0.015175100 |
| 3:05:30 AM 9/18 | 0.993 | 0.016127865 |
| 11:12:57 PM 9/17 | 62.000 | 0.016025931 |
| 10:50:41 PM 9/17 | 463.228 | 0.016041887 |
| 9:33:59 PM 9/17 | 67.000 | 0.016252595 |

Your Transactions

Trades Orders Funds

Updates

Important Twitter

Notices

The only official URL for EtherDelta is <https://etherdelta.com>. Bookmark it once and use the bookmark.

Do not send your tokens directly to the smart contract, or they will be lost and unrecoverable. Use the Deposit form (upper left) to send the proper deposit transaction.

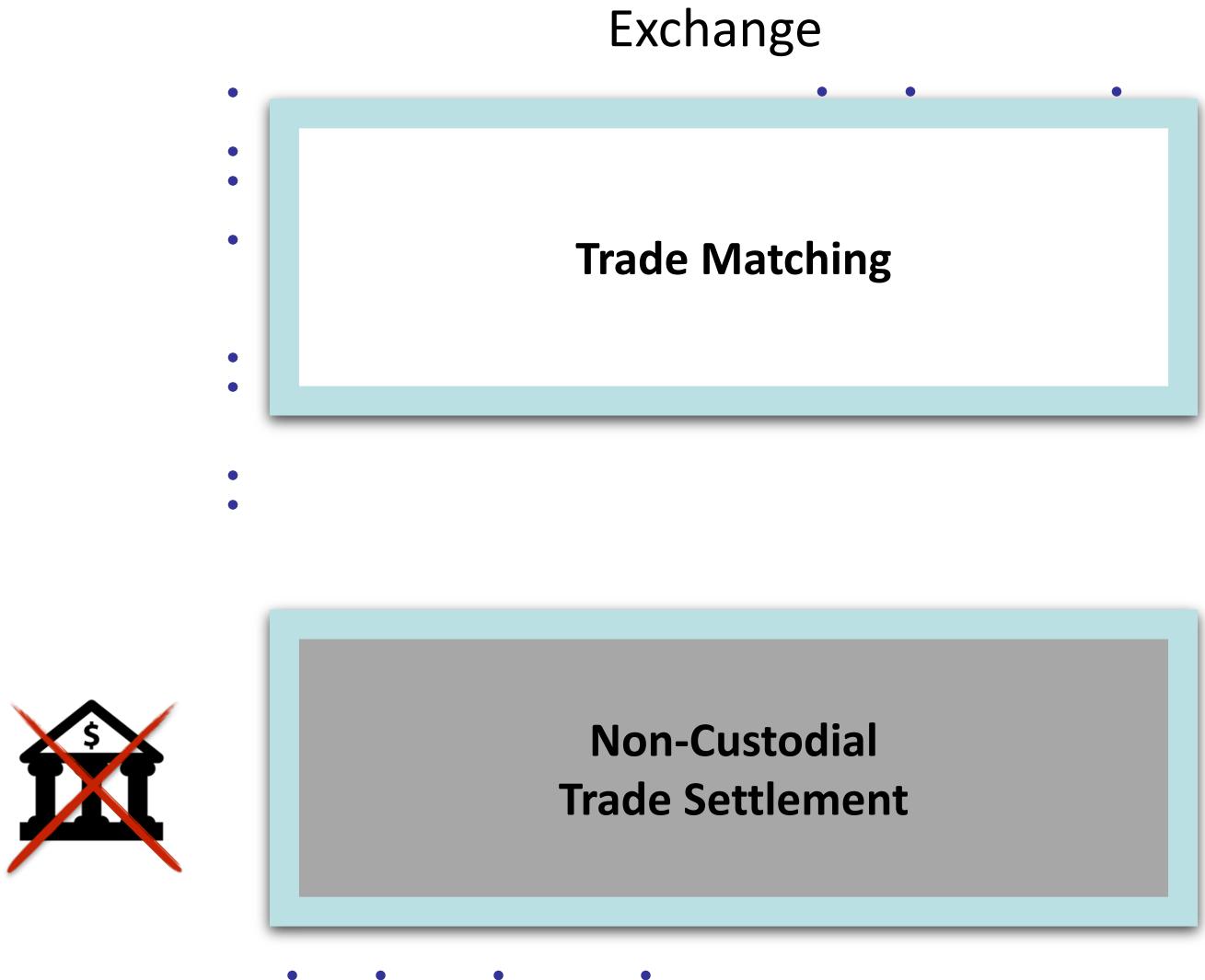
The only official representatives in the chat

LOB DEX: Lessons Learned

- Advantages:
 - No KYC/AML
 - No fees paid to the exchange
 - No impermanent loss (explained later in AMM)

- Disadvantages:
 - Fees for deposit, withdraw, trade creation/cancel
 - Slow execution
 - Not fully decentralized (mediating server)

Settlement Layer



Why do we need DEX?



Alice is rich
(aka a “whale”)



Bob is nifty
trader

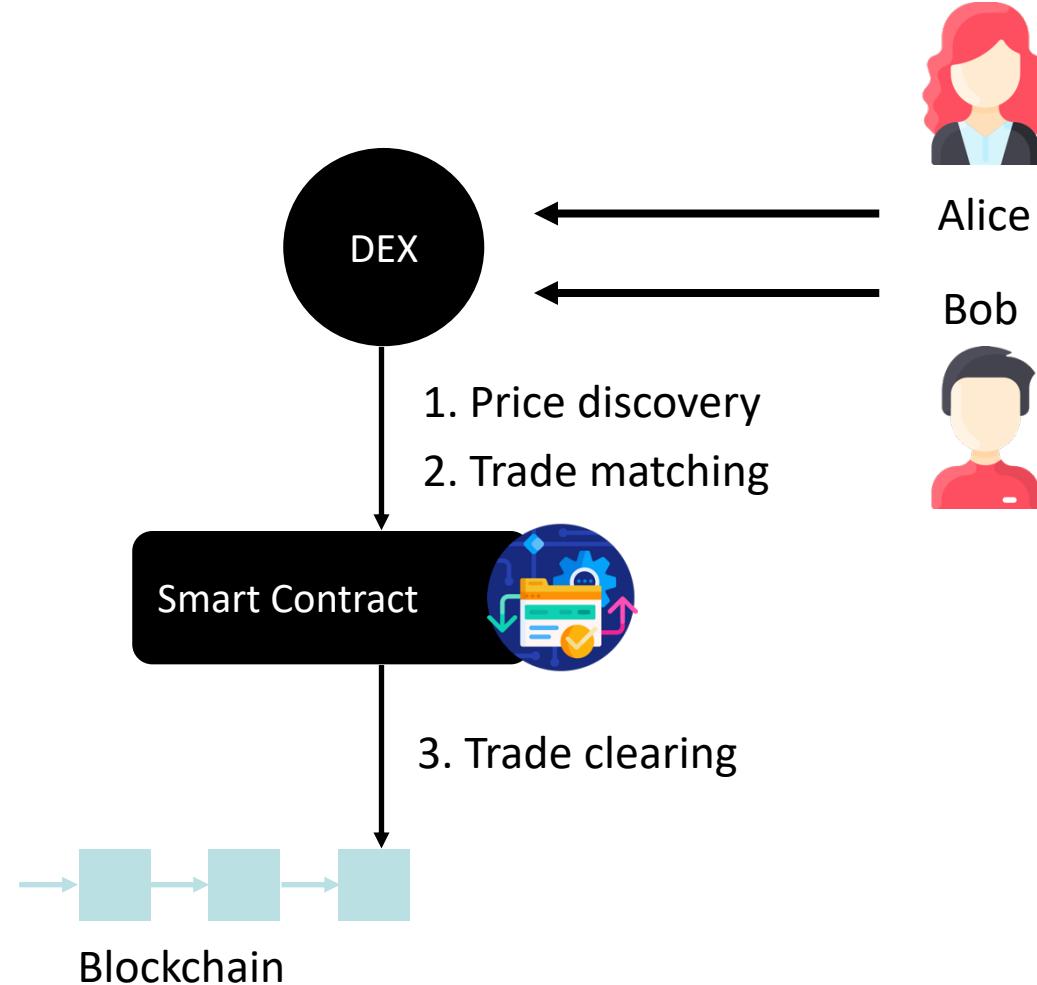
Alice wants to provide her
money to traders to earn fees

Bob wants to buy
the latest coins

..but has to trust someone
to manage her money

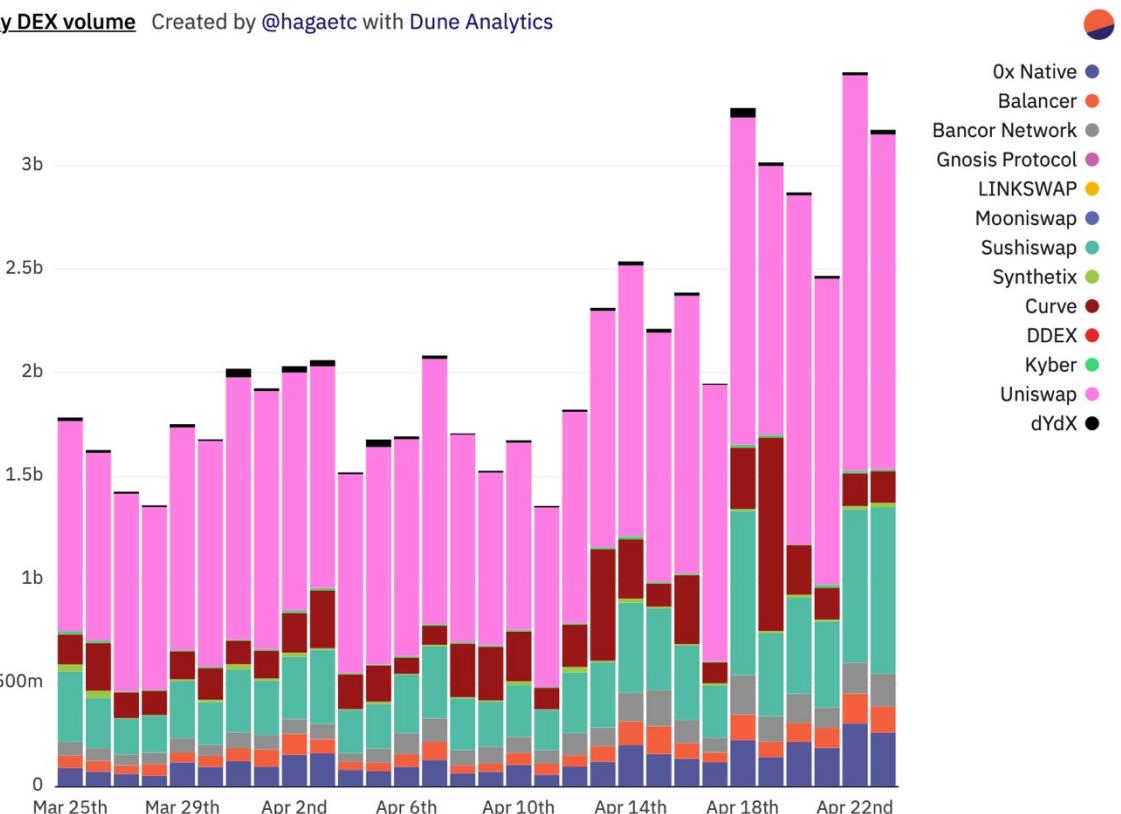
..but struggles to find
a trusted source to buy

DEX System Architecture

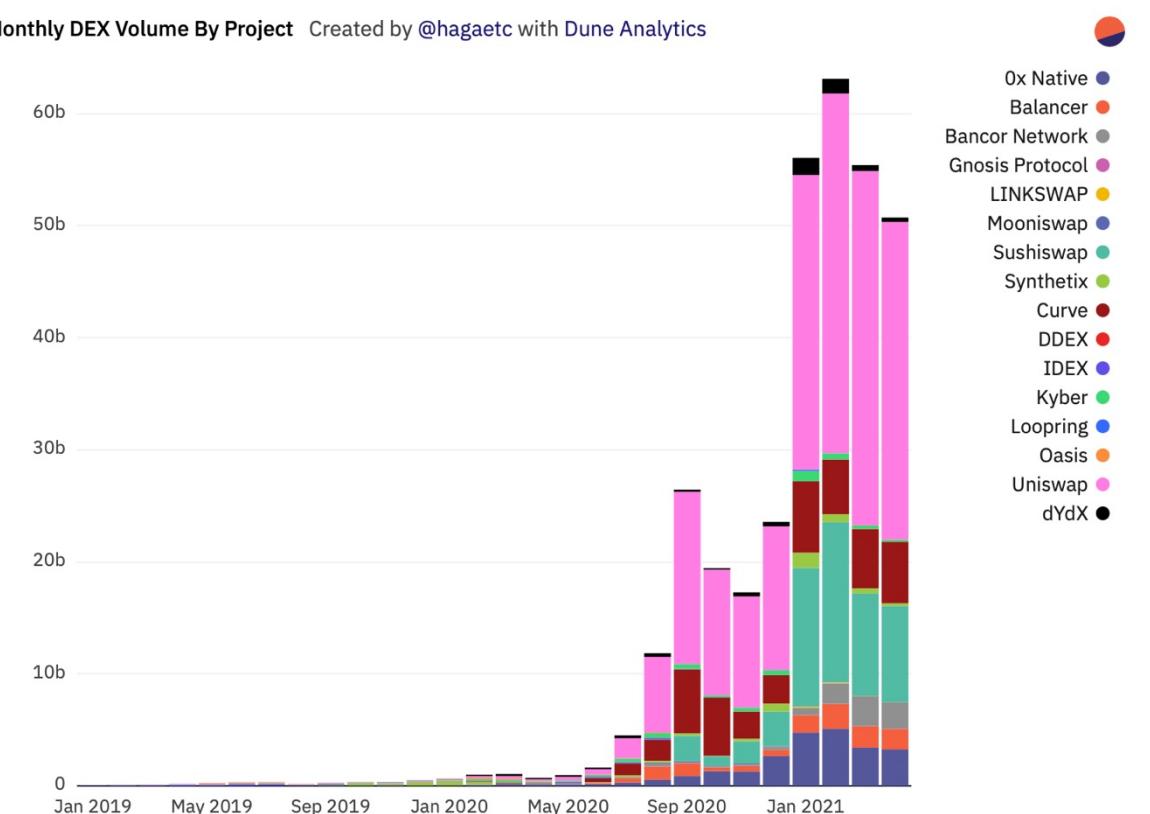


DEX trading volume

Daily DEX volume Created by @hagaetc with Dune Analytics



Monthly DEX Volume By Project Created by @hagaetc with Dune Analytics



Daily Volume:
- DEXes: 3.5B
- Binance: 49B
- Nasdaq: 234B

Source:

<https://defiprime.com/dex-volume>

<http://www.nasdaqtrader.com/Trader.aspx?id=DailyMarketSummary>

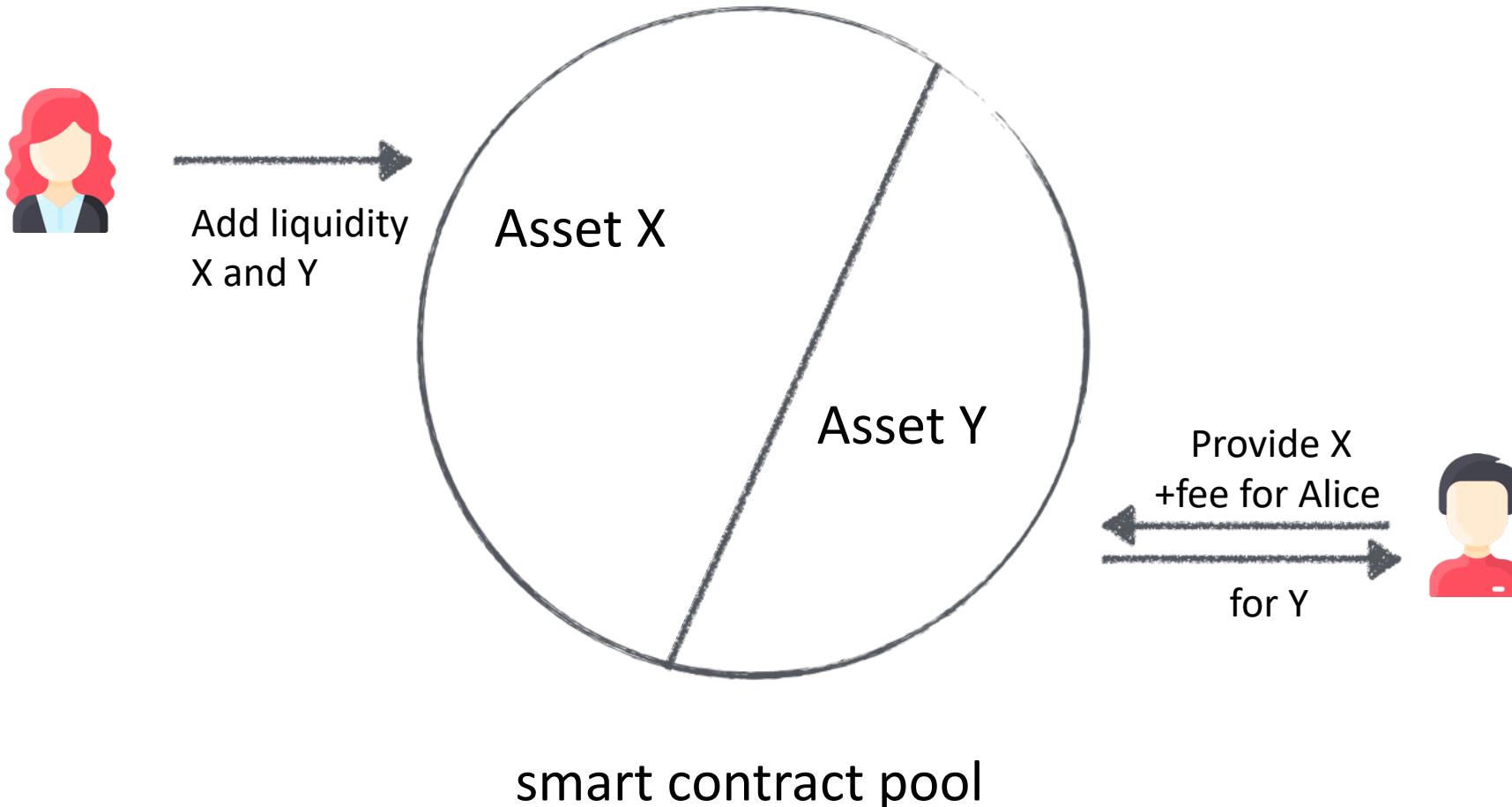
<https://coinmarketcap.com/rankings/exchanges/>

A night-time satellite view of Earth from space, showing city lights and auroras.

Automated Market Maker

Liquidity Pool

Idea: Let a smart contract do the market making.



AMM – Automated Market Maker

Idea: Let a smart contract do the market making.

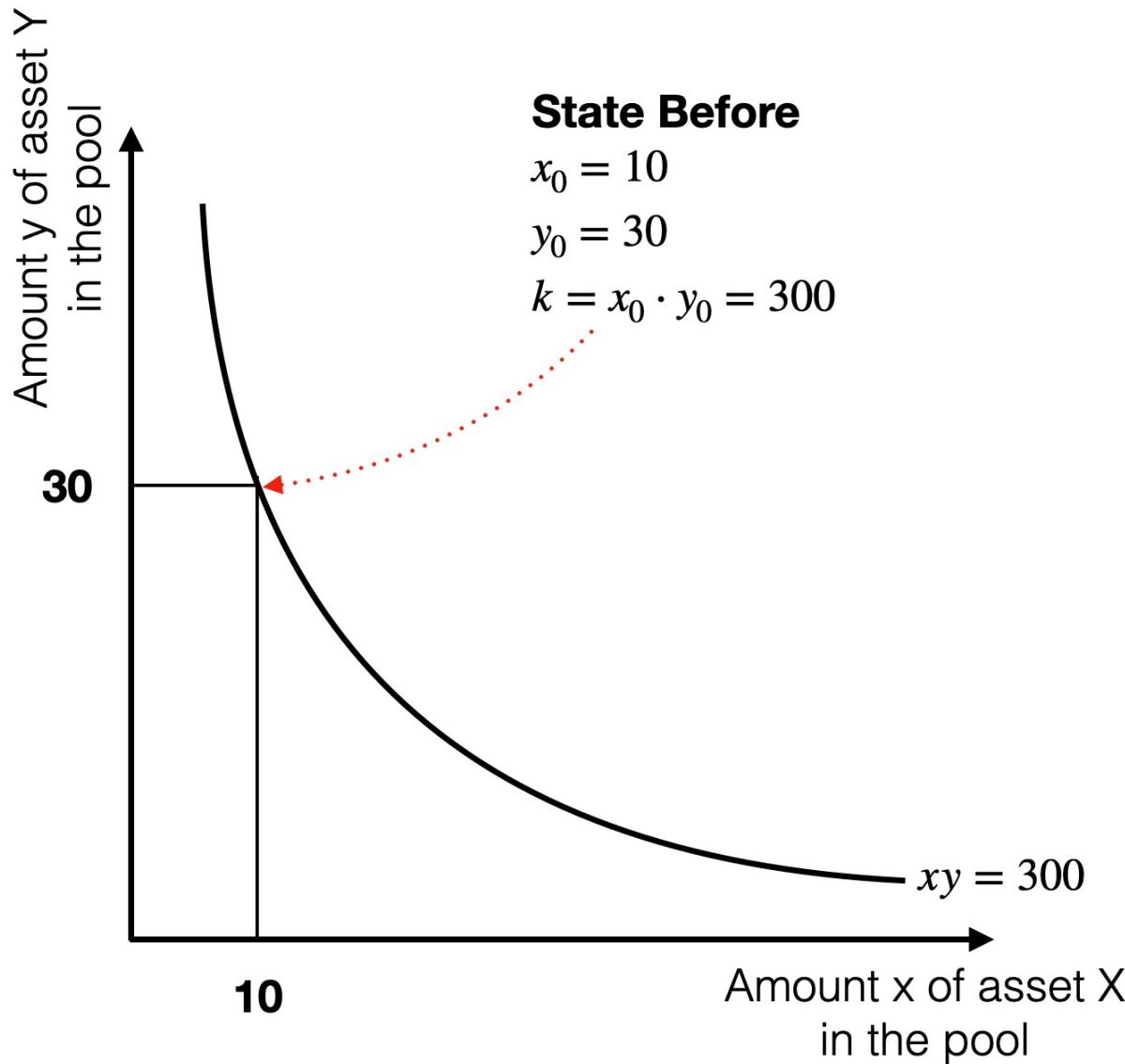
$$x \times y = k$$

The diagram illustrates the mathematical relationship of a Constant Product AMM. At the top is the equation $x \times y = k$. Three arrows point downwards from the variables x and y to the labels "Asset X quantity" and "Asset Y quantity" respectively. A single arrow points downwards from the product k to the label "constant".

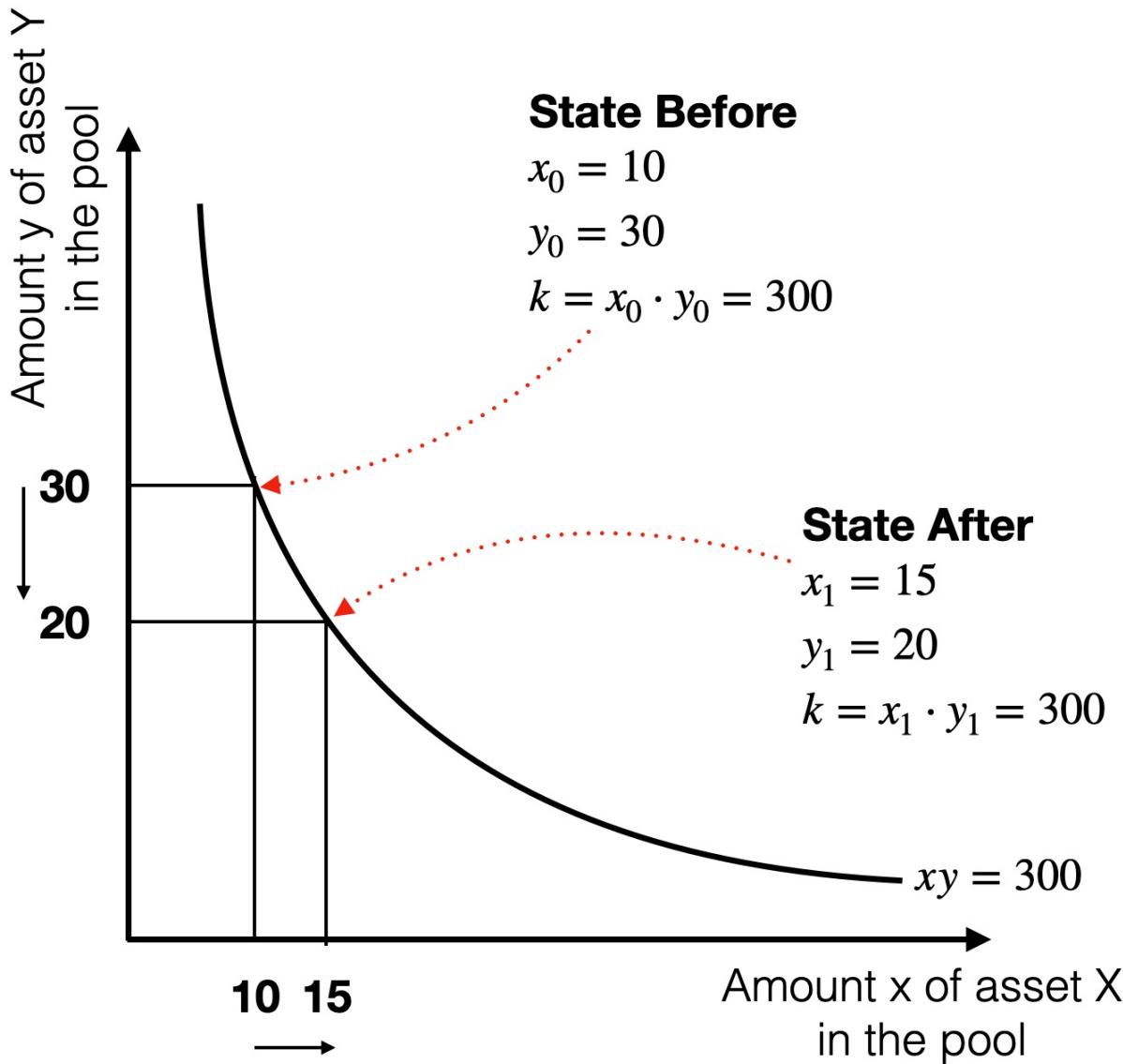
Properties:

- Instant liquidity, irrespective of the trade size
- Purchase of asset X **increases price** of X and **decreases the price** of Y
- Ratio of asset X and Y sets the price
- Known as Constant Product (CP) AMM

AMM Example

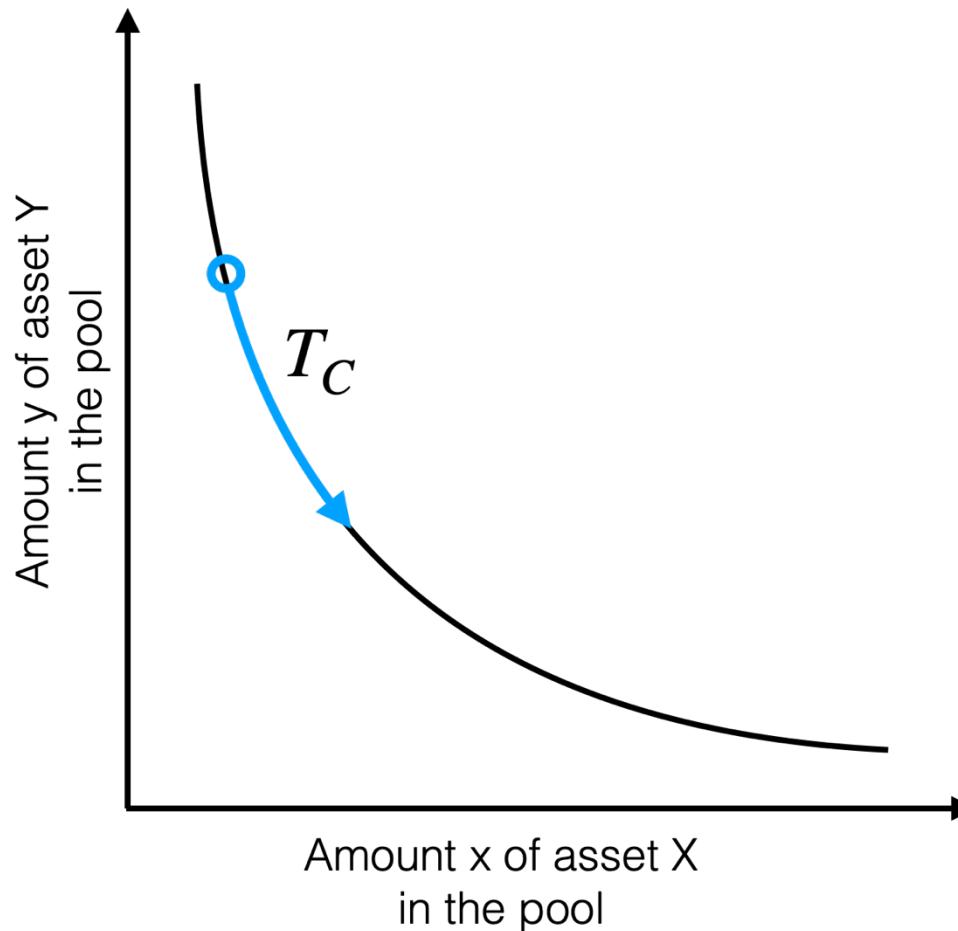


AMM Example

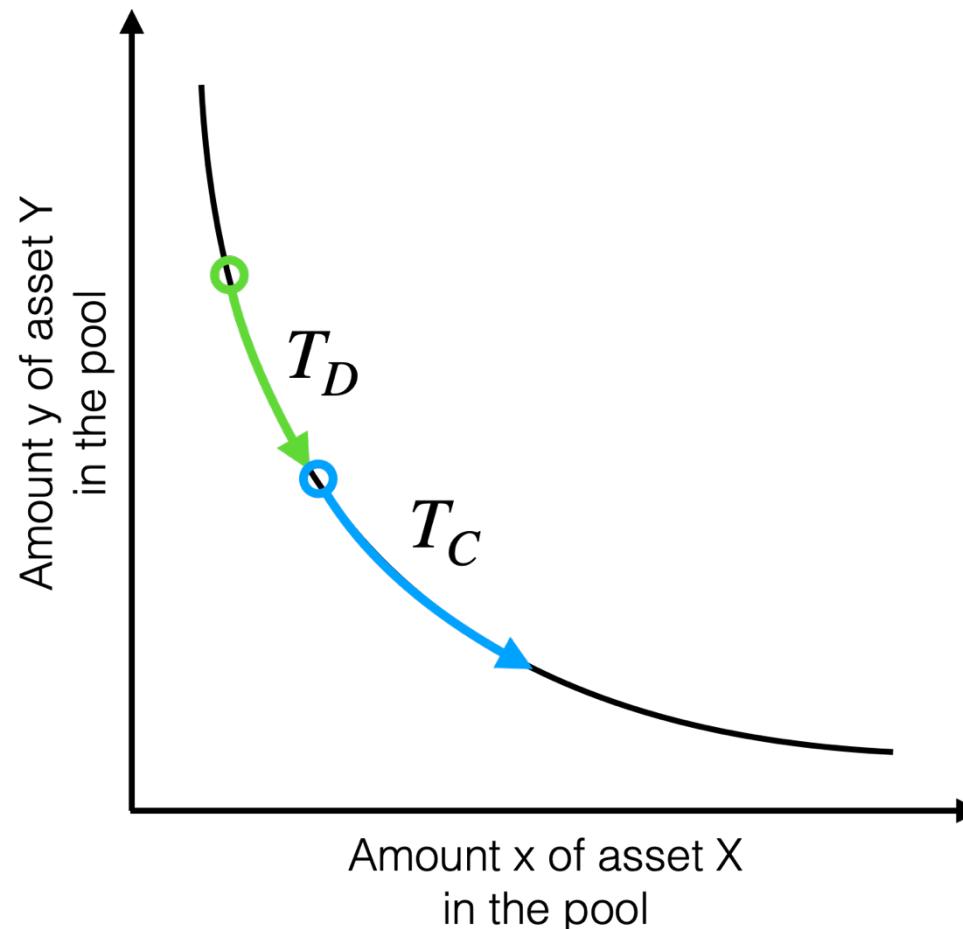


Expected Slippage

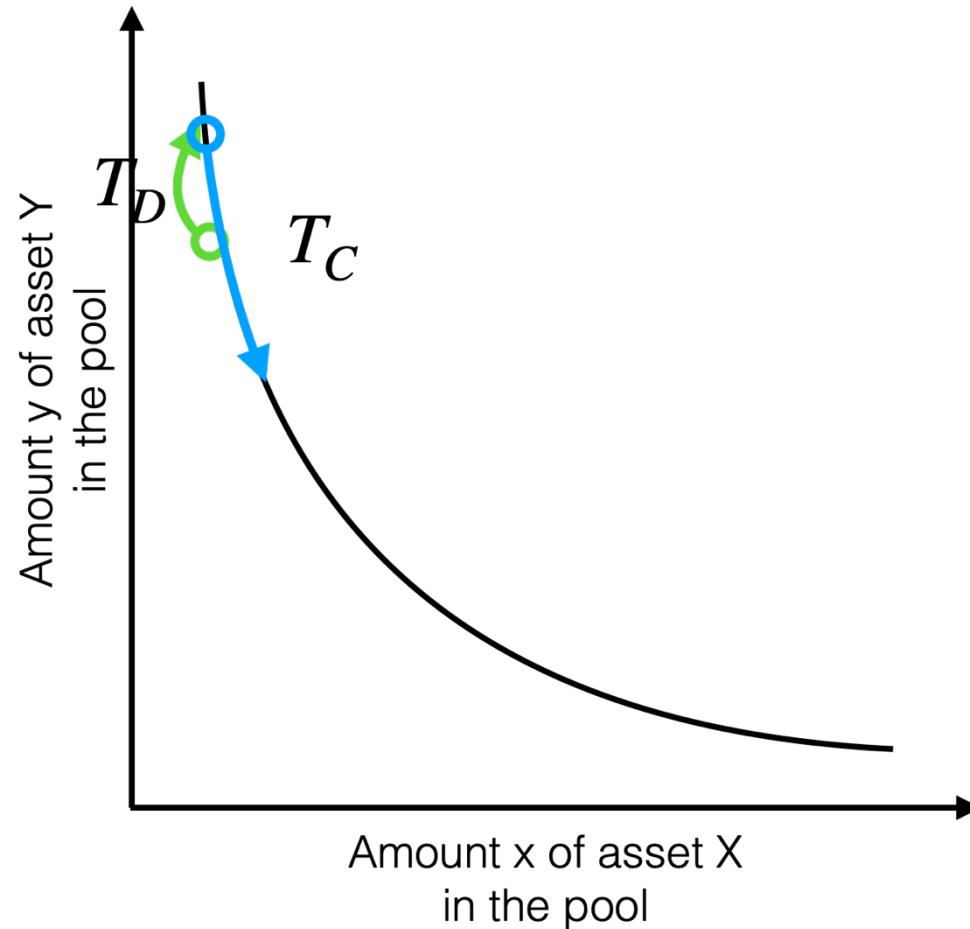
The expected increase or decrease in price based on the trading volume and available liquidity.



Unexpected Slippage \rightarrow Worse Execution Price

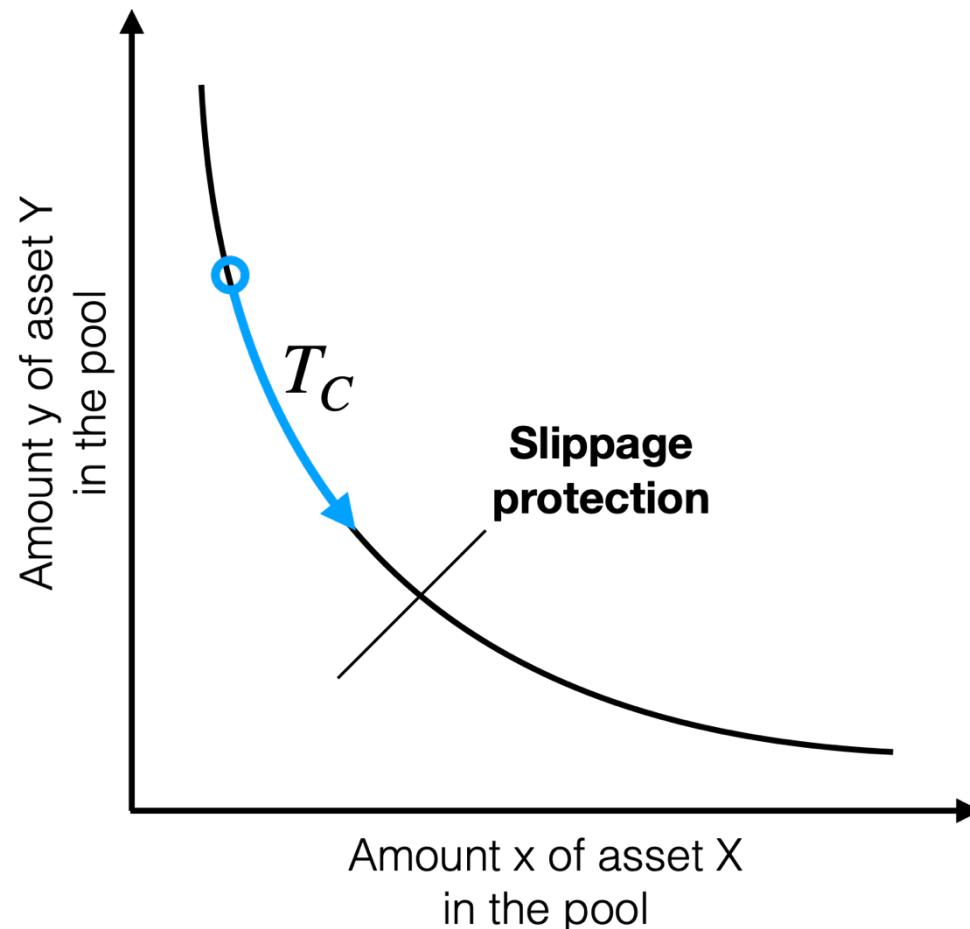


Unexpected Slippage → Better Execution Price



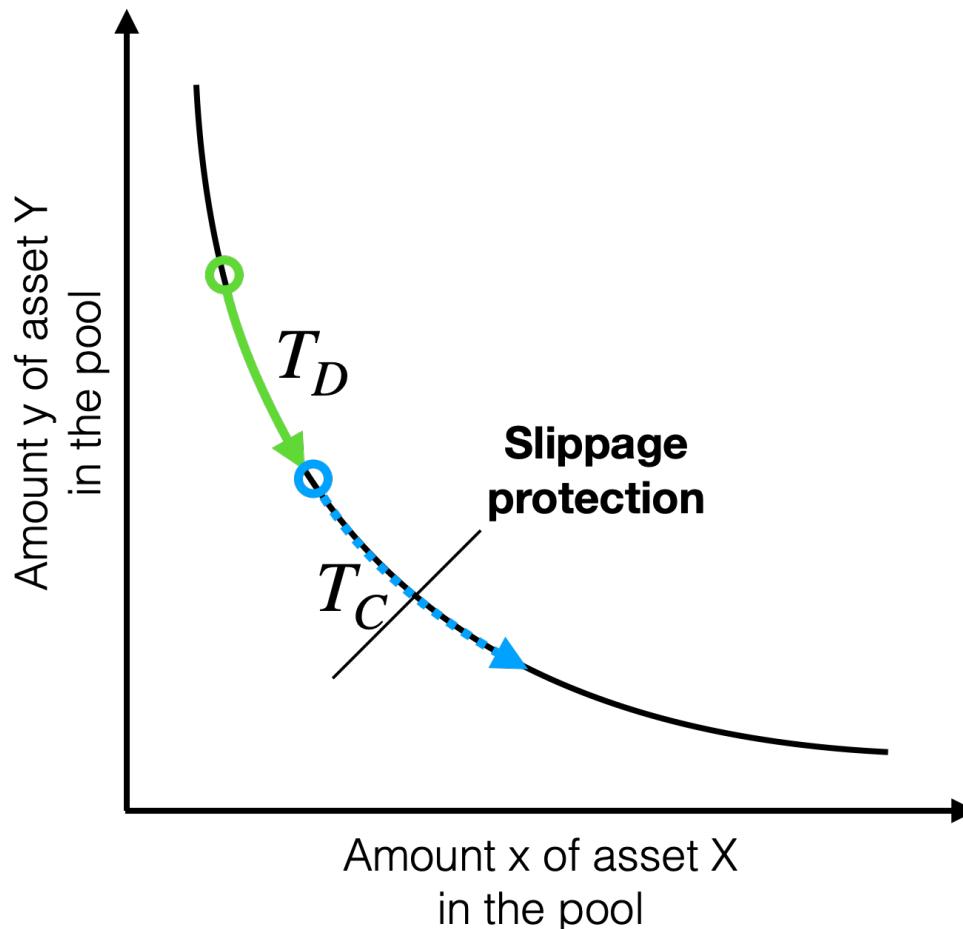
Slippage Protection

Configures a slippage protection threshold to prevent unacceptable slippage



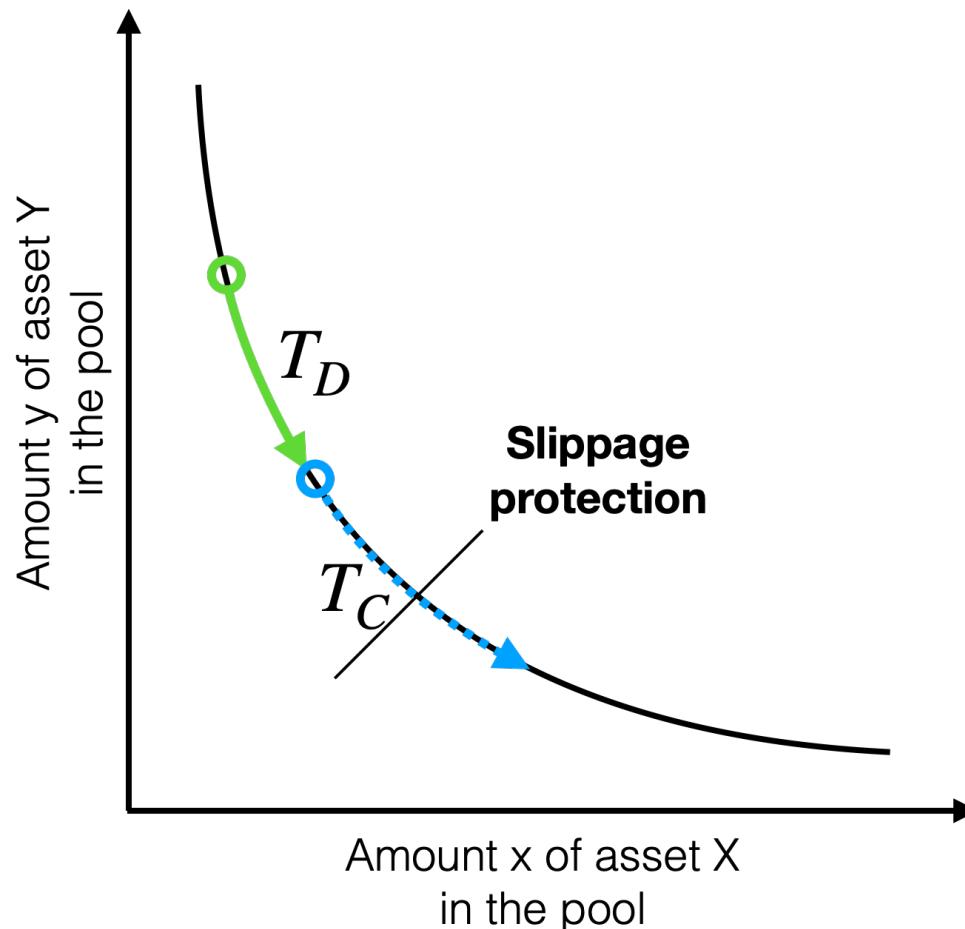
Slippage Protection

A transaction **fails** when crossing the slippage limit.



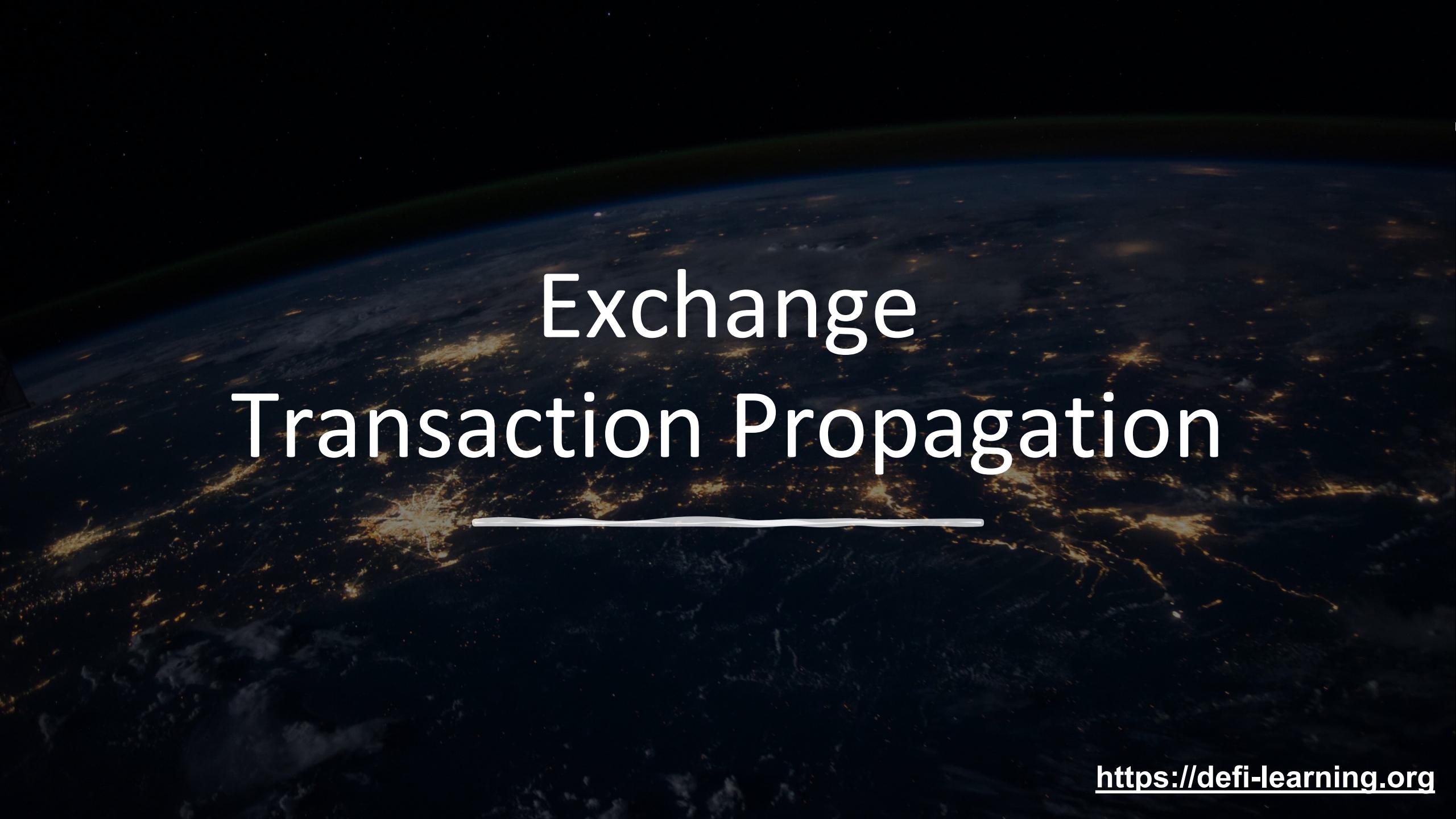
Slippage Protection

A transaction **fails** when crossing the slippage limit.



Pros and Cons of an AMM

- (+) No Order Book maintenance
 - But arbitrage required
- (+) Simple implementation for CP AMM
 - Low gas costs
- (-) Danger of impermanent loss/coin de-peg
 - Total loss of funds possible
- (-) High slippage for low liquidity markets
 - Please do observe your slippage tolerance
- (-) Users vulnerable to sandwich attacks
 - See security lecture

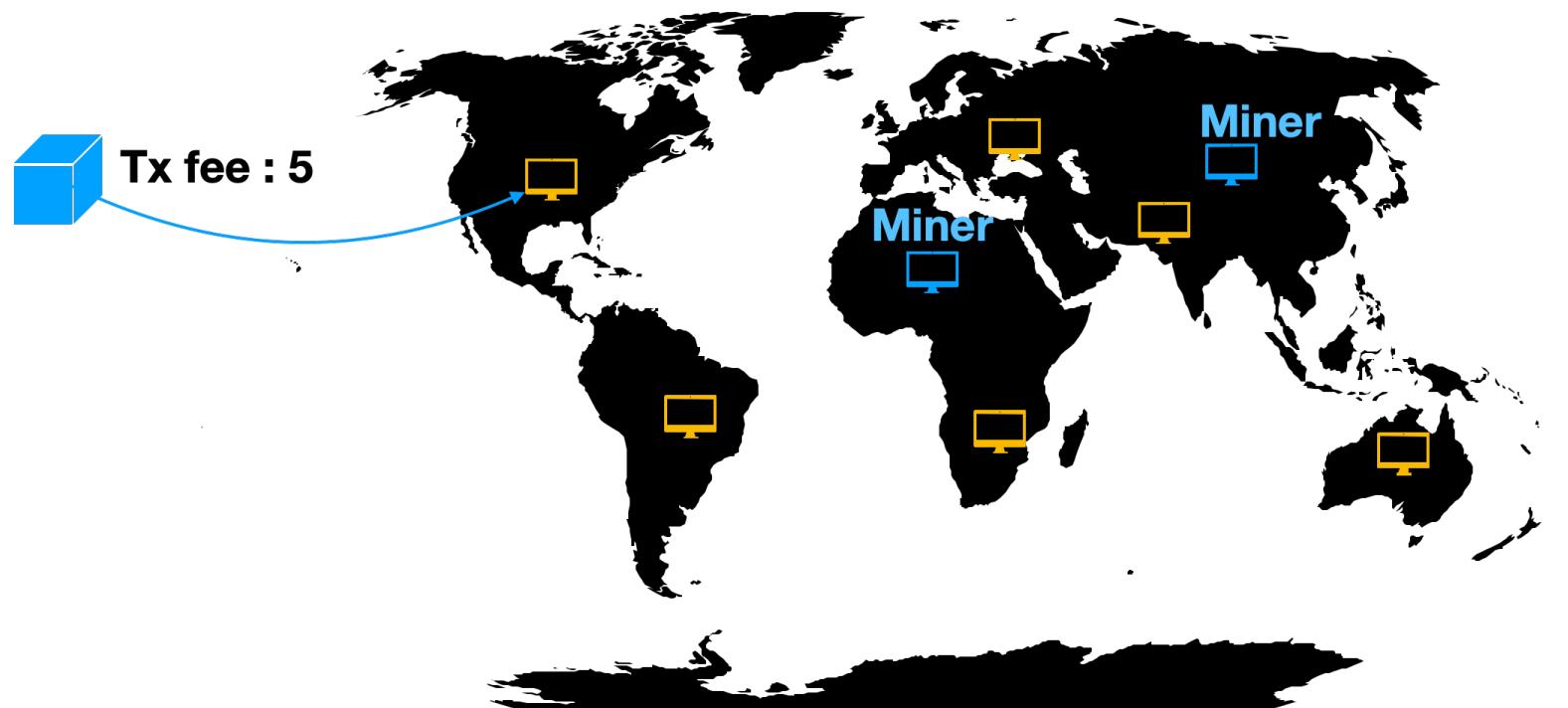


Exchange Transaction Propagation

Exchange Transaction Propagation

Trader

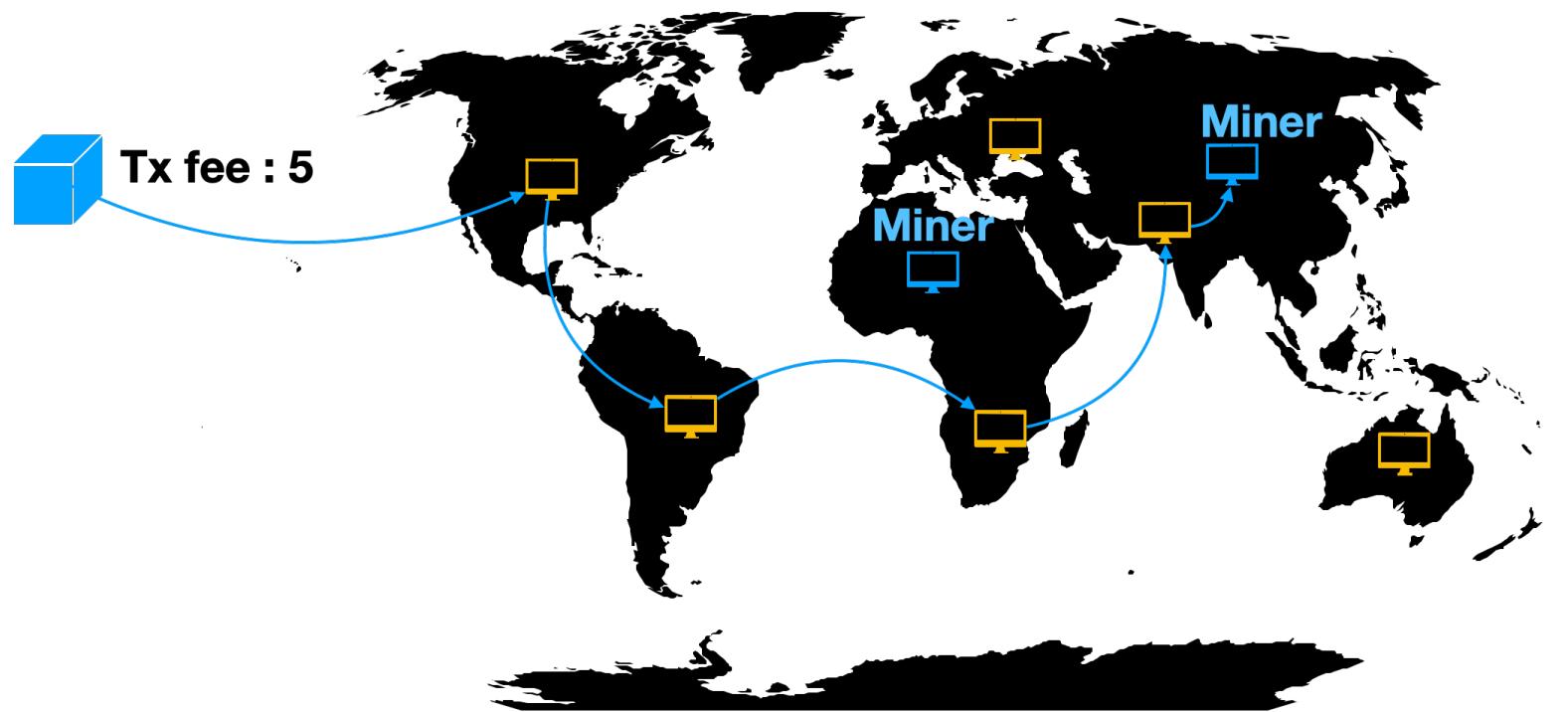
P2P Network



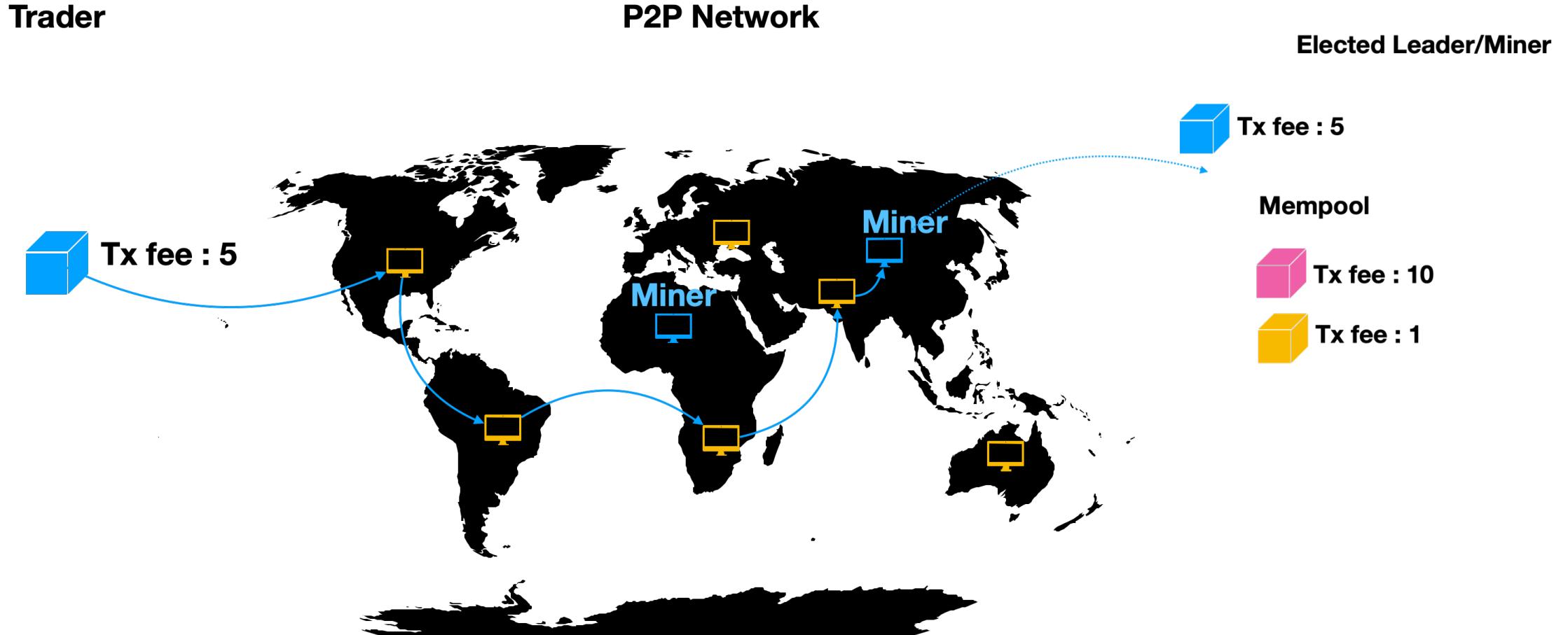
Exchange Transaction Propagation

Trader

P2P Network



Exchange Transaction Propagation

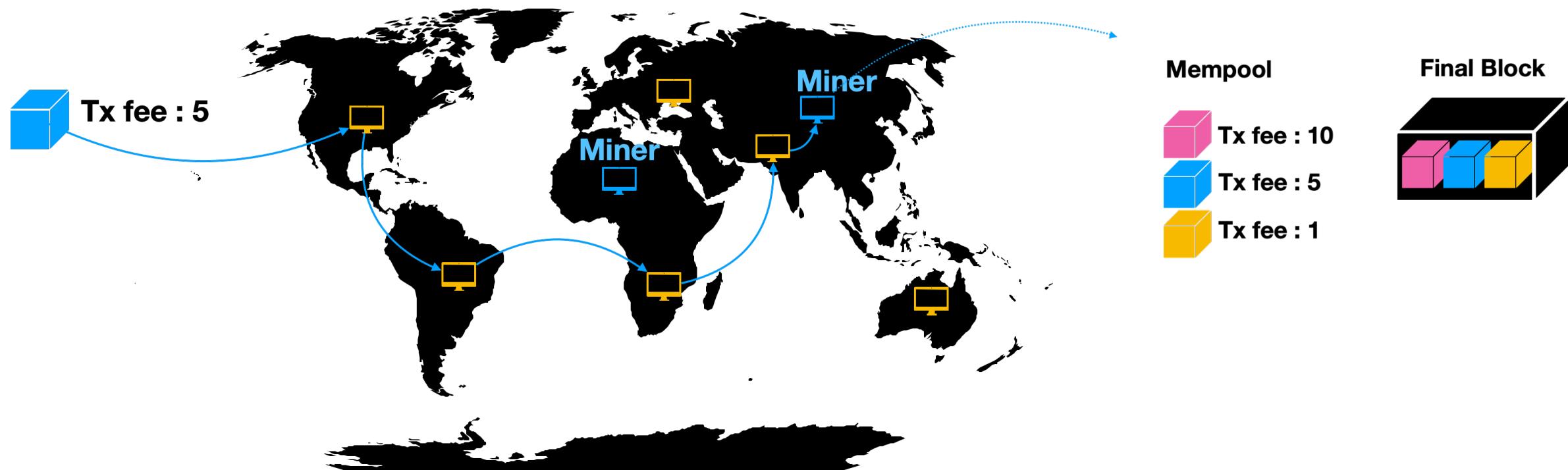


Exchange Transaction Propagation

Trader

P2P Network

Elected Leader/Miner



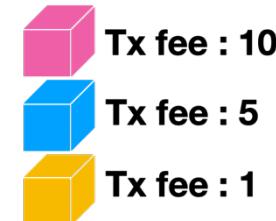
Exchange Transaction Propagation

- Asynchronous Blockchain P2P Network

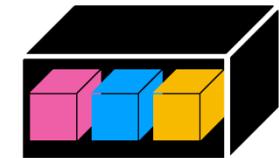
Elected Leader/Miner

- Best effort propagation
- Transparency
- High-Frequency Trading

Mempool



Final Block



- Inclusion based on a fee auction

- Price Gas Auction (PGA)
 - On the public P2P network
- Sealed Bid Gas Auction (SGA)
 - On centralized network relay services



Pegged and Stablecoin AMM

Pegged/Stablecoin Swap



USDC



USDT



DAI



WBTC



renBTC



sETH



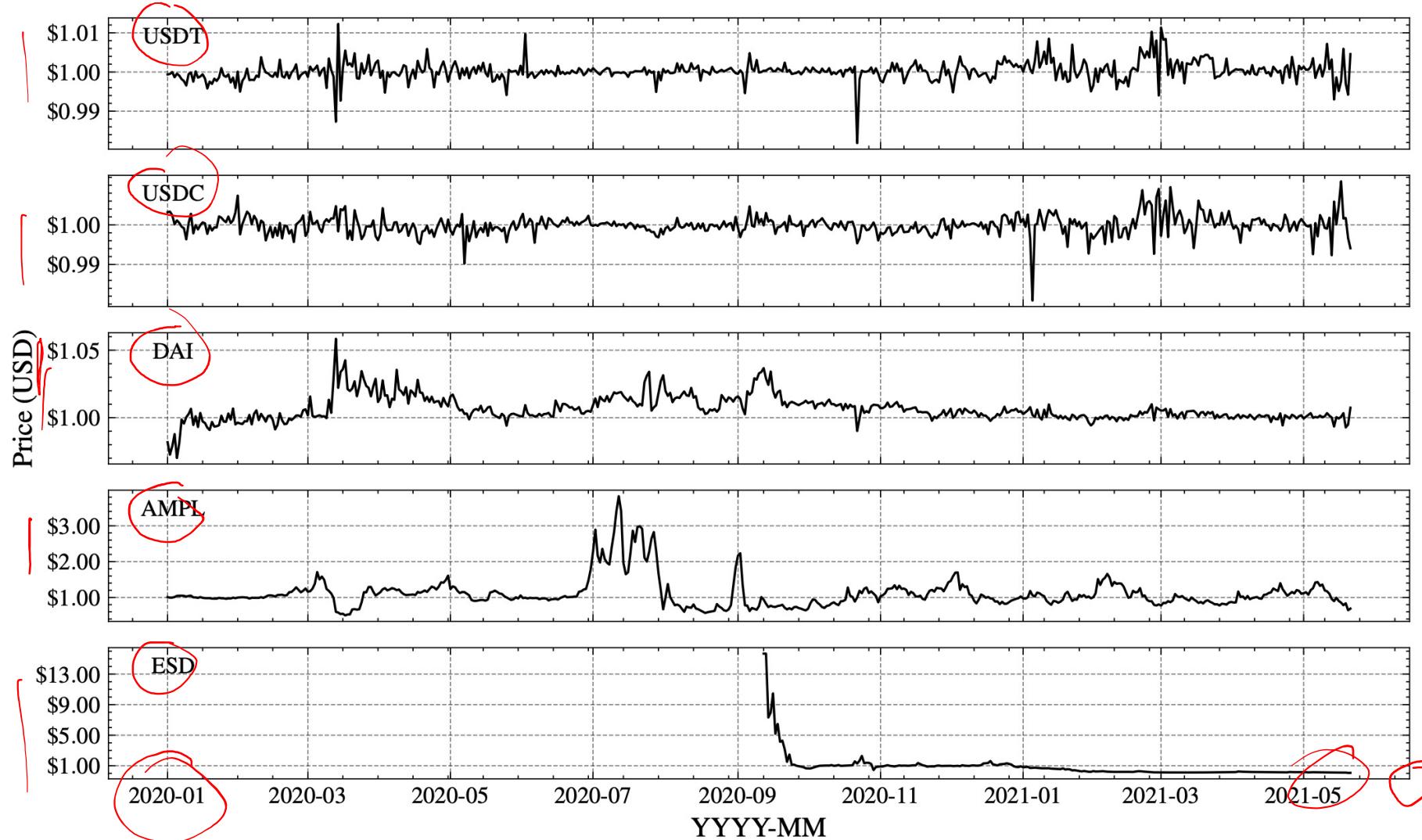
stETH

USD derivatives

Pegged coins

- Three Stablecoin Types
 - Reserve-based
 - Collateral-based
 - Algorithmic

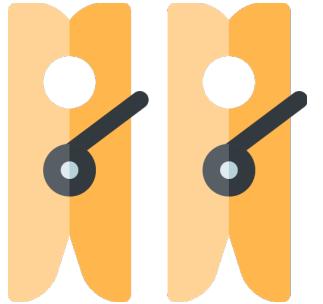
Pegged/Stablecoin Swap



Pegged/Stablecoins

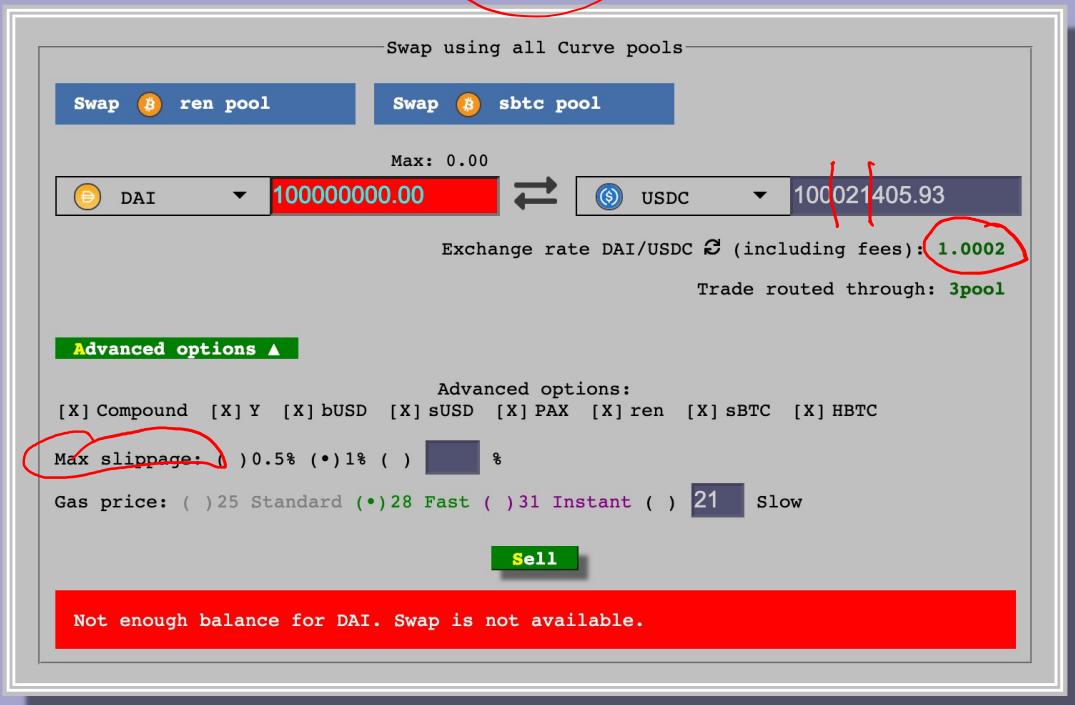
- Pegged/Stablecoin prices move in expectation together
 - The exchange rate should ideally remain 1 to 1
 - A default CP AMM is not optimized for such case

- Stablecoin AMM pros/cons:
 - (+) Better prices for bigger volumes (i.e. more liquidity) ↗
 - (-) Potentially higher gas costs ↗
 - (-) Danger of a de-peg of a stablecoin ↗



Pegged/Stablecoin Swap

Curve



Swap using all Curve pools

Swap ren pool Swap sbtc pool

Max: 0.00

DAI 100000000.00 USDC 100021405.93

Exchange rate DAI/USDC (including fees): 1.0002

Trade routed through: 3pool

Advanced options ▾

Advanced options:
[X] Compound [X] Y [X] bUSD [X] sUSD [X] PAX [X] ren [X] sBTC [X] HBTC

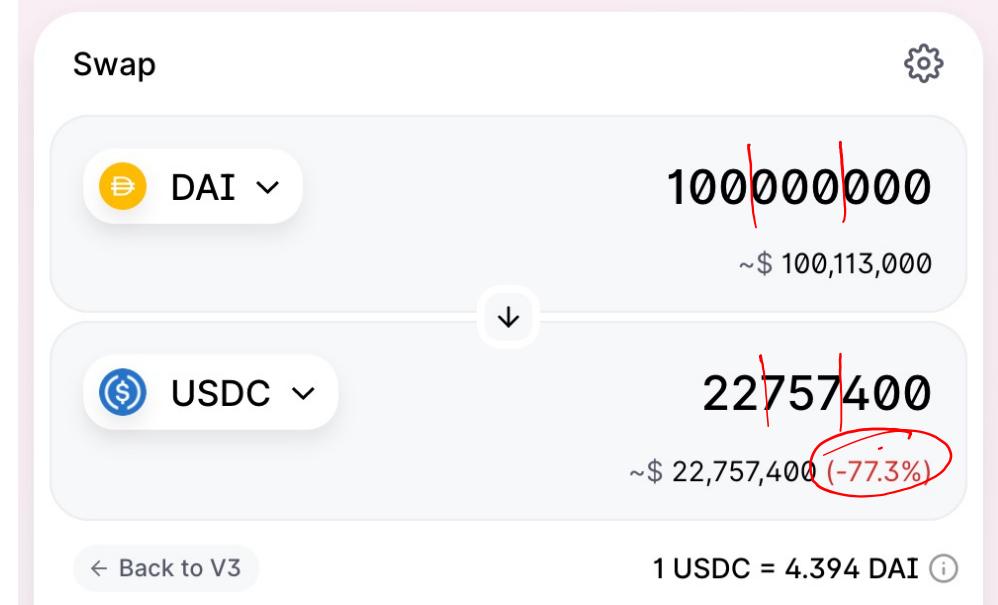
Max slippage: () 0.5% (•) 1% () 5% %

Gas price: () 25 Standard (•) 28 Fast () 31 Instant () 21 Slow

Sell

Not enough balance for DAI. Swap is not available.

Uniswap



Swap

DAI 100000000

~\$ 100,113,000

USDC 22757400

~\$ 22,757,400 (-77.3%)

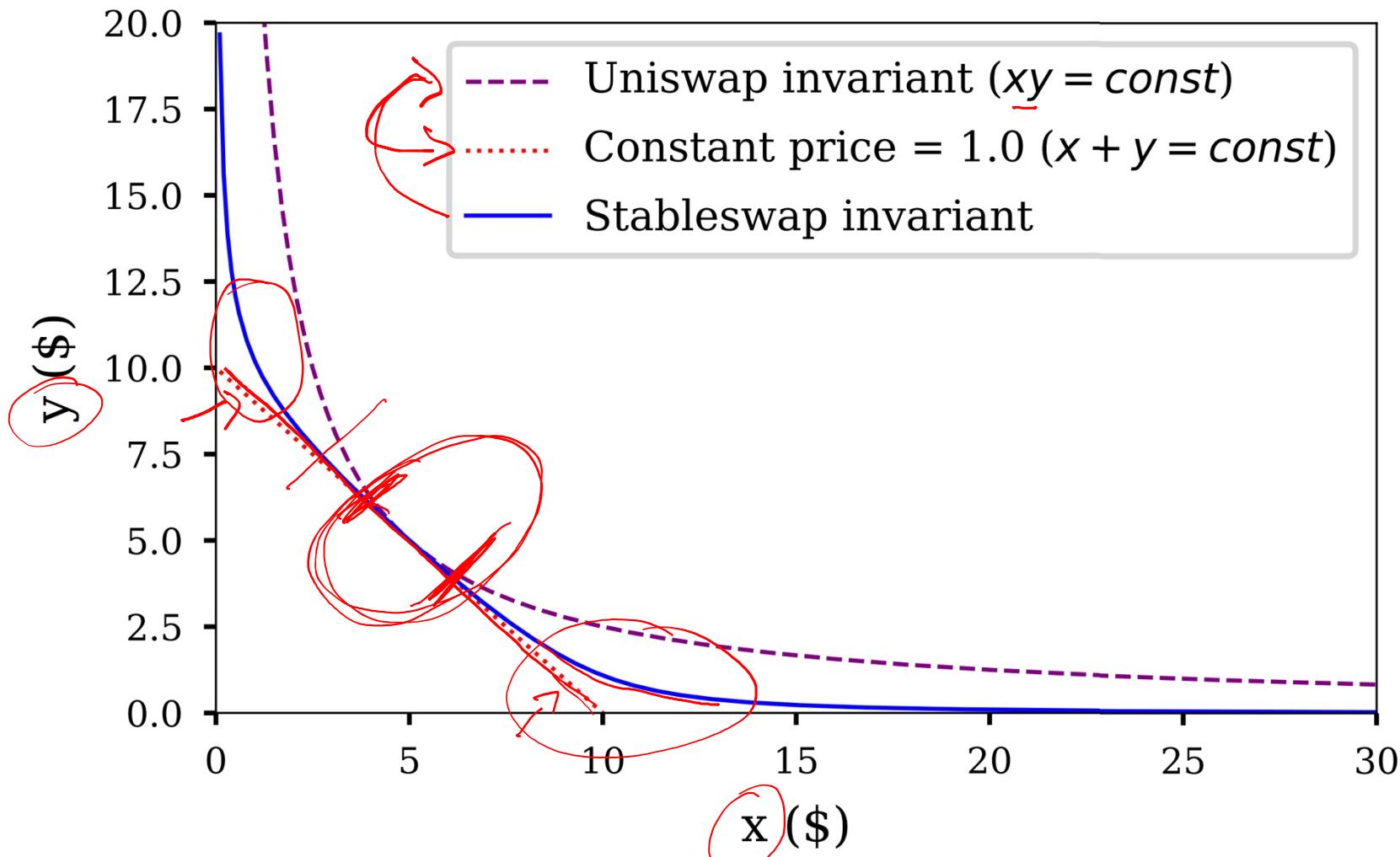
1 USDC = 4.394 DAI

Back to V3

- Significant liquidity differences among exchanges
 - Here an example for a 100M USD swap from DAI to USDC

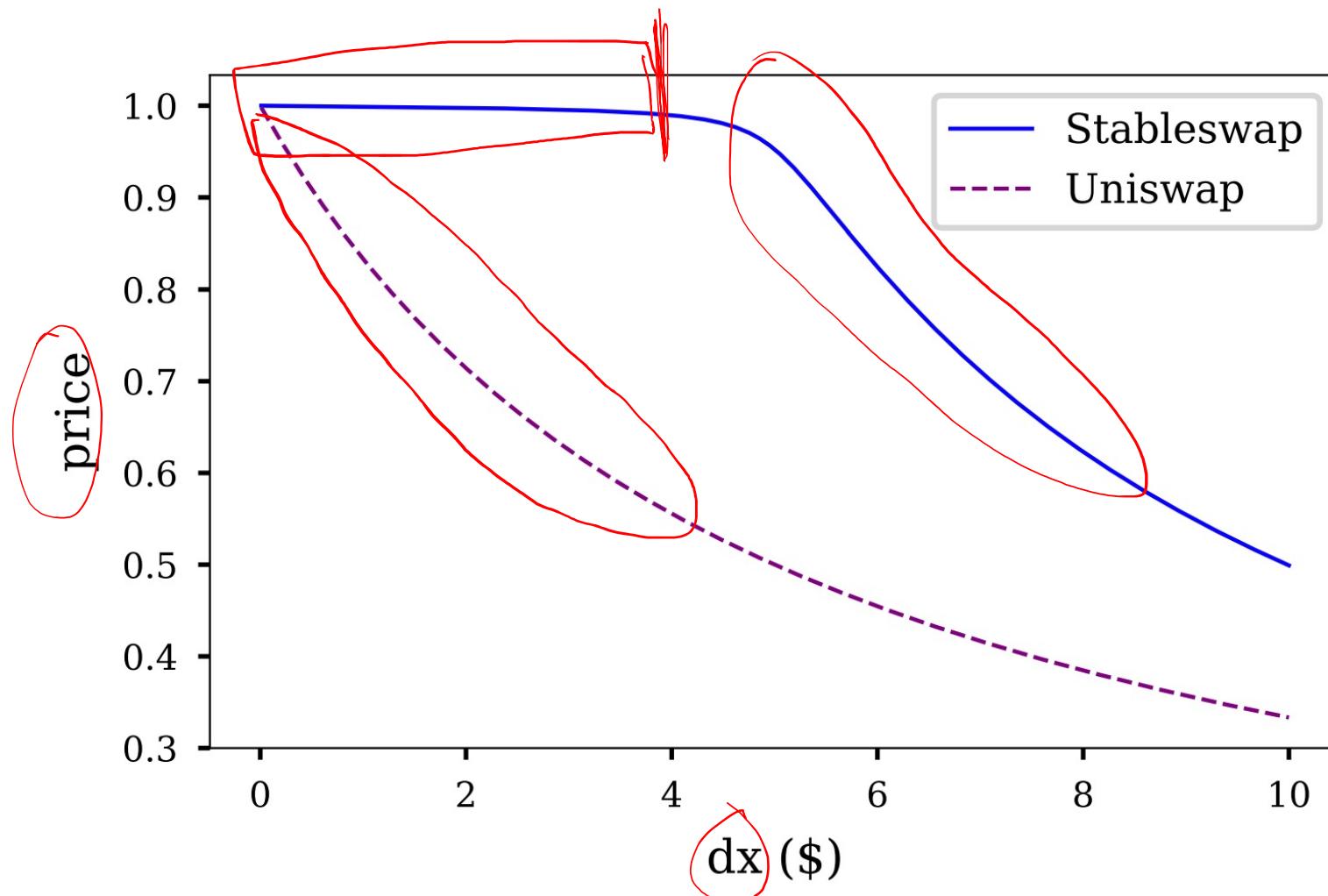
Price Curve

Stableswap (aka Curve Finance)



Slippage Comparison

Stableswap (aka Curve Finance)

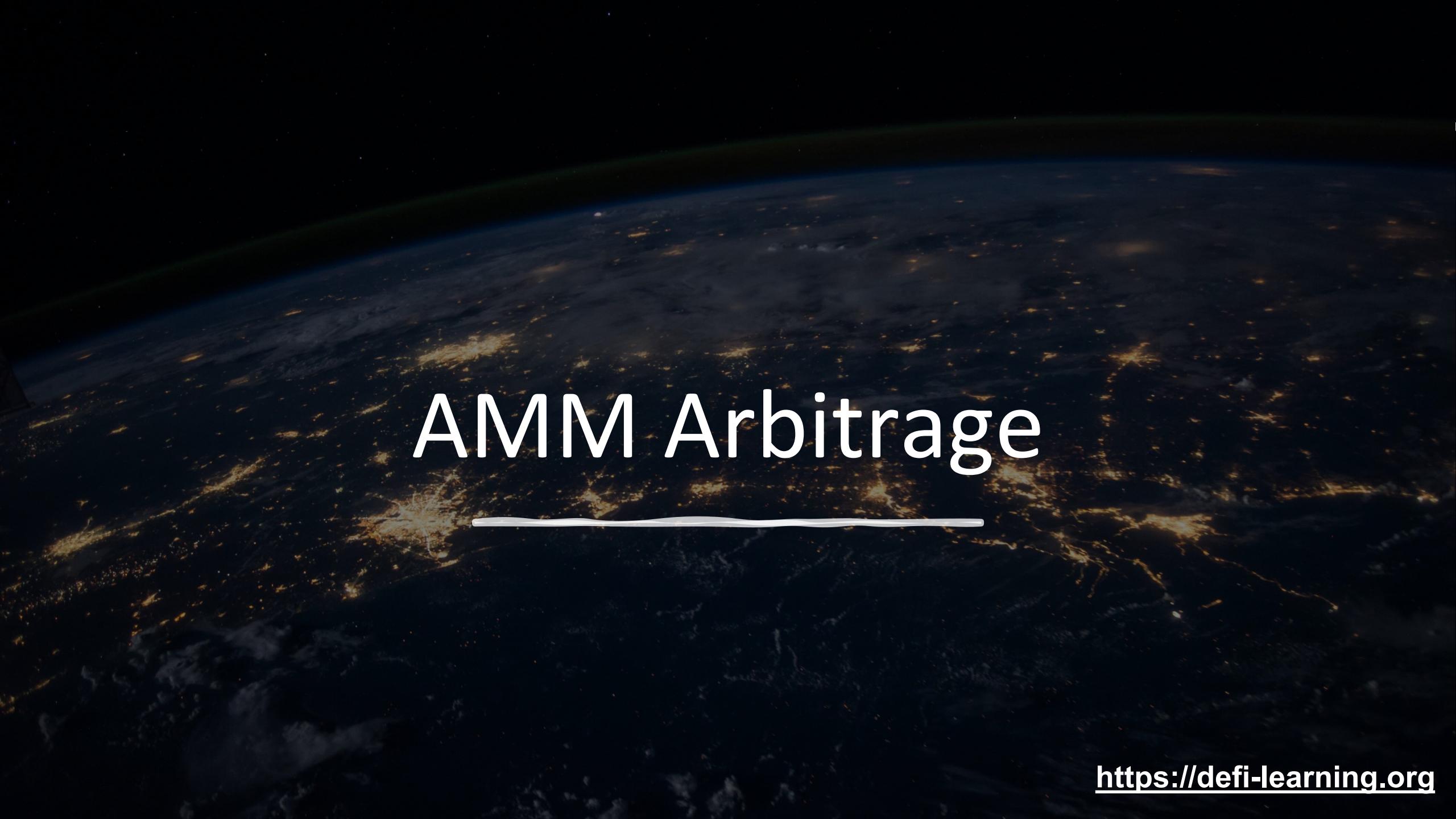


What happens if a coin de-pegs?

What happens if a coin gets blacklisted?

AMM Whitepaper

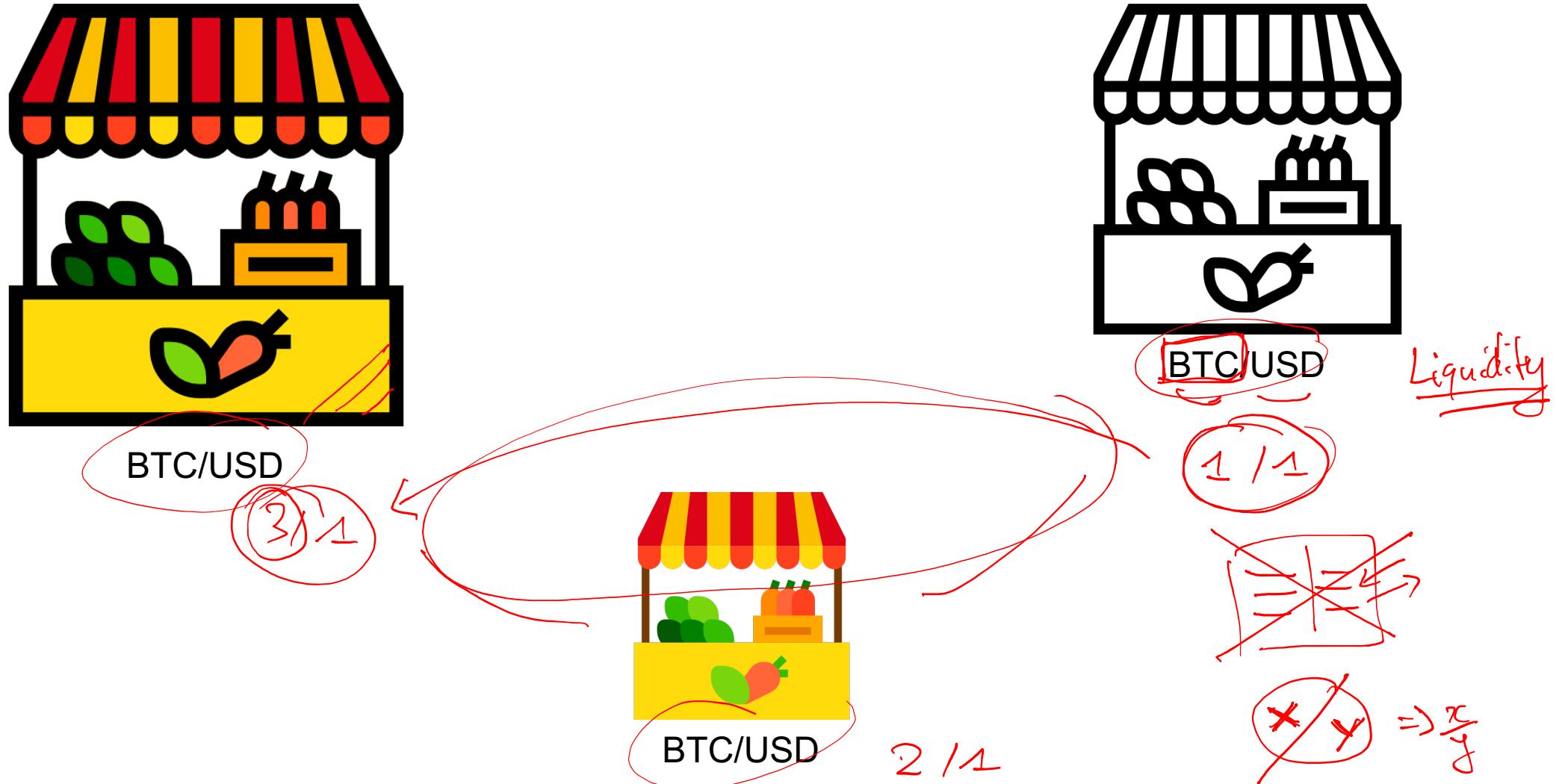
- Check out the whitepapers of different projects
 - These are not peer-reviewed academic works
 - Be aware of possible missing items/nuances
 - Projects do not always disclose the full details
- Curve:
 - <https://curve.fi/files/stableswap-paper.pdf>
 - <https://curve.fi/files/crypto-pools-paper.pdf>
- Uniswap:
 - <https://uniswap.org/whitepaper.pdf>
 - <https://uniswap.org/whitepaper-v3.pdf>

A wide-angle, low-light photograph of Earth at night, taken from space. The curvature of the planet is visible against the black void of space. City lights are scattered across continents as glowing yellow and white dots, with major urban areas appearing as larger, brighter clusters. The aurora borealis is visible as a green, ribbon-like glow in the upper atmosphere over the Northern Hemisphere. The overall scene conveys a sense of global connectivity and the beauty of our planet from above.

AMM Arbitrage

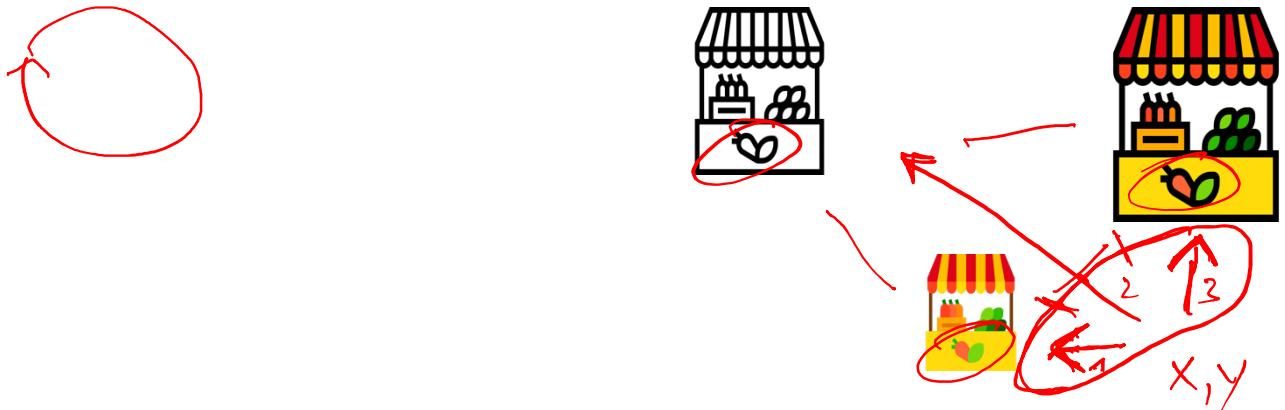
<https://defi-learning.org>

Arbitrage

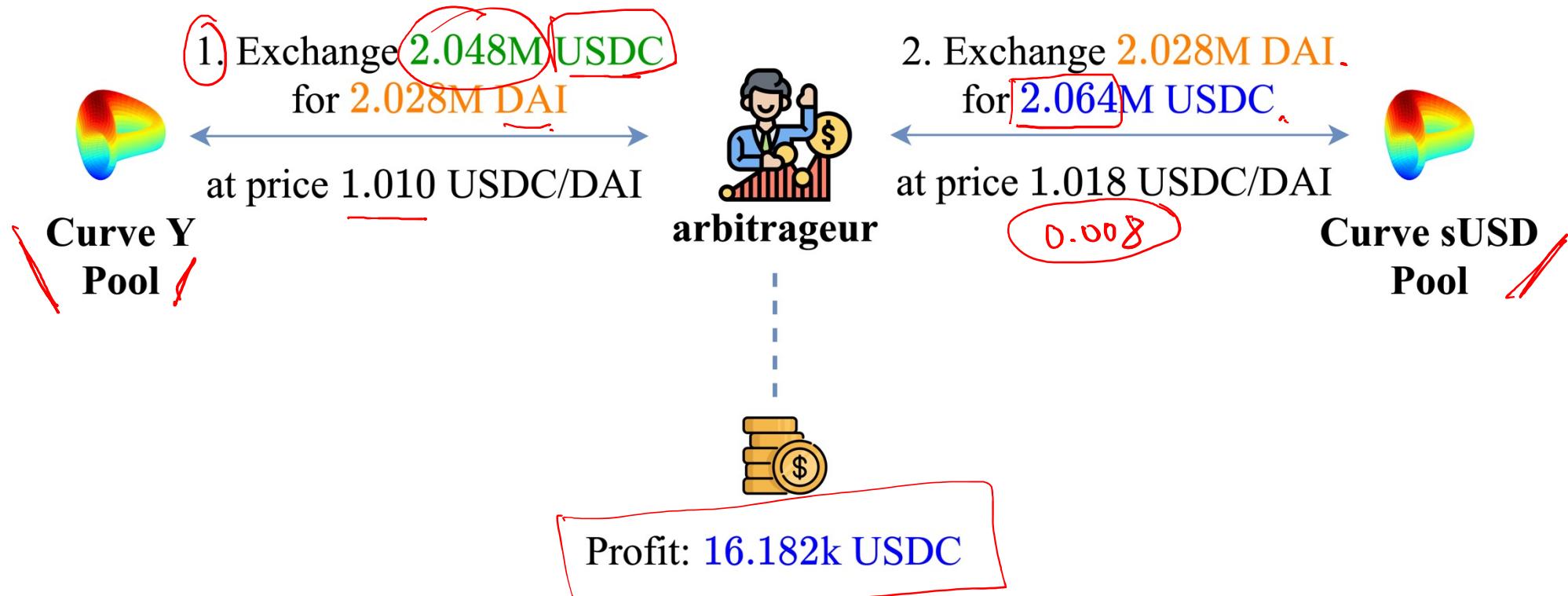


Arbitrage

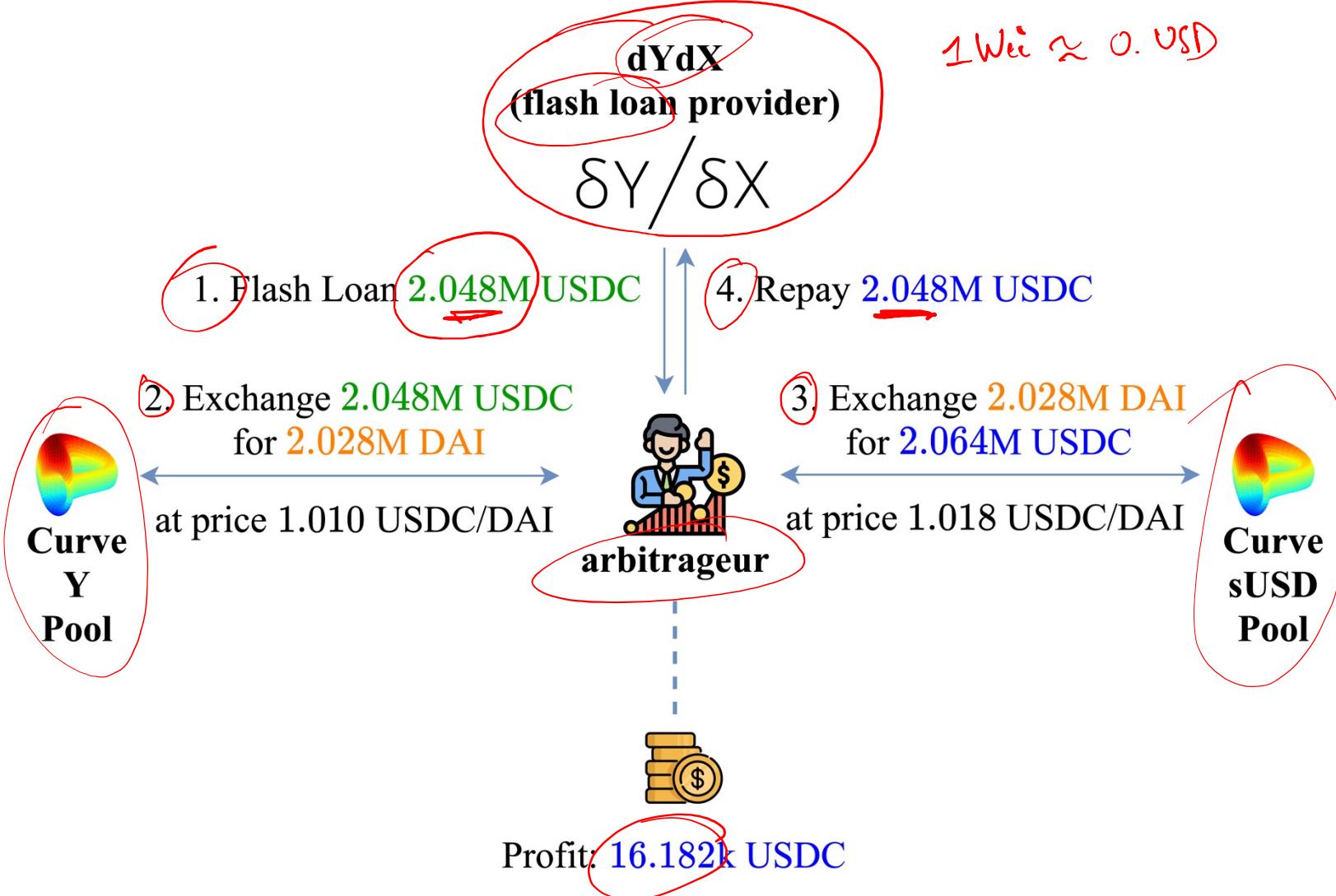
- Multiple Markets with
 - the same assets X and Y
 - different prices for X and Y
- Prices are synchronized by “arbitrageurs”
 - Profit from the price difference
 - Also referred to as “spread”
 - Requires to perform at least one transaction

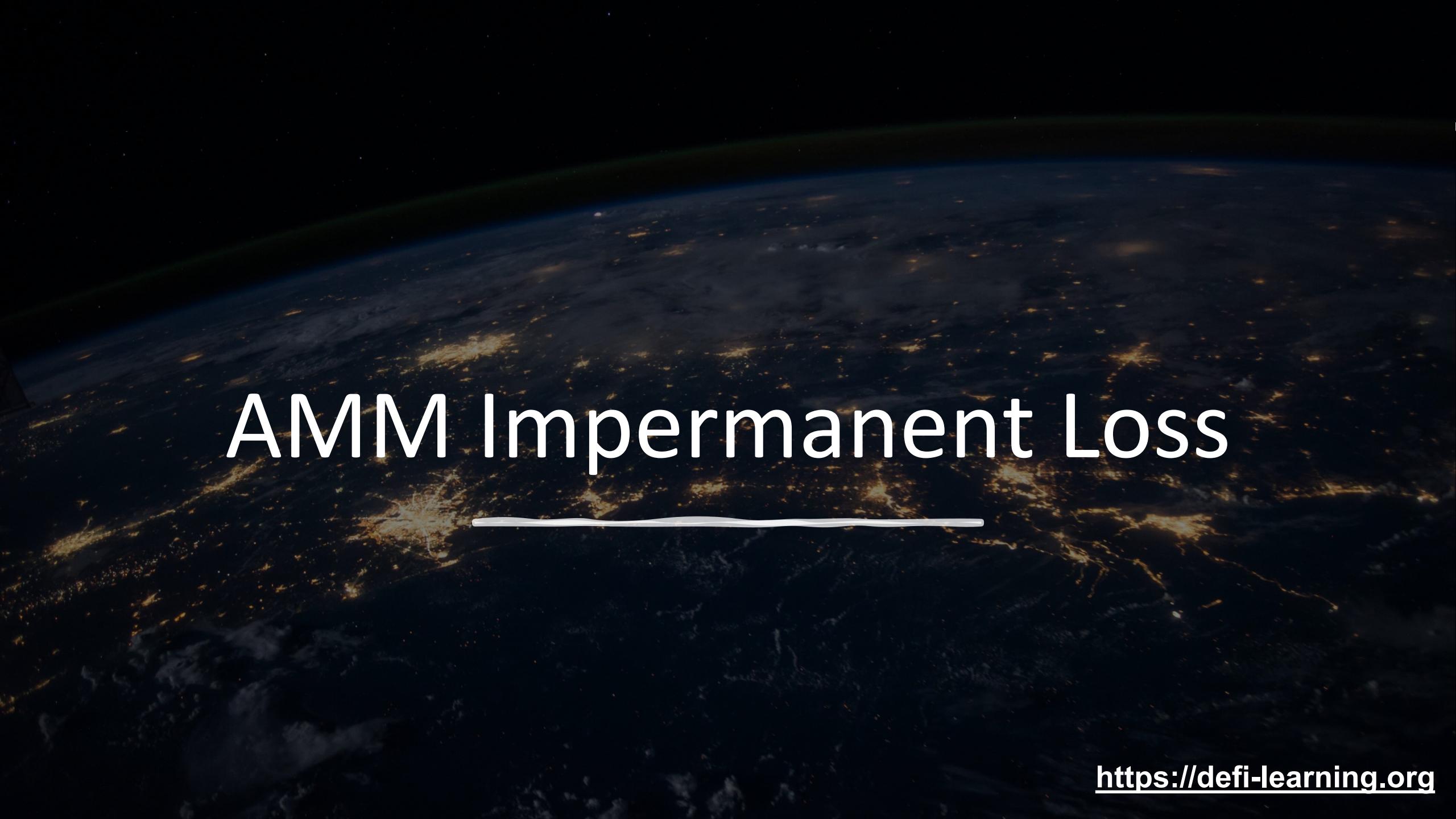


Arbitrage on two markets



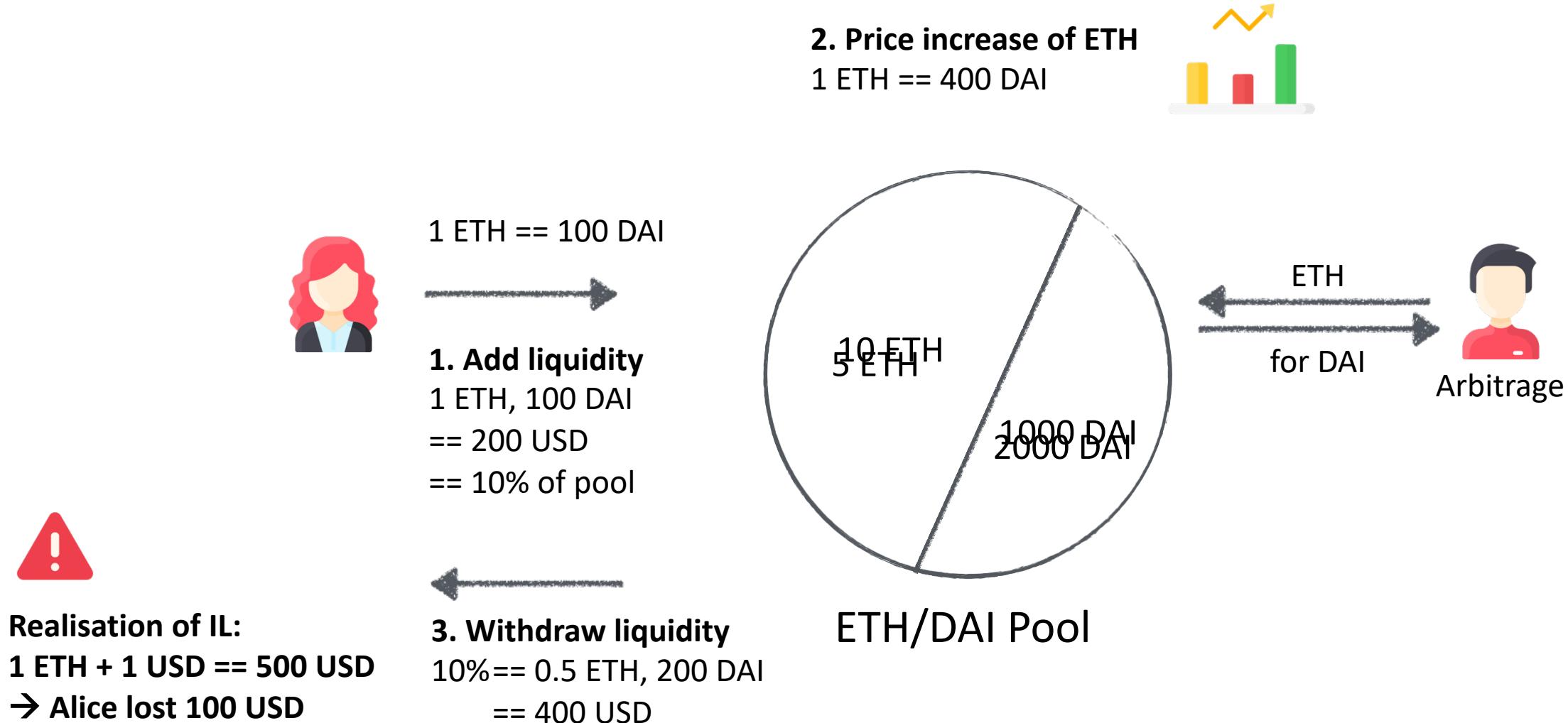
Arbitrage (with Flash Loan)



A night-time satellite view of Earth from space, showing city lights and auroras.

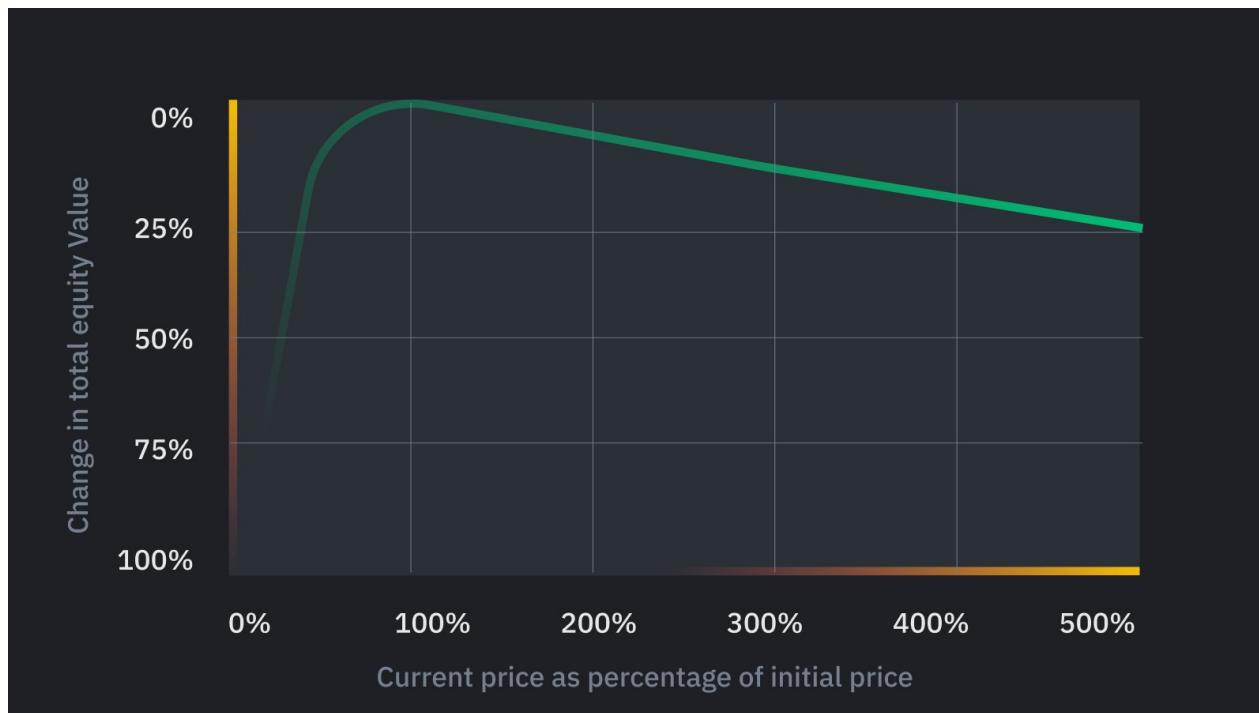
AMM Impermanent Loss

Impermanent Loss Example



Impermanent Loss

- Impermanent == not permanent
 - Realized upon withdraw only!
- IL can result in total loss
 - Trading fees may compensate
 - Liquidity mining may compensate
 - Similar to a de-peg of a Stablecoin
- Possible Solutions
 - Challenging
 - Change of the bonding curve



Impermanent Loss Calculator

The screenshot shows a web browser window with the title "Impermanent Loss Calculator" from "dailydefi.org". The page explains that it uses Uniswap's constant product formula to determine impermanent loss, noting that fees are not included. It has sections for "Initial Prices" and "Future Prices" with input fields for Token A and Token B. In the "Initial Prices" section, Token A is \$100 and Token B is \$100. In the "Future Prices" section, Token A is \$1000 and Token B is \$100. The "Results" section shows an impermanent loss of 42.50%. It also provides calculations for holding \$500 of each token and for providing liquidity.

This calculator uses Uniswap's [constant product formula](#) to determine impermanent loss.

Fees are not included within results.

Initial Prices

Token A -

Token B -

Future Prices

Token A -

Token B -

Results

Impermanent loss: 42.50%

If \$500 of Token A and \$500 of Token B were held

- Have 5.00 Token A and 5.00 Token B
- Value if held: \$5,500.00

If \$500 of Token A and \$500 of Token B were provided as liquidity

- Have 1.58 Token A and 15.81 Token B (in liquidity pool)
- Value if providing liquidity: \$3,162.28



AMM Liquidity Mining

Liquidity Mining == Incentive

- 2 Types of rewards in DeFi Pools
 - Trading fees (e.g. 0.03% in Curve)
 - Liquidity Mining rewards
- Liquidity Mining
 - An incentive to provide liquidity to a pool
 - Proportional rewards in terms of liquidity
 - Can be added/removed anytime
 - Retrospective airdrops possible → address history is valuable



Liquidity Mining

Curve

| Curve pools | | | |
|---|----------|--------------------------------|----------|
| Pool | Base APY | Rewards APY | Volume ▾ |
| tricrypto CRYPTO V2 [?] USDT + wBTC + WETH | 3.73% | +2.04%→5.11% CRV | \$28.7m |
| 3pool USD DAI + USDC + USDT | 0.63% | +3.14%→7.84% CRV | \$120.3m |
| sUSD USD DAI + USDC + USDT + sUSD | 0.57% | +2.59%→6.48% CRV +1.78% SNX | \$12.5m |
| ren BTC renBTC + wBTC | 0.41% | +5.84%→14.59% CRV | \$9.9m |
| ironbank USD cyDAI + cyUSDC + cyUSDT | 4.11% | +4.68%→11.70% CRV | \$7.7m |
| bbtc BTC BBTC + sbtcCrv | 0.36% | +2.60%→6.51% CRV | \$6.9m |
| busd v2 USD BUSD + 3Crv | 0.89% | +5.25%→13.13% CRV | \$6.7m |
| lusd USD LUSD + 3Crv | 0.58% | +4.90%→12.25% CRV | \$5.6m |
| sbtc BTC renBTC + wBTC + sBTC | 0.36% | +4.67%→11.67% CRV | \$5.1m |
| tbtc BTC tBTC + sbtcCrv | 0.81% | +13.77%→34.42% CRV | \$4.6m |

[See All Pools](#)

Alpha Homora v2

| Farm Pools (18 Pools) | | | |
|---|--------------------|--|----------------------|
| ALL | YIELD FARMING ⓘ | LIQUIDITY PROVIDING ⓘ | Search |
|  Yield Farming Uniswap DPI/ETH | 33.26 % 12.89 % | Yield Farming ⓘ 18.74 % Trading Fee 7.34 % Alpha APR 16.32 % Borrow APY -9.15 % | FARM |
|  Yield Farming Sushiswap SUSHI/ETH | 63.58 % 27.87 % | Yield Farming ⓘ 38.67 % Trading Fee 17.74 % Alpha APR 16.32 % Borrow APY -9.15 % | FARM |
|  Yield Farming Sushiswap DPI/ETH | 35.51 % 14.00 % | Yield Farming ⓘ 24.62 % Trading Fee 3.71 % Alpha APR 16.32 % Borrow APY -9.15 % | FARM |
|  Yield Farming Sushiswap LINK/ETH | 58.90 % 22.62 % | Yield Farming ⓘ 34.06 % Trading Fee 16.26 % Alpha APR 19.52 % Borrow APY -10.94 % | FARM |

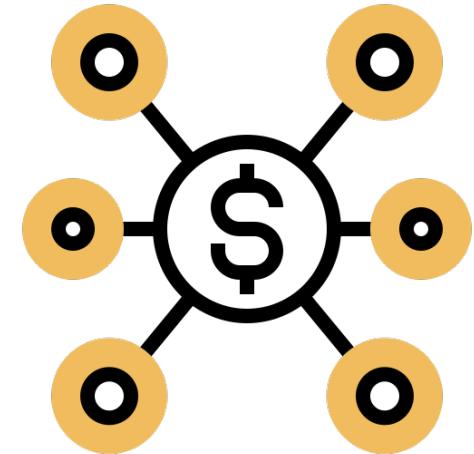


DEX Aggregator

<https://defi-learning.org>

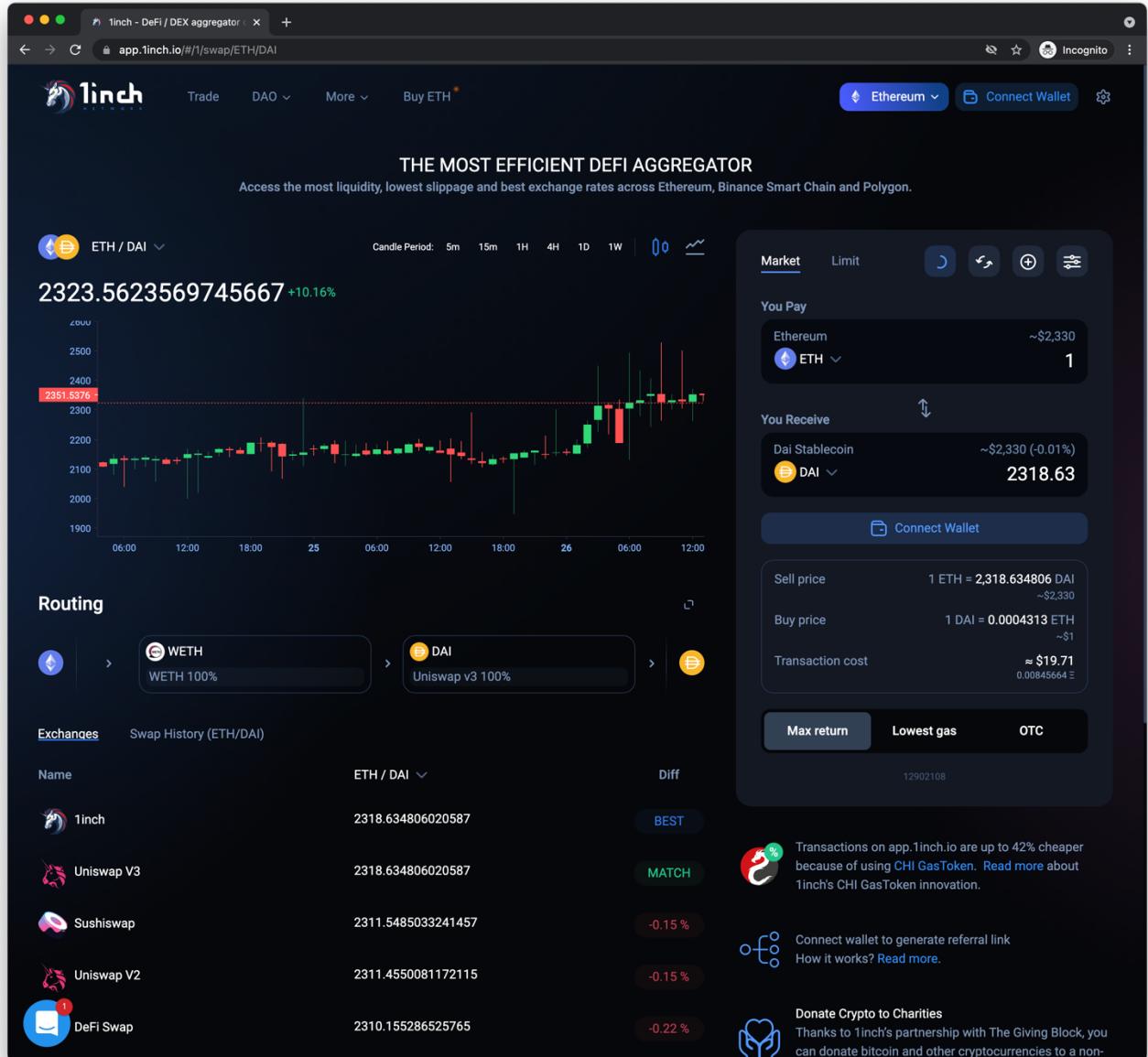
DEX Aggregator

- Users may ask
 - Where do I get the best price for a trade?
 - Where is the deepest liquidity?
- Two types of aggregators
 - Off-chain aggregator (1inch, paraswap)
 - (+) Can spawn multiple chains, very flexible
 - (-) Operator can front-run users
 - On-chain aggregator (swapswap)
 - (+) atomic routing & arbitrage
 - (-) unlikely to efficiently cover 4+ exchanges



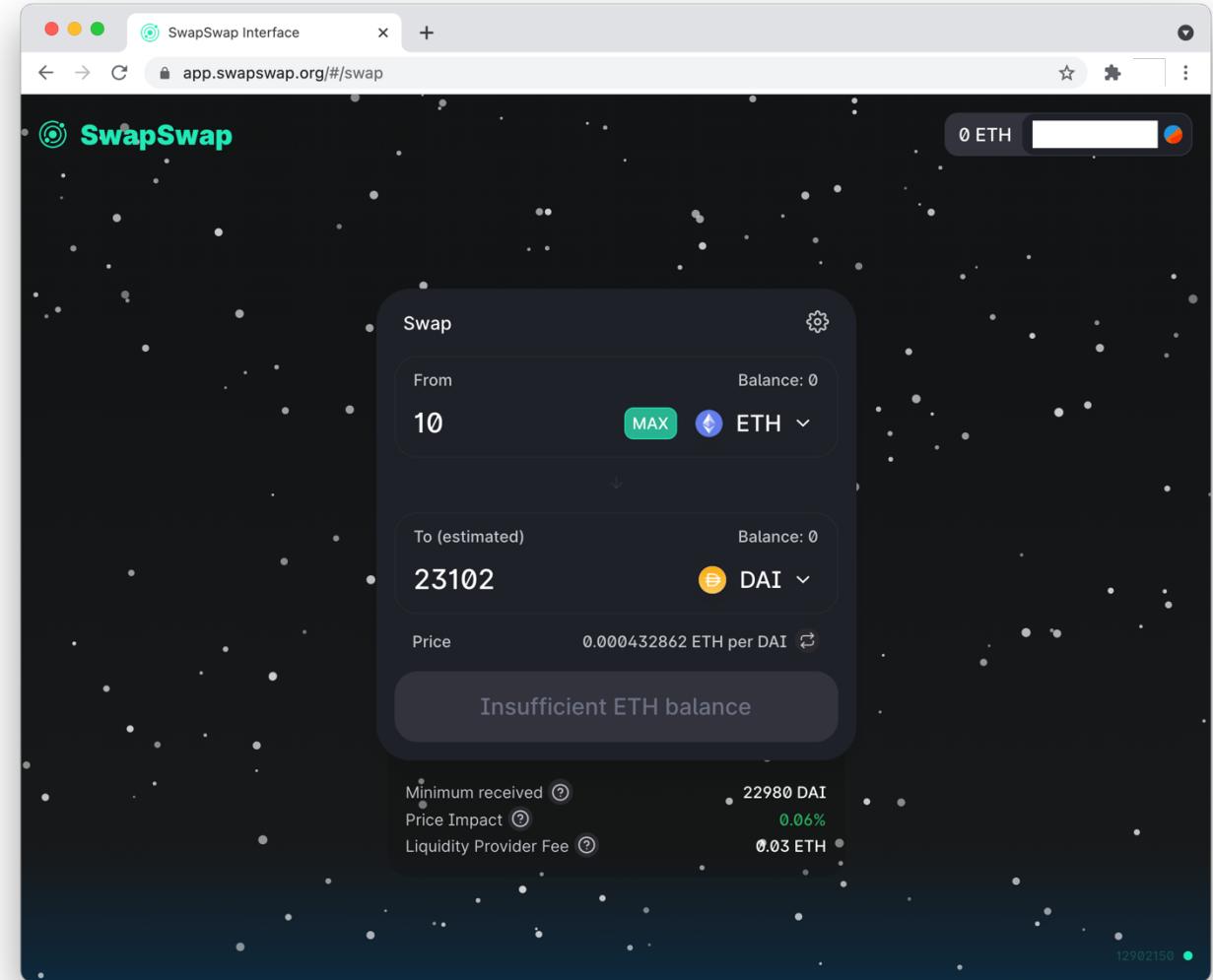
1inch

- Aggregates many DEX
 - Very verbose UI for users
- Routing
 - Explains which route taken
 - No arbitrage performed



SwapSwap

- Aggregates 2 DEX
 - Uniswap and Sushiswap
 - No UI change for the user
- Routing & Arbitrage
 - Routes a swap if the smart contract deems routing profitable
 - Performs arbitrage with flash loans if deemed profitable by the smart contract





How to detect trading opportunities in DeFi?

How to detect arbitrage/profitable opportunities?

- Bellman Ford Algorithm
 - Negative cycle detection
 - Works among multiple markets
 - Used in traditional finance and DeFi

- Theorem Solver (SMT)
 - Needs to encode the DeFi model
 - Apply heuristics for path pruning

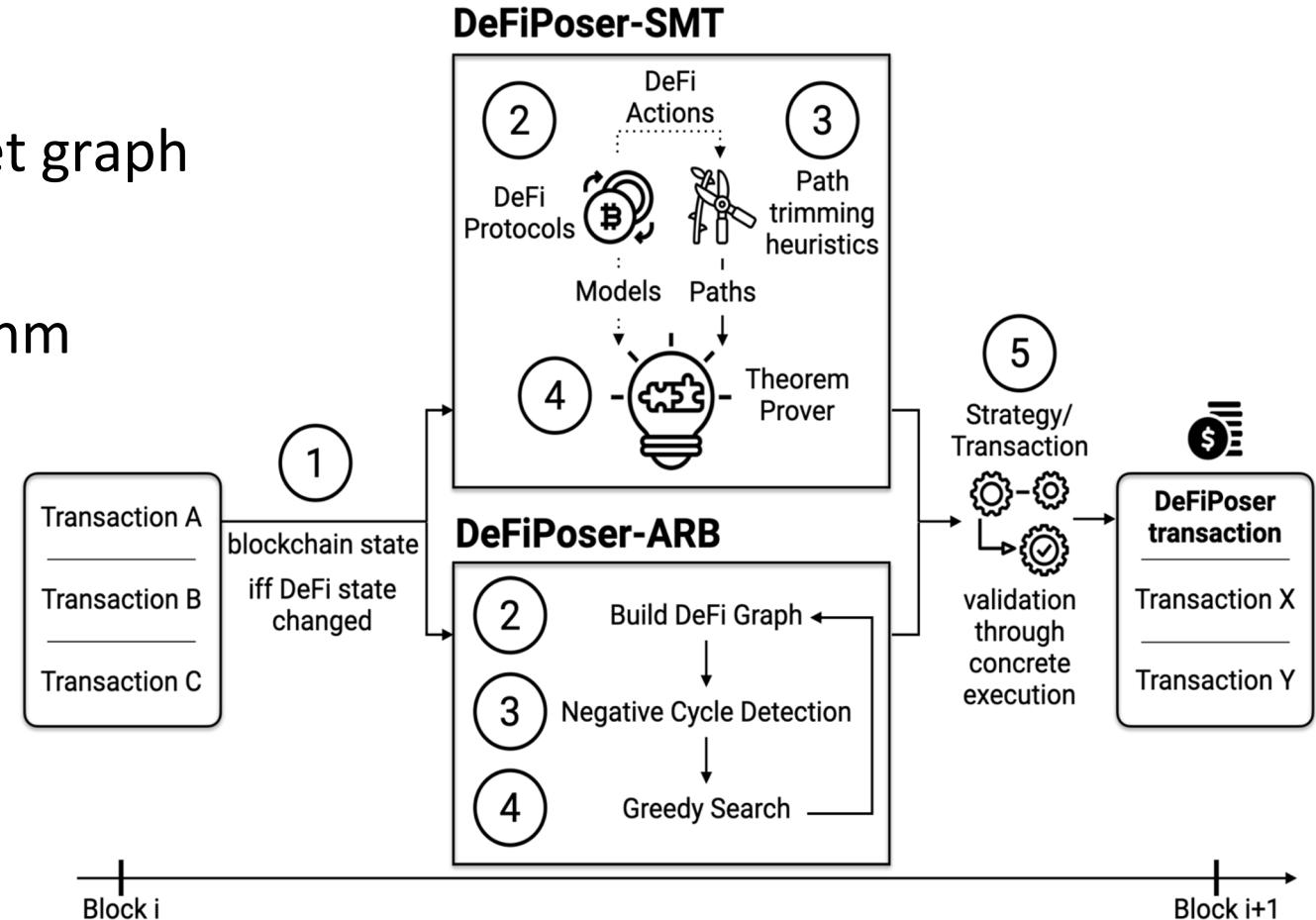
DeFiPoser-ARB and DeFiPoser-SMT [S&P'21]

■ DeFiPoser-ARB

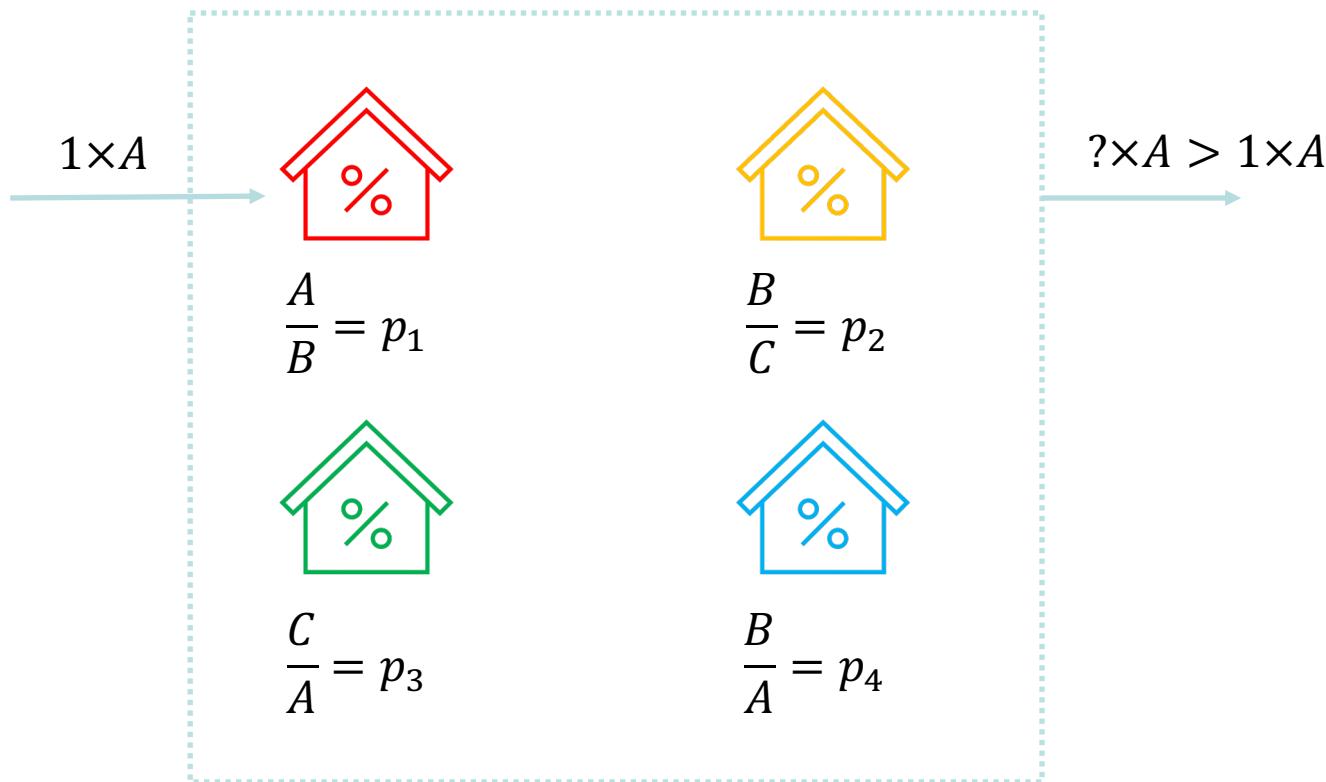
- builds a directed DeFi market graph
- identifies negative cycles
- Bellman Ford-Moore algorithm

■ DeFiPoser-SMT

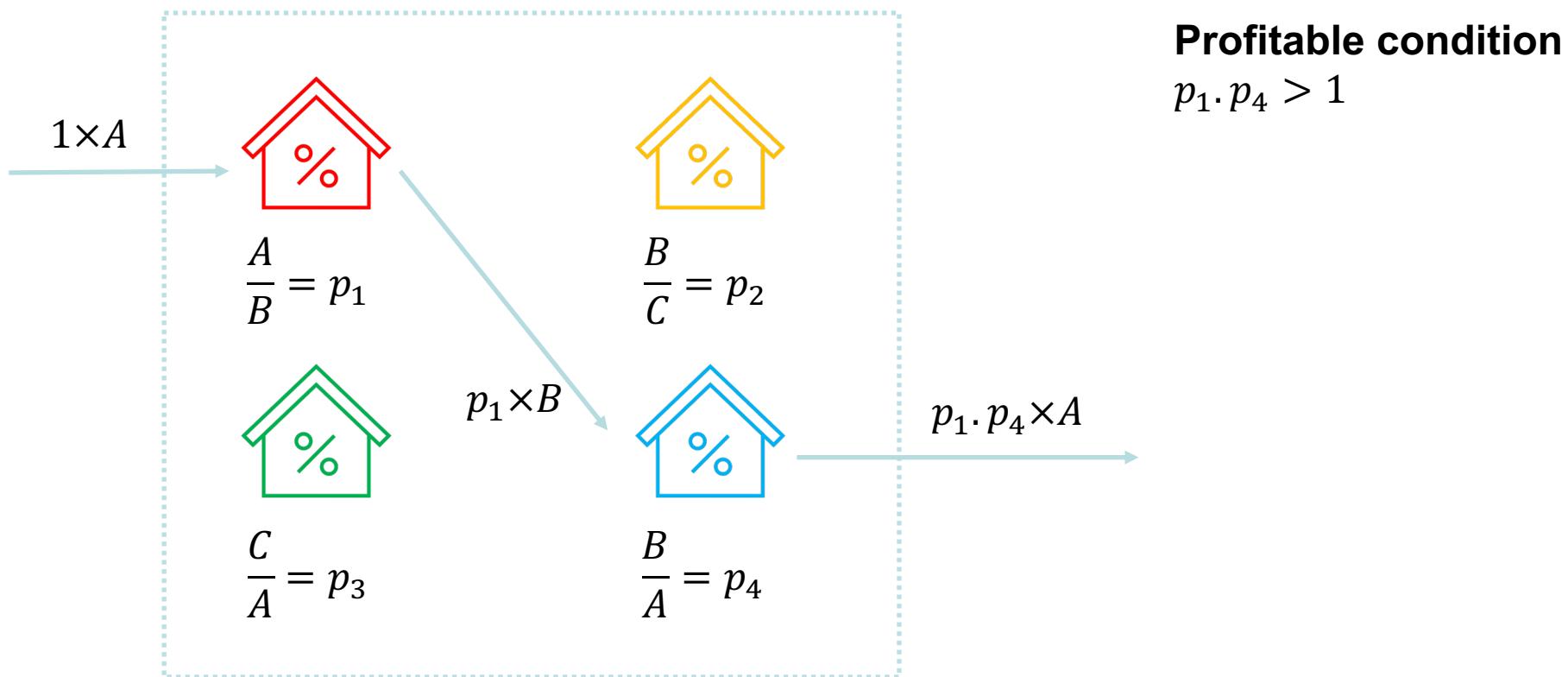
- state transition model
- prunes search space
- theorem prover



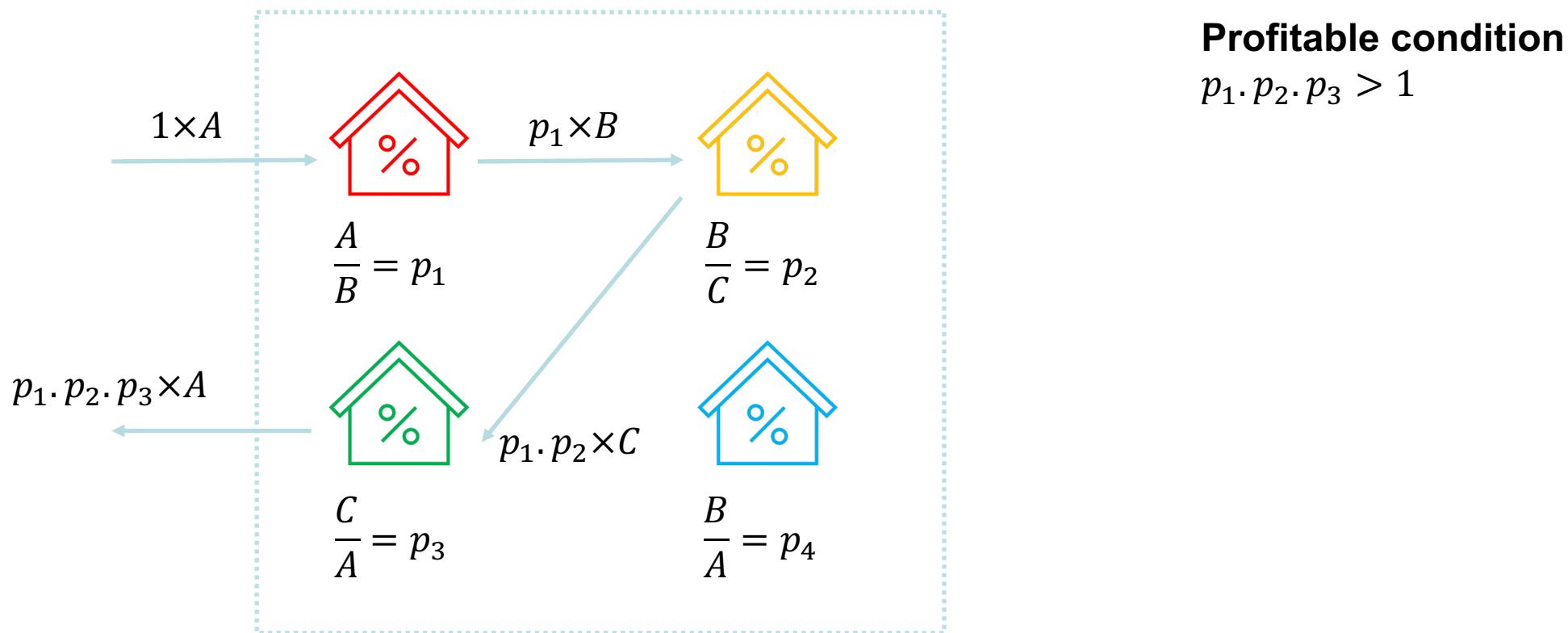
DeFiPoser-ARB



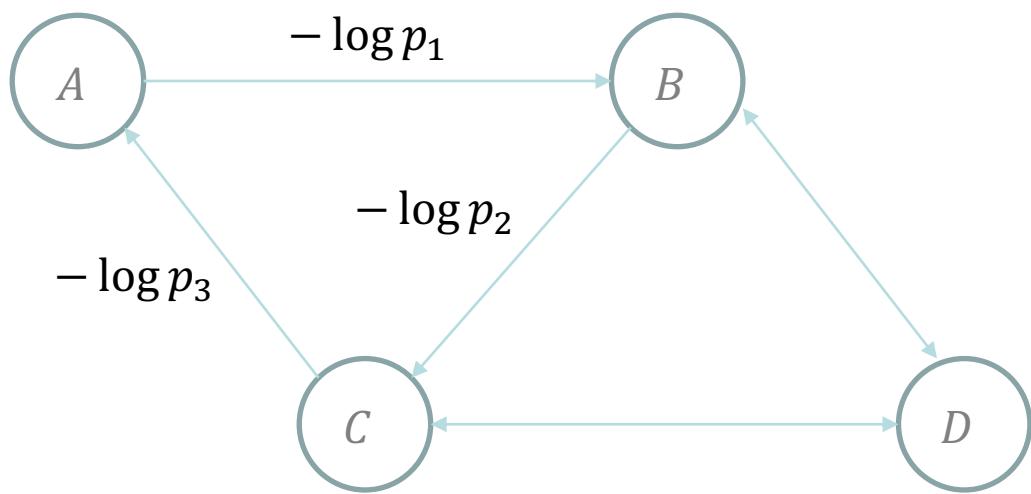
DeFiPoser-ARB



DeFiPoser-ARB



DeFiPoser-ARB



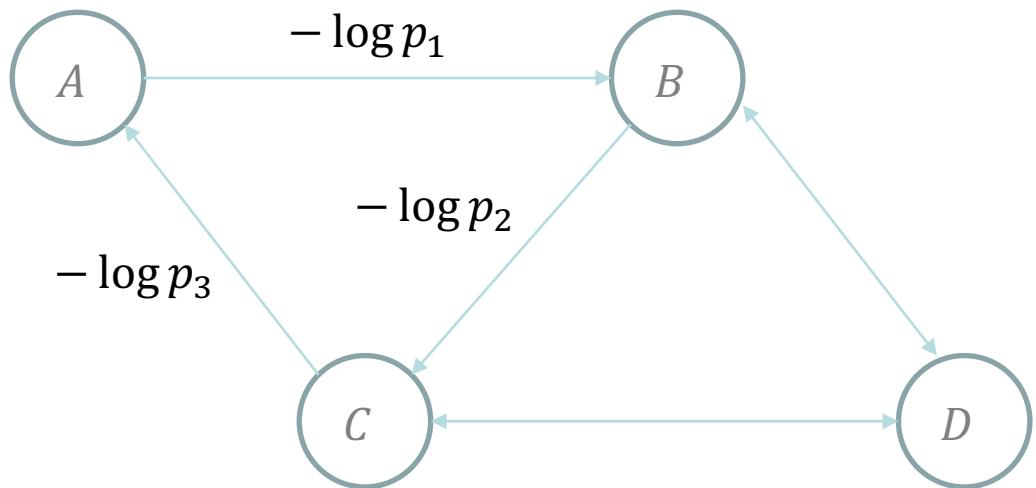
Profitable condition

$$p_1 \cdot p_2 \cdot p_3 > 1$$

\Updownarrow

$$(-\log p_1) + (-\log p_2) + (-\log p_3) < 0$$

DeFiPoser-ARB

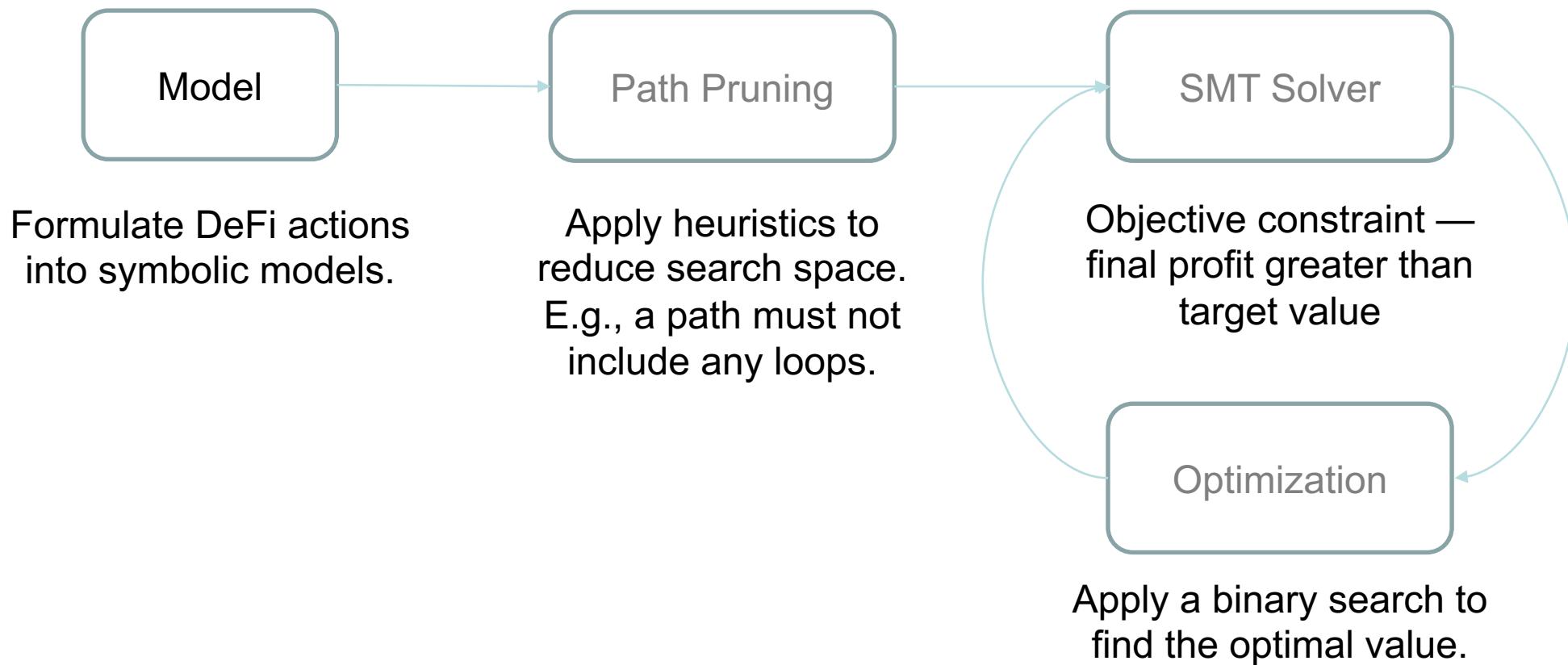


$$\prod_i p_i > 1 \iff \sum_i (-\log p_i) < 0$$

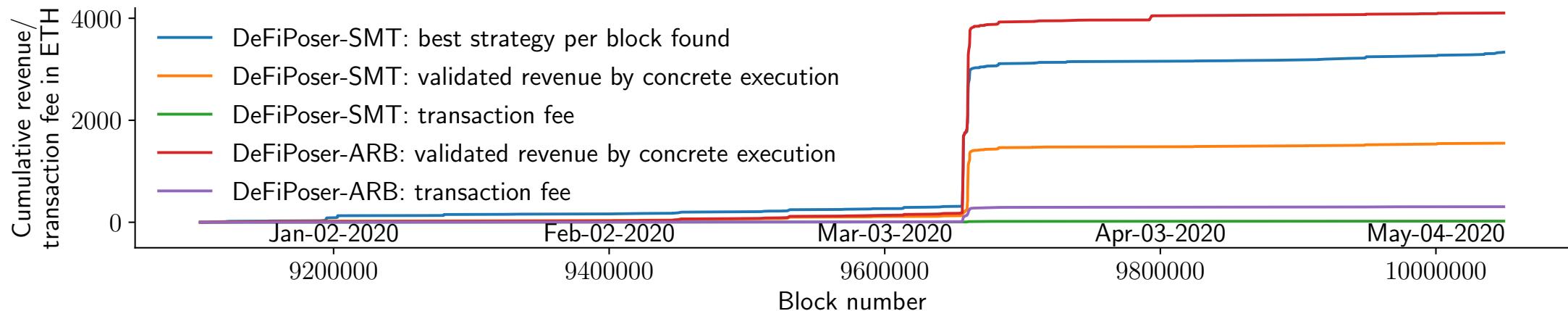
BellmanFord-Moore algorithm

$O(|N^2| \cdot |E|)$

DeFiPoser-SMT



DeFiPoser Evaluation



- 96 actions on Uniswap, Bancor, MakerDAO, total of 25 assets
- Block 9100000 (Dec-13-2019) to 10050000 (May-12-2020)
- Validation by concrete execution
 - Weekly revenue estimate:
 - DeFiPoser-ARB: 191.48 ETH (76,592 USD)
 - DeFiPoser-SMT: 72.44 ETH (28,976 USD)

Bellman Ford vs. SMT

| | DeFiPoser-ARB | DeFiPoser-SMT |
|--------------------------------|---|---|
| Path generation | Bellman-Ford-Moore, Walk to the root; No acyclic paths | Pruning with heuristics; Any paths within the heuristics |
| Path selection | Combines multiple sub-paths | Selects the highest revenue path |
| Manual DeFi modeling | Not required | Required |
| Captures non-cyclic strategies | No | Yes (e.g., bZx) |
| Optimally chosen parameters | No | Yes (subject to inaccuracy of binary search) |
| Maximum Revenue | 81.31 ETH (32,524 USD) | 22.40 ETH (8,960 USD) |
| Total Revenue (over 150 days) | 4,103.22 ETH (1,641,288 USD) | 1,552.32 ETH (620,928 USD) |
| Lines of code (Python) | 300 | 2, 300 |