Decentralized Finance

Decentralized Exchanges (DEX)

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





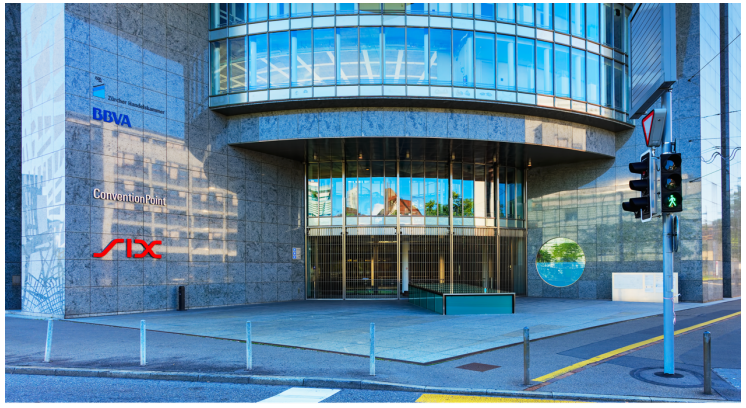
Stanford University

Imperial College London

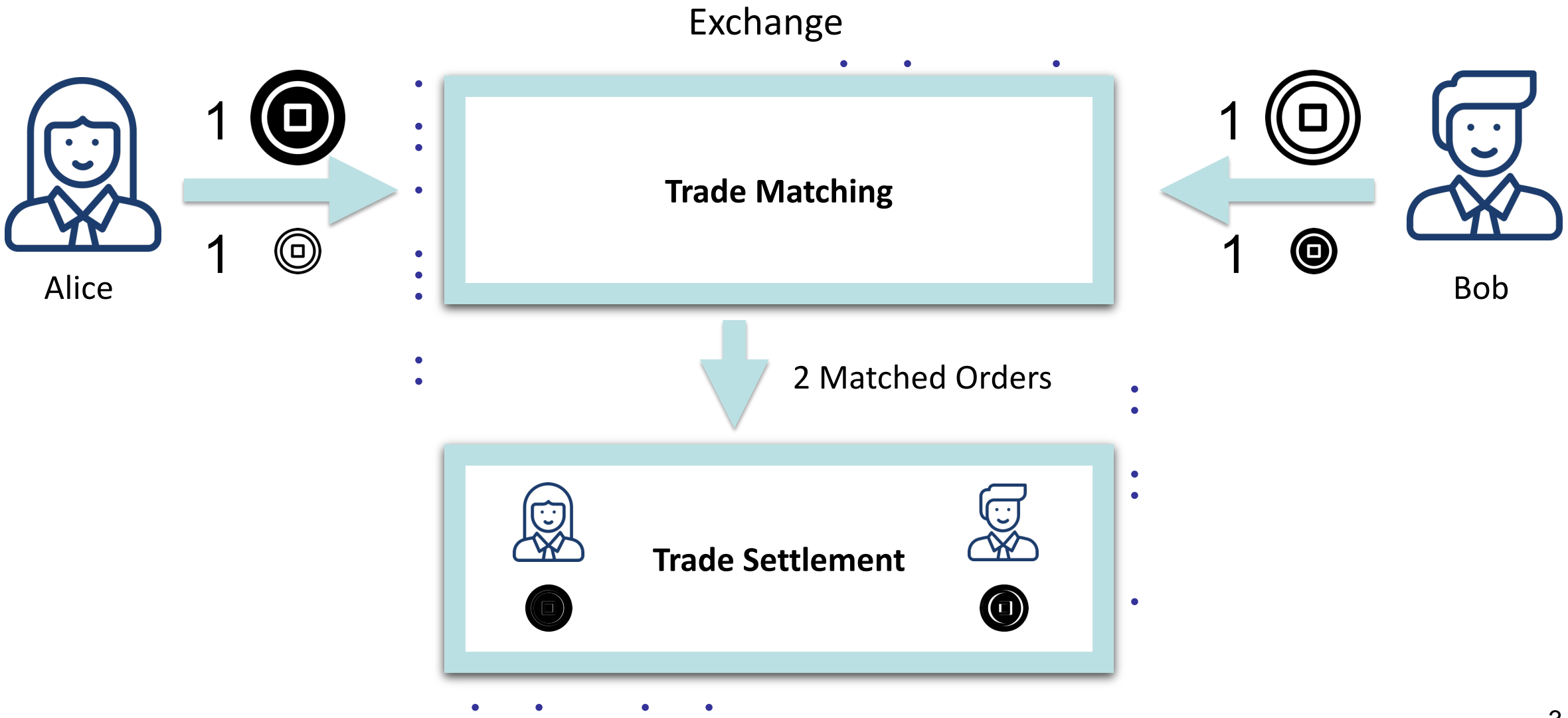
UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN

Berkeley UNIVERSITY OF CALIFORNIA

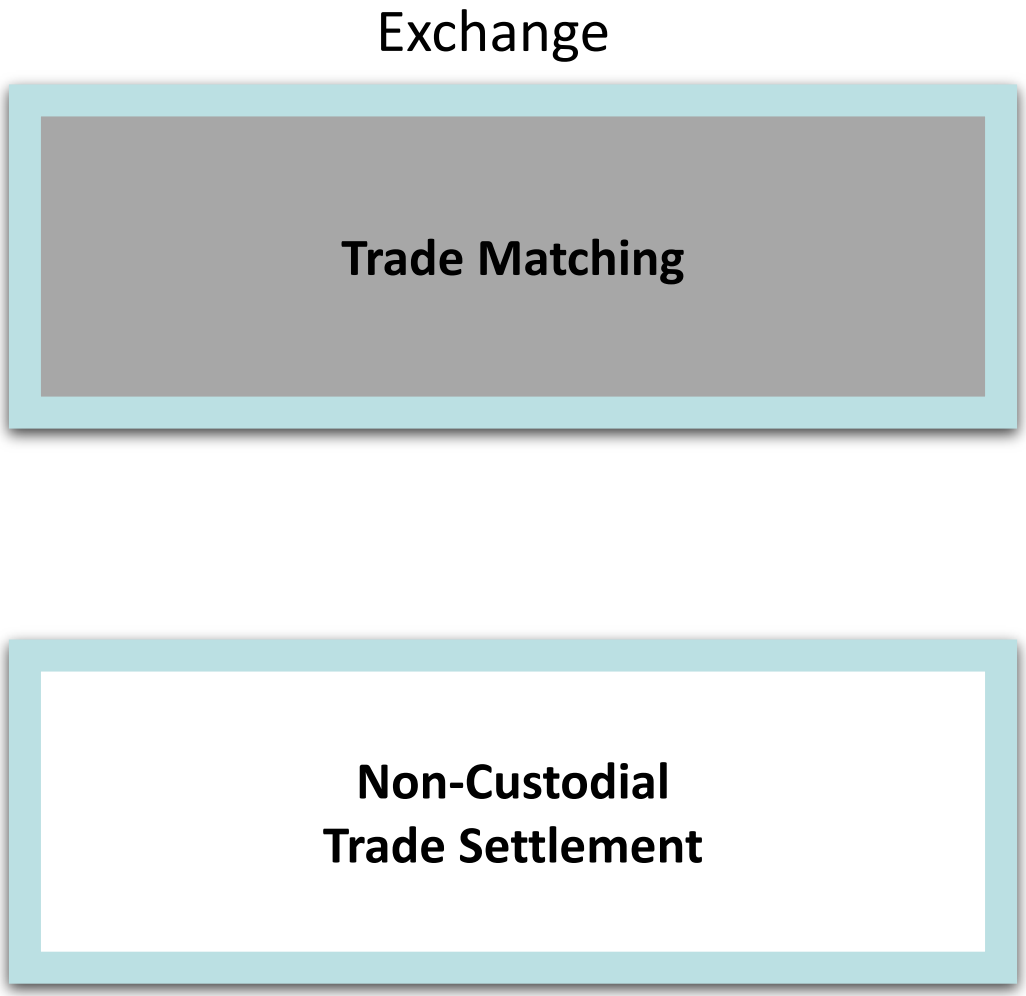
Financial Exchanges



Financial Exchanges 101



Trade Matching Models



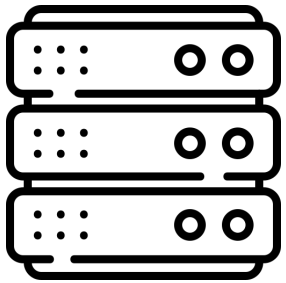
Order Book

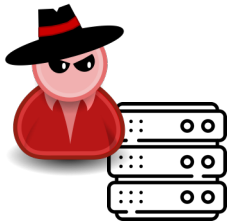

418.41
Mid Market Price
$418.10 $418.15 $418.20 $418.25 $418.30 $418.35 $418.40 $418.45 $418.50 $418.55 $418.60 $418.65 $418.70
ORDER BOOK
Market size Price (USD) My size Market size Price (USD) My size
21.23336000 418.40 -
0.01000000 418.39 -
0.01000000 418.31 -
0.01000000 418.30 -
0.01000000 418.29 -
0.01000000 418.28 -
0.01000000 418.27 -
0.05000000 418.26 -
0.01000000 418.23 -
0.01000000 418.22 -
0.01000000 418.21 -
1.45900000 418.20 -
0.01000000 418.19 -
1.47000000 418.17 -
1.45800000 418.14 -
1.49000000 418.10 -
2.27100000 418.07 -
0.06000000 418.06 -
0.06000000 418.05 -
1.53300000 418.04 -
0.07000000 418.03 -
0.76670000 418.00 -
1.48500000 417.99 -
1.49300000 417.92 -
16.48700000 417.91 -
0.01000000 417.90 -
1.43800000 417.89 -
1.21400000 417.88 -
0.32578000 418.68 -
0.02256000 418.67 -
0.15730000 418.66 -
0.95597000 418.65 -
0.16940000 418.64 -
1.37110400 418.63 -
2.69360000 418.62 -
0.03200000 418.61 -
0.17200000 418.60 -
6.42753821 418.59 -
1.96500000 418.58 -
3.35532000 418.57 -
0.07500000 418.56 -
0.03750000 418.55 -
0.80500000 418.54 -
0.30670000 418.53 -
5.93968000 418.52 -
0.03500000 418.51 -
6.11465568 418.50 -
1.59490000 418.49 -
2.36500000 418.48 -
0.39489096 418.47 -
1.03616569 418.46 -
0.04434039 418.45 -
0.58720572 418.44 -
2.41500000 418.43 -
0.02500000 418.42 -
9.51880170 418.41 -

Two Order Book Models

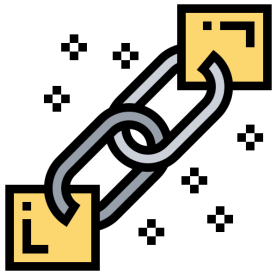
Server

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

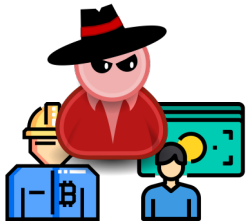




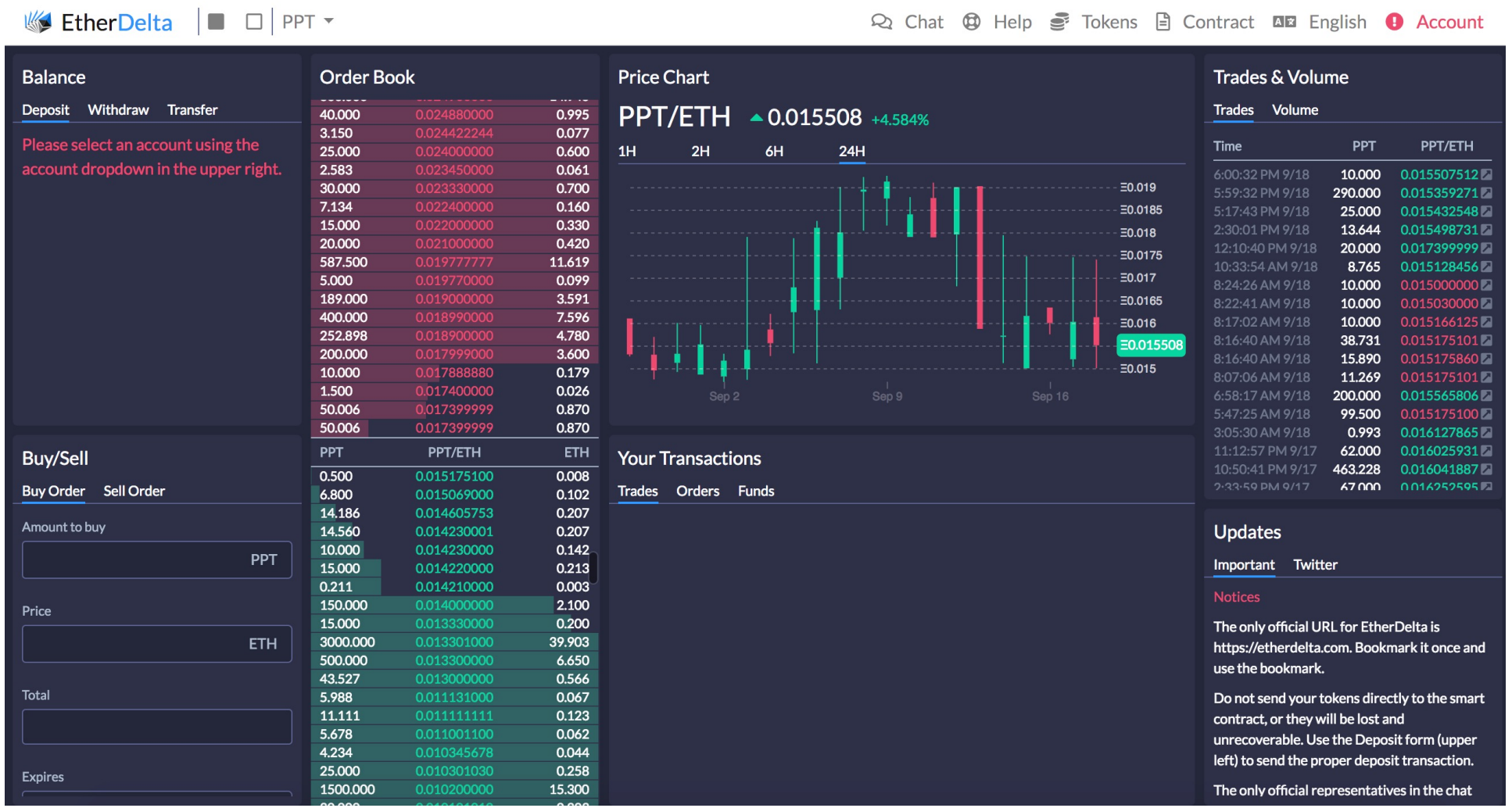
On-Chain



- \+ 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.
Buy/Sell
Buy Order
Sell Order
Amount to buy
PPT
Price
ETH
Total
Expires
Order Book
40.000 0.024880000 0.995
3.150 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
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
Price Chart
PPT/ETH 0.015508 +4.584%
1H 2H 6H 24H
Ξ0.019
Ξ0.0185
Ξ0.018
Ξ0.0175
Ξ0.017
Ξ0.0165
Ξ0.016
Ξ0.015508
Ξ0.015
Sep 2
Sep 9
Sep 16
Your Transactions
Trades
Orders
Funds
Trades & Volume
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
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

Exchange

Trade Matching

Non-Custodial
Trade Settlement

Why do we need DEX?

Alice is rich
(aka a “whale”)

Alice wants to provide her money to traders to earn fees

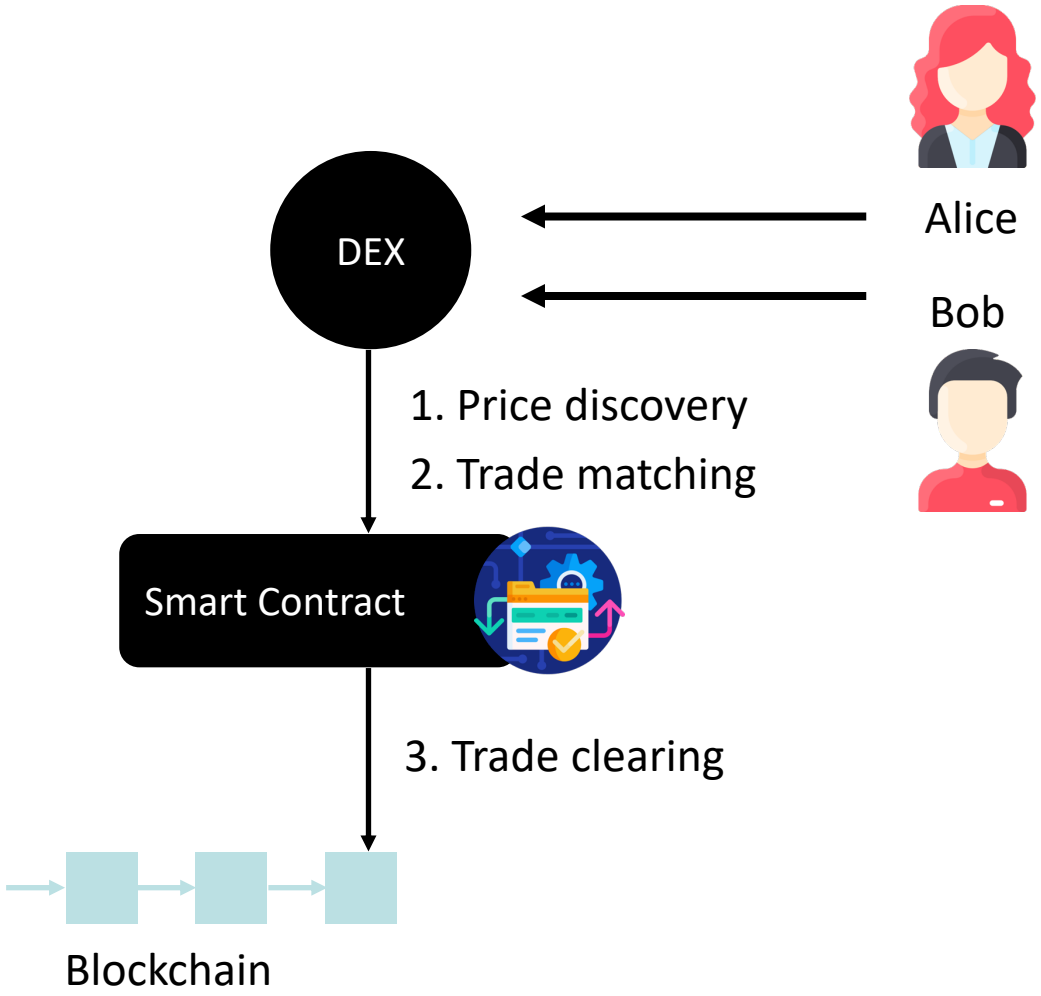
..but has to trust someone to manage her money

Bob is nifty trader

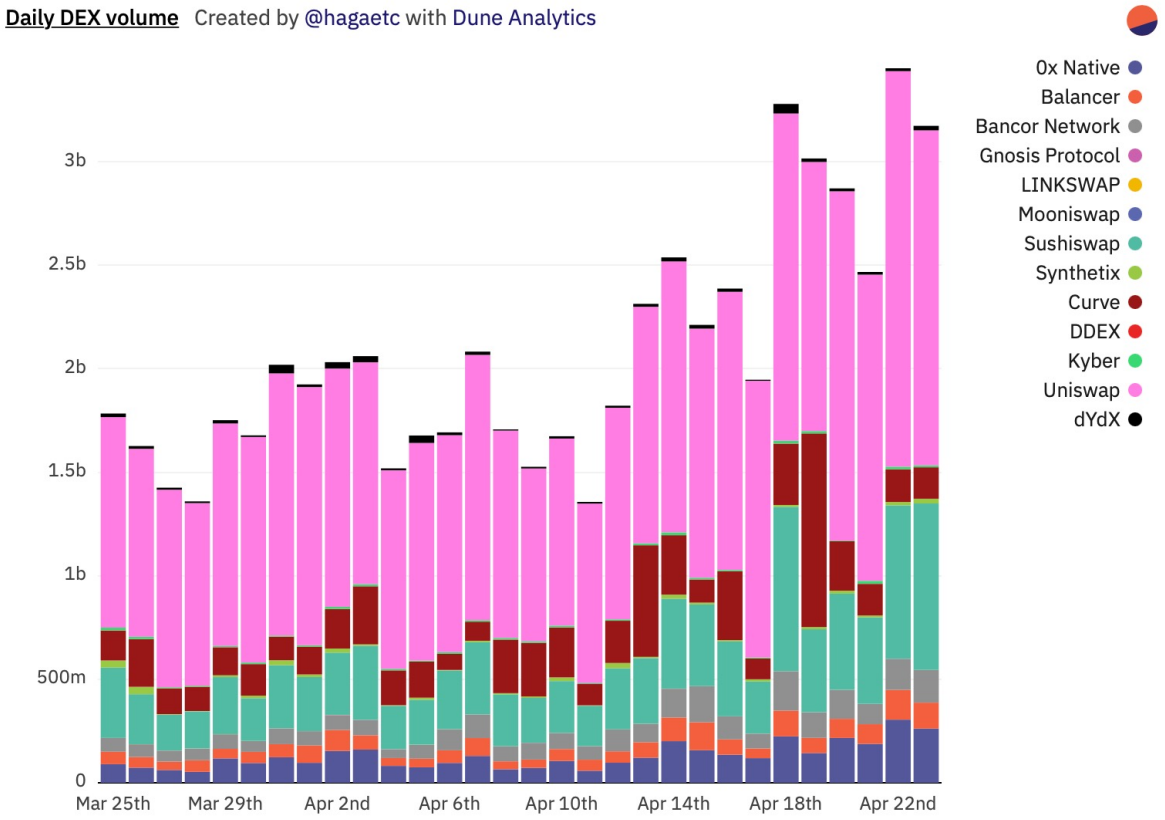
Bob wants to buy the latest coins

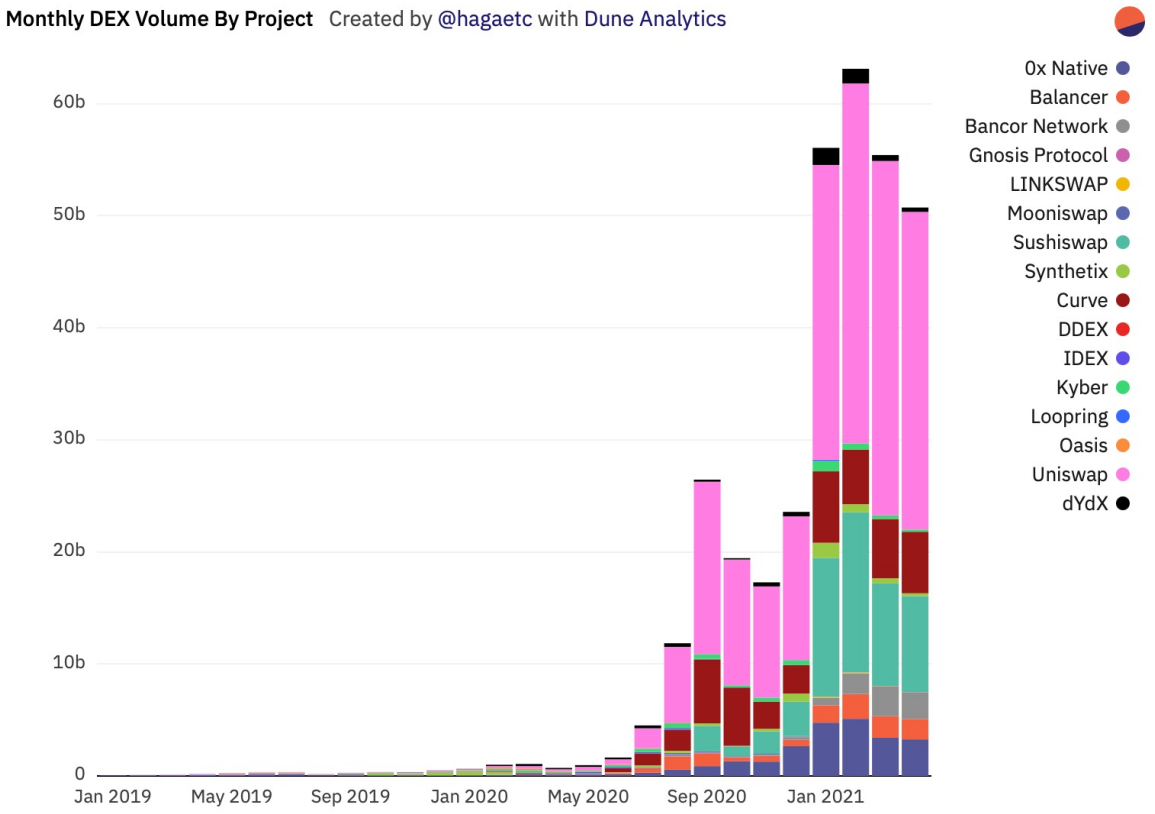
..but struggles to find a trusted source to buy

DEX System Architecture



DEX trading volume





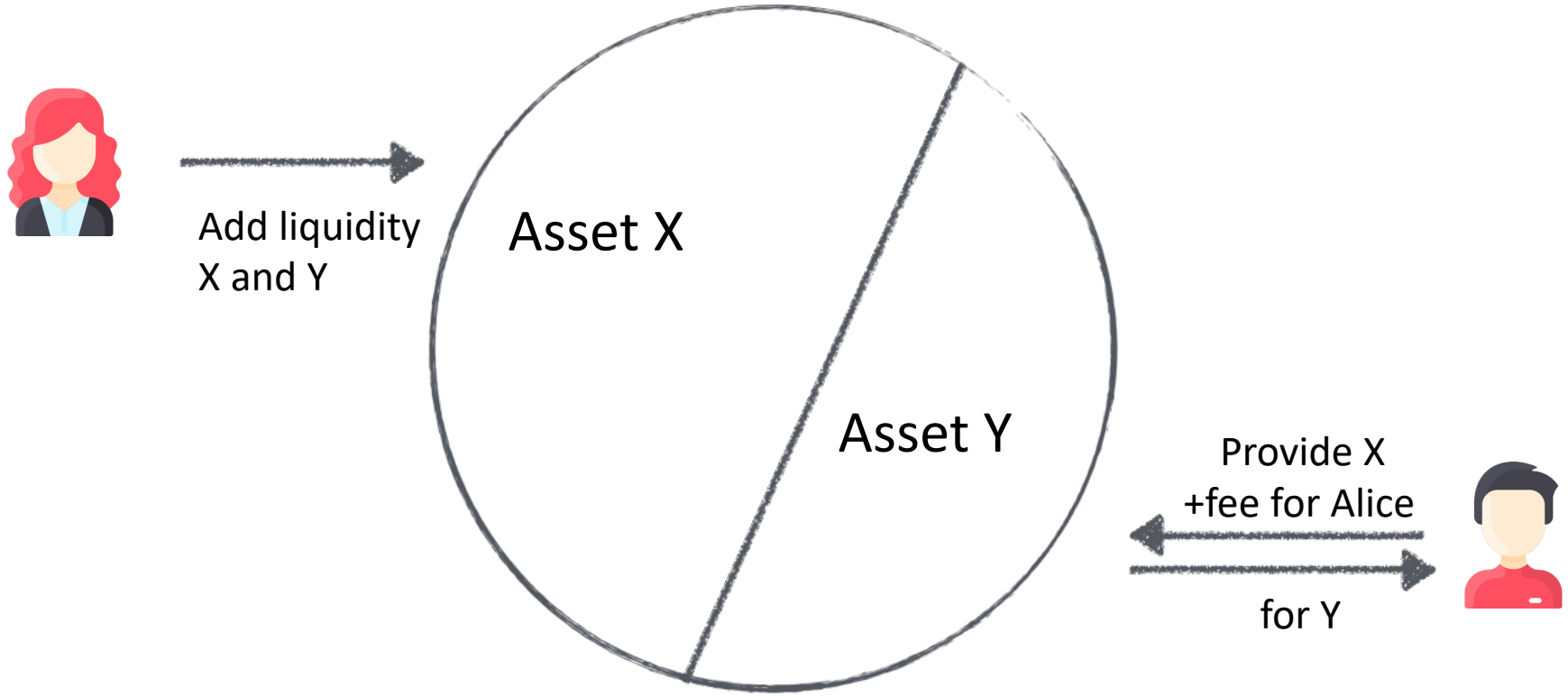
Daily Volume:
- DEXes: 3.5B
- Binance: 49B
- Nasdaq: 234B

Source:
https://defiprime.com/dex-volume
http://www.nasdaqtrader.com/Trader.aspx?id=DailyMarketSummary
https://coinmarketcap.com/rankings/exchanges/


Automated Market Maker
https://defi-learning.org

Liquidity Pool

Idea: Let a smart contract do the market making.



smart contract pool

AMM – Automated Market Maker

Idea: Let a smart contract do the market making.

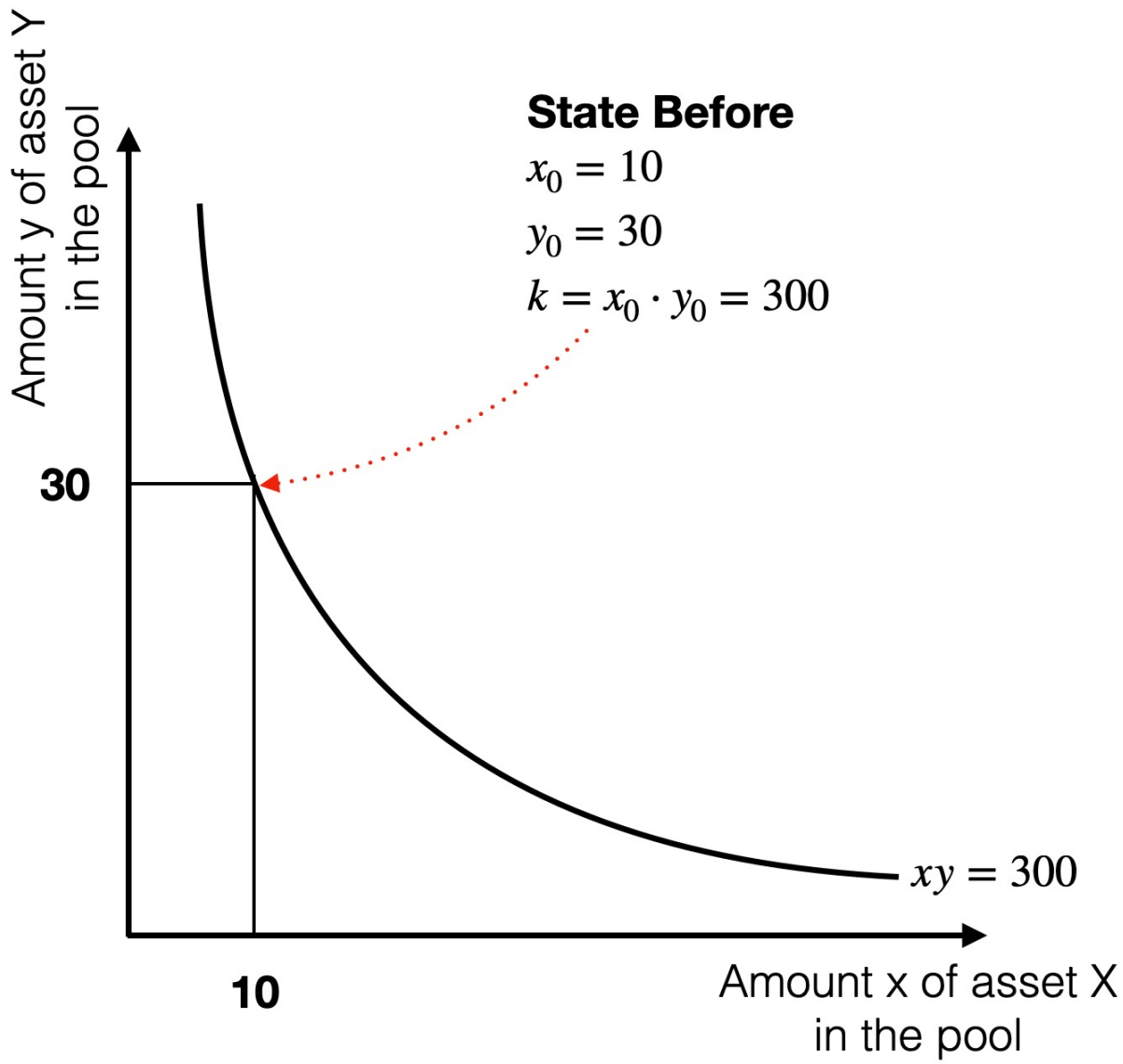
$$x \times y = k$$

- x: Asset X quantity
- y: Asset Y quantity
- k: constant

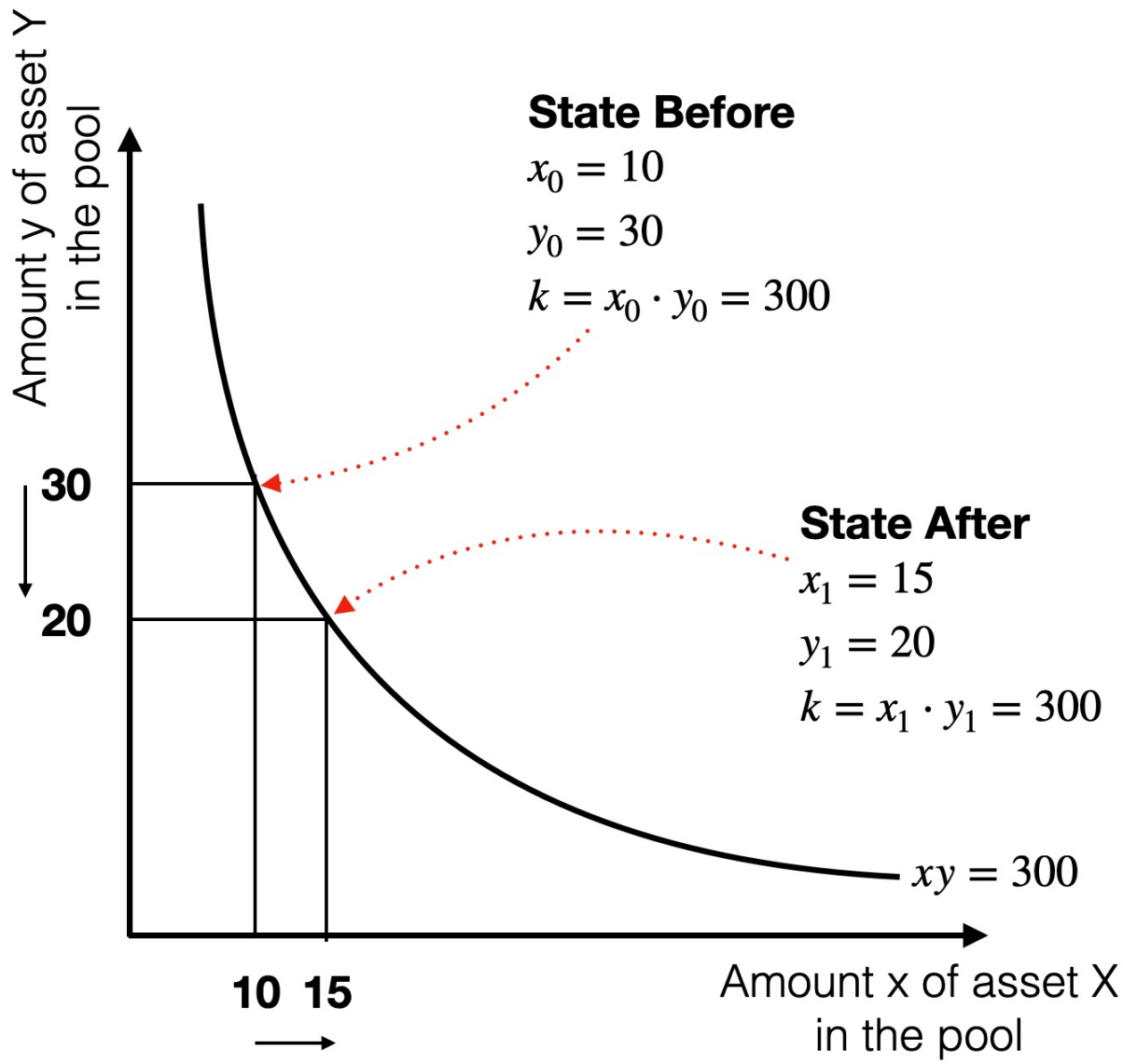
Properties:

- 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

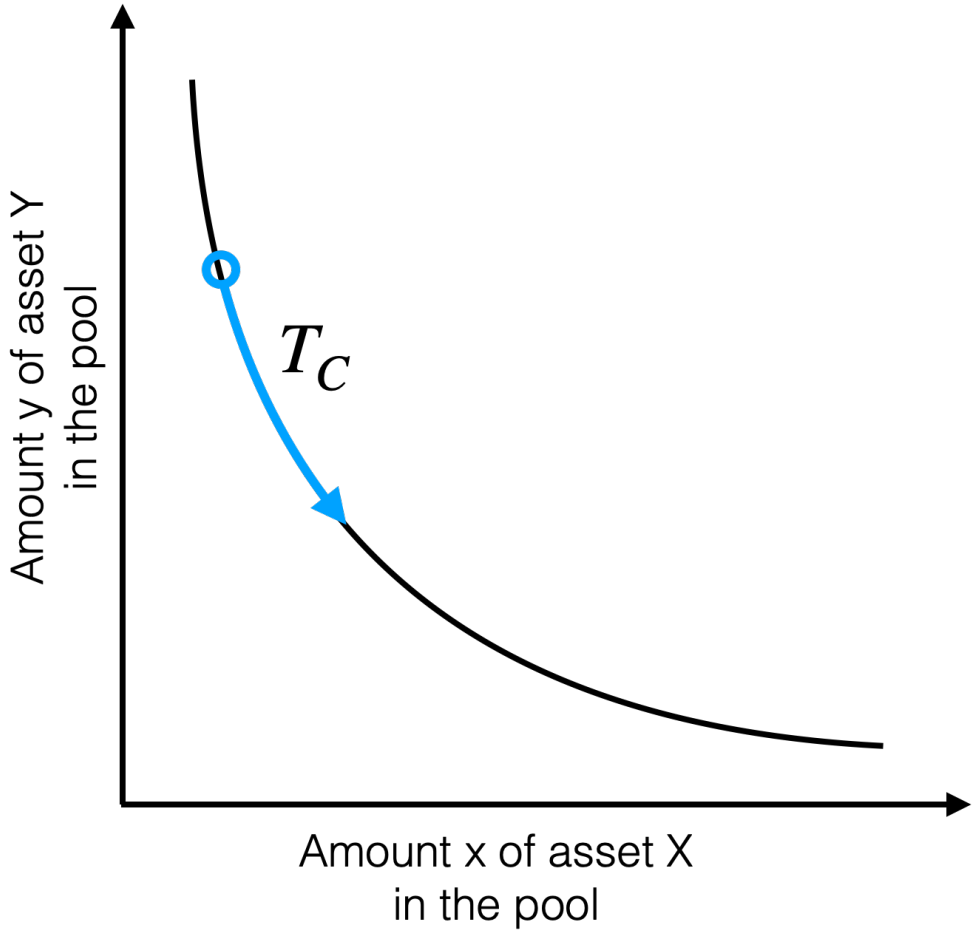

Amount y of asset Y
in the pool
State Before
$x_0 = 10$
$y_0 = 30$
$k = x_0 \cdot y_0 = 300$
30
$xy = 300$
10
Amount x of asset X
in the pool

AMM Example

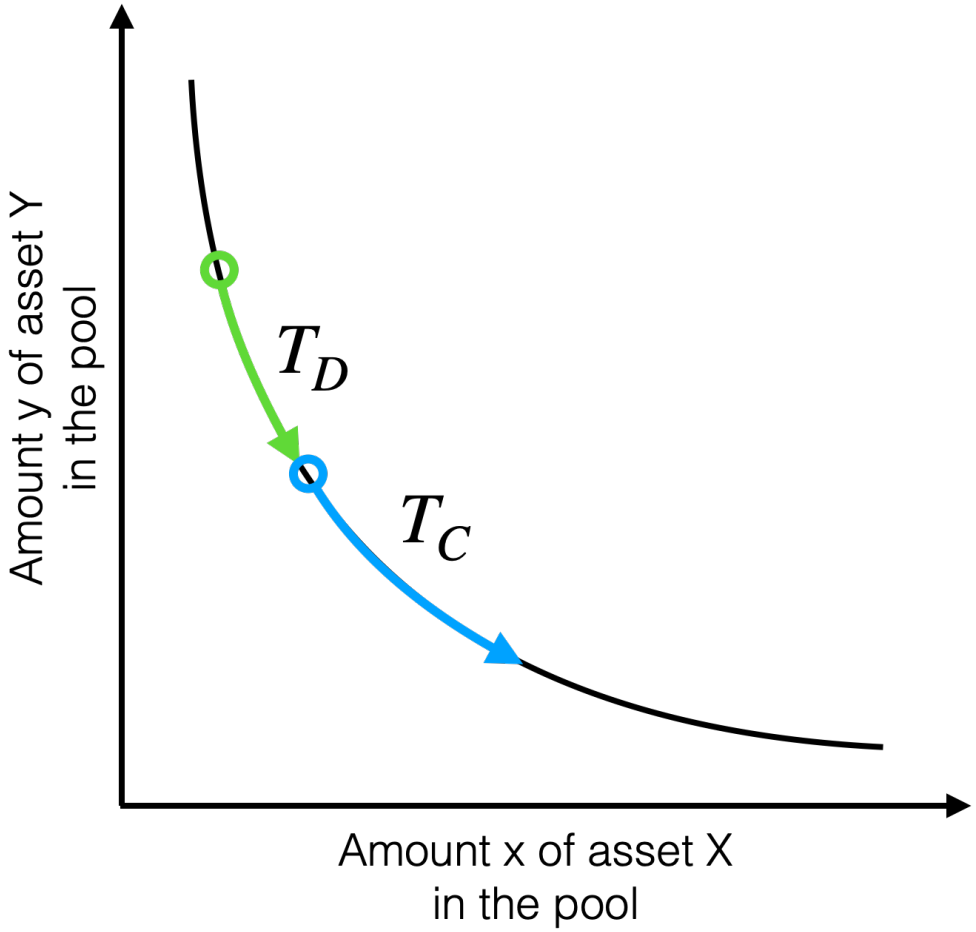

Amount y of asset Y
in the pool
State Before
$x_0 = 10$
$y_0 = 30$
$k = x_0 \cdot y_0 = 300$
30
20
State After
$x_1 = 15$
$y_1 = 20$
$k = x_1 \cdot y_1 = 300$
$xy = 300$
10 15
Amount x of asset X
in the pool

Expected Slippage

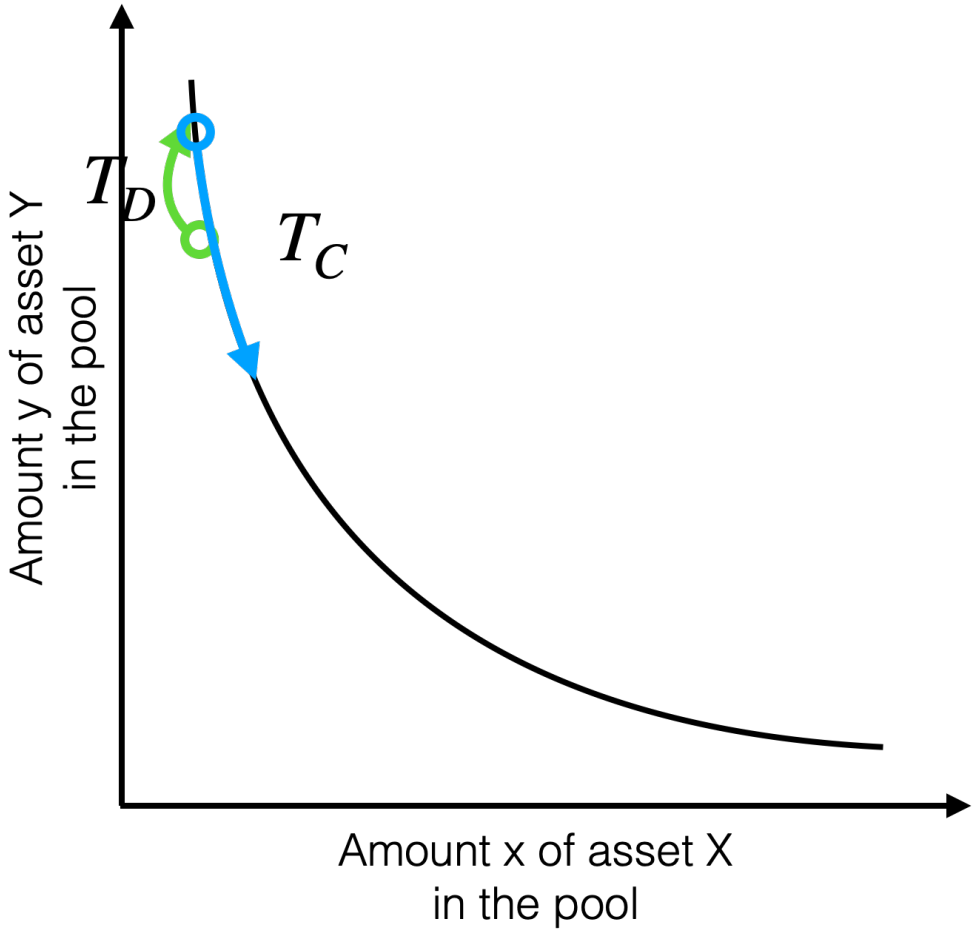
The expected increase or decrease in price based on the trading volume and available liquidity.



Unexpected Slippage → Worse Execution Price

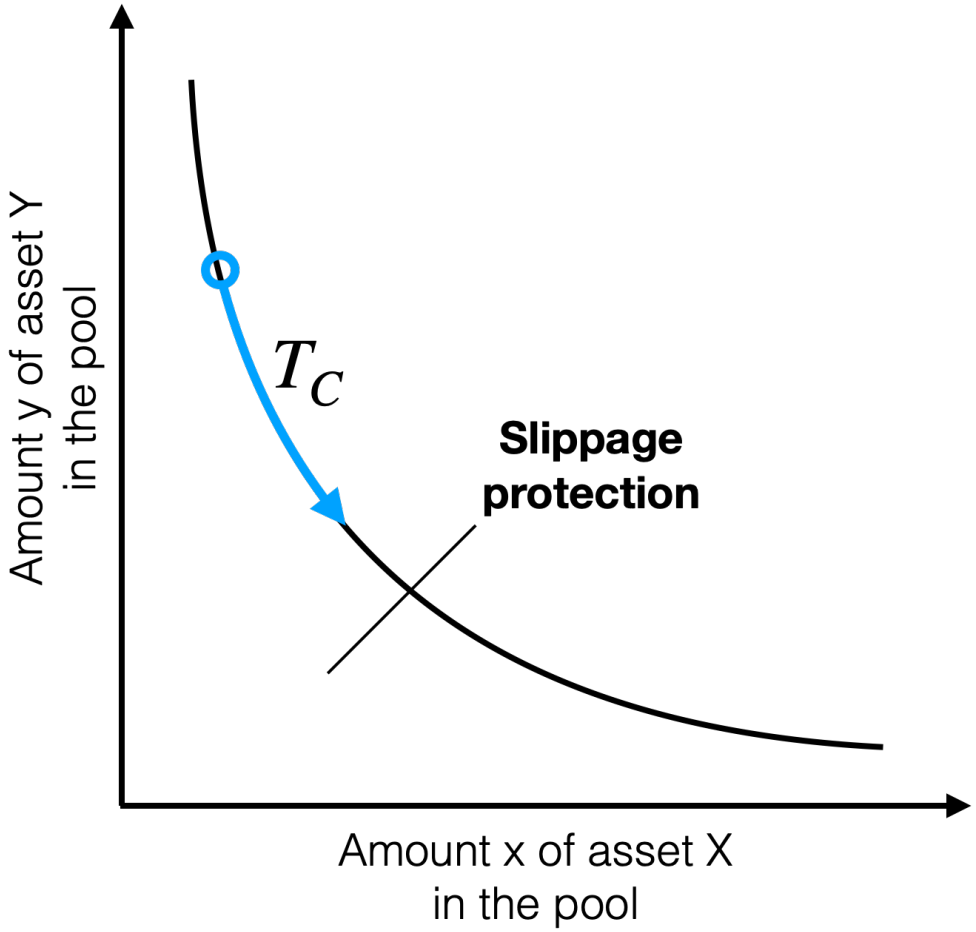


Unexpected Slippage → Better Execution Price



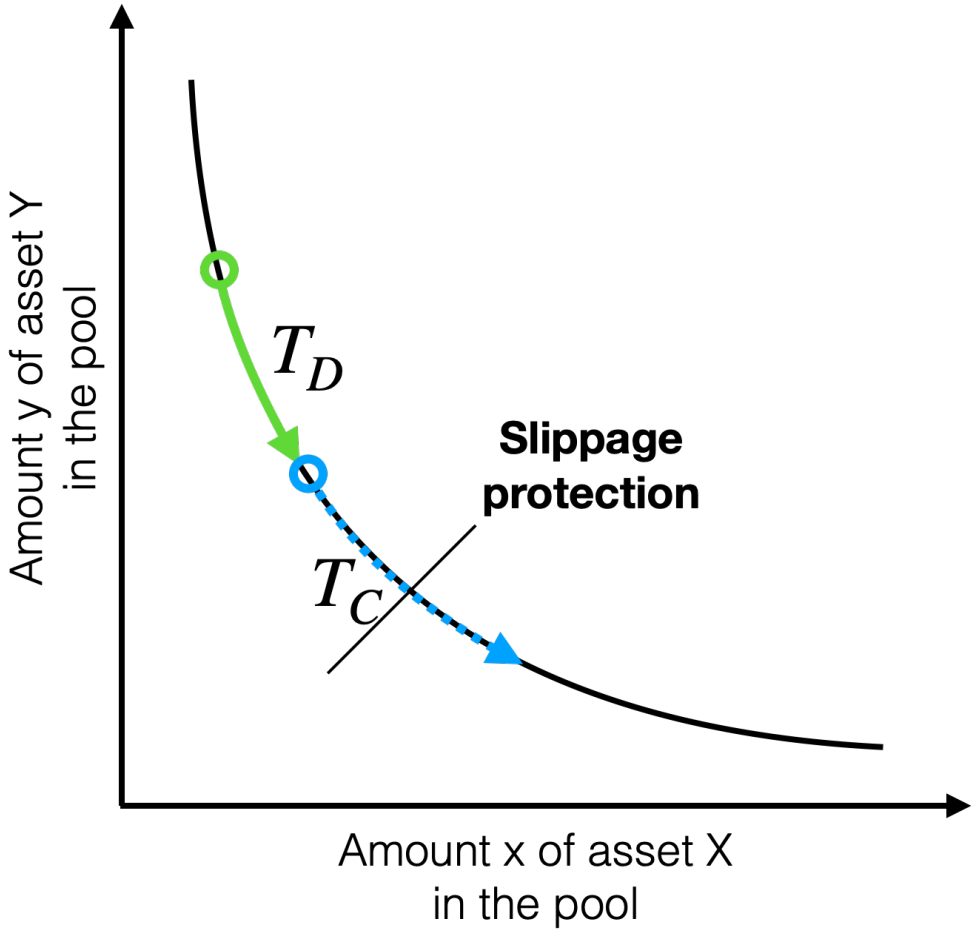
Slippage Protection

Configures a slippage protection threshold to prevent unacceptable slippage



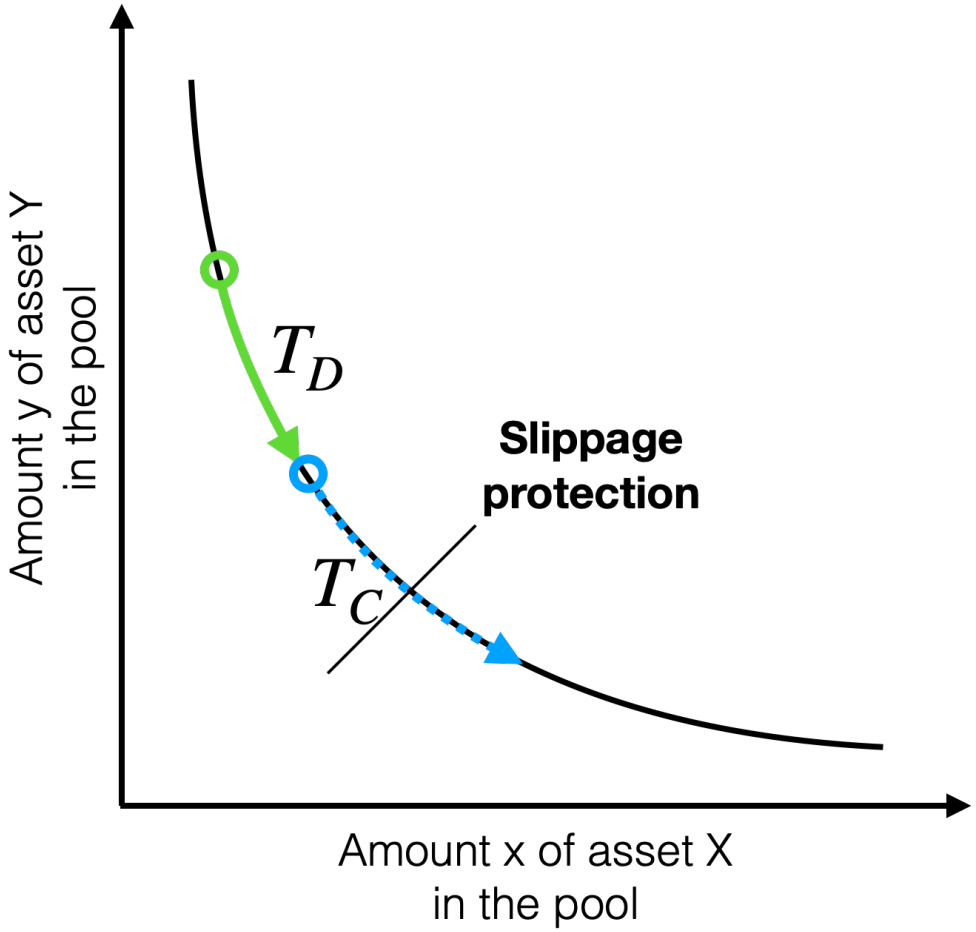
Slippage Protection

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



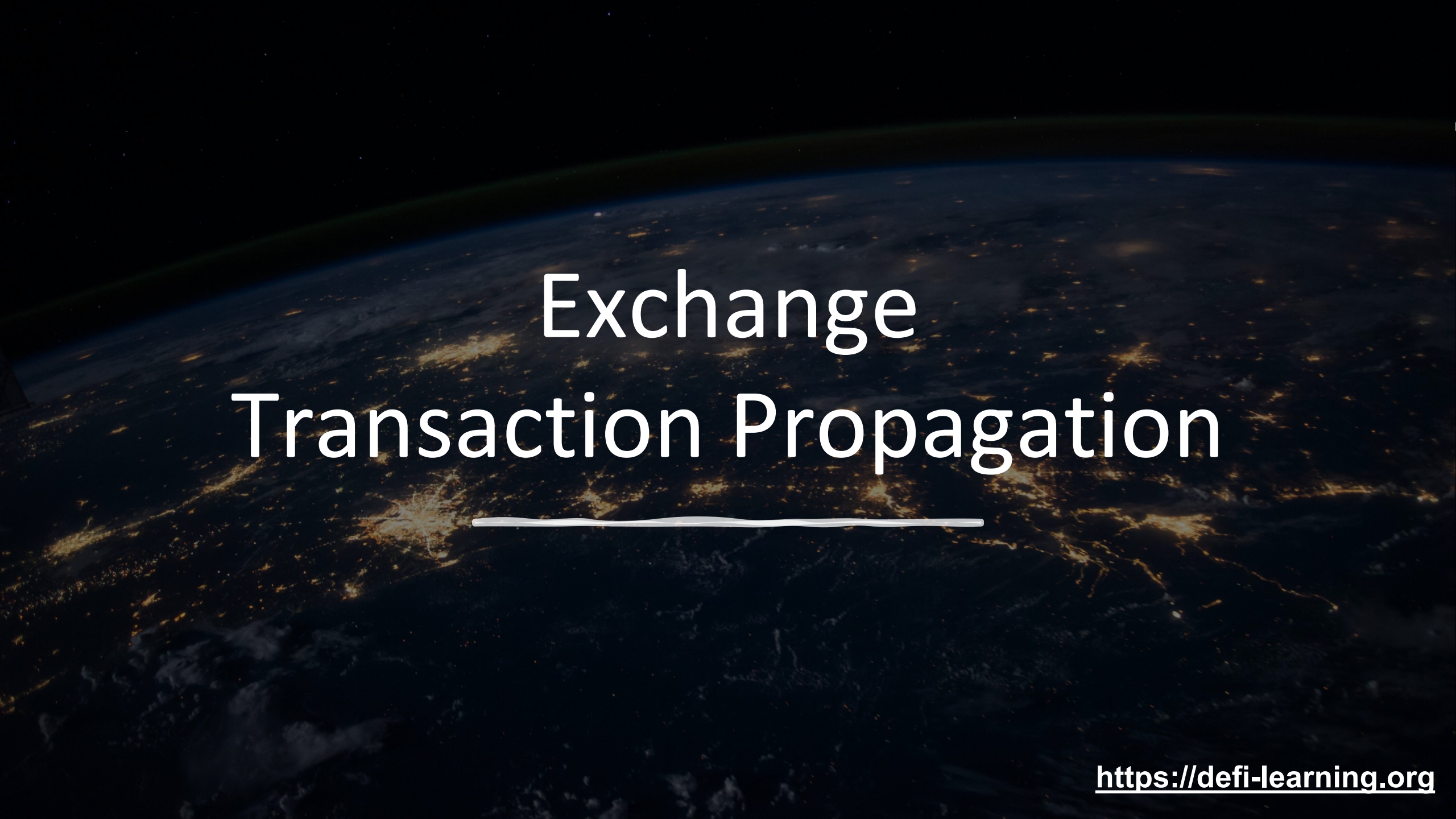
Slippage Protection

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



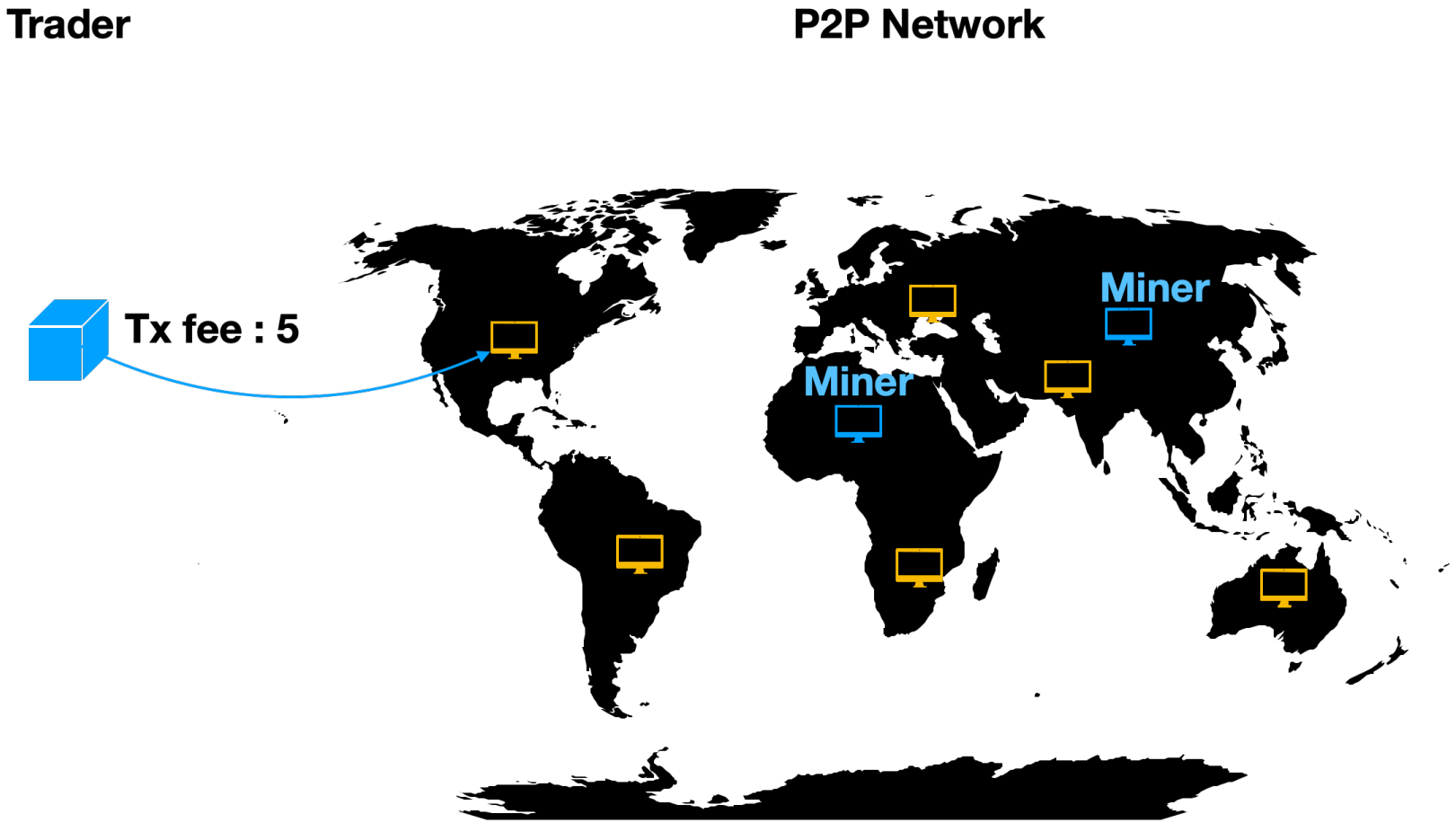
Pros and Cons of an AMM

- (+) 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 tolarence
- (-) Users vulnerable to sandwich attacks
  - See security lecture

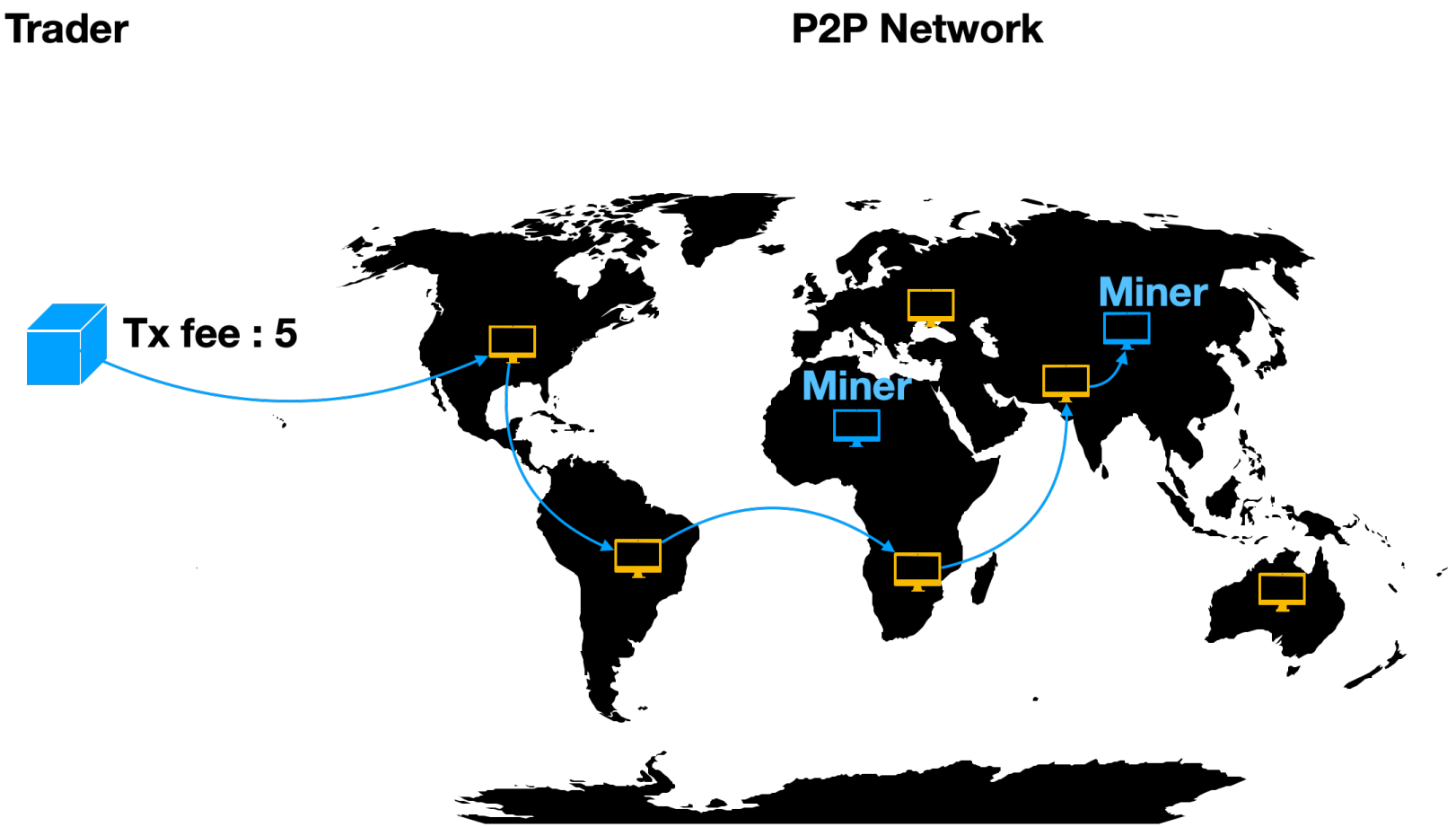


https://defi-learning.org

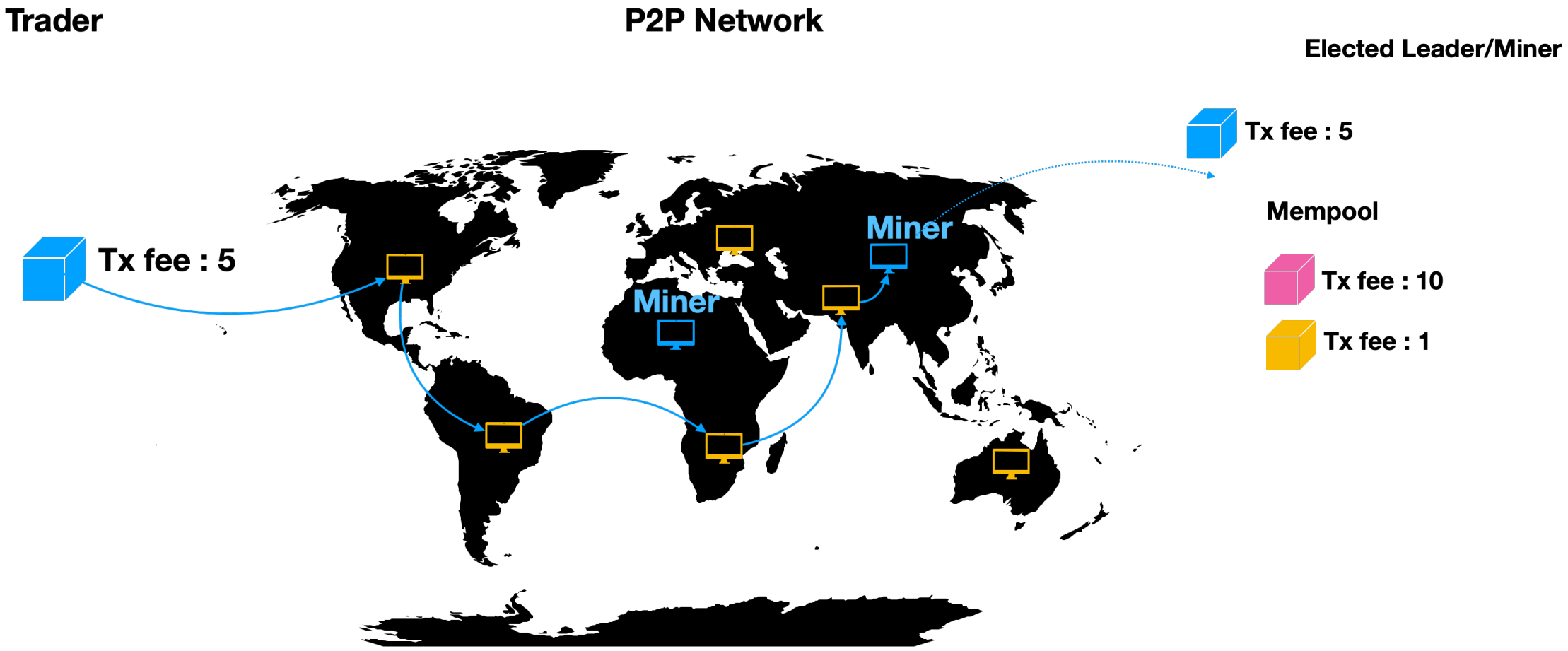
Exchange Transaction Propagation



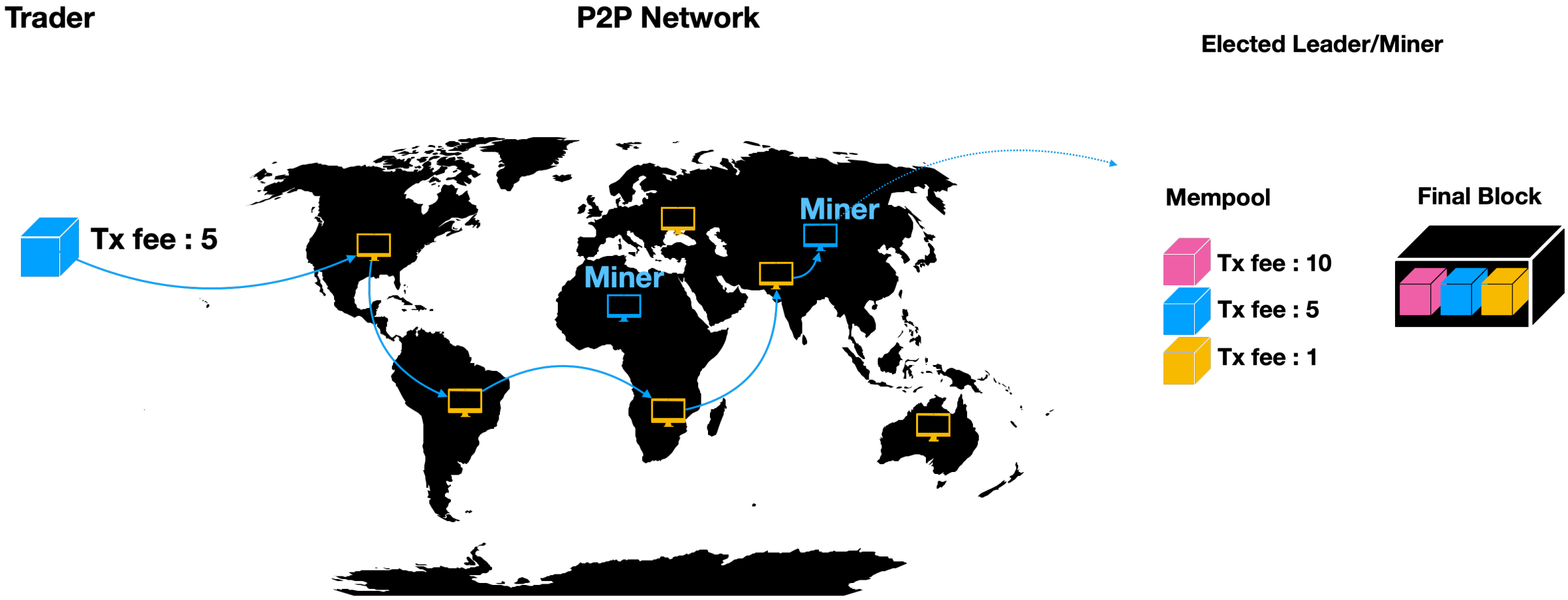
Exchange Transaction Propagation



Exchange Transaction Propagation

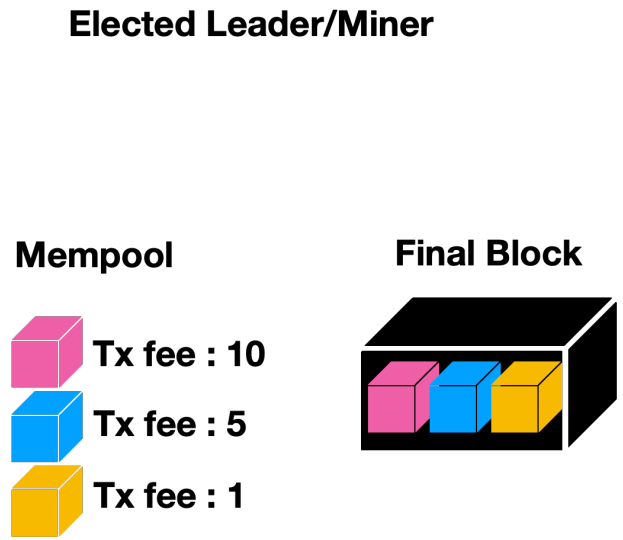


Exchange Transaction Propagation



Exchange Transaction Propagation

- Asynchronous Blockchain P2P Network
  - Best effort propagation
  - Transparency
  - High-Frequency Trading
- Inclusion based on an 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
https://defi-learning.org

Pegged/Stablecoin Swap

USDC USDT DAI

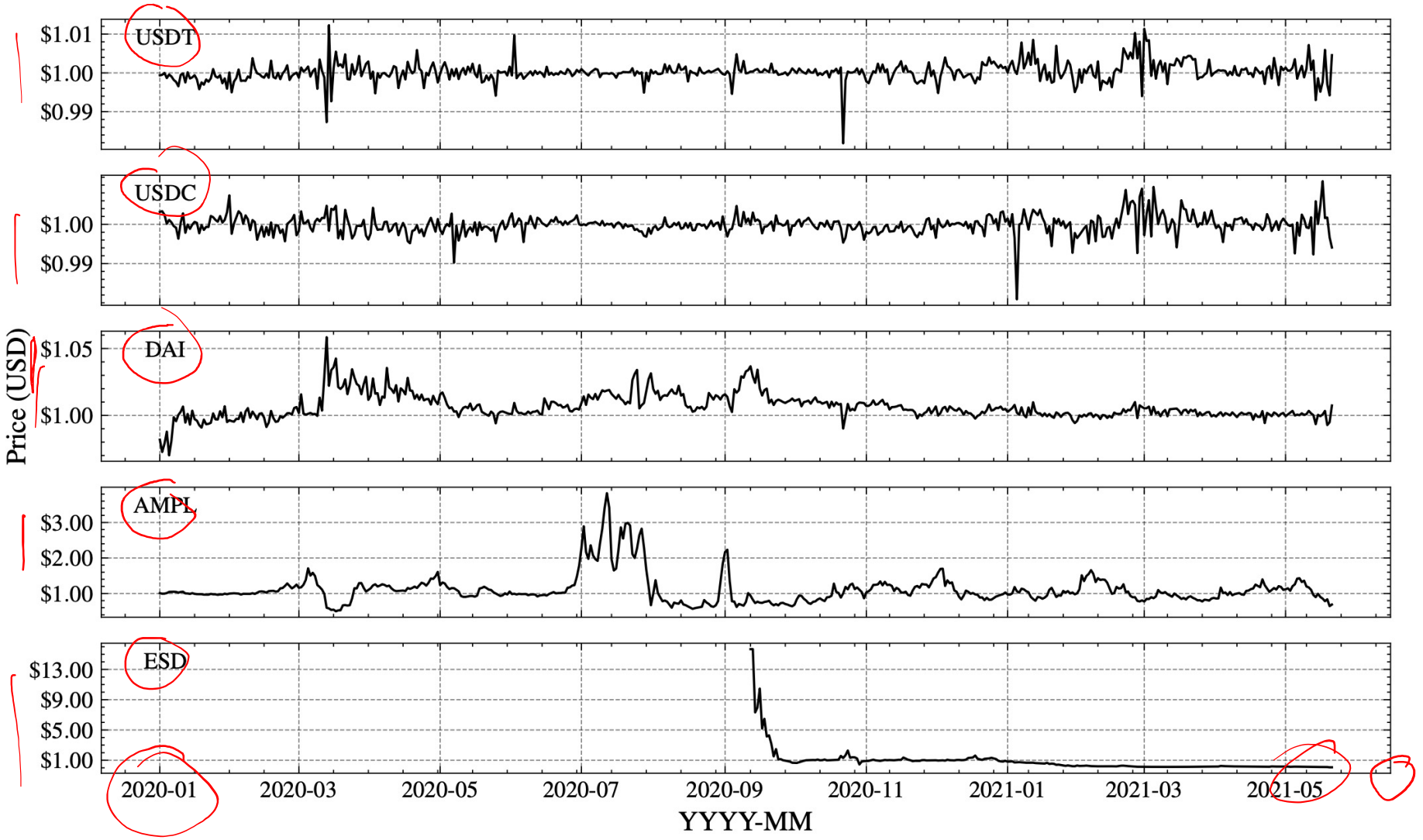
USD derivatives

WBTC renBTC sETH stETH

Pegged coins

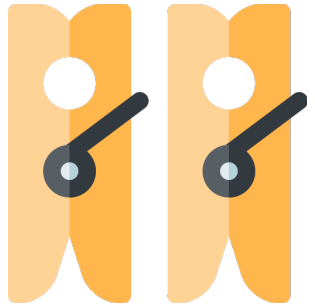
- Three Stablecoin Types
  - Reserve-based
  - Collateral-based
  - Algorithmic

Pegged/Stablecoin Swap



Pegged/Stablecoins

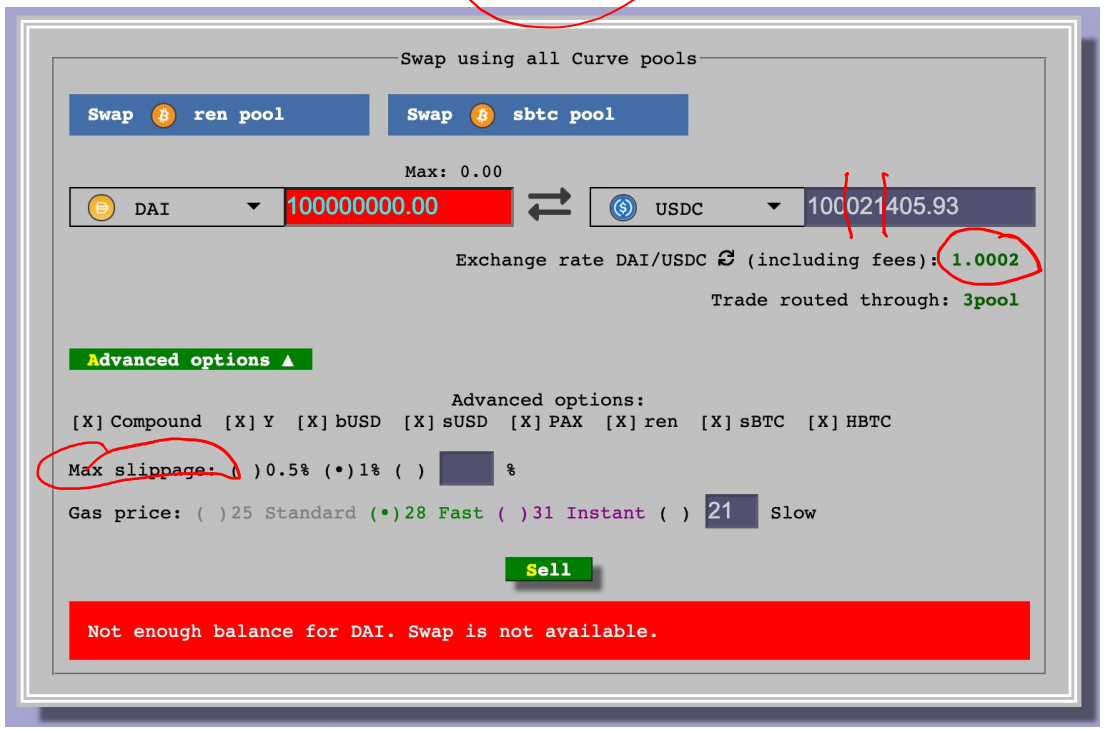
- Pegged/Stablecoin prices move in expectation together
  - The exchange rate should ideally remain 1 to 1
  - A default CP AMM is not optimized for such case



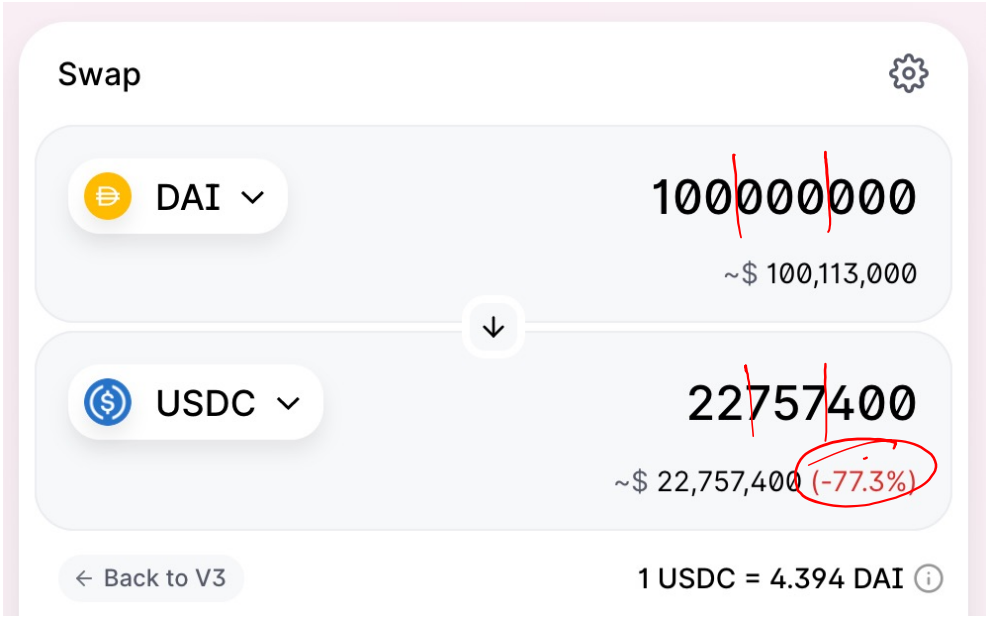
- Stablecoin AMM pros/cons:
  - (+) Better prices for bigger volumes (i.e. more liquidity)
  - (-) Potentially higher gas costs
  - (-) Danger of a de-peg of a stablecoin

Pegged/Stablecoin Swap

Curve



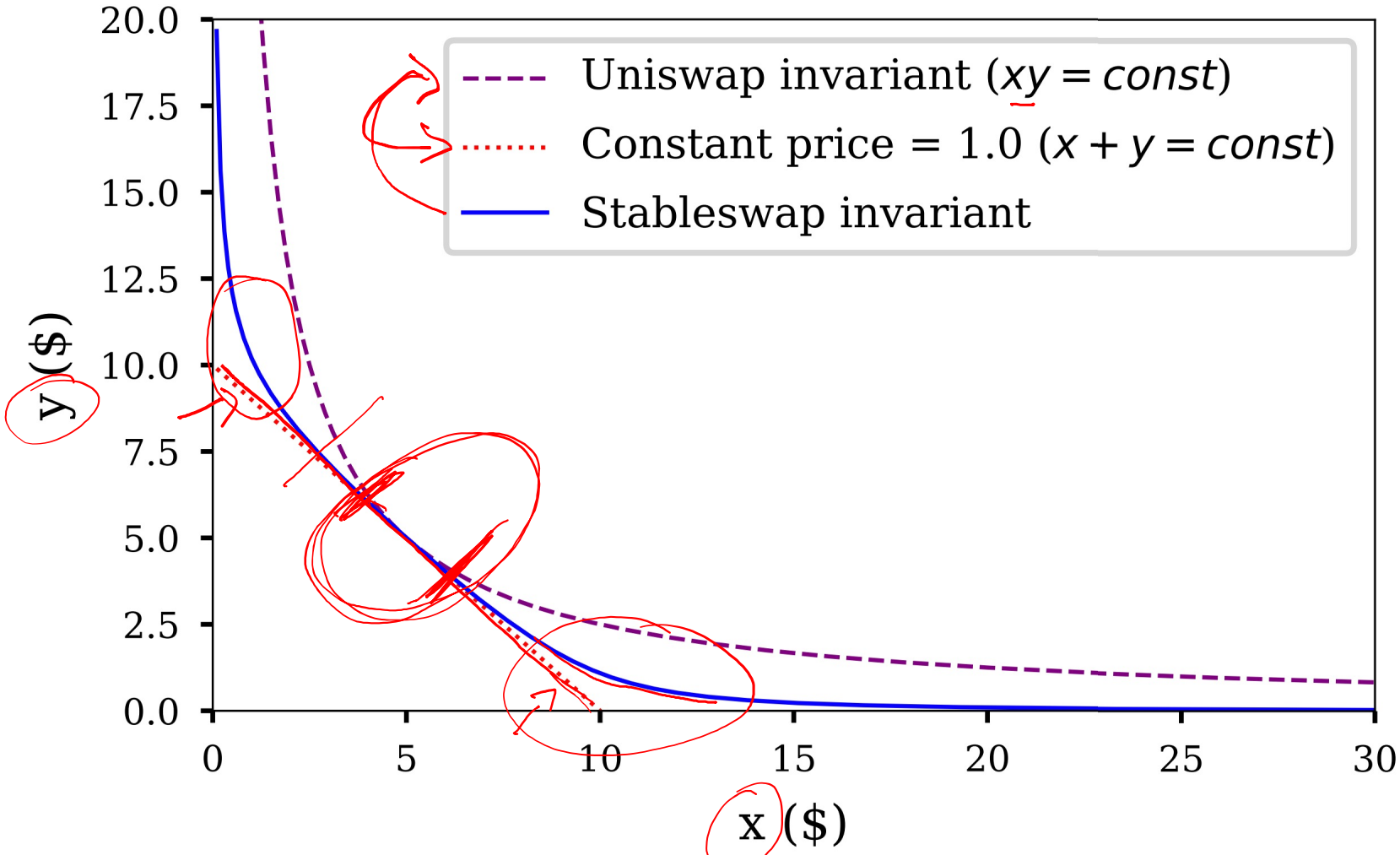
Uniswap



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

Price Curve

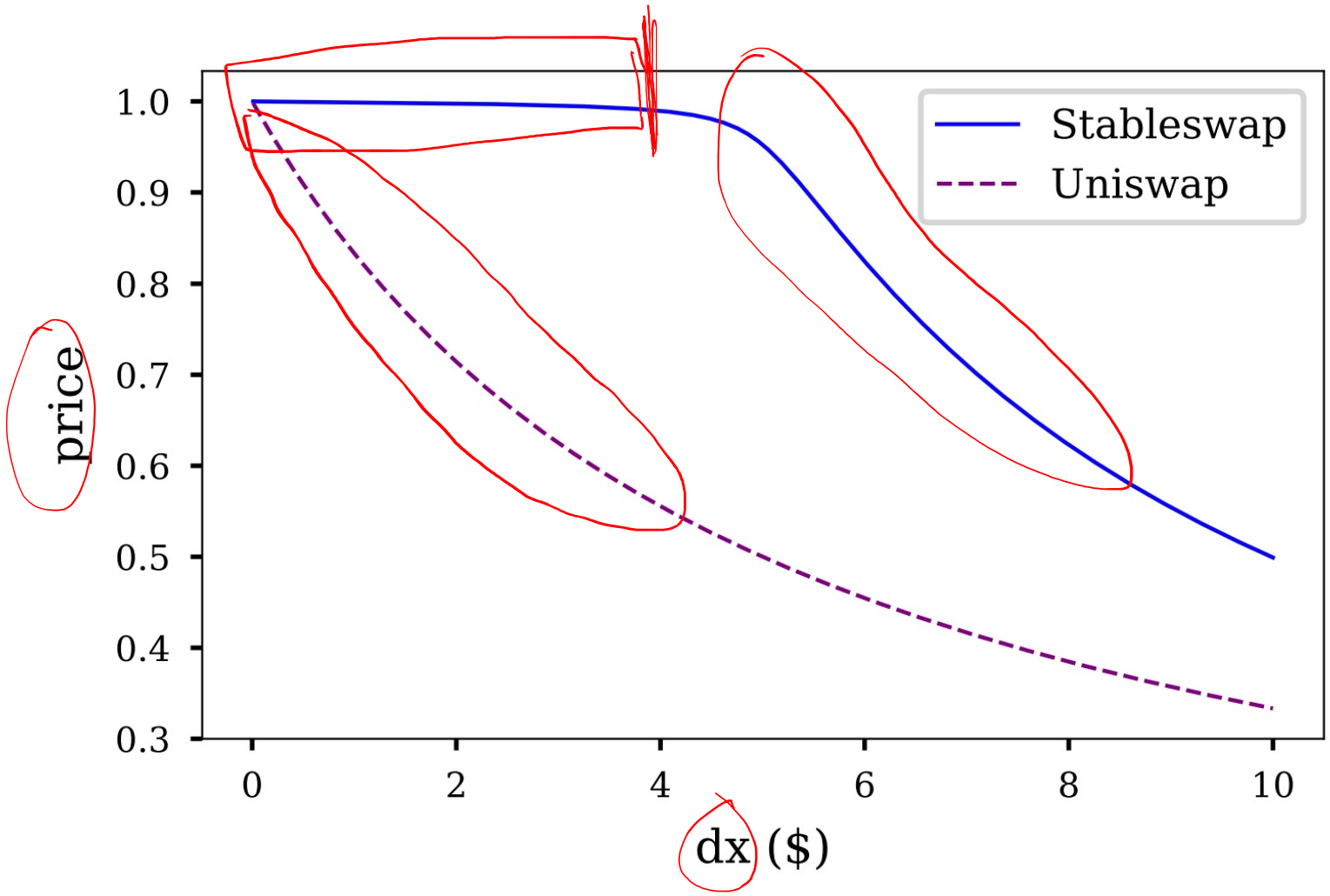
Stableswap (aka Curve Finance)



initially,
x = 5
y = 5

Slippage Comparison

Stableswap (aka Curve Finance)



What happens if a coin de-pegs?

What happens if a coin gets blacklisted?

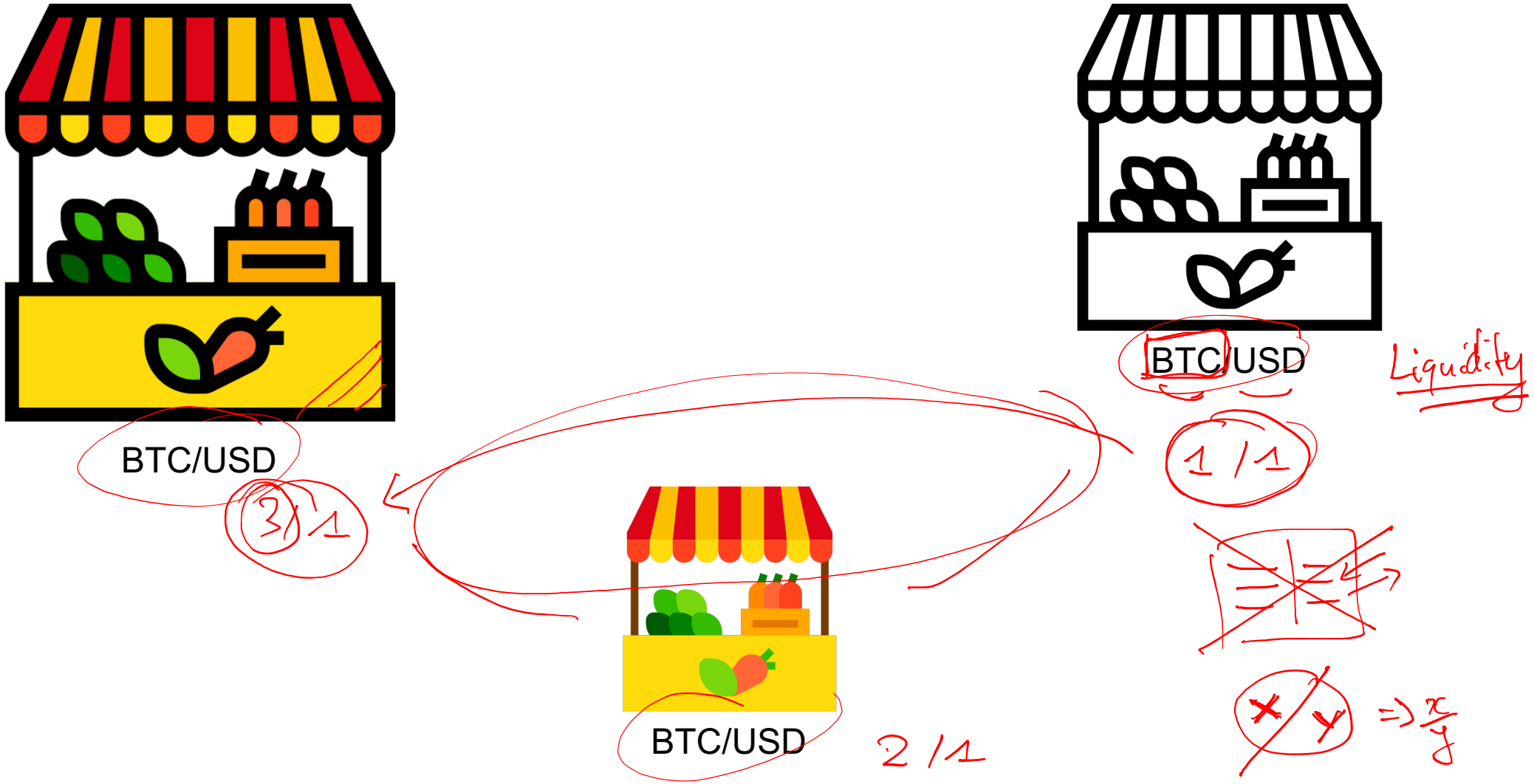
AMM Whitepaper

- 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

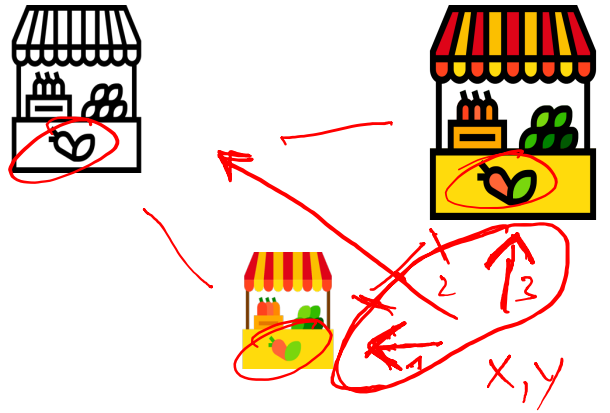

AMM Arbitrage
https://defi-learning.org

Arbitrage



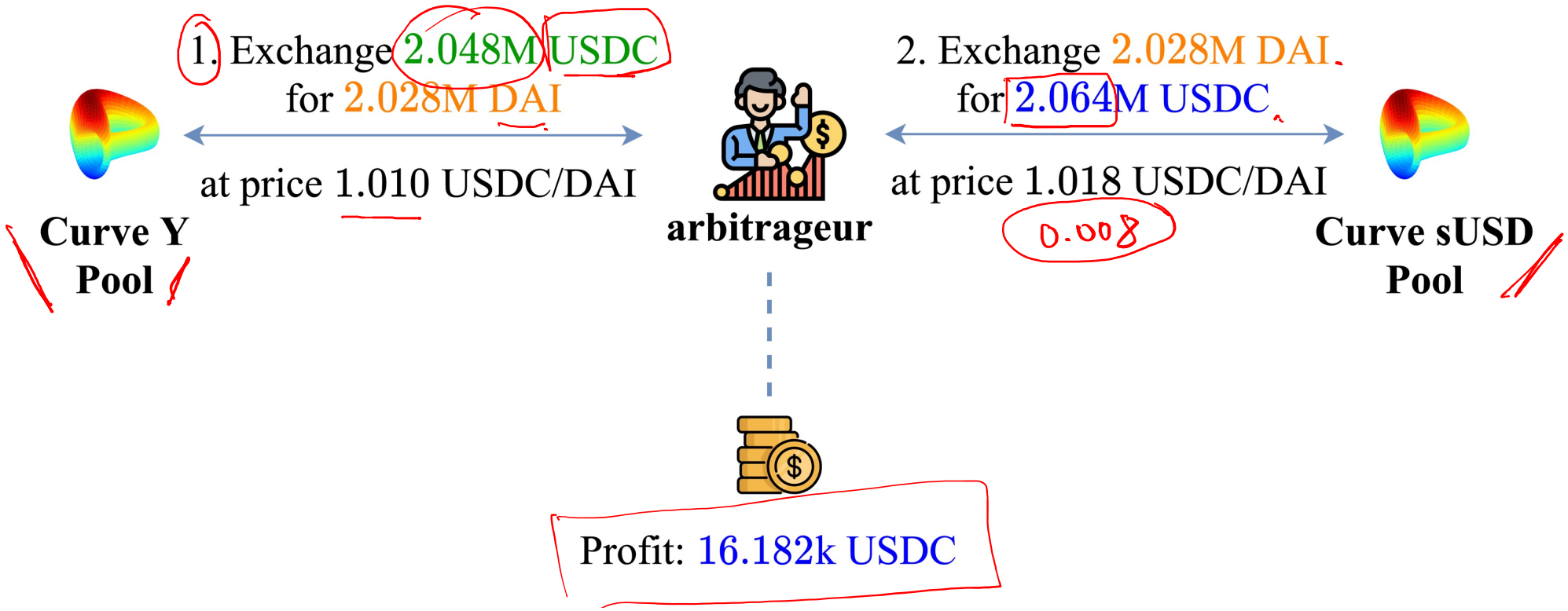
Arbitrage

- Multiple Markets with
  - the same assets X and Y
  - different prices for X and Y

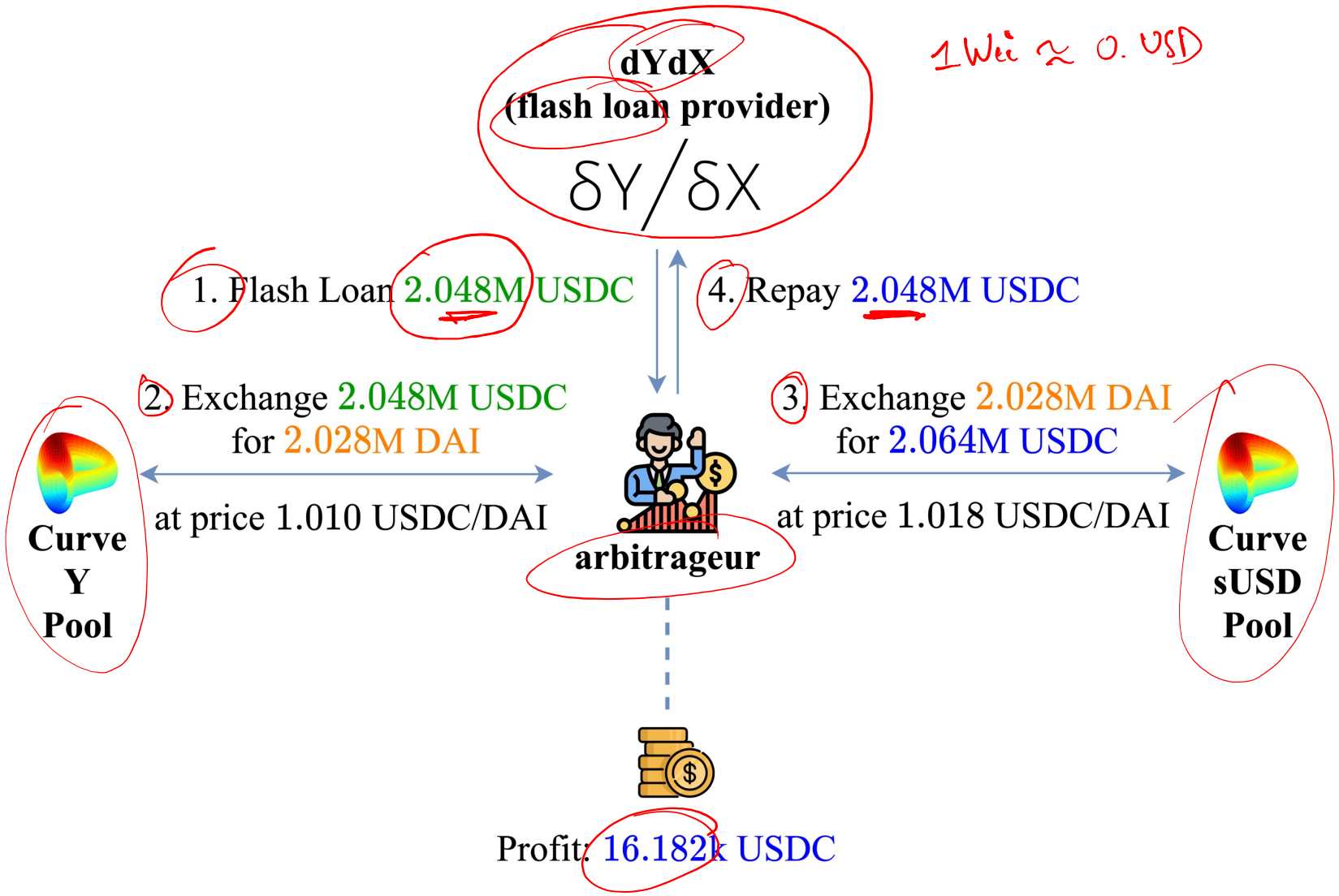


- Prices are synchronized by “arbitrageurs”
  - Profit from the price difference
    - Also referred to as “spread”
  - Requires to perform at least one transaction

Arbitrage on two markets



Arbitrage (with Flash Loan)



AMM Impermanent Loss

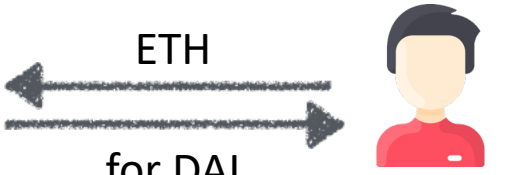
https://defi-learning.org

Impermanent Loss Example

2. Price increase of ETH
1 ETH == 400 DAI

1 ETH == 100 DAI

1. Add liquidity
1 ETH, 100 DAI
== 200 USD
== 10% of pool



ETH/DAI Pool

ETH

for DAI

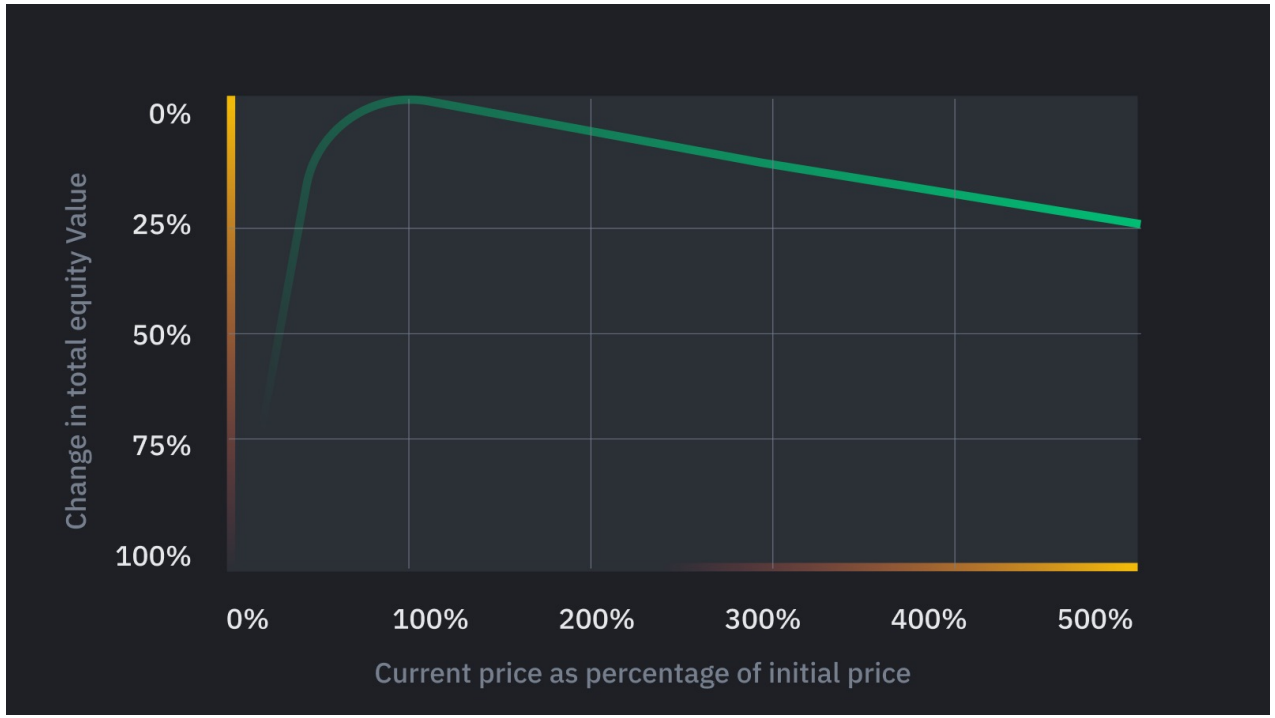
Arbitrage

Realisation of IL:
1 ETH + 1 USD == 500 USD
→ Alice lost 100 USD

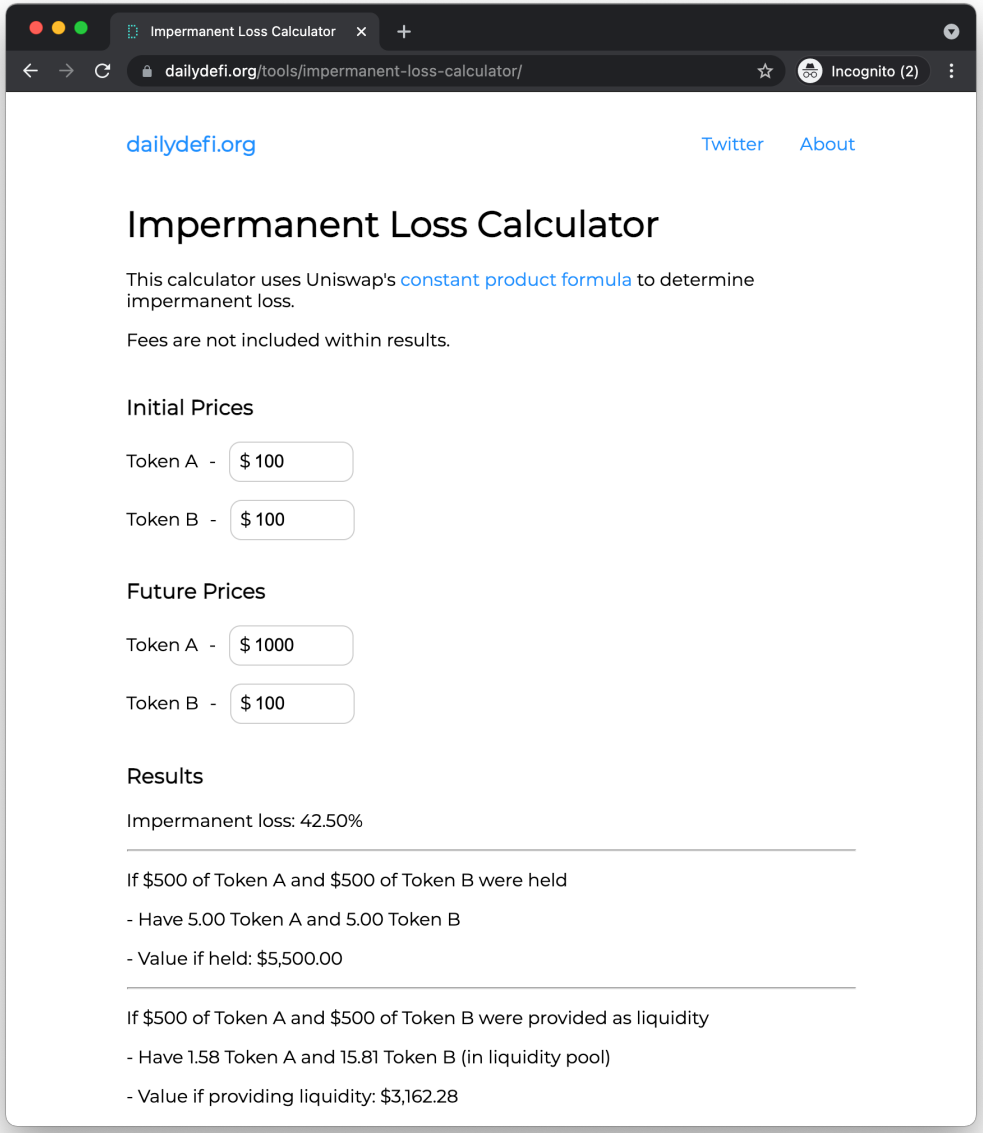
3. Withdraw liquidity
10%== 0.5 ETH, 200 DAI
== 400 USD

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




AMM Liquidity Mining
https://defi-learning.org

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
busdv2 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) Search

ALL | YIELD FARMING | LIQUIDITY PROVIDING

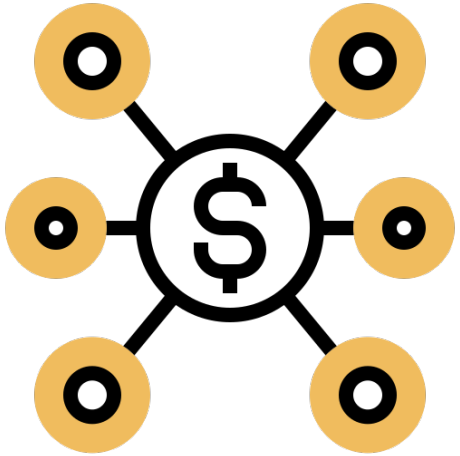
Yield Farming Uniswap DPI/ETH	33.26 % ~~12.89 %~~	Yield Farming Trading Fee Alpha APR Borrow APY	18.74 % 7.34 % 16.32 % -9.15 %	FARM
Yield Farming Sushiswap SUSHI/ETH	63.58 % ~~27.87 %~~	Yield Farming Trading Fee Alpha APR Borrow APY	38.67 % 17.74 % 16.32 % -9.15 %	FARM
Yield Farming Sushiswap DPI/ETH	35.51 % ~~14.00 %~~	Yield Farming Trading Fee Alpha APR Borrow APY	24.62 % 3.71 % 16.32 % -9.15 %	FARM
Yield Farming Sushiswap LINK/ETH	58.90 % ~~22.62 %~~	Yield Farming Trading Fee Alpha APR Borrow APY	34.06 % 16.26 % 19.52 % -10.94 %	FARM

DEX Aggregator

https://defi-learning.org

DEX Aggregator

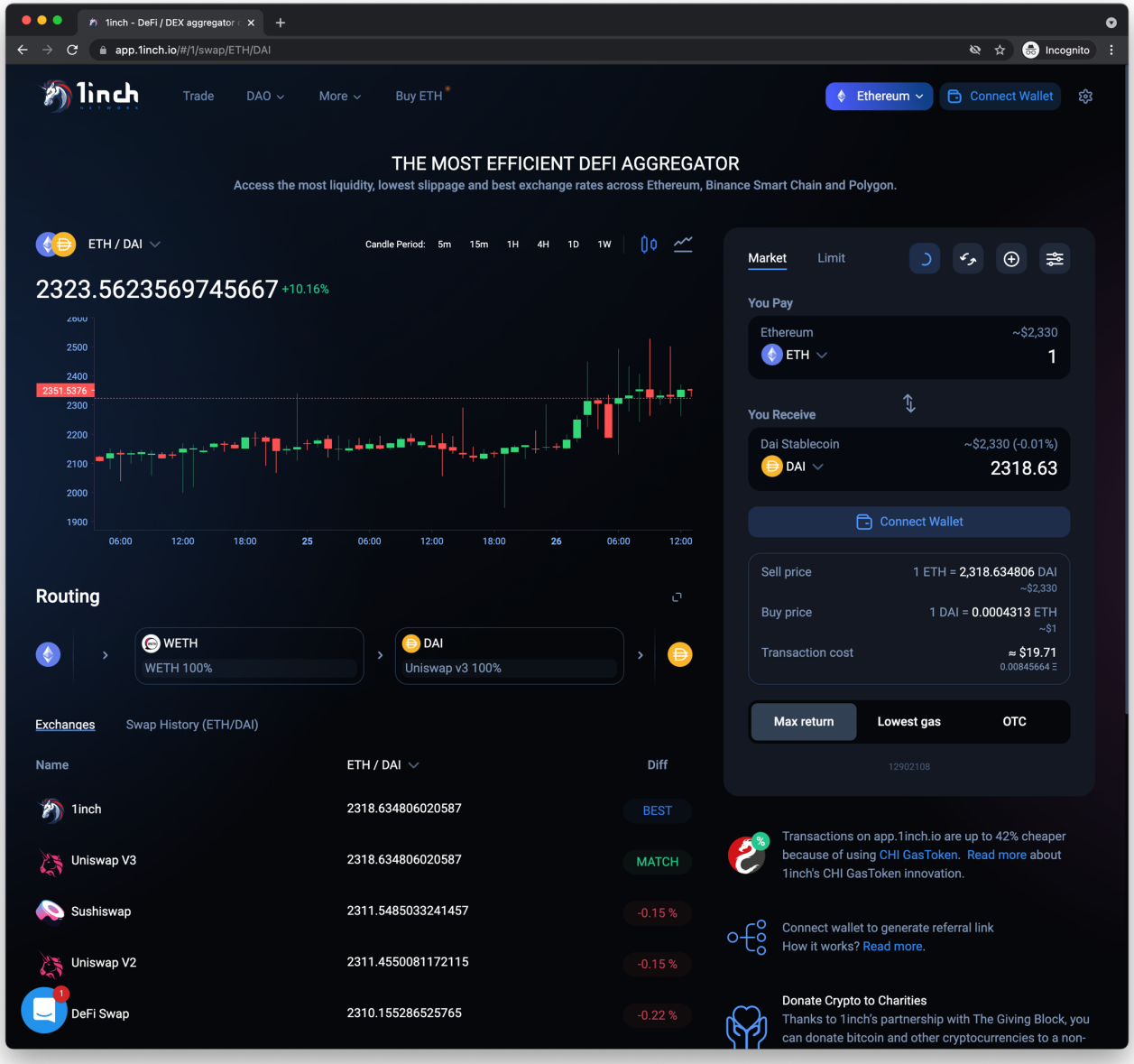
- Users may ask
  - Where do I get the best price for a trade?
  - Where is the deepest liquidity?



- 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

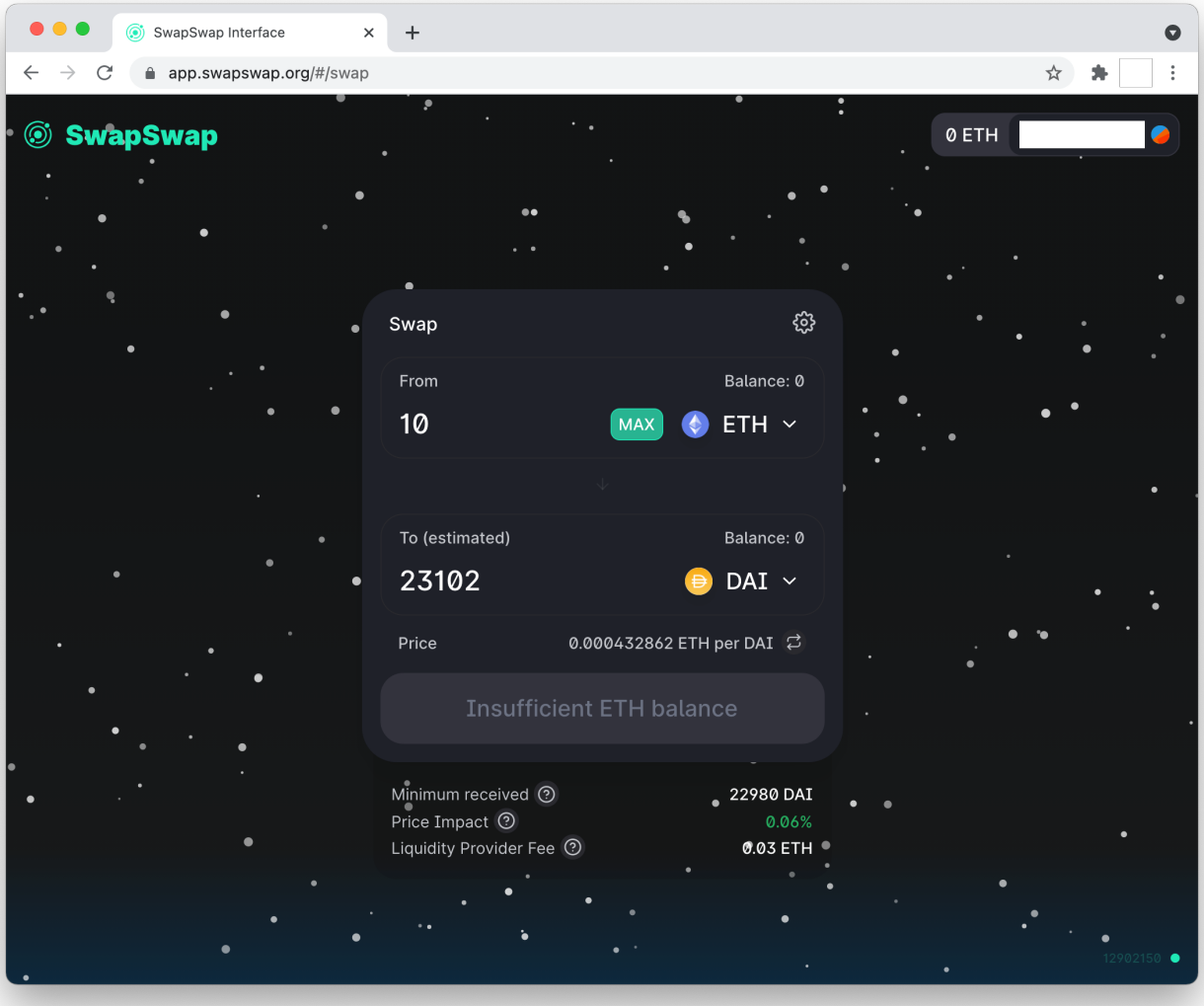
1inch

- 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?

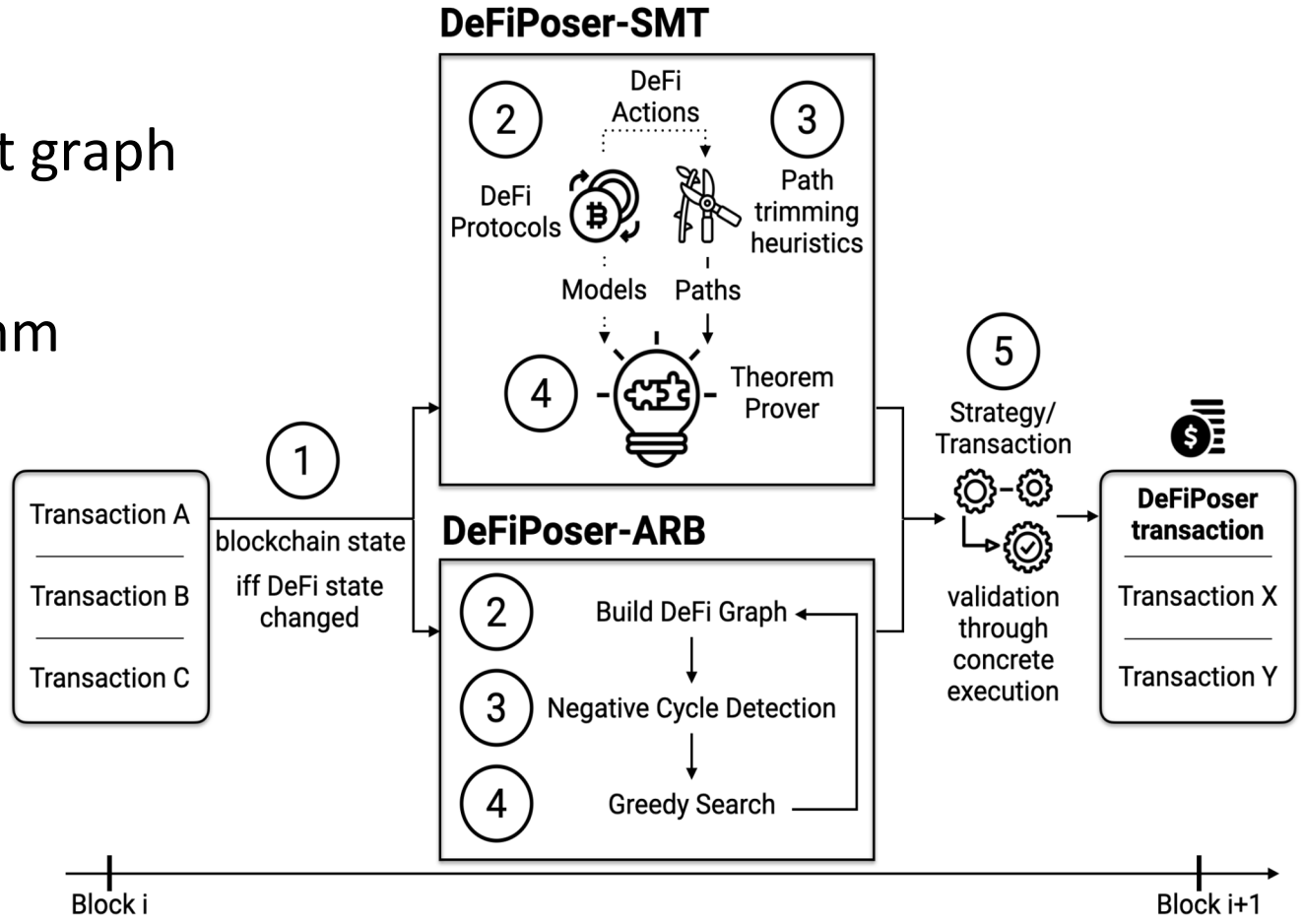
https://defi-learning.org

How to detect arbitrage/profitable opportunities?

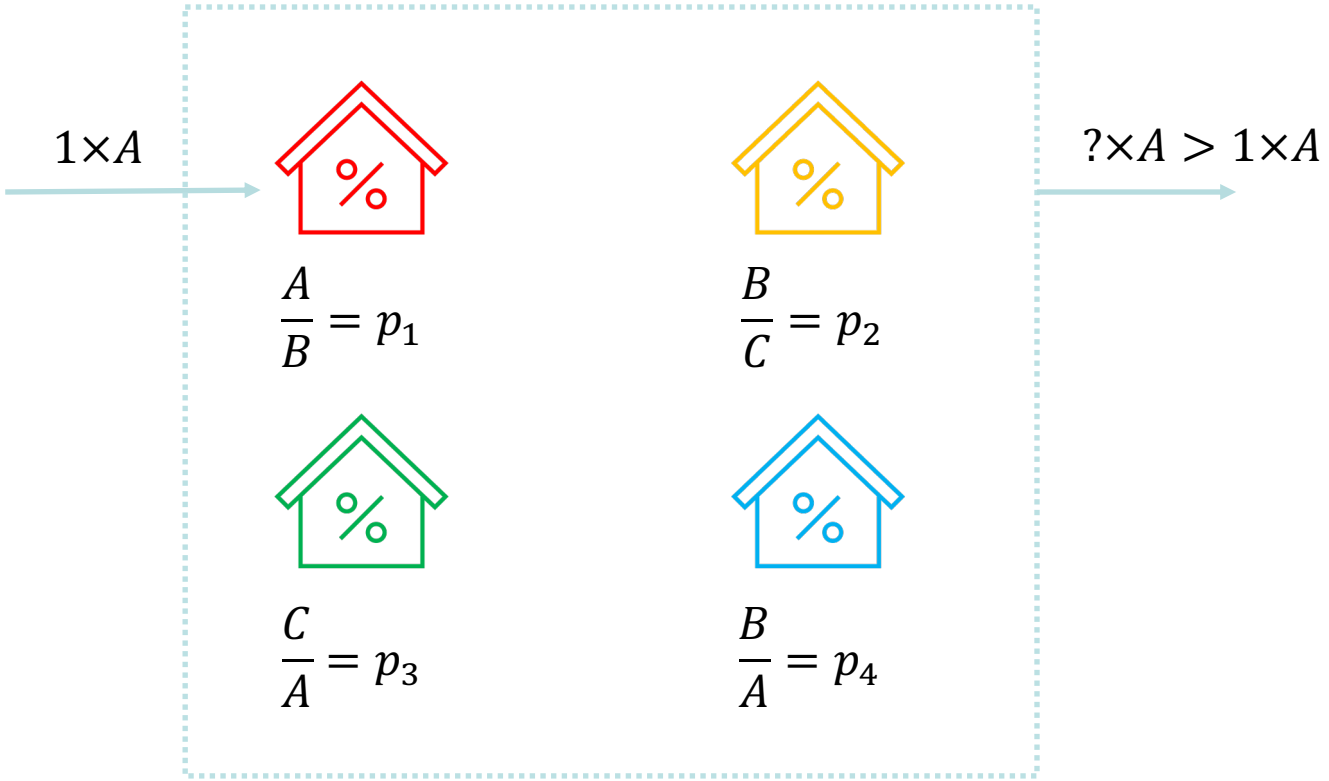
- Bellman Ford Algorithm
  - Negative cycle detection
  - Works among multiple markets
  - Used in traditional finance and DeFi
- Theorem Solver (SMT)
  - Needs to encode the DeFi model
  - Apply heuristics for path pruning

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

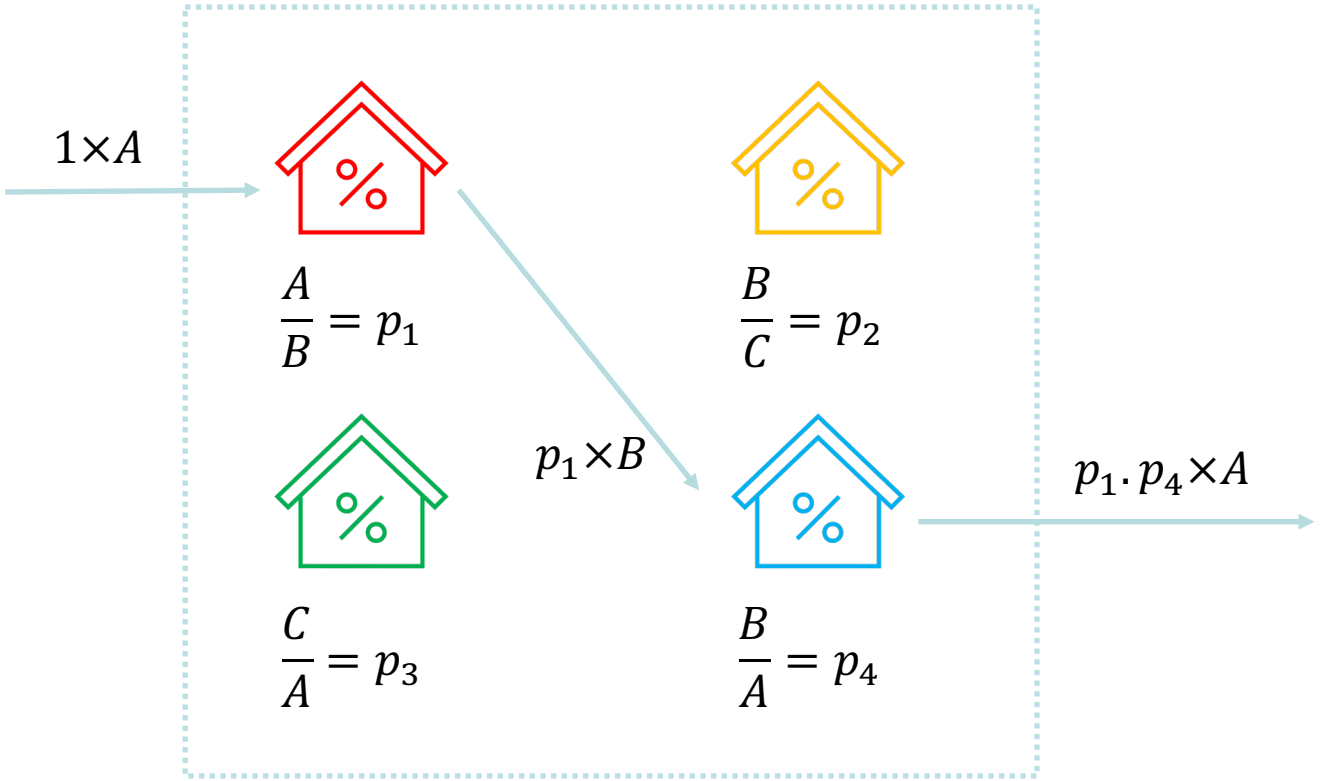
- DeFiPoser-ARB
  - builds a directed DeFi market graph
  - identifies negative cycles
  - Bellman Ford-Moore algorithm
- DeFiPoser-SMT
  - state transition model
  - prunes search space
  - theorem prover



DeFiPoser-ARB



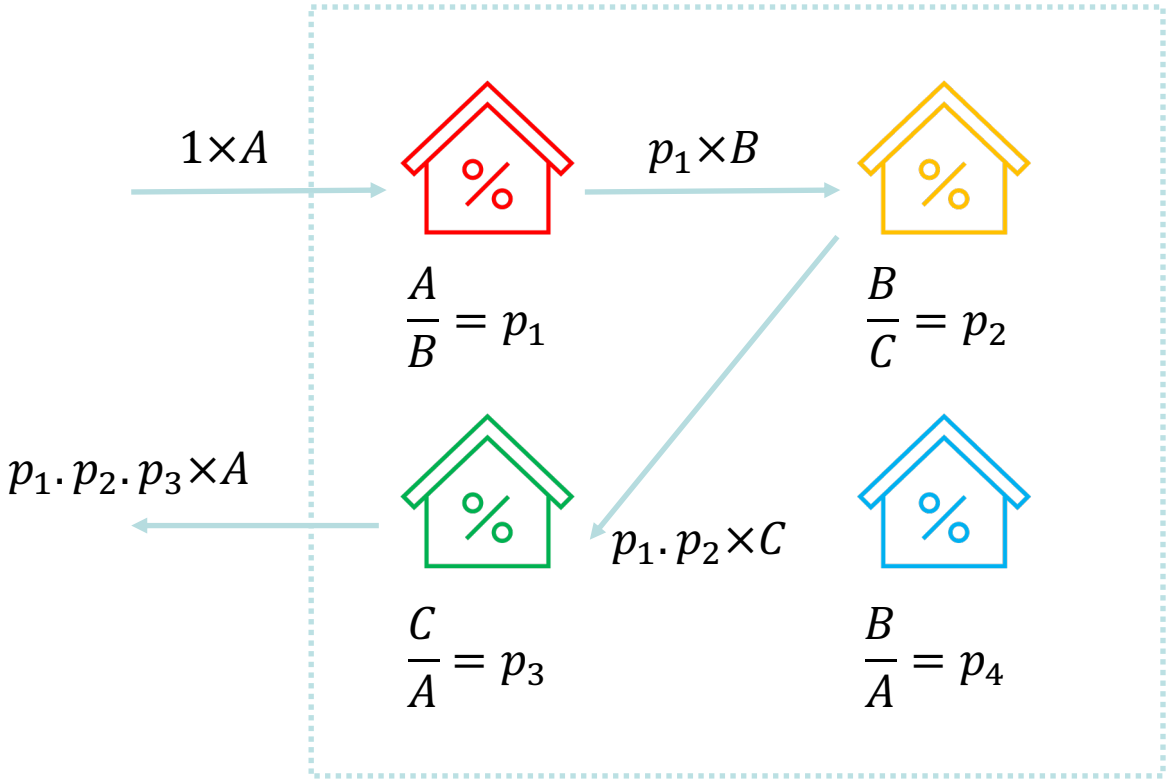
DeFiPoser-ARB



Profitable condition

$p_1 . p_4 > 1$

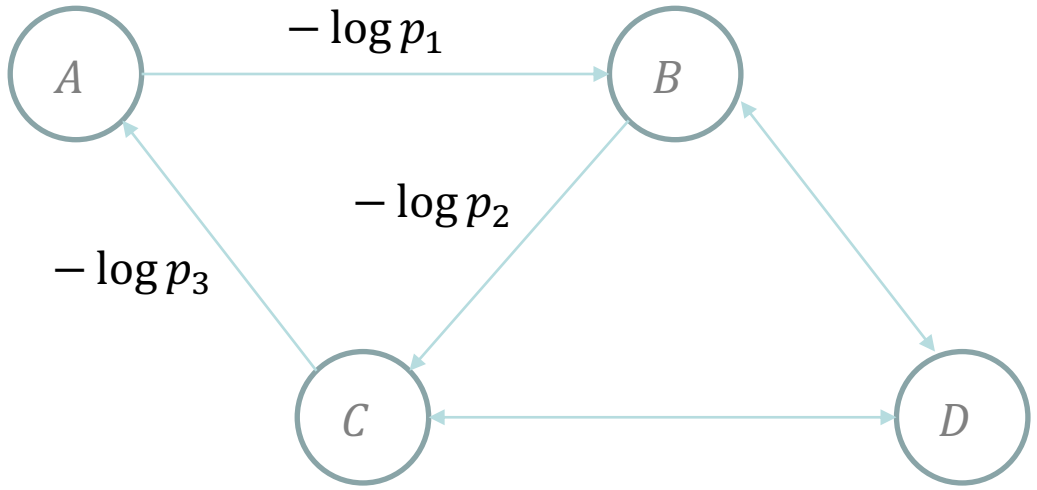
DeFiPoser-ARB



Profitable condition

$p_1 . p_2 . p_3 > 1$

DeFiPoser-ARB



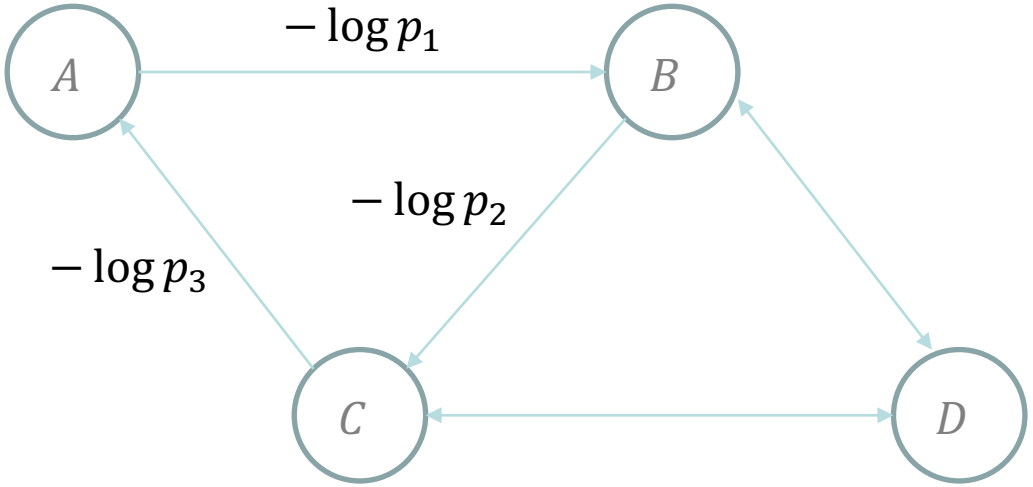
Profitable condition

$p_1 . p_2 . p_3 > 1$

$\Updownarrow$

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

DeFiPoser-ARB



$$\prod_i p_i > 1$$

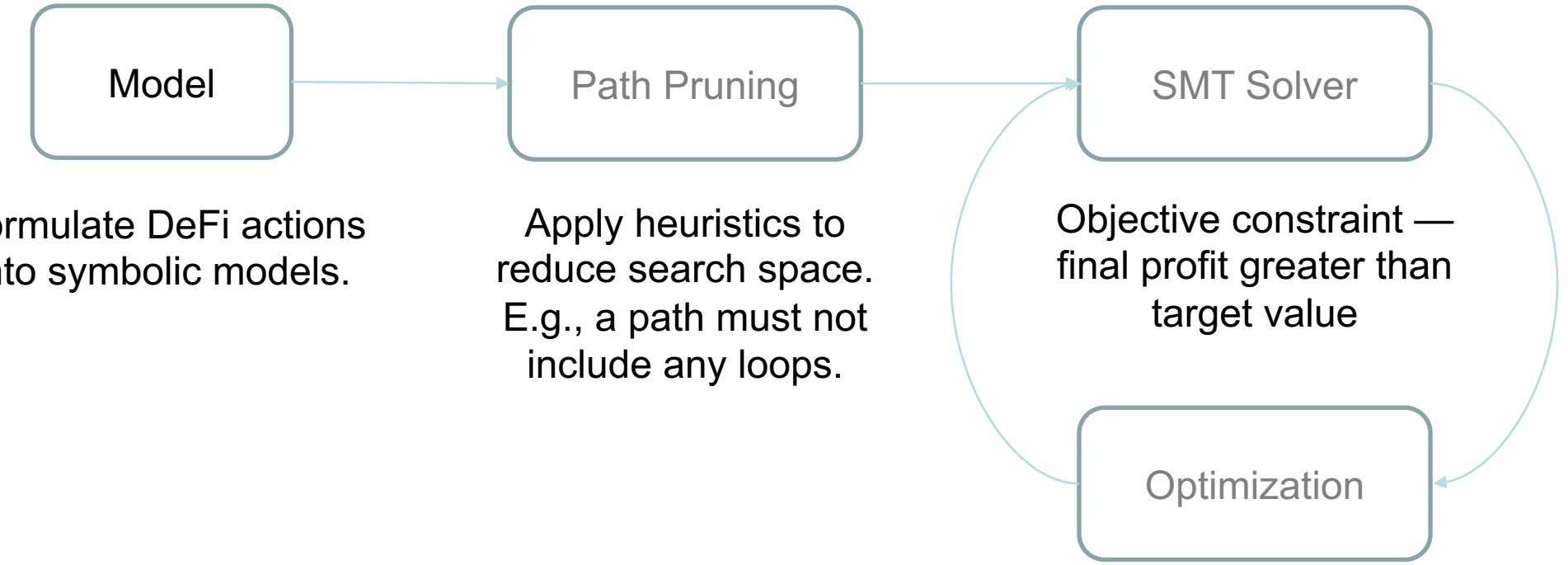
$$\Updownarrow$$

$$\sum_i (-\log p_i) < 0$$

BellmanFord-Moore algorithm

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

DeFiPoser-SMT



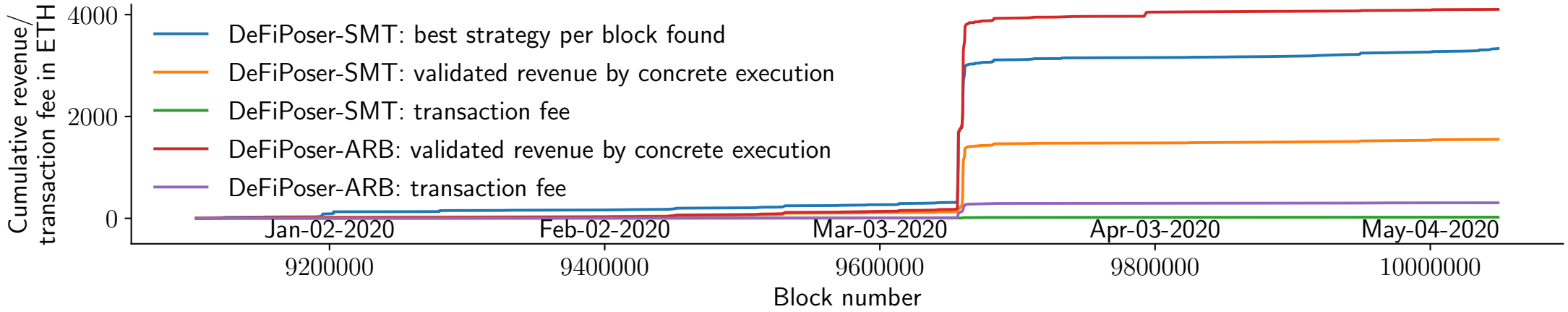
Formulate DeFi actions into symbolic models.

Apply heuristics to reduce search space. E.g., a path must not include any loops.

Objective constraint — final profit greater than target value

Apply a binary search to find the optimal value.

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