Decentralized Exchanges (DEX) II

Instructor: Paruj Ratanaworabhan

Source: “Decentralized Exchanges (DEX)” by A. Gervais, UCB DeFi course

AMM in Actions: Moving Within and Between Curves

$$\mathsf{A}[70:\tau_0, 80:\tau_1] \mid \mathsf{B}[30:\tau_0]$$

$$\xrightarrow{\mathsf{A}:\mathsf{xfer}(\mathsf{B},10:\tau_1)} \mathsf{A}[70:\tau_0, 70:\tau_1] \mid \mathsf{B}[30:\tau_0, 10:\tau_1] \tag{1}$$

$$\xrightarrow{\mathsf{A}:\mathsf{dep}(70:\tau_0,70:\tau_1)} \mathsf{A}[70:(\tau_0,\tau_1)] \mid \mathsf{B}[\cdots] \mid (70:\tau_0, 70:\tau_1) \tag{2}$$

$$\xrightarrow{\mathsf{B}:\mathsf{swapL}(30:\tau_0,20:\tau_1)} \mathsf{A}[\cdots] \mid \mathsf{B}[0:\tau_0, 31:\tau_1] \mid (100:\tau_0, 49:\tau_1) \tag{3}$$

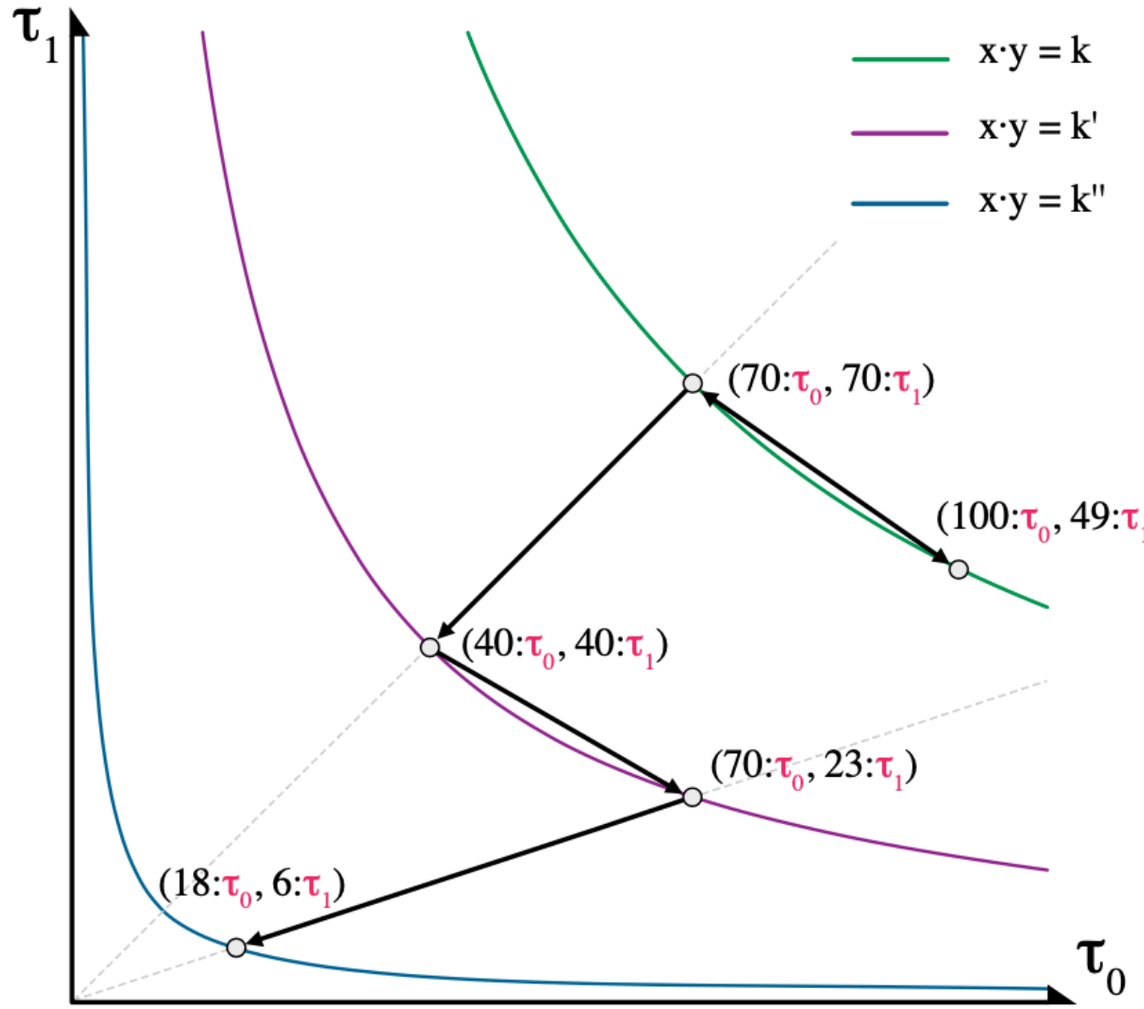
$$\xrightarrow{\mathsf{B}:\mathsf{swapR}(29:\tau_0,21:\tau_1)} \mathsf{A}[\cdots] \mid \mathsf{B}[30:\tau_0, 10:\tau_1] \mid (70:\tau_0, 70:\tau_1) \tag{4}$$

$$\xrightarrow{\mathsf{B}:\mathsf{rdm}(30:(\tau_0,\tau_1))} \mathsf{A}[30:\tau_0, 30:\tau_1, 40:(\tau_0,\tau_1)] \mid \mathsf{B}[\cdots] \mid (40:\tau_0, 40:\tau_1) \tag{5}$$

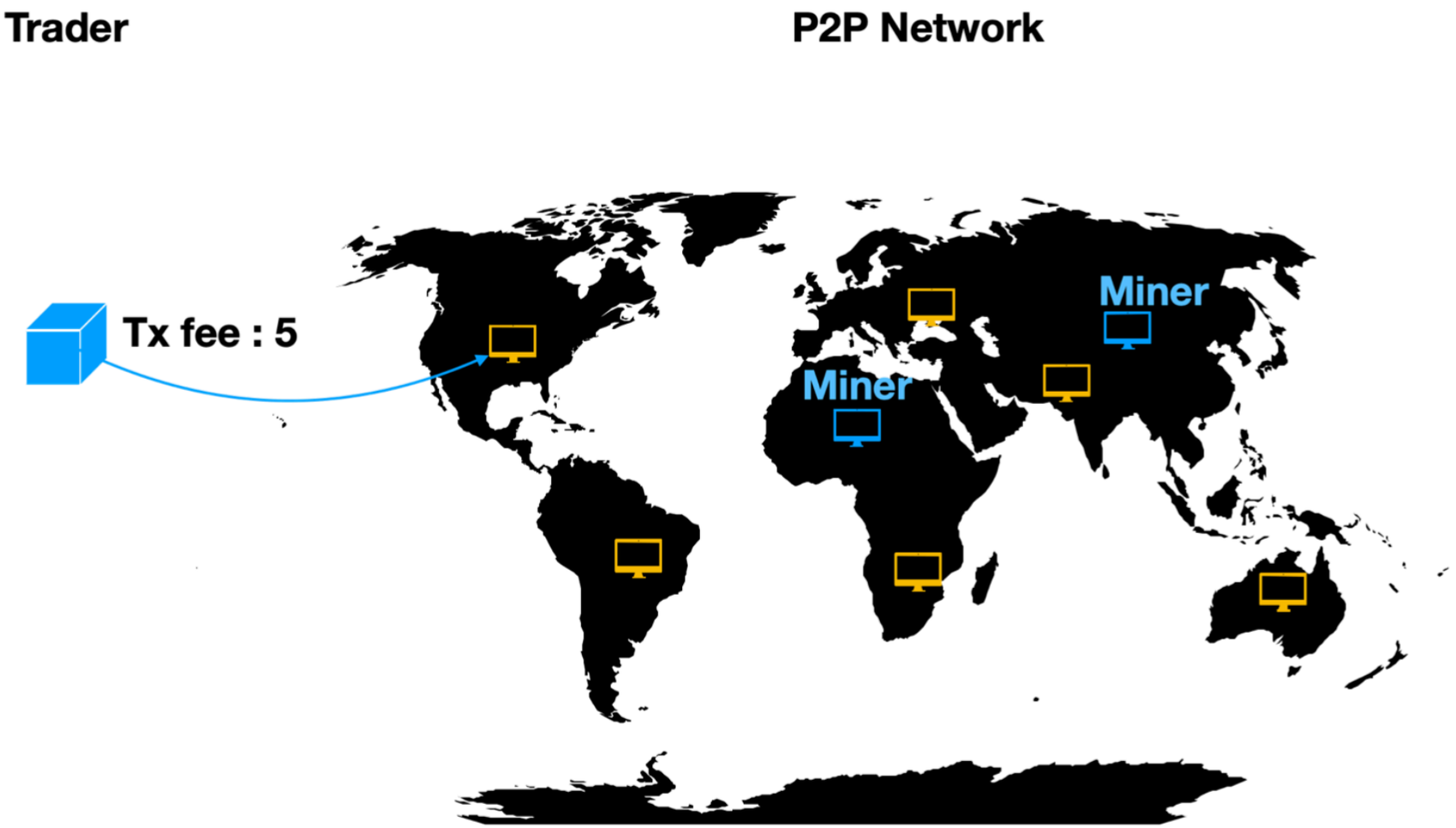
$$\xrightarrow{\mathsf{B}:\mathsf{swapL}(30:\tau_0,16:\tau_1)} \mathsf{A}[\cdots] \mid \mathsf{B}[0:\tau_0, 27:\tau_1] \mid (70:\tau_0, 23:\tau_1) \tag{6}$$

$$\xrightarrow{\mathsf{A}:\mathsf{rdm}(30:(\tau_0,\tau_1))} \mathsf{A}[82:\tau_0, 47:\tau_1, 10:(\tau_0,\tau_1)] \mid \mathsf{B}[\cdots] \mid (18:\tau_0, 6:\tau_1) \tag{7}$$

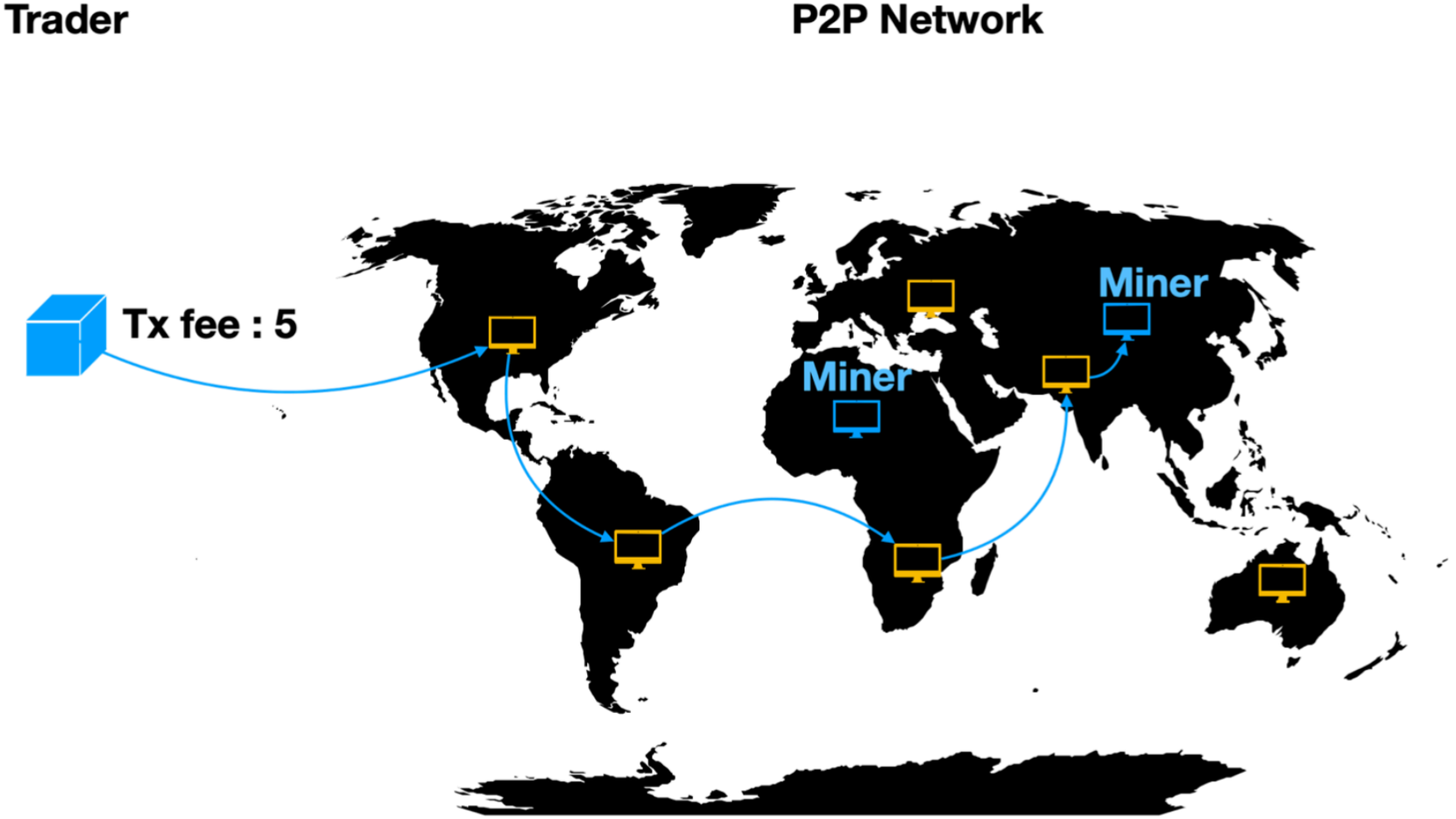
Fig. 1: Interactions between two users and an AMM.



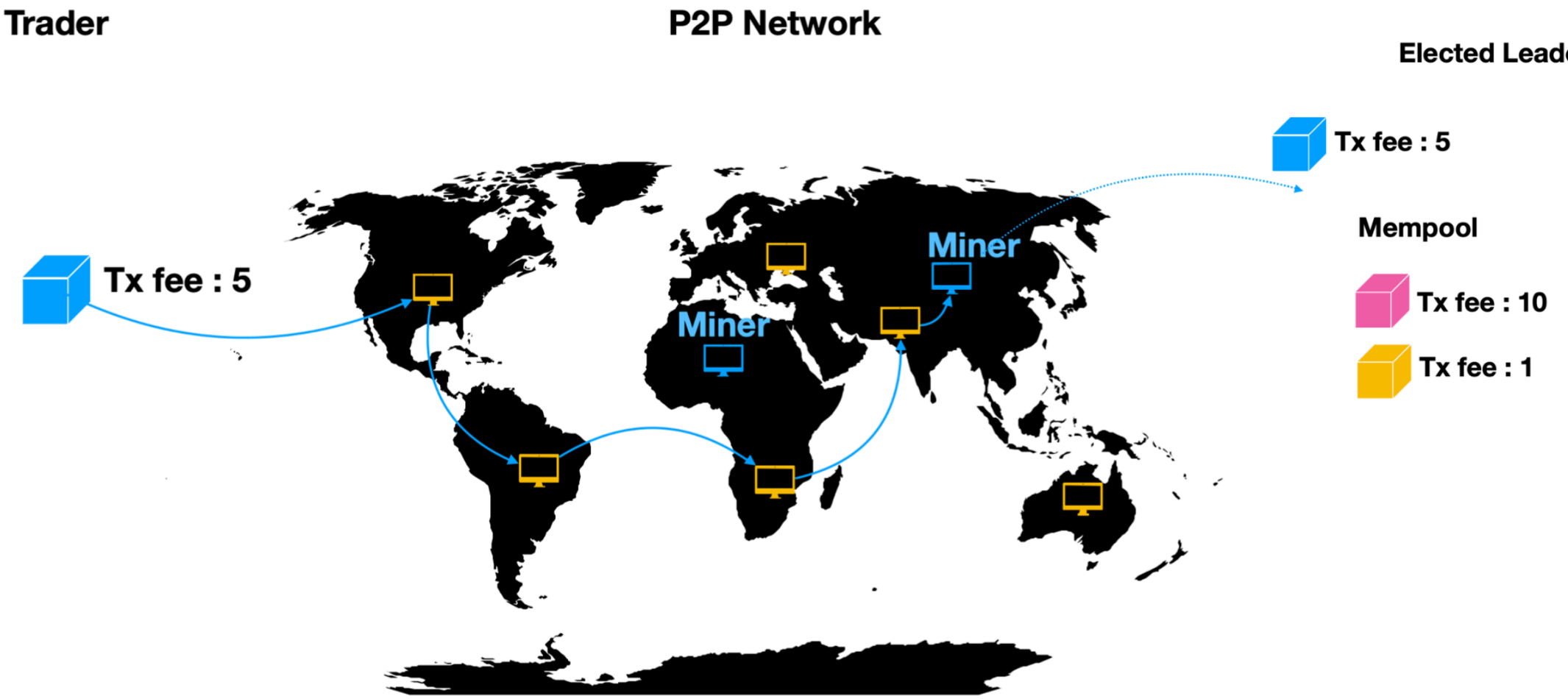
Exchange Transaction Propagation



Exchange Transaction Propagation

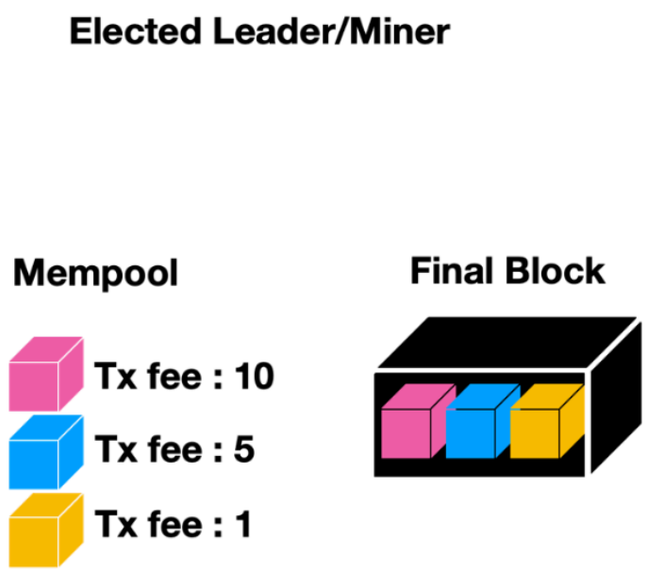


Exchange Transaction Propagation



Exchange Transaction Propagation

- Asynchronous Blockchain P2P Network
  - Best effort propagation
  - Transparency
  - High-Frequency Trading
- Inclusion based on a fee auction
  - Price Gas Auction (PGA)
    - On the public P2P network



Pegged/Stablecoin Swap


USDC


USDT


DAI


WBTC


renBTC


sETH

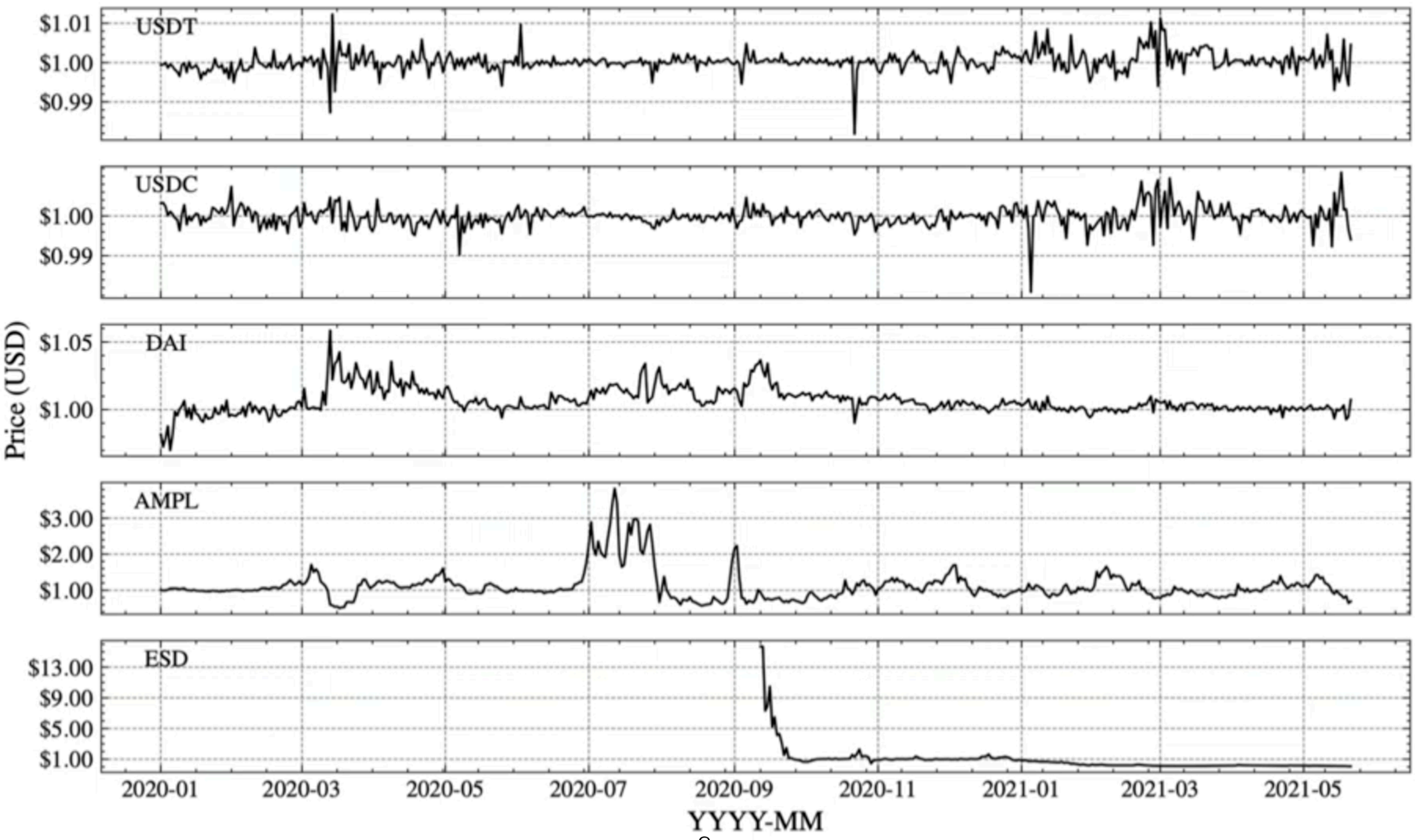

stETH

USD derivatives

Pegged coins

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

Pegged/Stablecoin Swap



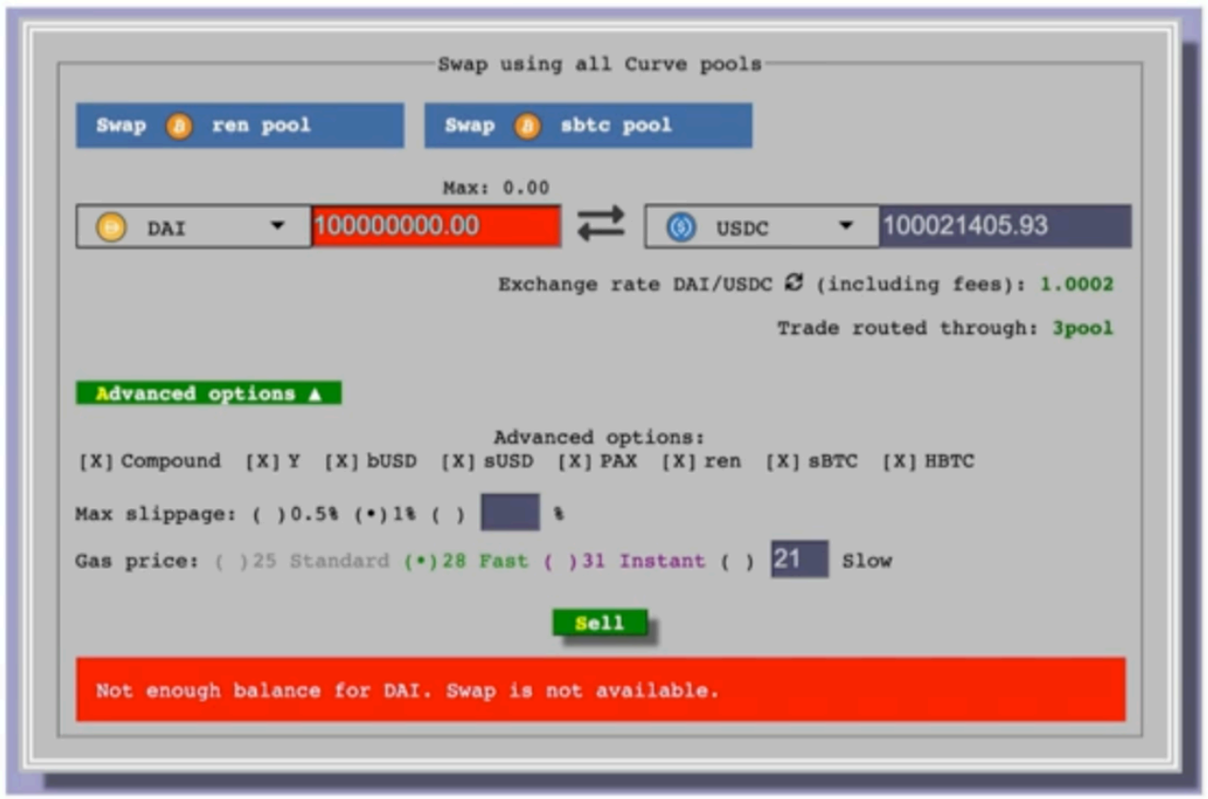
Pegged/Stablecoins

- 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

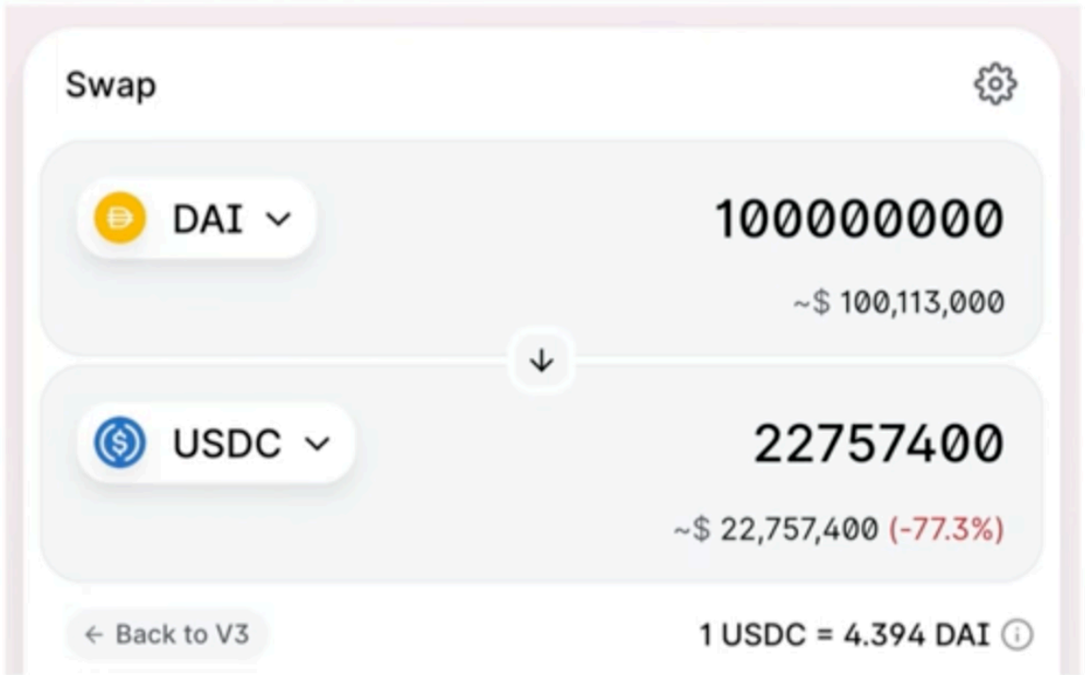
- Stablecoin AMM pros/cons:
  - (+) Better prices for bigger volumes (i.e. more liquidity)
  - (-) Potentially higher gas costs
  - (-) Danger of a de-peg of a stablecoin

Pegged/Stablecoin Swap

Curve



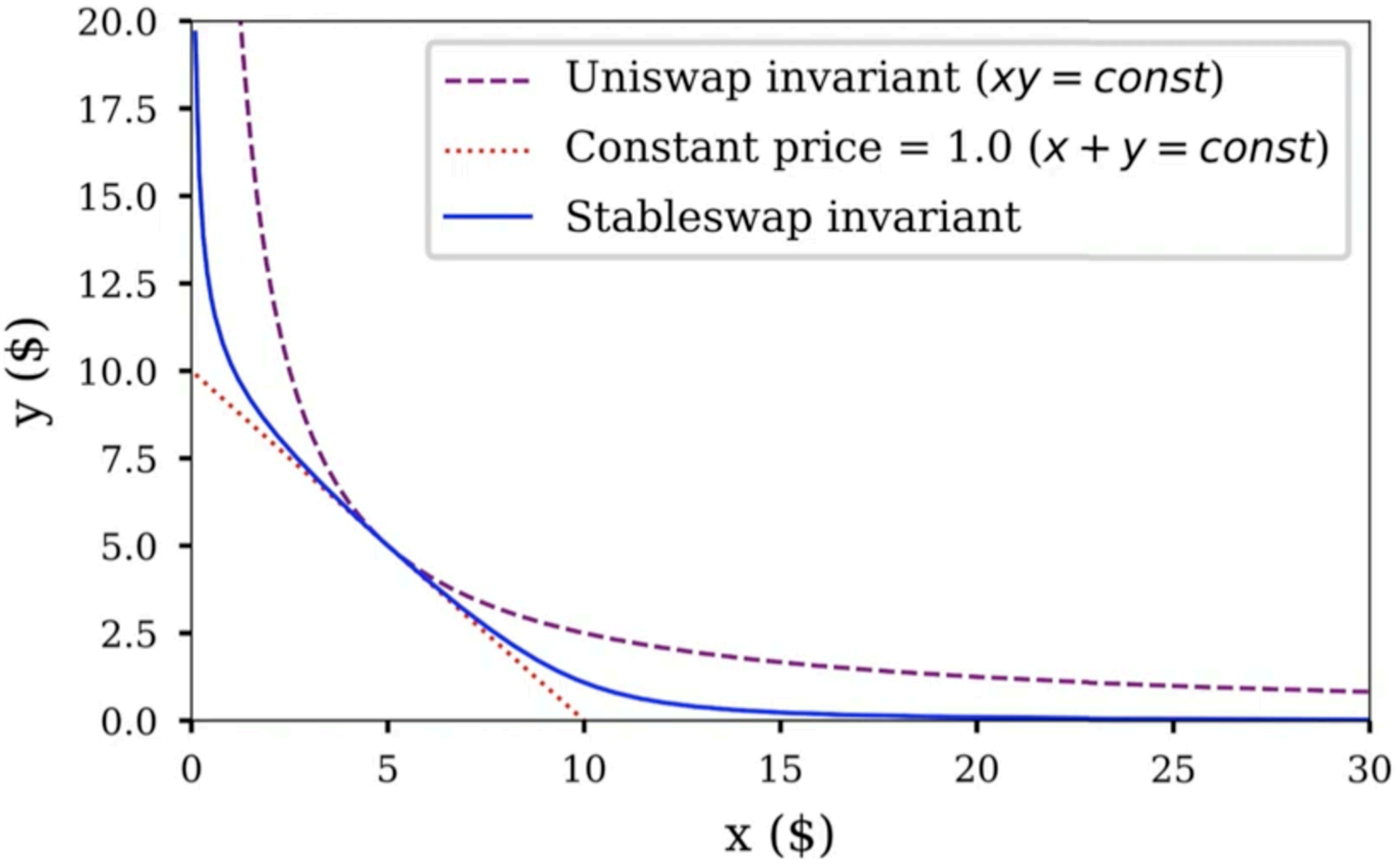
Uniswap



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

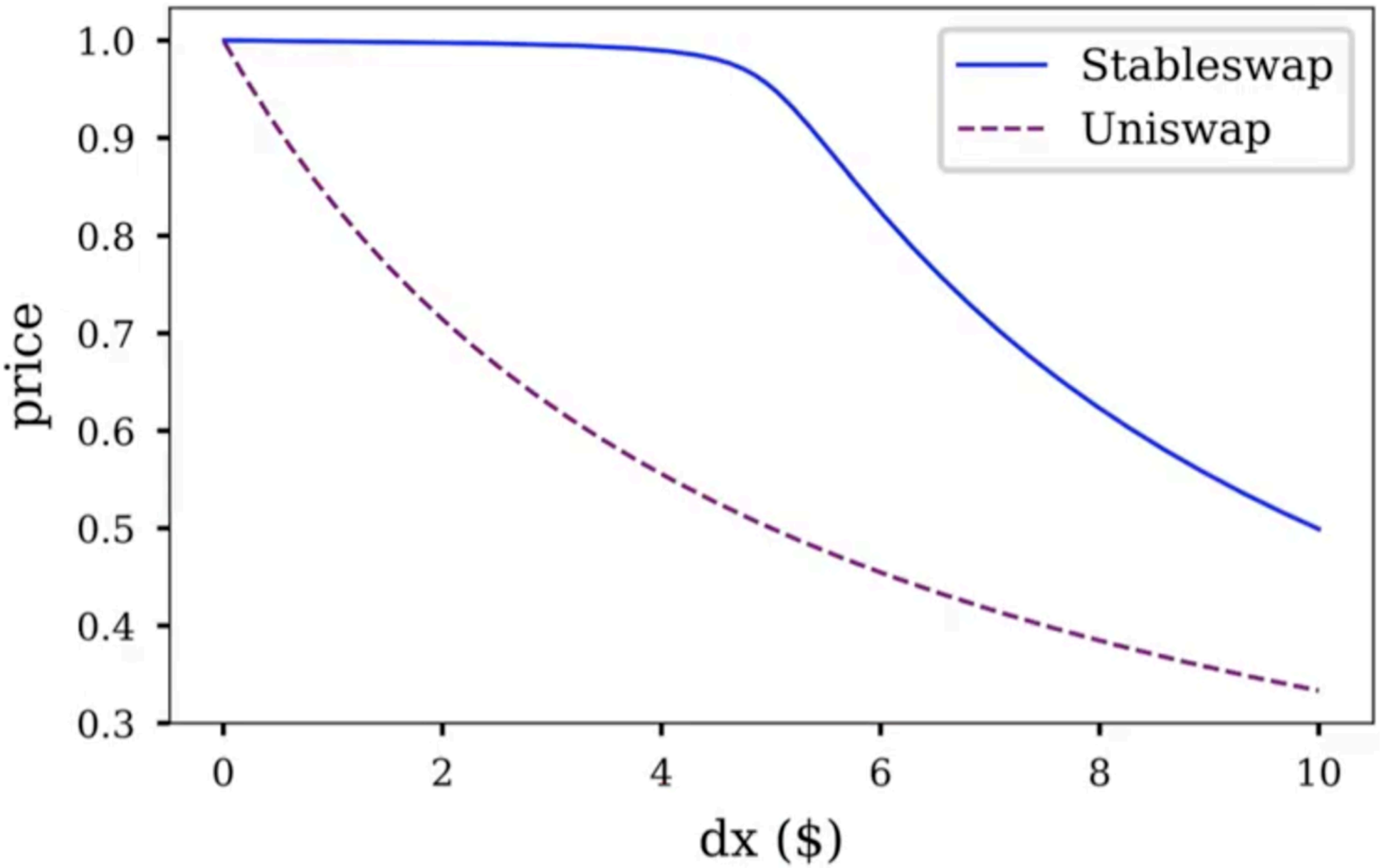
Price Curve

Stableswap (aka Curve Finance)



Slippage Comparison

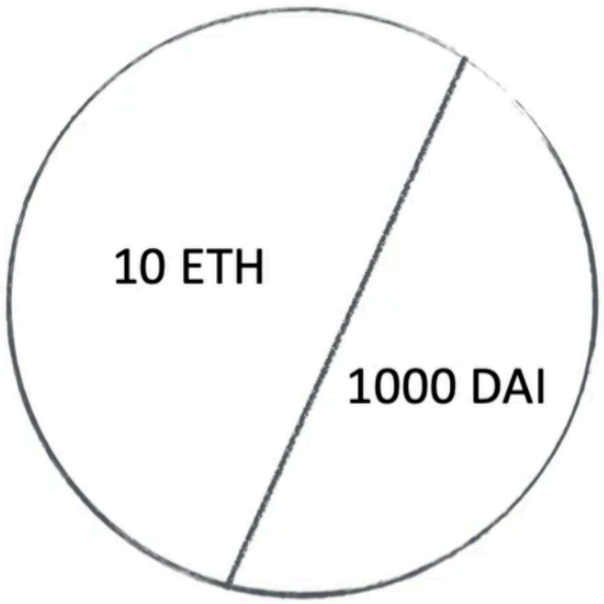
Stableswap (aka Curve Finance)



Impermanent Loss Example

1 ETH == 100 DAI

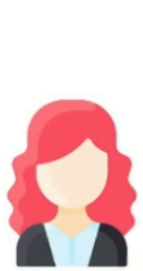
1. Add liquidity
1 ETH, 100 DAI
== 200 USD
== 10% of pool



ETH/DAI Pool

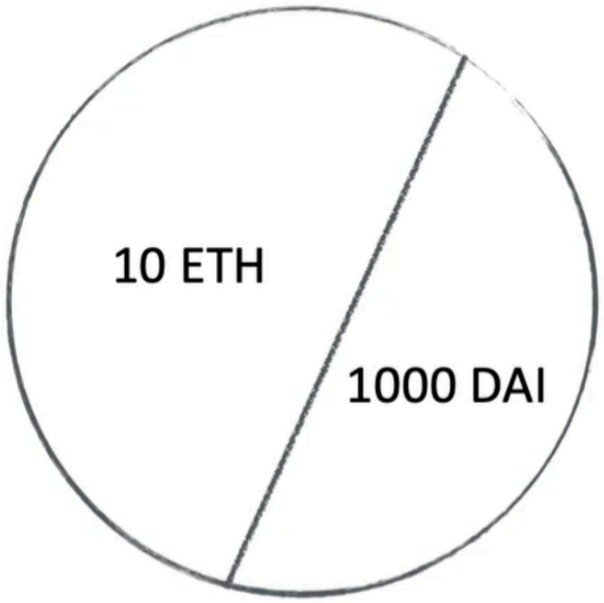
Impermanent Loss Example

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



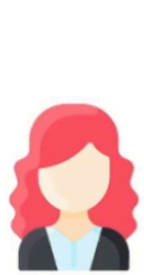
1 ETH == 100 DAI

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



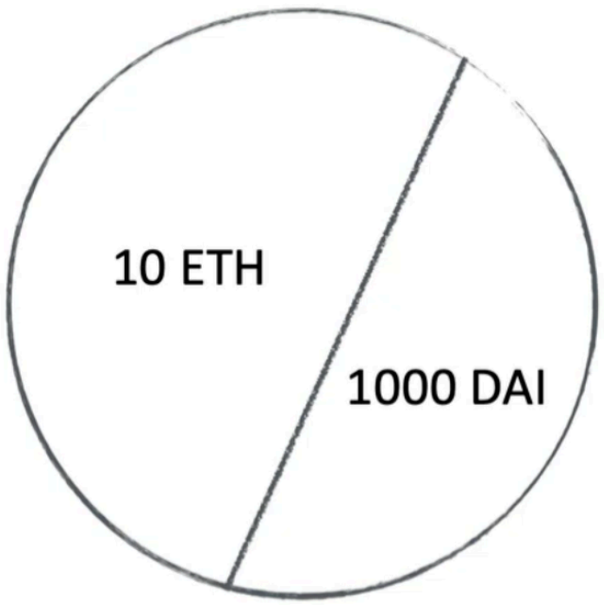
ETH/DAI Pool

Impermanent Loss Example



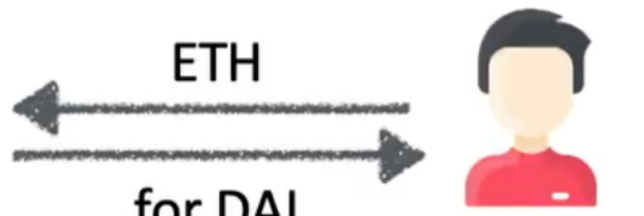
1 ETH == 100 DAI

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



ETH/DAI Pool

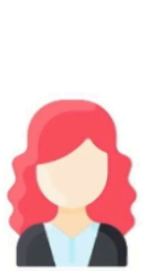
2. Price increase of ETH
1 ETH == 400 DAI



Arbitrage

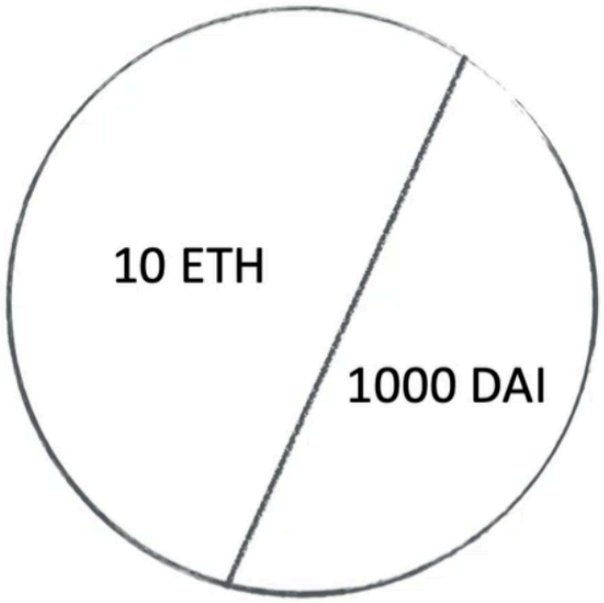
Impermanent Loss Example

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

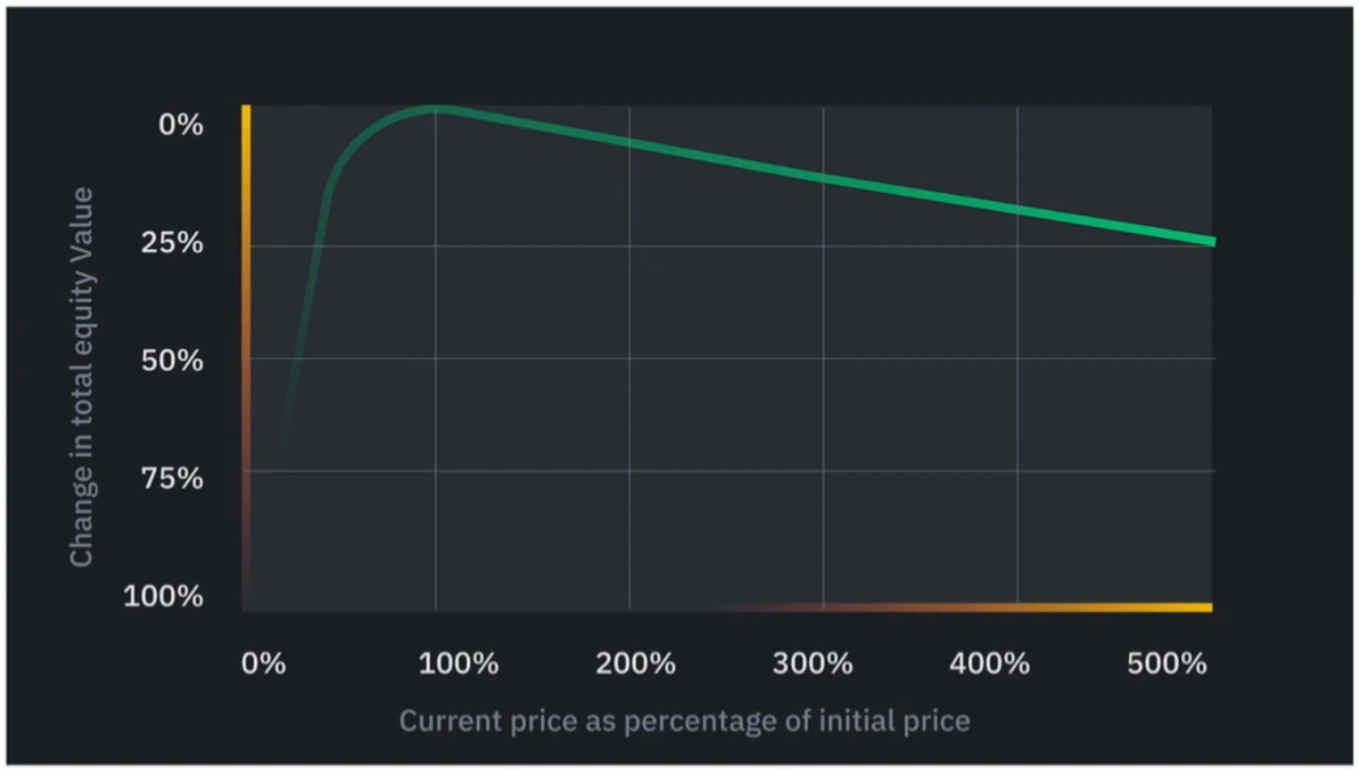
3. Withdraw liquidity
10%== 0.5 ETH, 200 DAI
== 400 USD

Realising Impermanent Loss

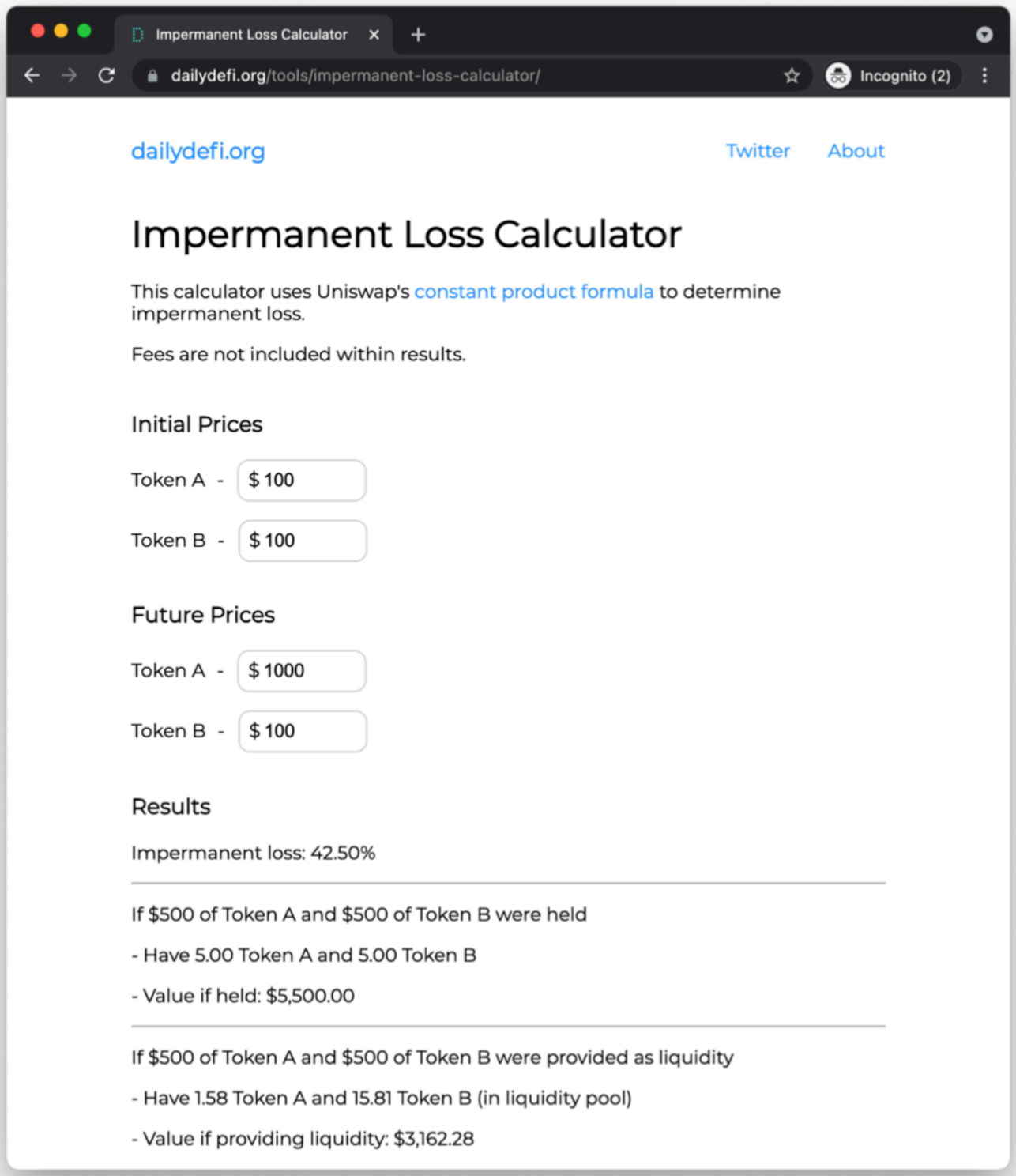
- DAI is a stable coin whose value is stable at 1 USD (provided that it does not loose the peg)
- If did not participate in the pool:
  - Total asset = 1 ETH + 100 DAI = 500 USD
- Total asset left from participating in the pool after withdrawal
  - Total asset = 0.5 ETH + 200 DAI = 400 USD
- Better to not participating in the pool in the first place; lost 100 USD in the process

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



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

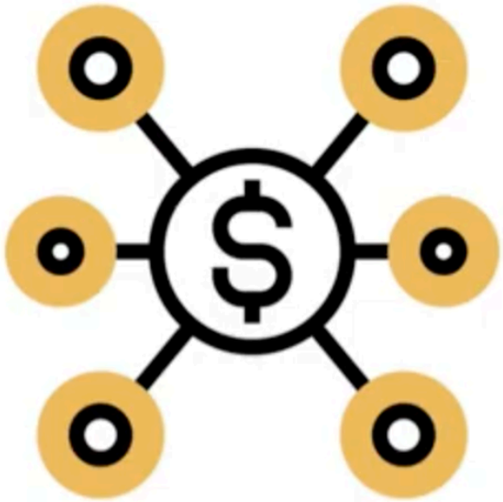
Farm Pools (18 Pools) — Search

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

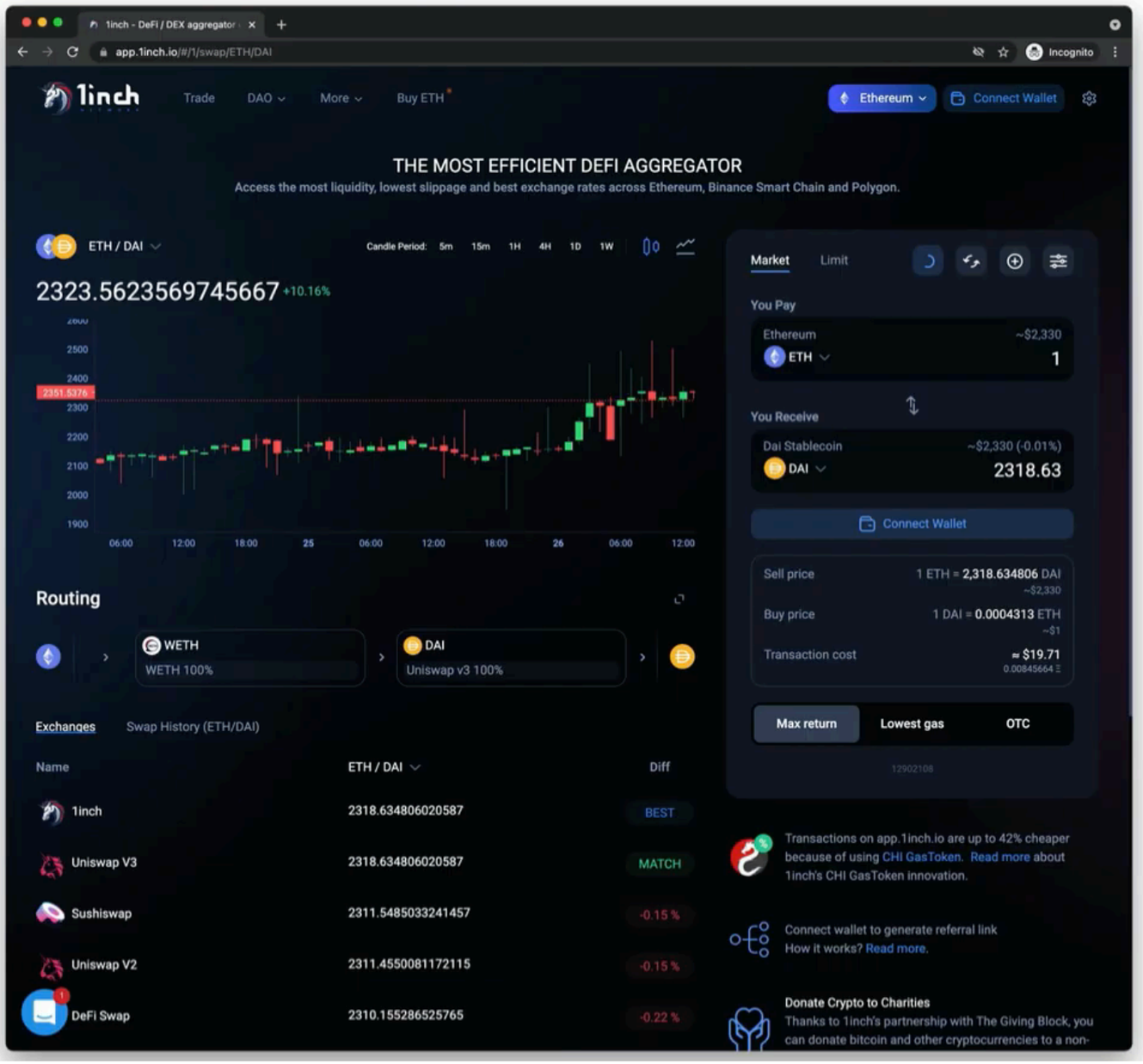
- Users may ask
  - Where do I get the best price for a trade?
  - Where is the deepest liquidity?



- 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

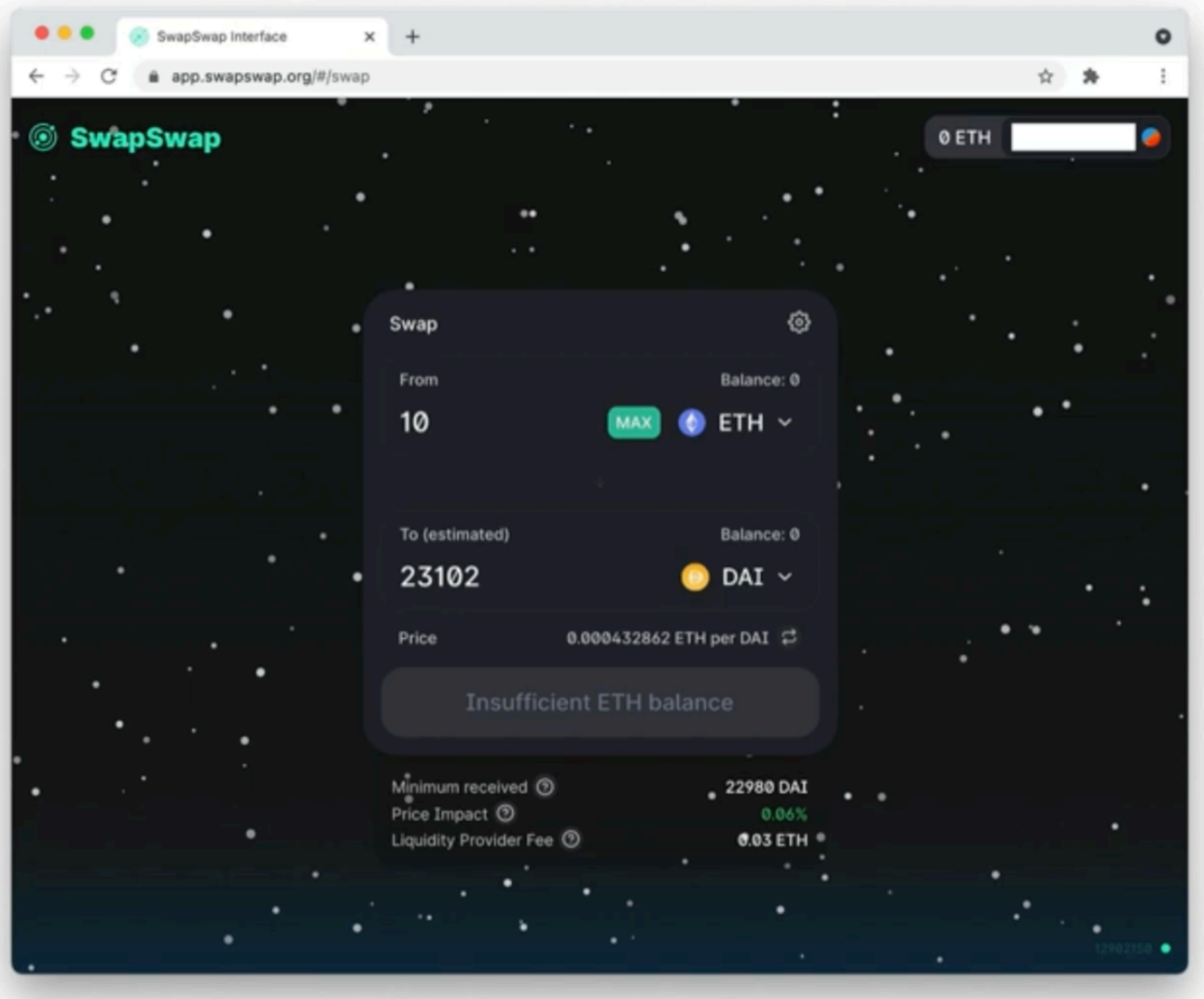
1inch

- 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



Arbitrage

BTC/USD

1 BTC : 40000 USD

BTC/USD

1 BTC : 35000 USD

BTC/USD

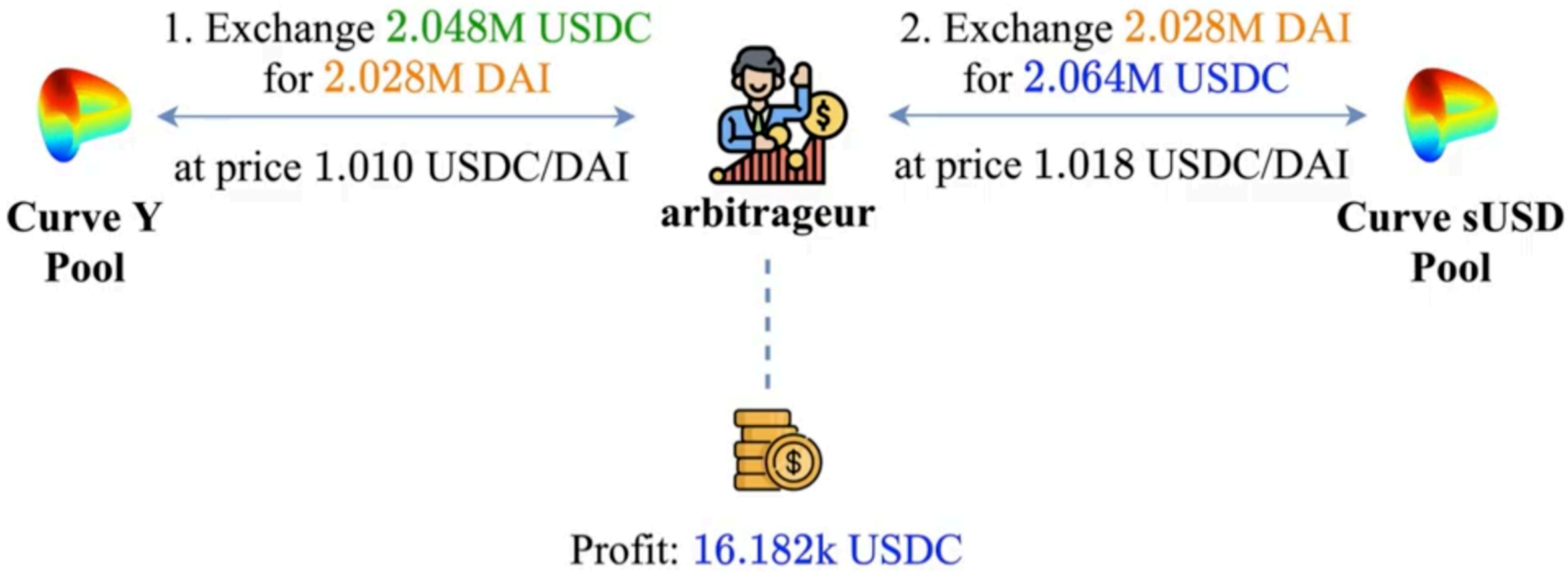
1 BTC : 30000 USD

Arbitrage

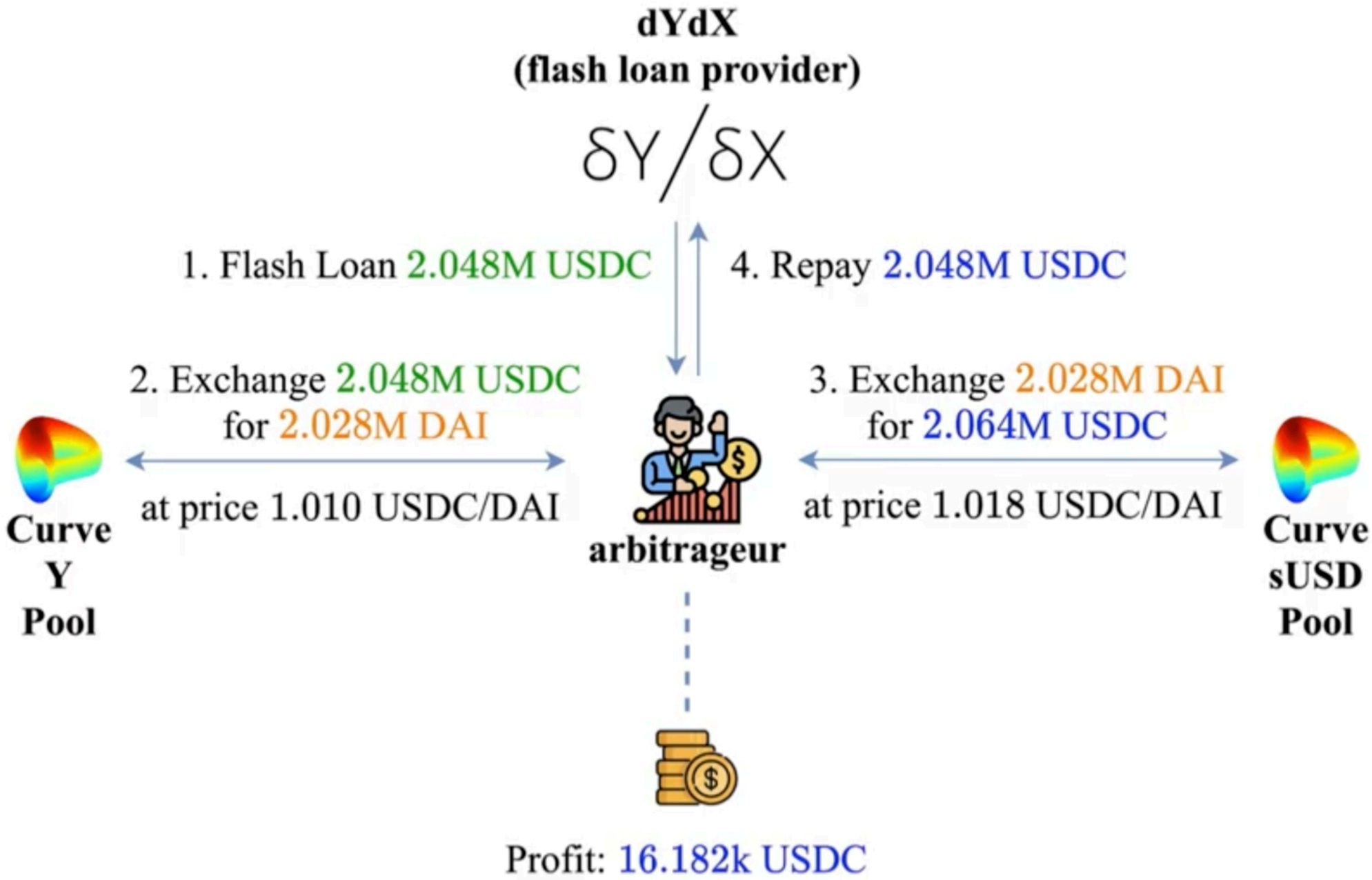
- Multiple Markets with
  - the same assets X and Y
  - different prices for X and Y

- 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)



How to detect arbitrage/profitable opportunities?

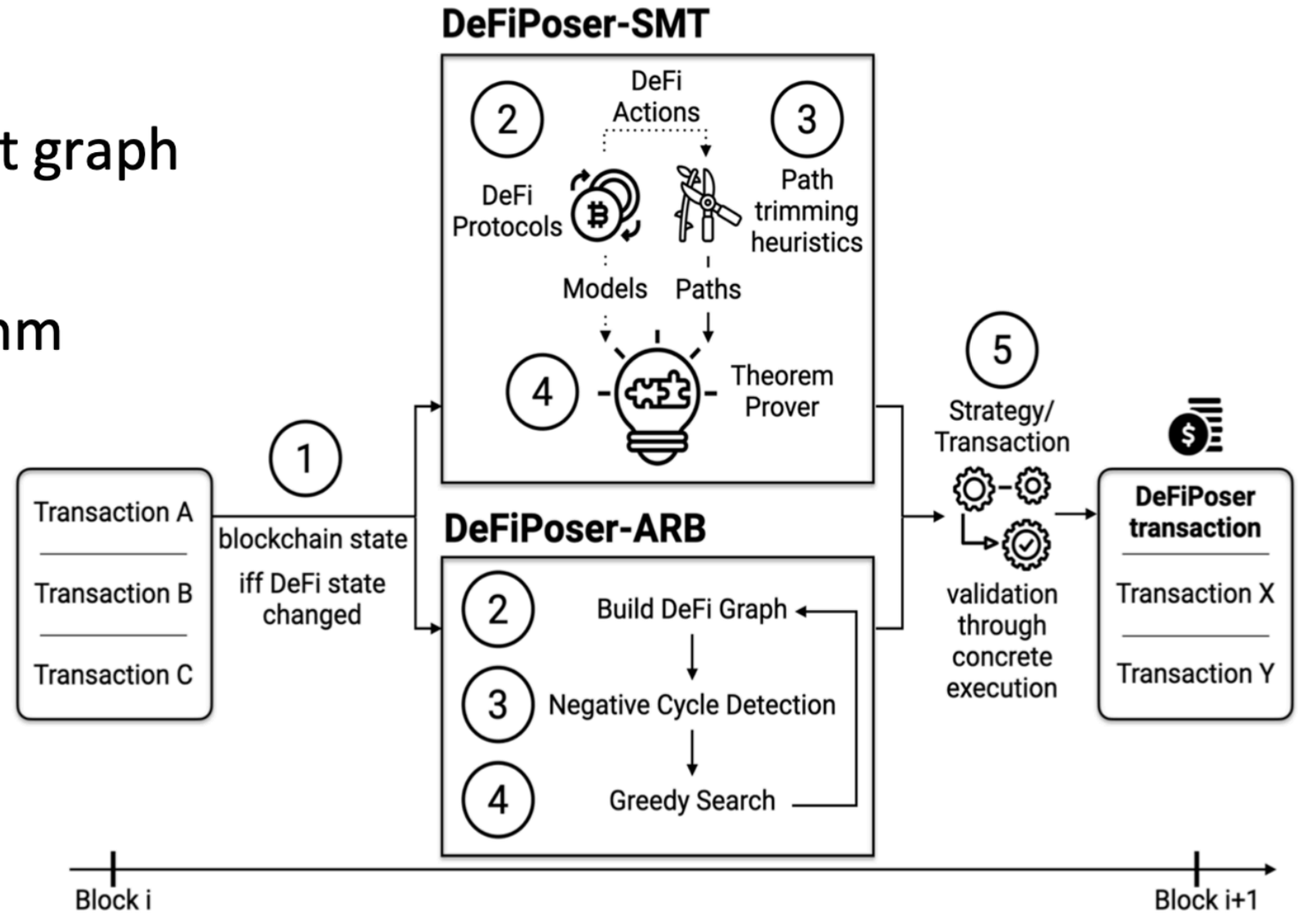
- Bellman Ford Algorithm
  - Negative cycle detection
  - Works among multiple markets
  - Used in traditional finance and DeFi

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

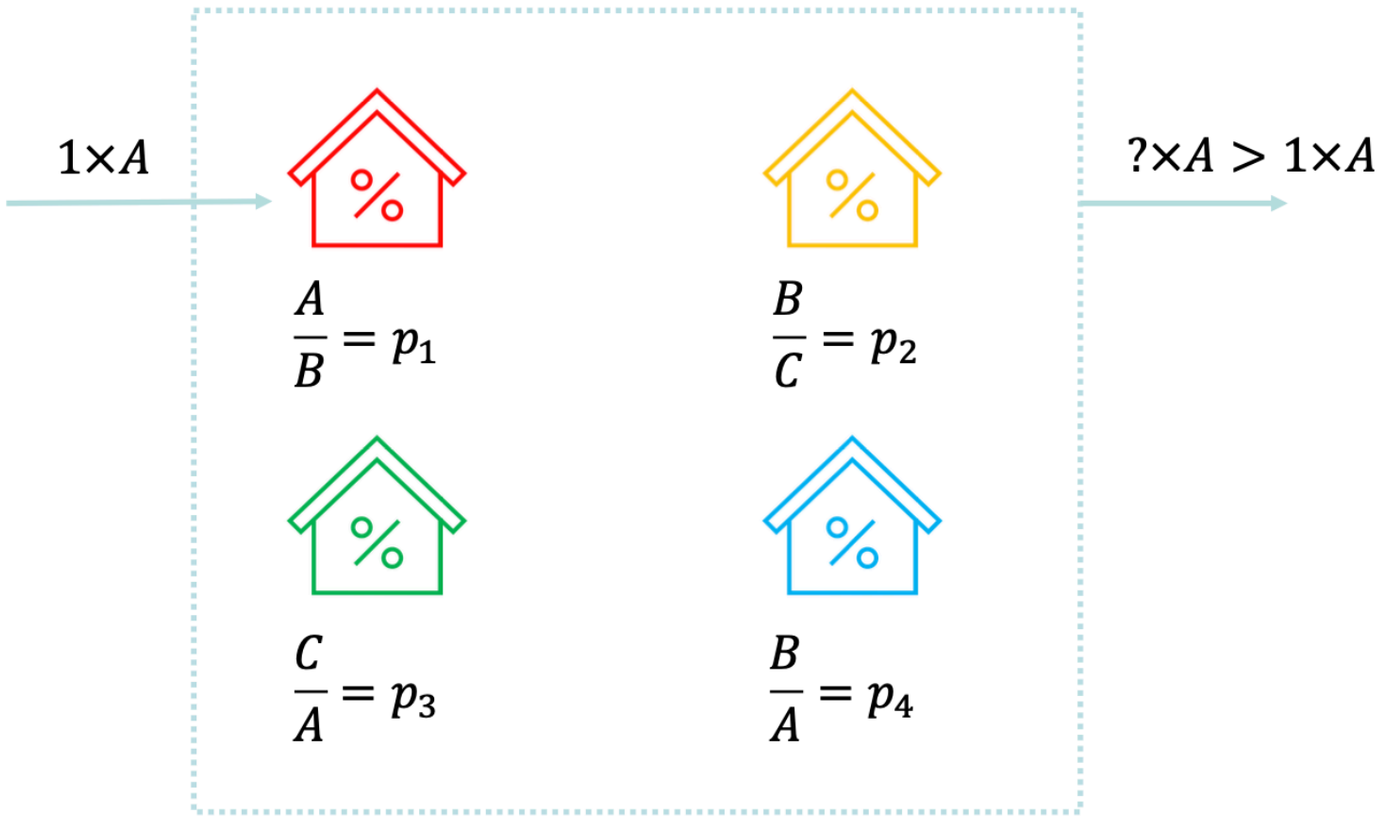
DeFiPoser-ARB and DeFiPoser-SMT

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

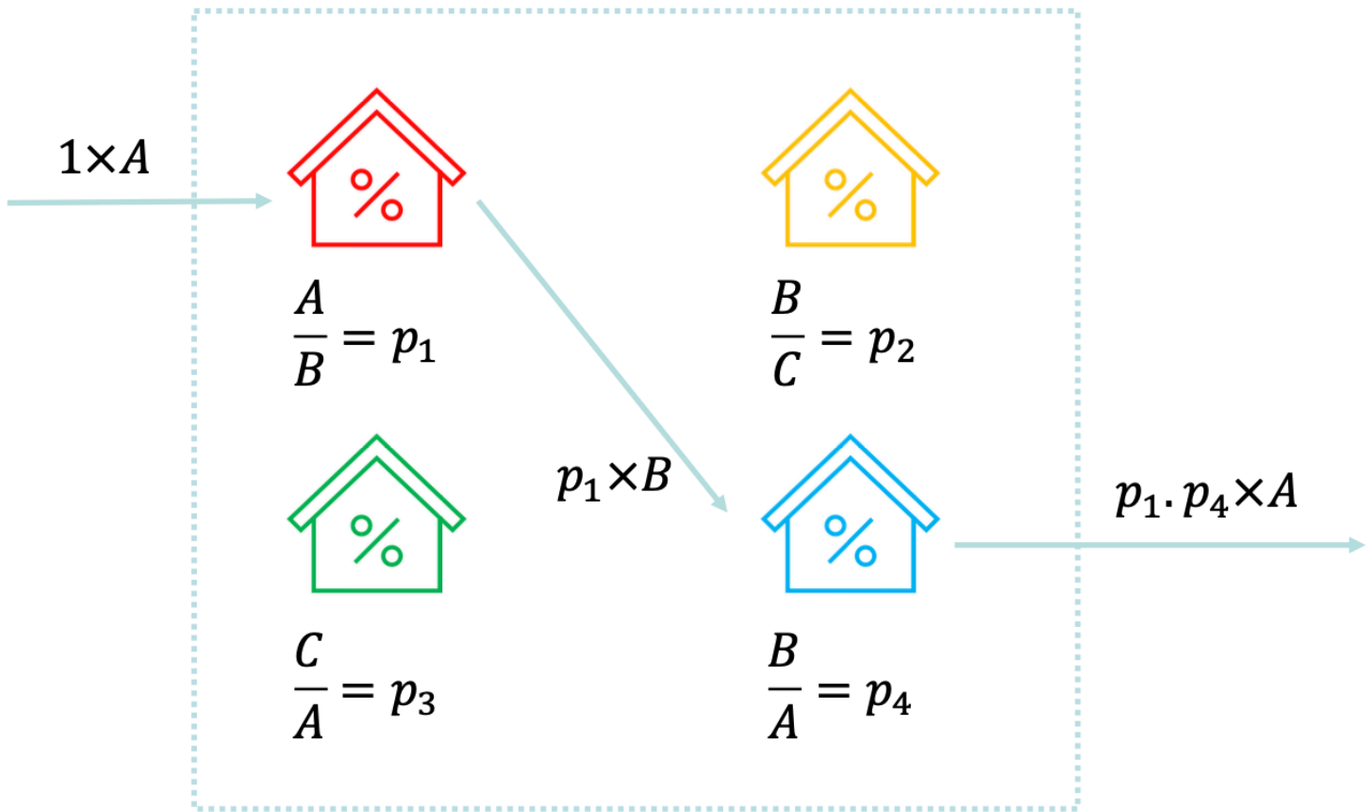
- DeFiPoser-SMT
  - state transition model
  - prunes search space
  - theorem prover



DeFiPoser-ARB



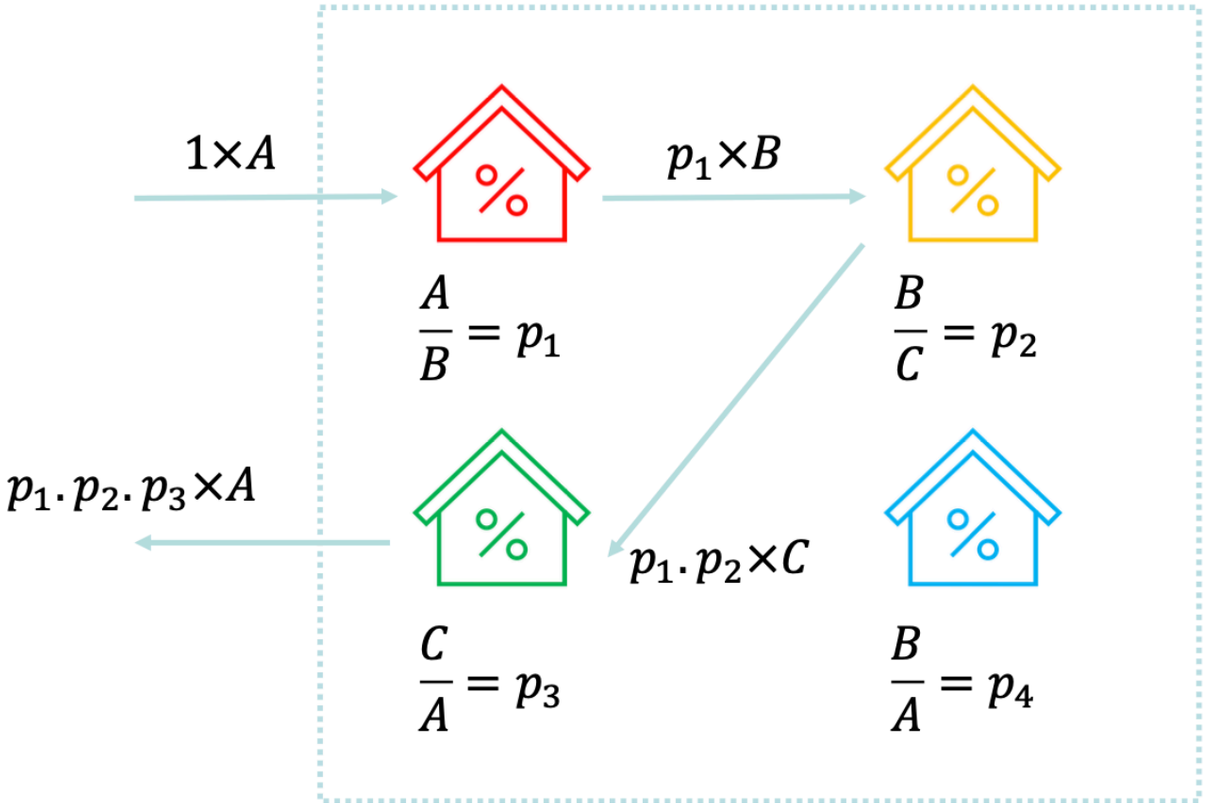
DeFiPoser-ARB



Profitable condition

$p_1 . p_4 > 1$

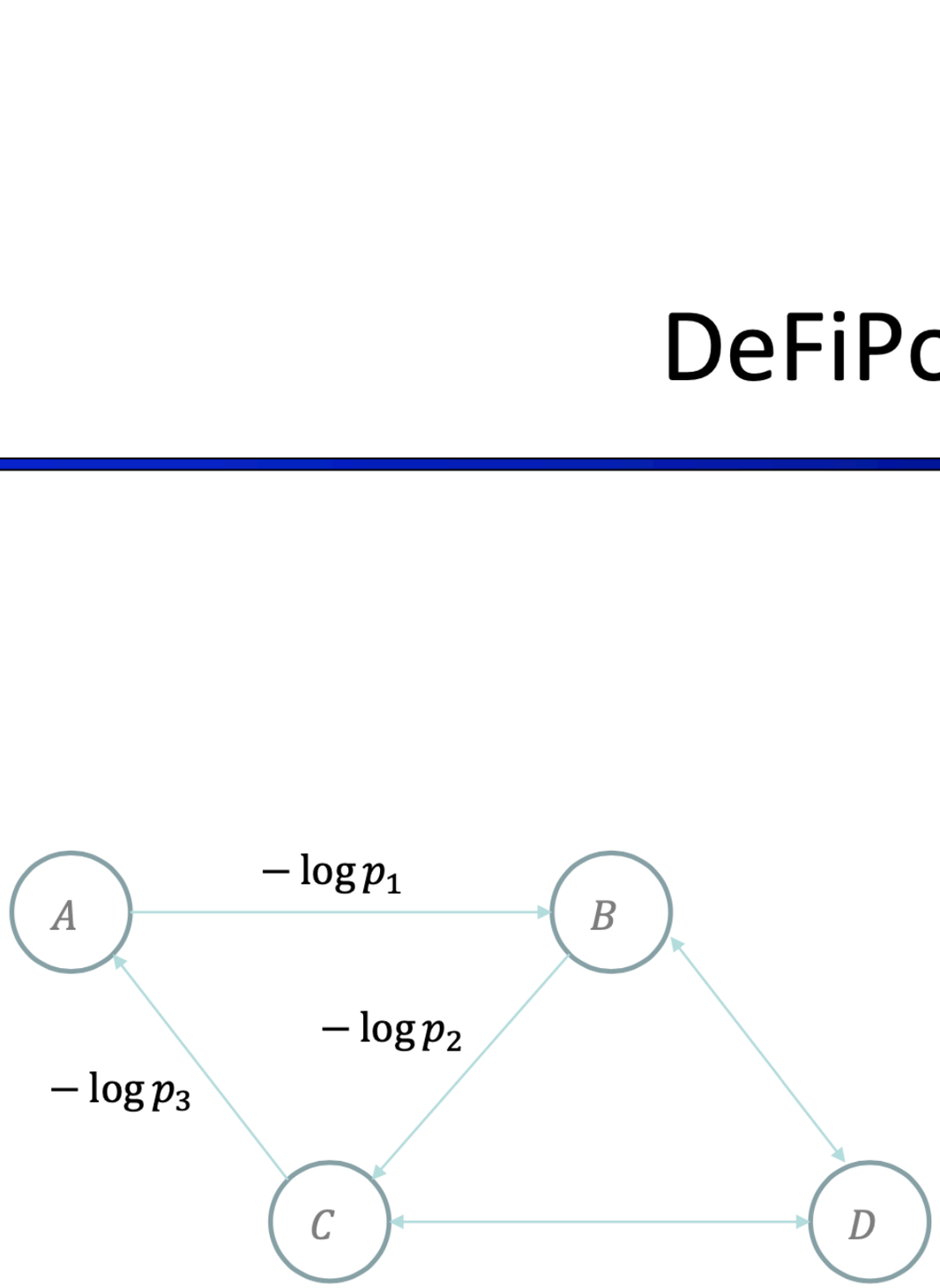
DeFiPoser-ARB



Profitable condition

$p_1.p_2.p_3 > 1$

DeFiPoser-ARB



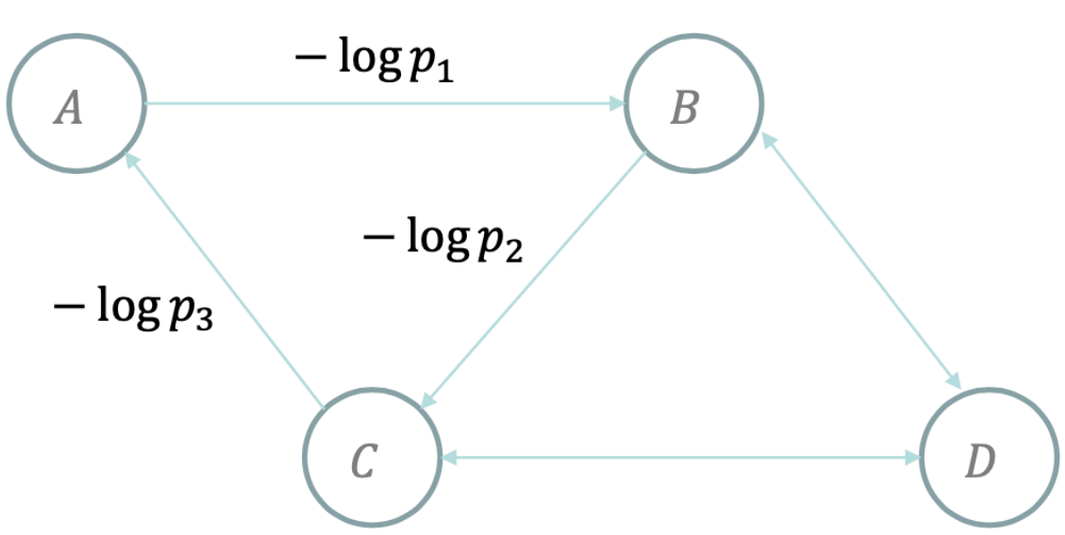
Profitable condition

$p_1 . p_2 . p_3 > 1$

$\Updownarrow$

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

DeFiPoser-ARB



$$\prod_i p_i > 1$$

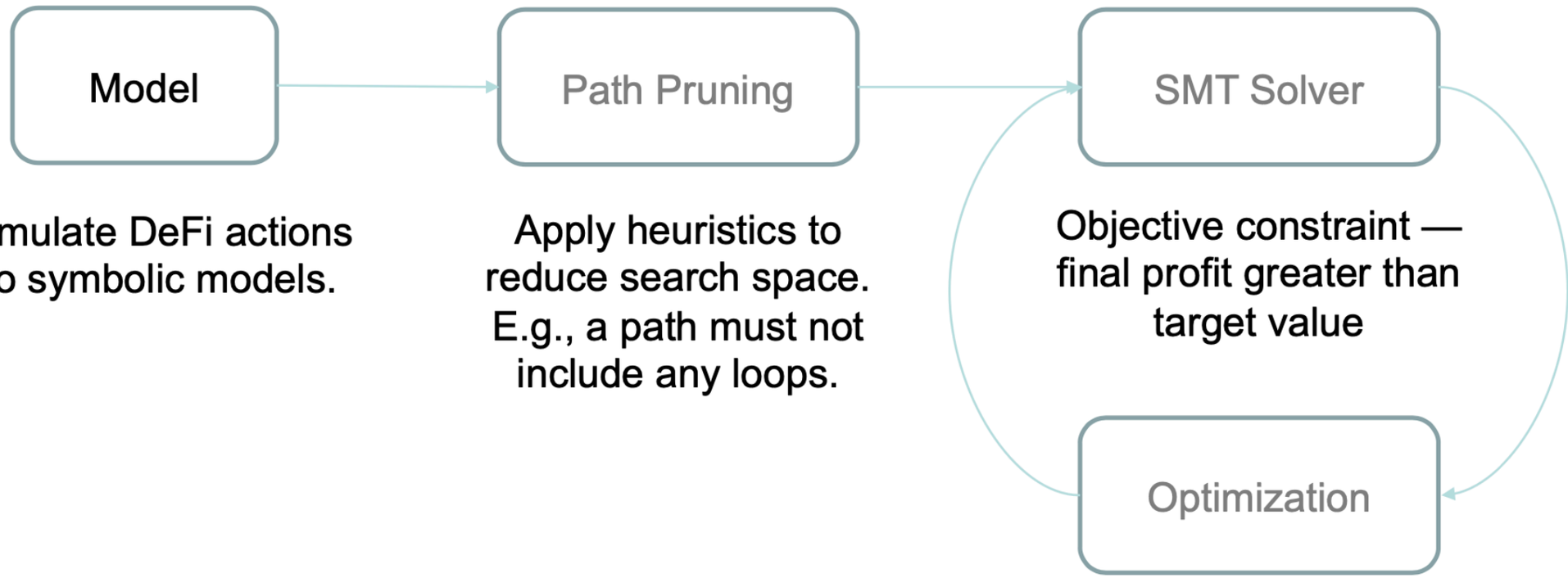
$$\Updownarrow$$

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

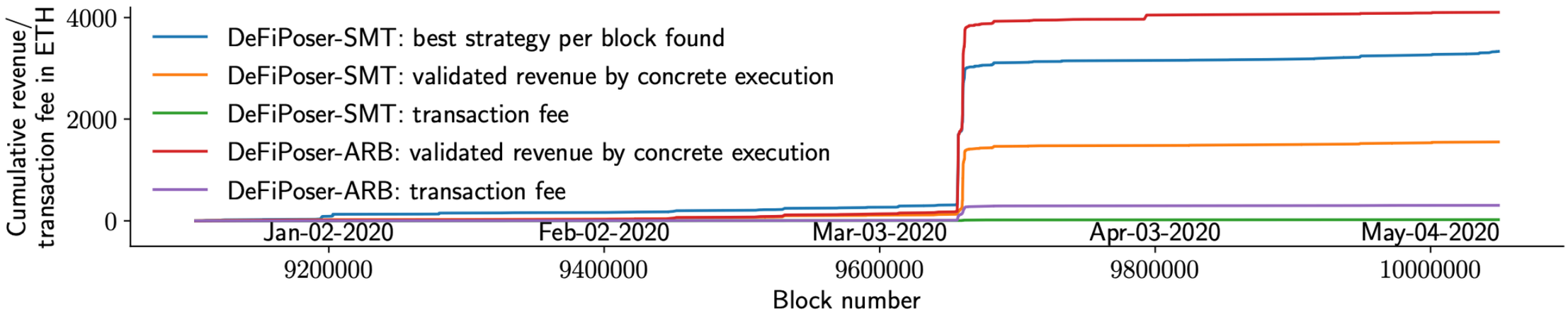
BellmanFord-Moore algorithm

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

DeFiPoser-SMT



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)

What We Have Learned

- Centralized exchanges, order book model, and market makers
- Decentralized exchanges and automated market maker model (AMM)
- Transaction propagation in peer-to-peer network
- Stable coin AMM
- Impermanent loss
- Liquidity mining
- Arbitraging