Market Manipulations on Decentralized Exchanges

Claudio J. Tessone
Blockchain & Distributed Ledger Technologies Group,

UZH Blockchain Center

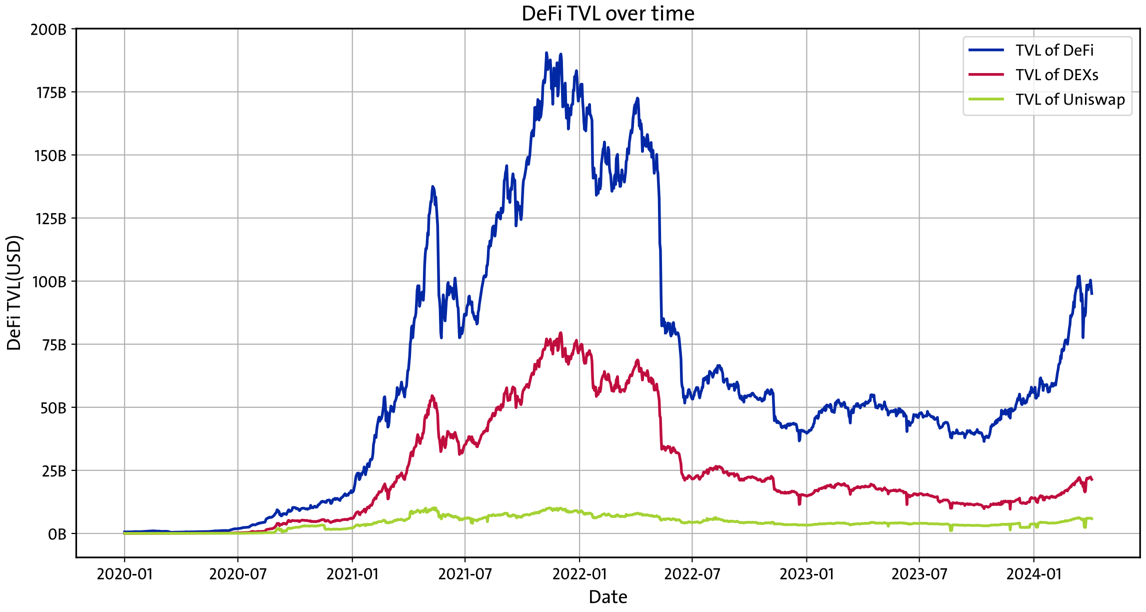
26 June 2024

Outlook

- ➢ DeFi and Uniswap introduction
- ➢ Features of Uniswap from network science
- ➢ Arbitrage opportunities
- ➢ Rug-pull attacks

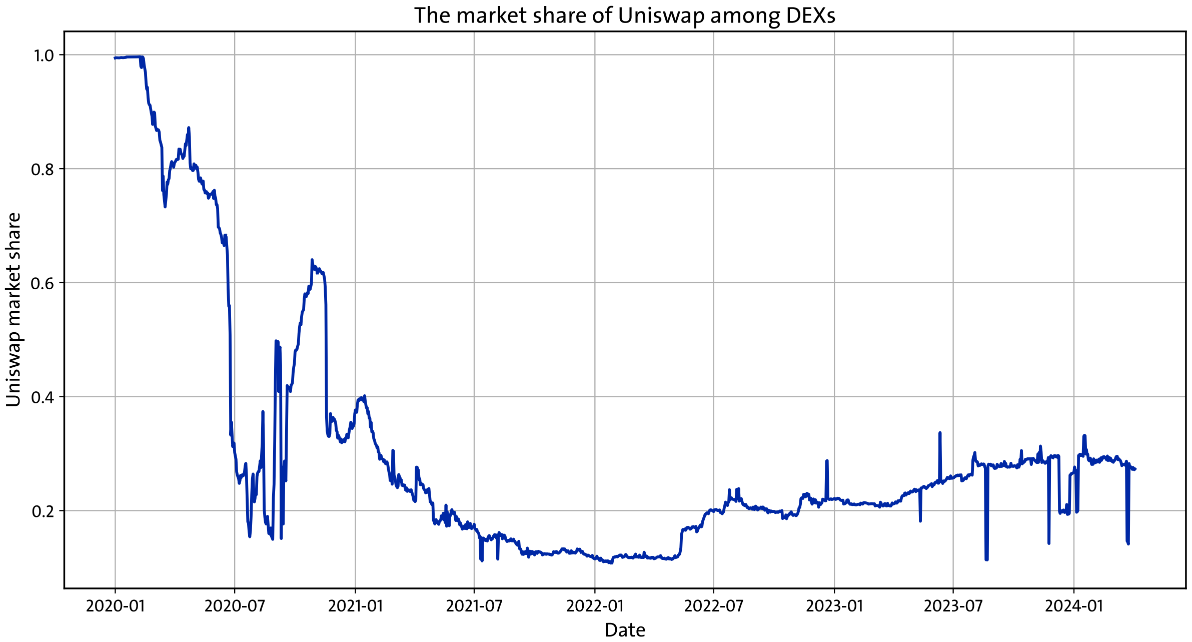
0

The rise of DeFi and decentralized exchanges (DEXs)



- DeFi advantages: permissionless, transparency, interoperability, etc.
- DEXs advantages: no intermediaries, no counterparty risk, 24/7 trading, etc.
- The TVL of DeFi reached its peak in 2021, and it rises again this year.

Uniswap as a leading DEX platform

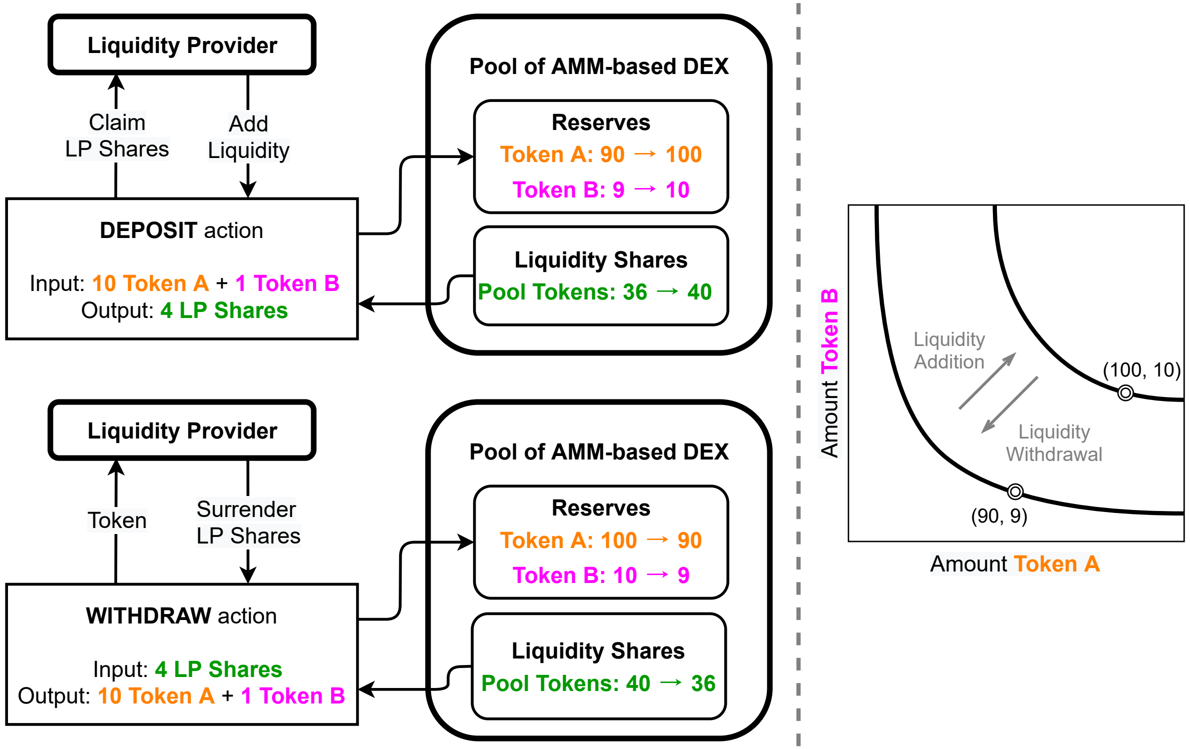


- Uniswap was launched in November 2018 and currently has four versions,
  The most widely used versions are V2 and V3, while V4 is under test.
- Uniswap still accounts for 27.3% of TVL among all decentralized exchanges.

Uniswap introduced Automated Market Makers that replaced limit order books with liquidity pools (reserves)

Prices are not set by market makers, but automatically determined by the state of the reserves

Pairs of tokens can be traded in Liquidity Pool



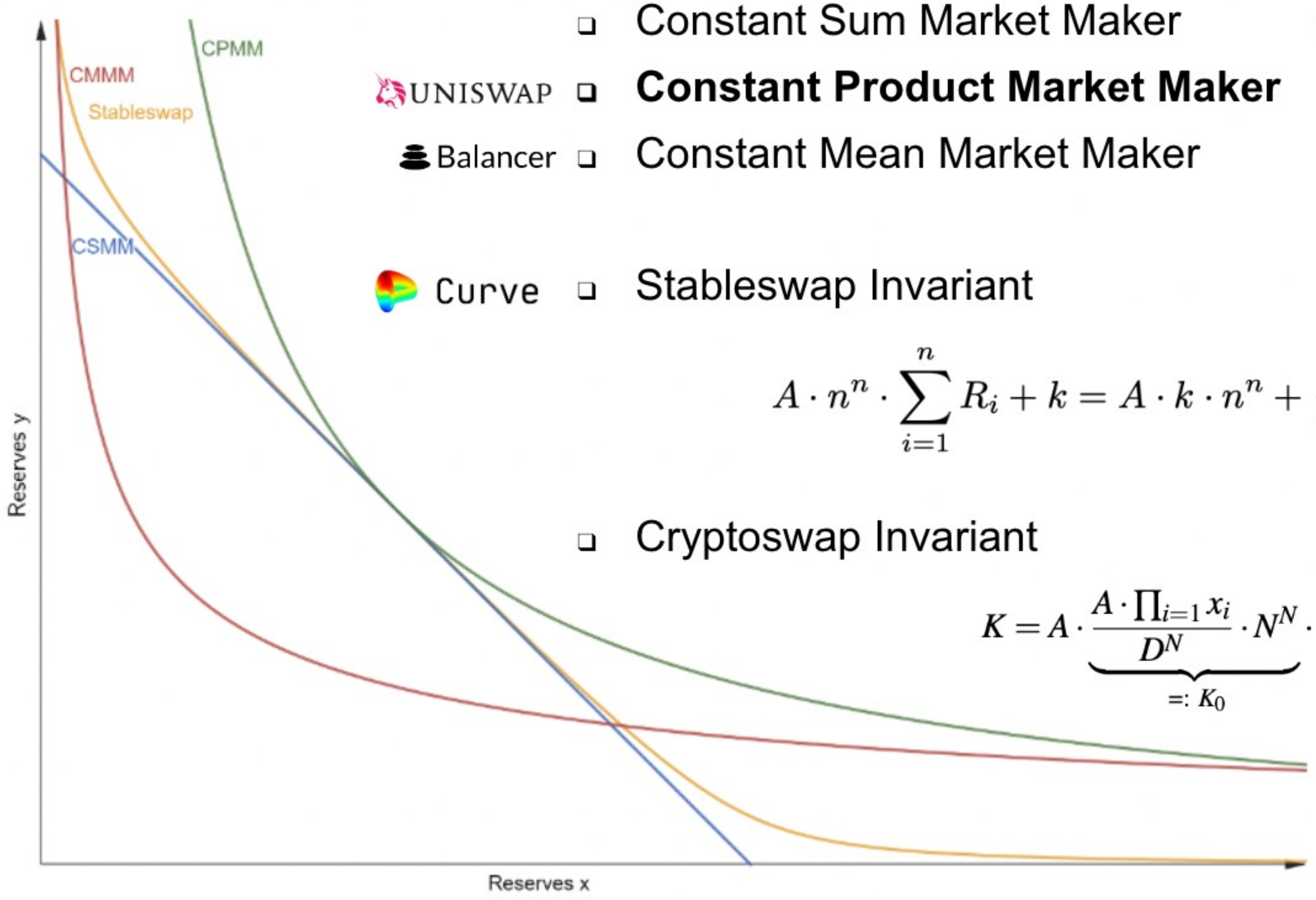
(a) Liquidity provision and withdrawal.

Any user can create a liquidity pool. ***It requires depositing funds of two tokens with reserves*** R_α ***and*** R_β***;***

$$k = R_\alpha R_\beta$$

k is a conserved quantity

Over time more types of AMMs were introduced



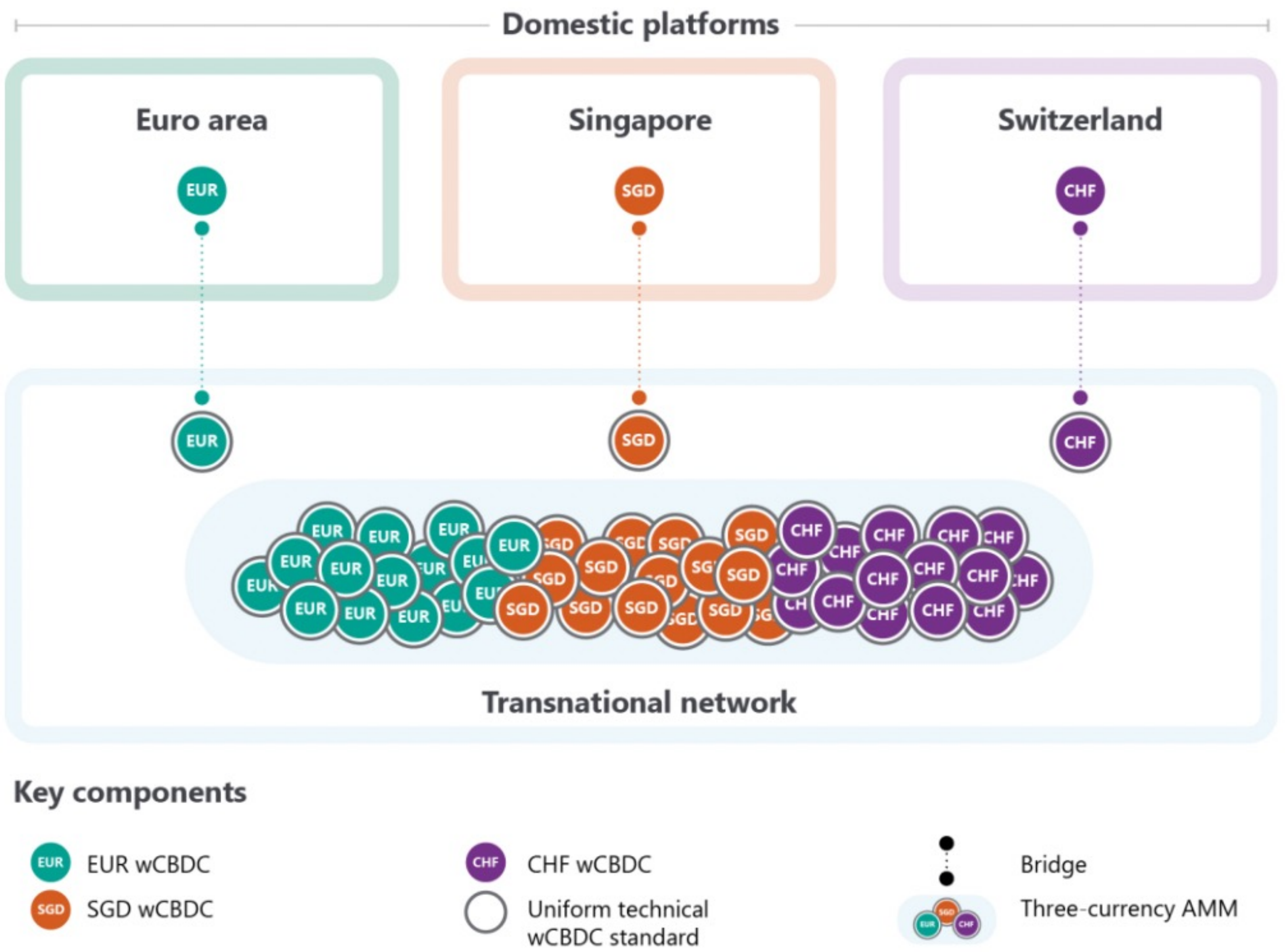
- Constant Sum Market Maker $x + y = k$
- UNISWAP **Constant Product Market Maker** $x \cdot y = k$
- Balancer Constant Mean Market Maker $\prod_{k=1}^{n} R_i^{w_i}$
- Curve Stableswap Invariant

$$A \cdot n^n \cdot \sum_{i=1}^{n} R_i + k = A \cdot k \cdot n^n + \frac{k^{n+1}}{n^n \prod_{i=1}^{n} R_i}$$

- Cryptoswap Invariant

$$K = A \cdot \underbrace{\frac{A \cdot \prod_{i=1} x_i}{D^N} \cdot N^N}_{=: K_0} \cdot \frac{\gamma^2}{(\gamma + 1 - K_0)^2}$$

Central Banks Pilots



Automated Market Makers can be applied for the FX market

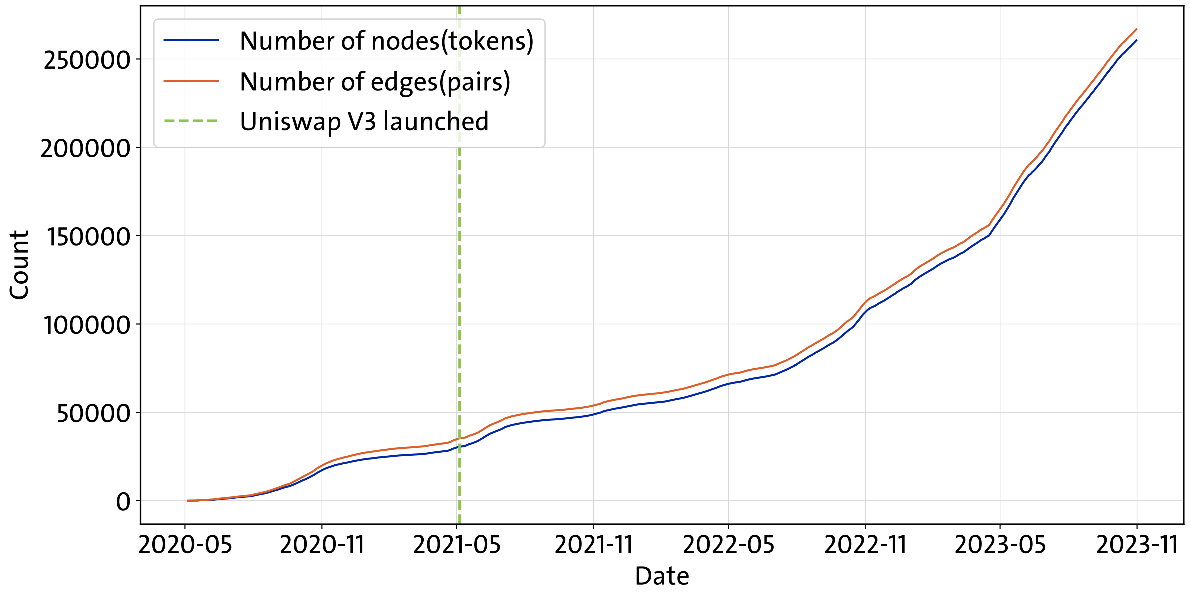
Creation of trading pairs are not centrally controlled

There is a latent risk: Anyone can create a trading pair using any two ERC-20 tokens.

Features of Uniswap from network science

1

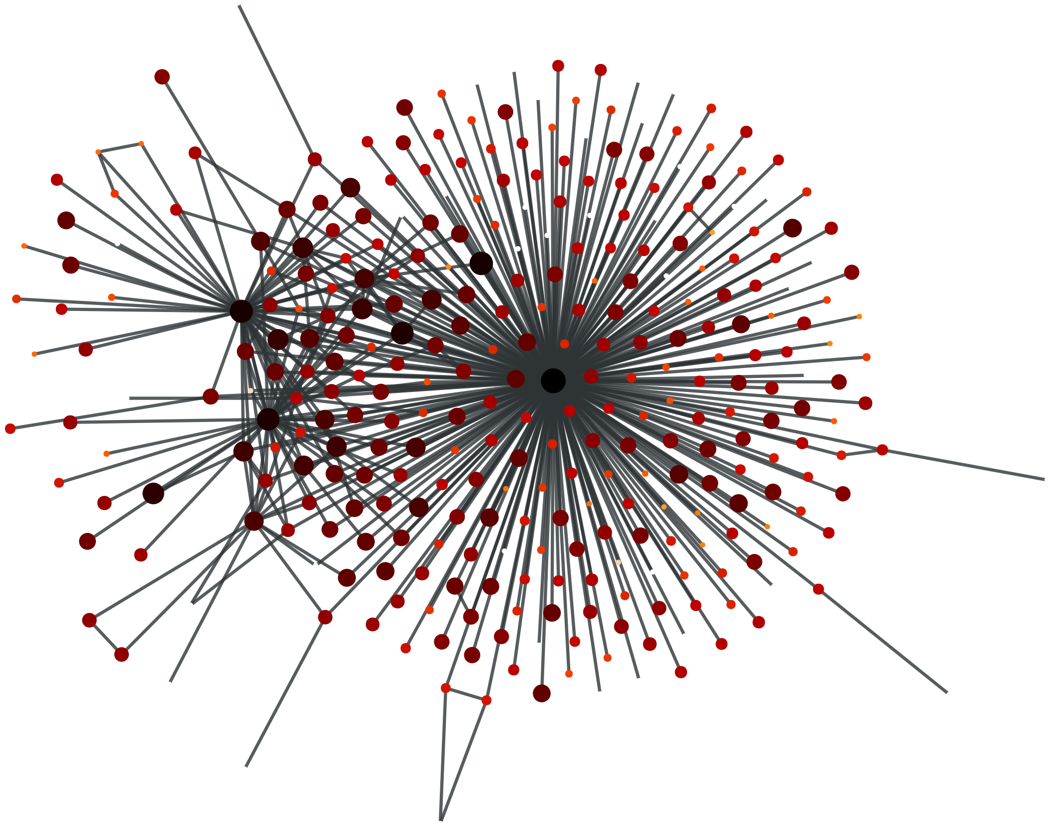
Network size evolution



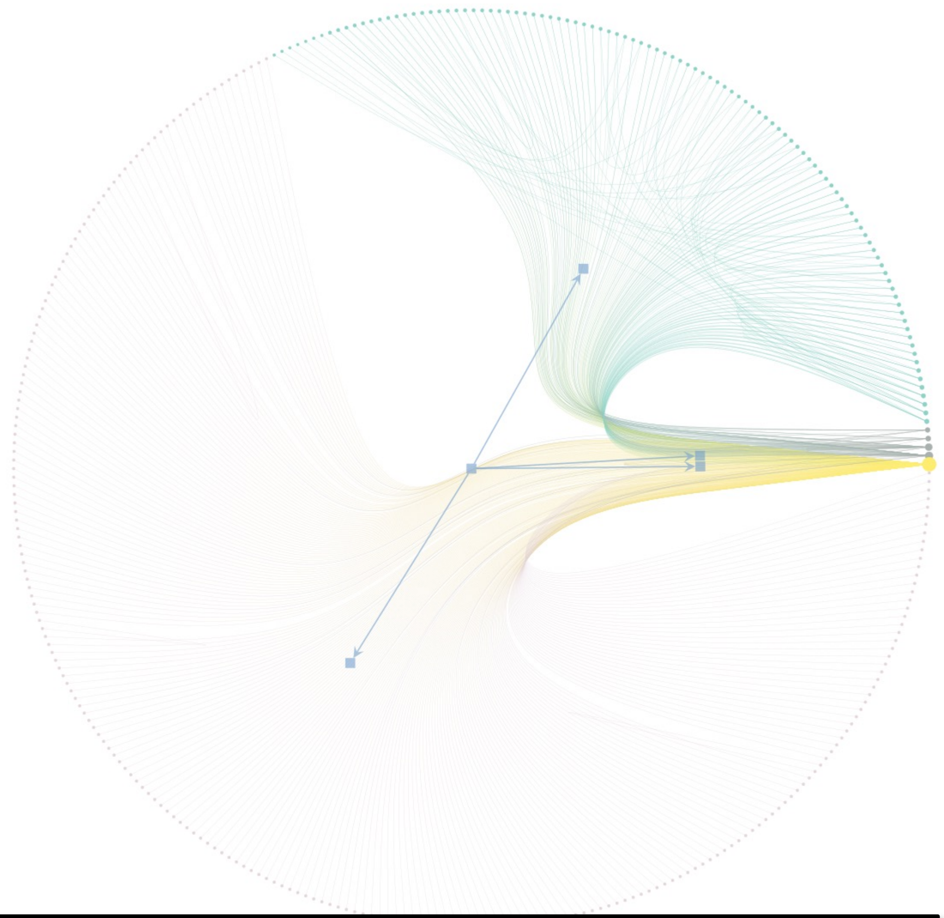
– The network has shown a clear growth trend from the initial 1 trading pair on May 5, 2020 to the latest 266,826 trading pairs on Oct 31, 2023, while Binance has just 1591 trading pairs.

Notably, there has been a significant liquidity pool created on Uniswap V2 after Uniswap V3 was launched on May 5.

A systemic view of Uniswap: Liquidity Pool Network

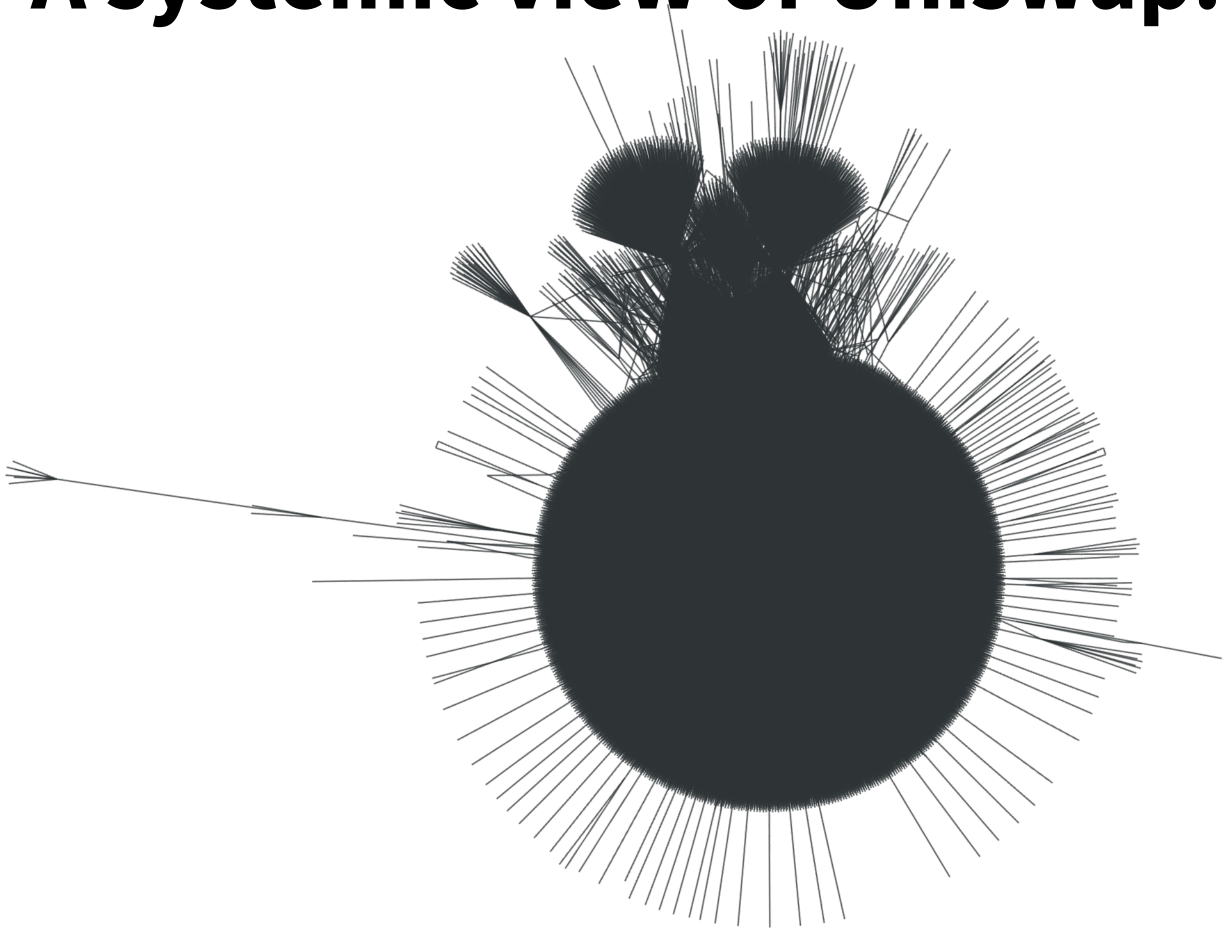


Snapshot 2020-08-31

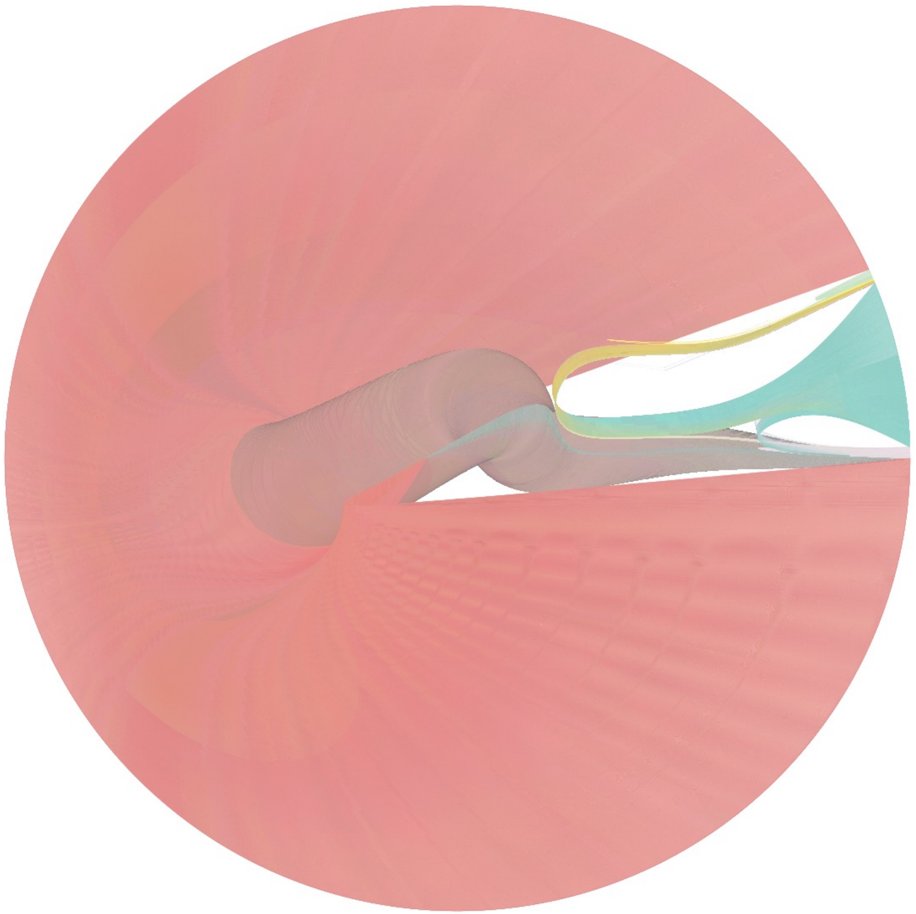


In this snapshot, nodes are tokens, and edges represent liquidity pools between them

A systemic view of Uniswap: Liquidity Pool Network

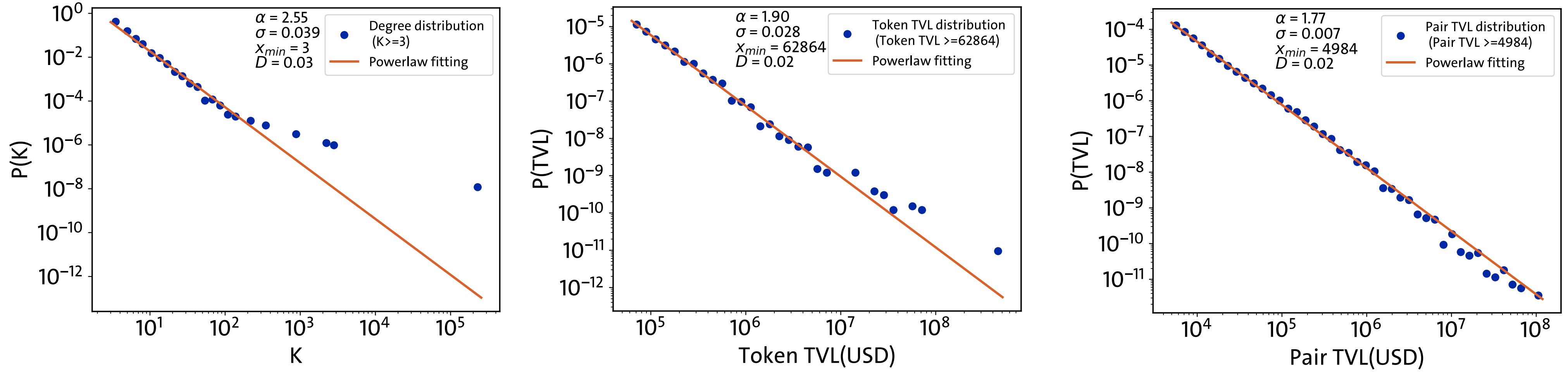


Snapshot 2022-08-31



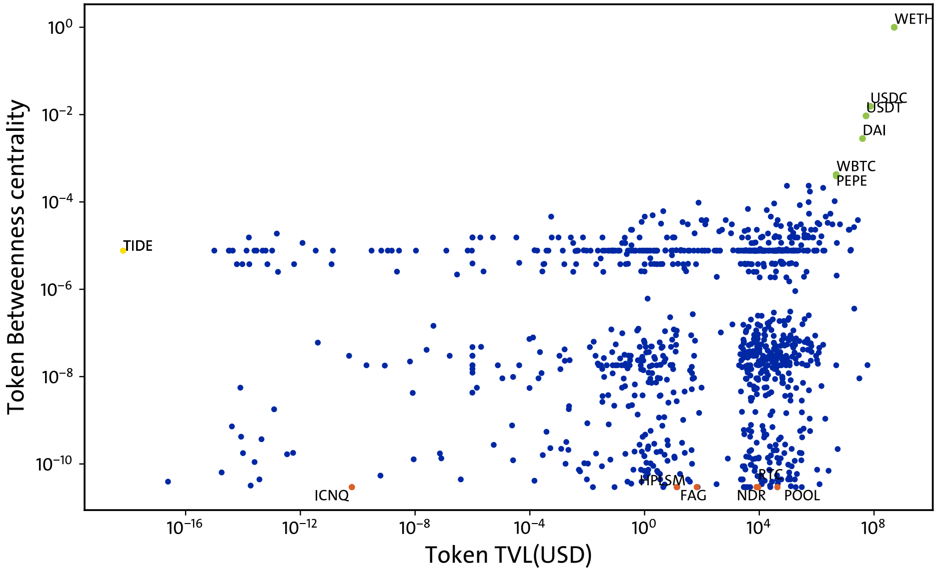
Over time, the network grew significantly and became more centralized

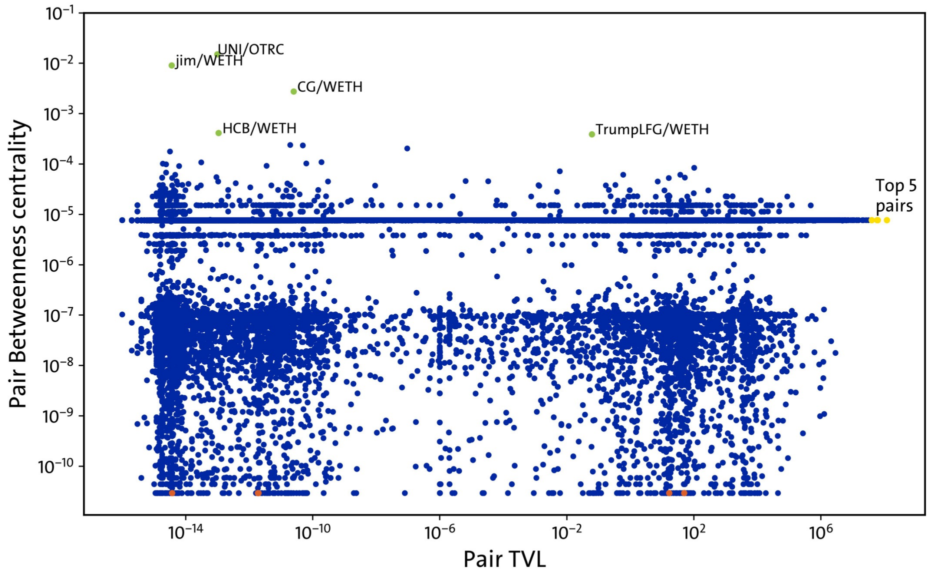
Degree, TVL of token and pair distribution



- The degree and TVL of tokens and pair distributions follow a power-law distribution.
- This indicates that the network connections and TVL are concentrated in a small proportion of tokens and pairs.

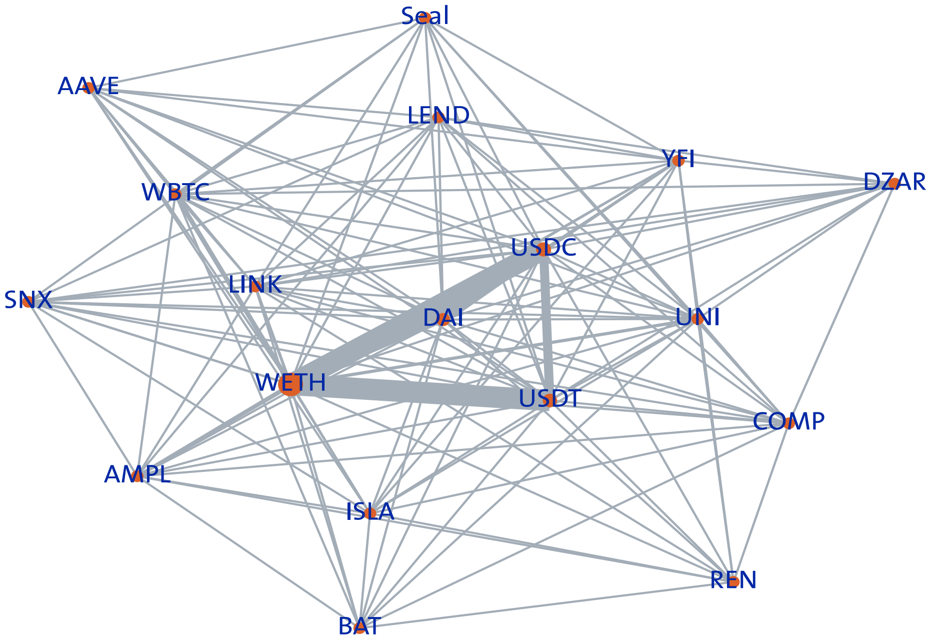
Important tokens and liquidity pools





- The betweenness in network is used to measure the importance of tokens and pairs in the Uniswap market network.
- In general, neither tokens nor pairs’ TVL have a linear relationship with TVL.
- The top 5 tokens with the highest TVL align with the top 5 tokens with the highest betweenness centrality, but this rule doesn’t work for the top pairs.

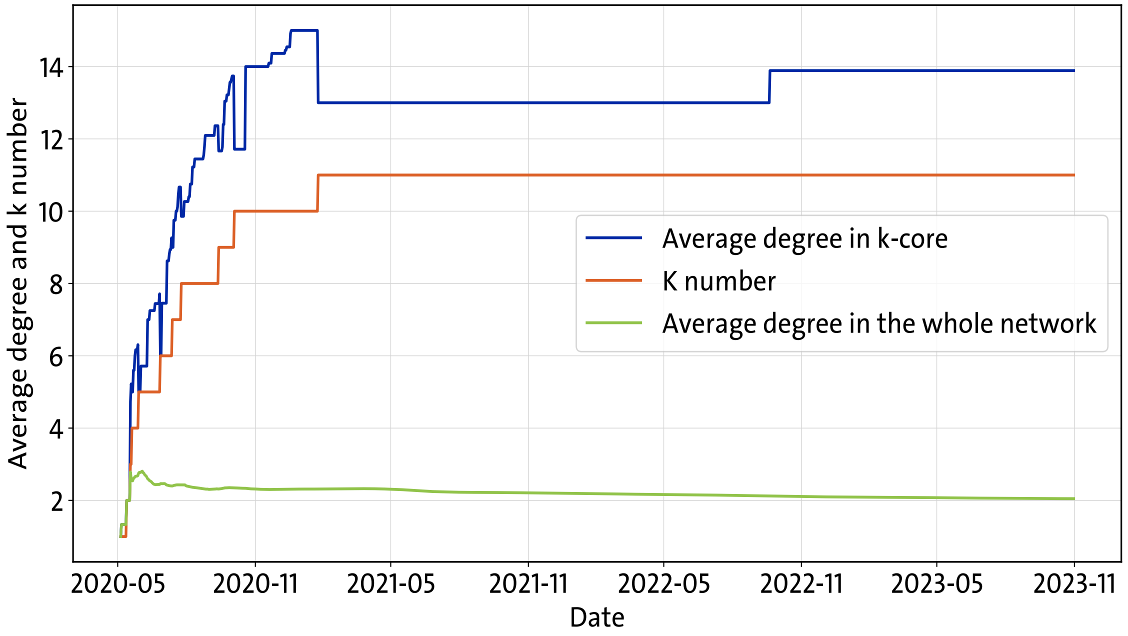
Core-periphery structure

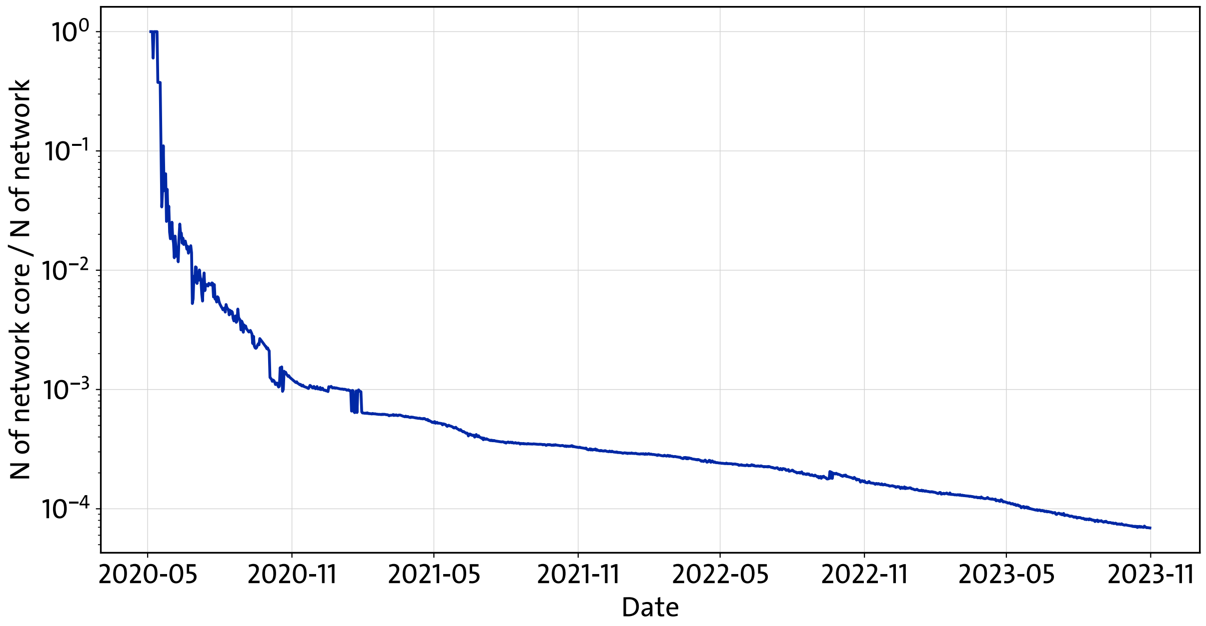


Metrics	Uniswap Network	Random Network
Number of Nodes	260544	260544
Avg. Degree (Largest Component)	2.05	2.05
K number in the k-core	11	2
Number of Nodes(k-Core Group)	18	128500
Avg. Degree (k-Core Group)	6.94	2.72

Comparing with the random network, the Uniswap network shows a core-periphery structure in terms of the number of nodes and average degree in the core group.

Core-periphery structure overtime





- The average degree within the network core exceeds that of the entire network over time, and the proportion of nodes within the network core diminishes.

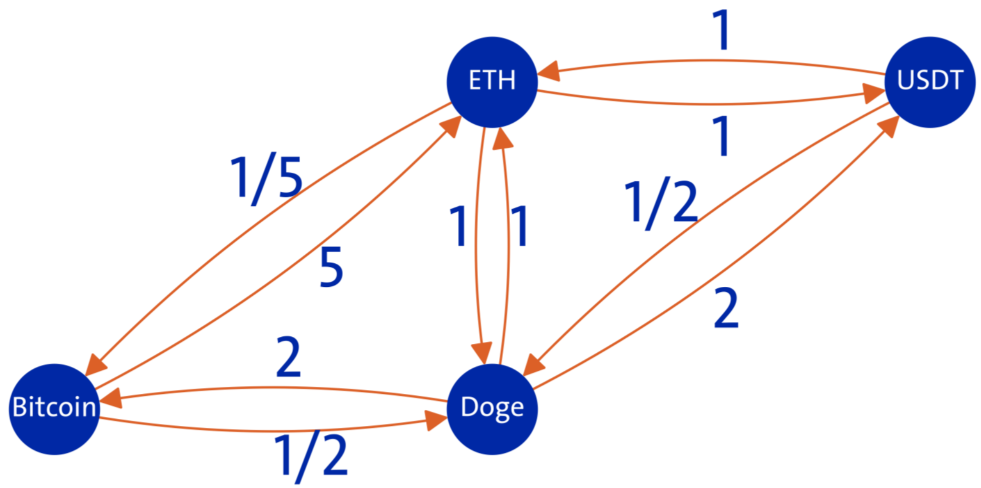
This indicates that the core-periphery structure of the network is becoming more prominent over time.

Arbitrage Opportunities

2

Arbitrage opportunities on Uniswap

- Inconsistent prices among multiple trading pairs on Uniswap
- Arbitrage exists in loops where the product of tokens' price is larger than 1.



- Product of tokens' price

$$\frac{ETH}{BTC}\times\frac{USDT}{ETH}\times\frac{Doge}{USDT}\times\frac{BTC}{Doge}=5\times1\times\frac{1}{2}\times2=5$$

- Arbitrage path

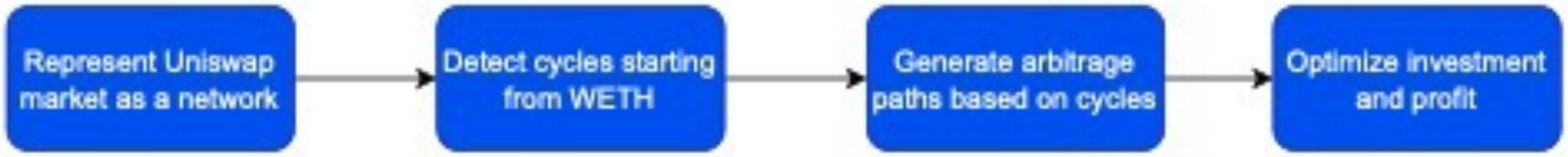
BTC⟶ ETH⟶ USDT⟶Doge⟶BTC

Arbitrage opportunities on Uniswap

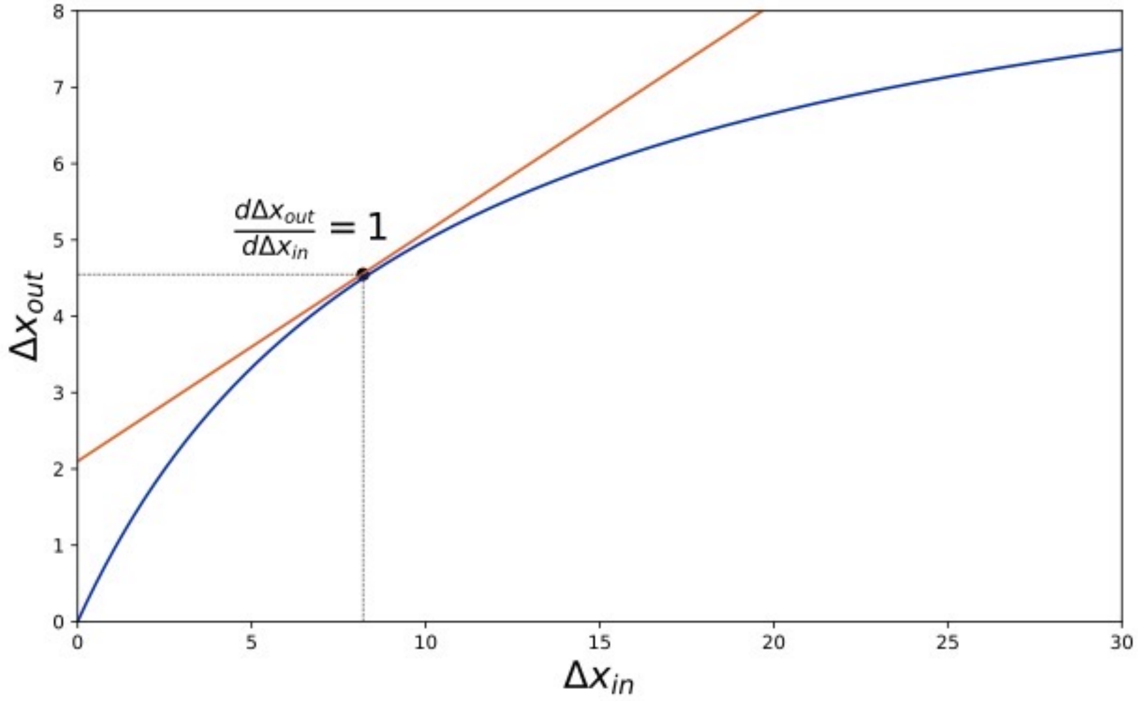
- **General arbitrage condition on Uniswap**
  - A cyclic arbitrage path involving n tokens $T_1, T_2, \ldots, T_n$, with $T_{n+1} = T_1$
  - λ is the swapping fee on Uniswap, each transaction will deduct a fixed transaction fee λ (0.3% on Uniswap V2)
  - If the product of the token prices, after subtracting swapping fees, is greater than 1, this indicates the existence of arbitrage opportunities

$$\prod_{i=1}^{n} \left(\frac{\text{Reserve of } T_{i+1}}{\text{Reserve of } T_i} \right) \times (1 - \lambda)^n > 1$$

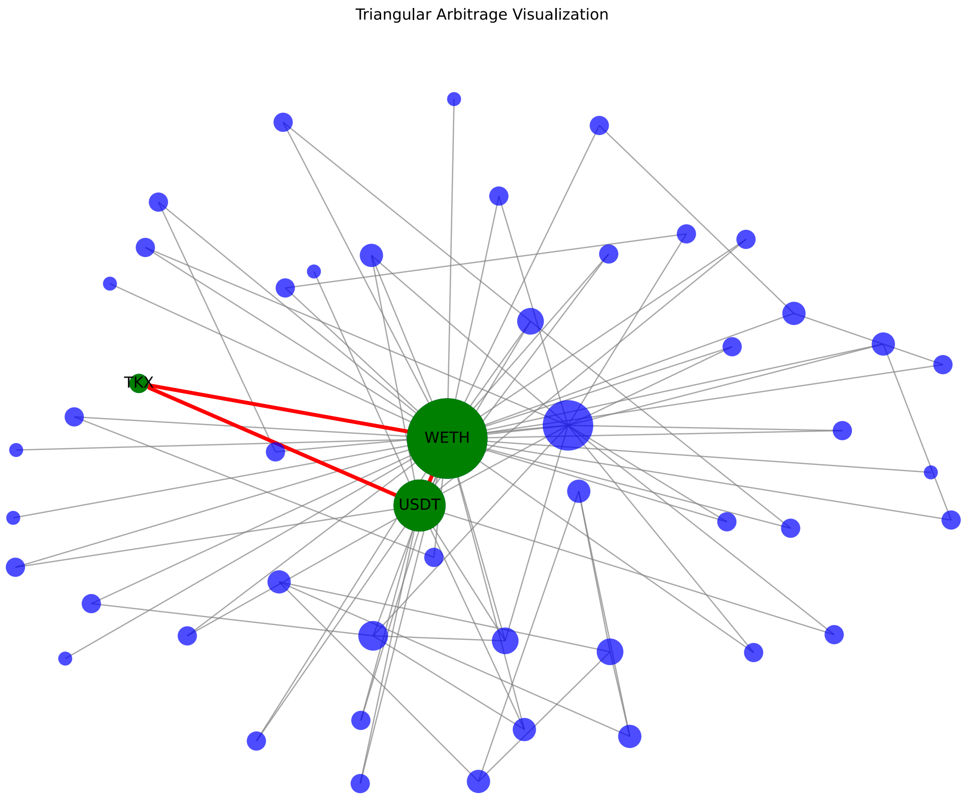
Arbitrage detection on Uniswap



- The relationship between the input amount and the output amount in arbitrage paths shows a convex and monotonically increasing pattern.
- The best input amount is the point where the marginal output amount equals the marginal input amount.

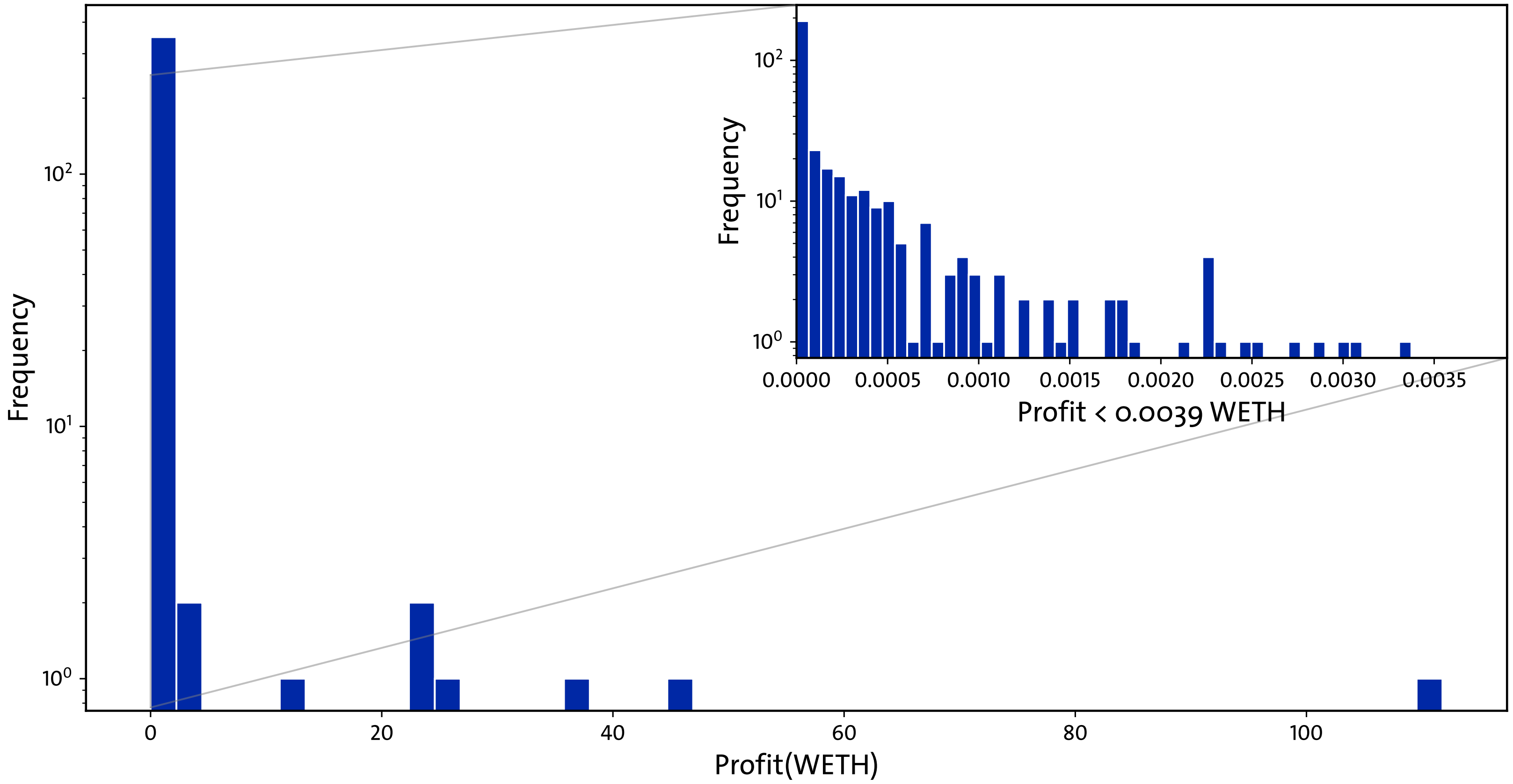


Triangular arbitrage



Arbitrage path: WETH → USDT → TKX → WETH

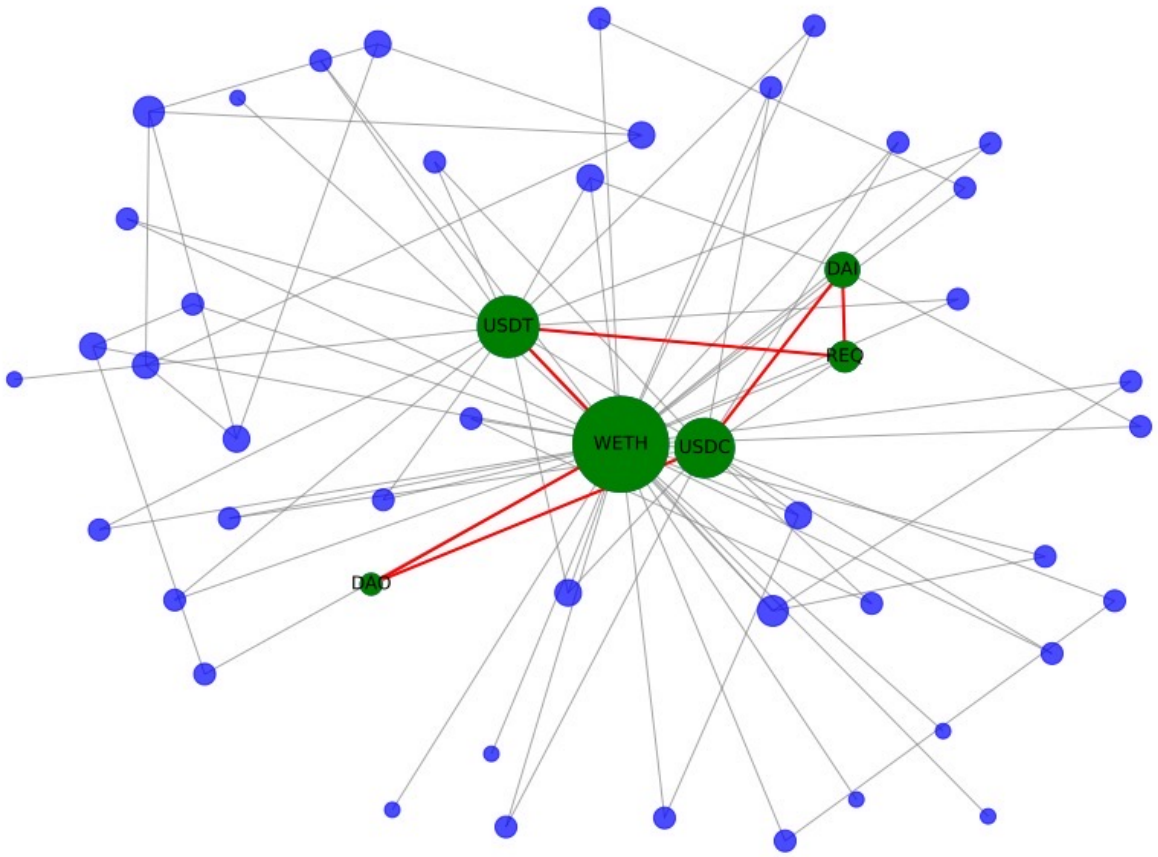
Triangular arbitrage



Among 507 triangular cycles, only 35 paths can achieve profits that can cover the transaction fees on block 18,012,051(Aug 28,2023)

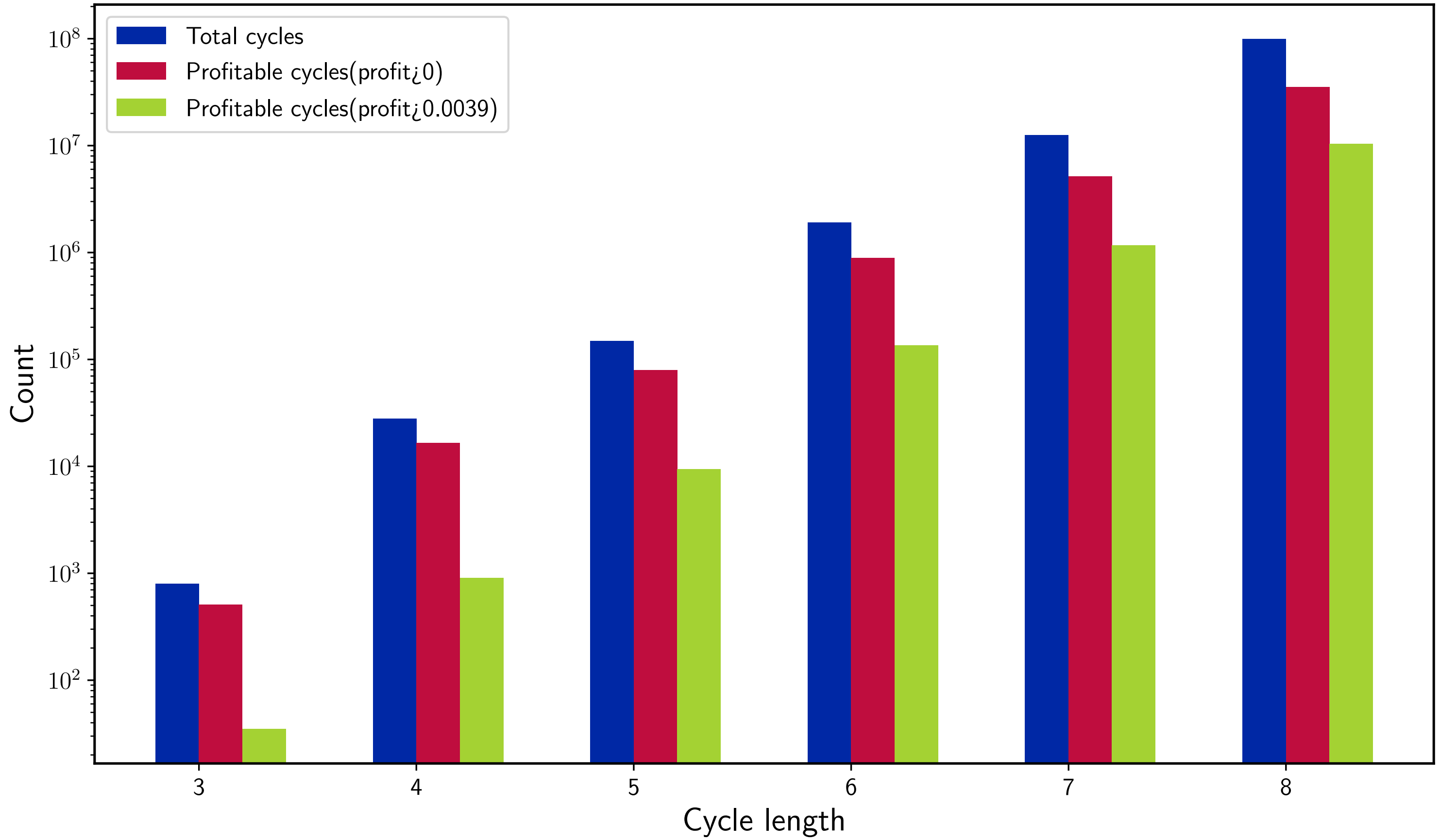
Triangular arbitrage opportunities are scarce at recent blocks

Arbitrage paths with longer length



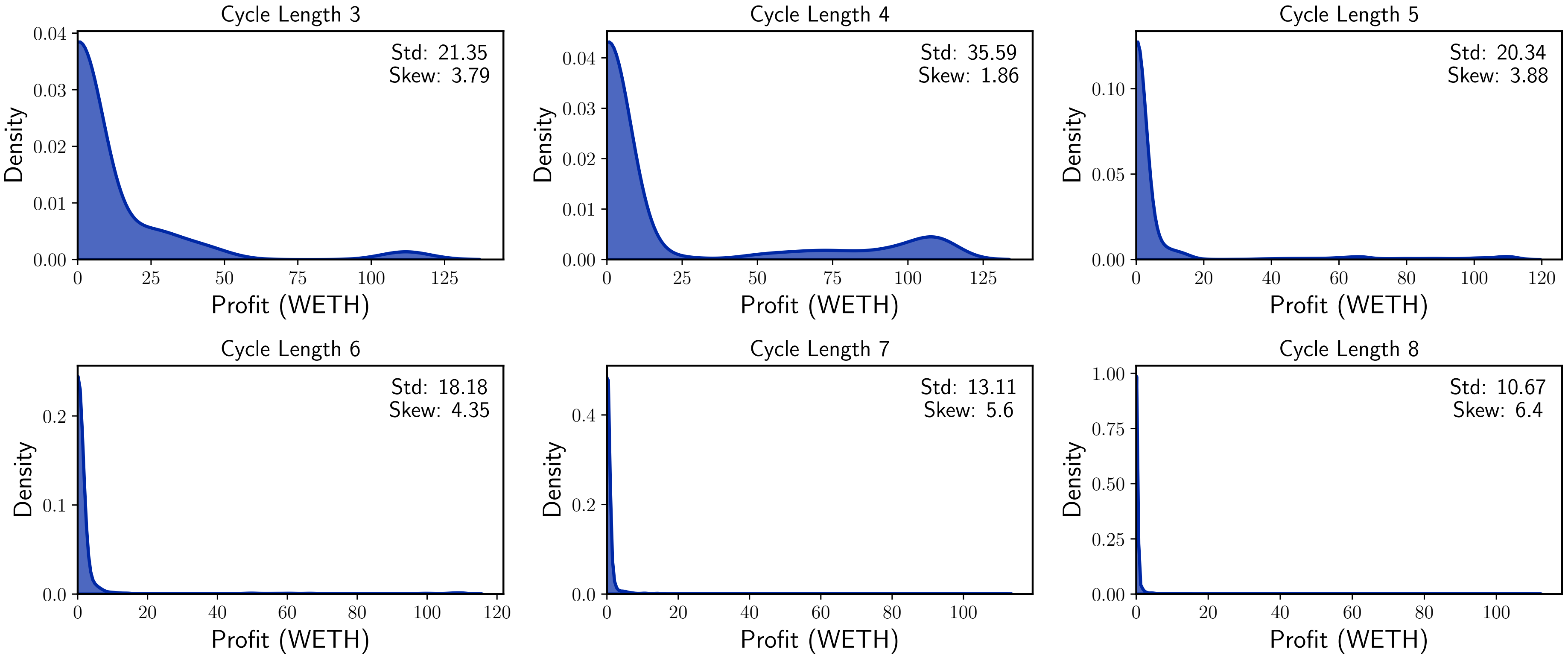
Arbitrage path: WETH → USDT → REQ → DAI → USDC → DAO → WETH

Arbitrage paths with longer length



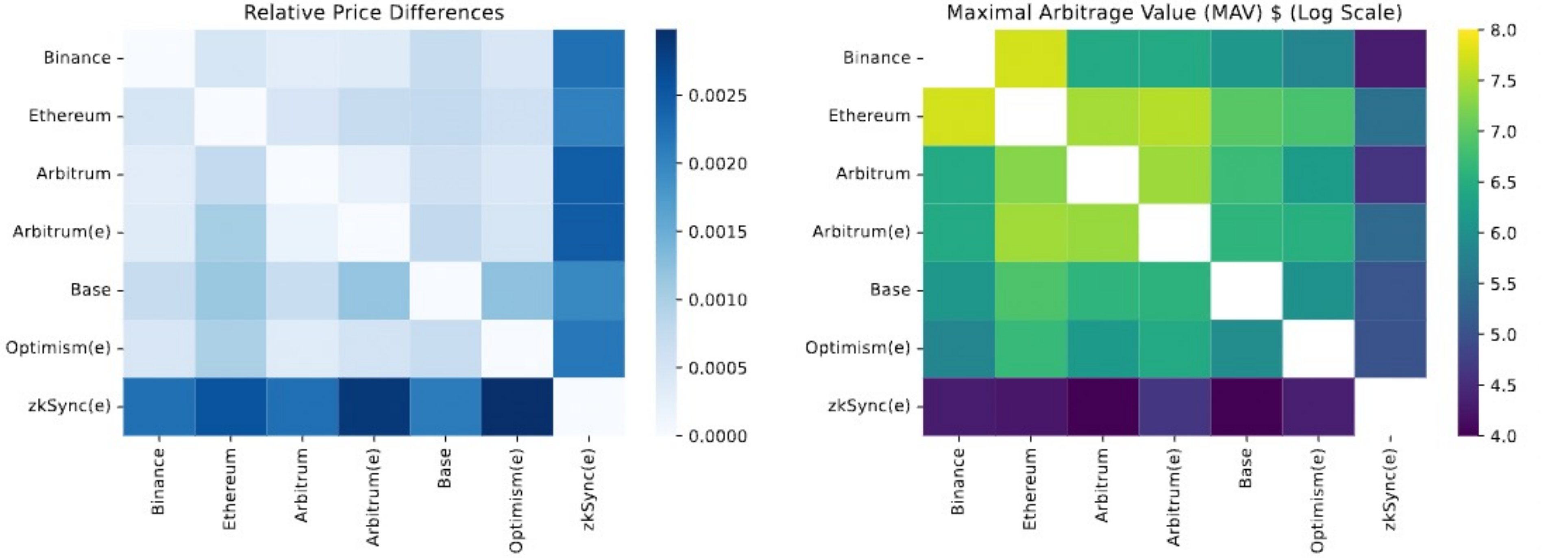
The longer the cycle length, the more opportunities for profitable arbitrage.

Arbitrage profits with longer length



Although the absolute number of cycles yielding high profits increases, the probability of discovering profitable arbitrage paths with high profits diminishes.

Interchain Arbitrage

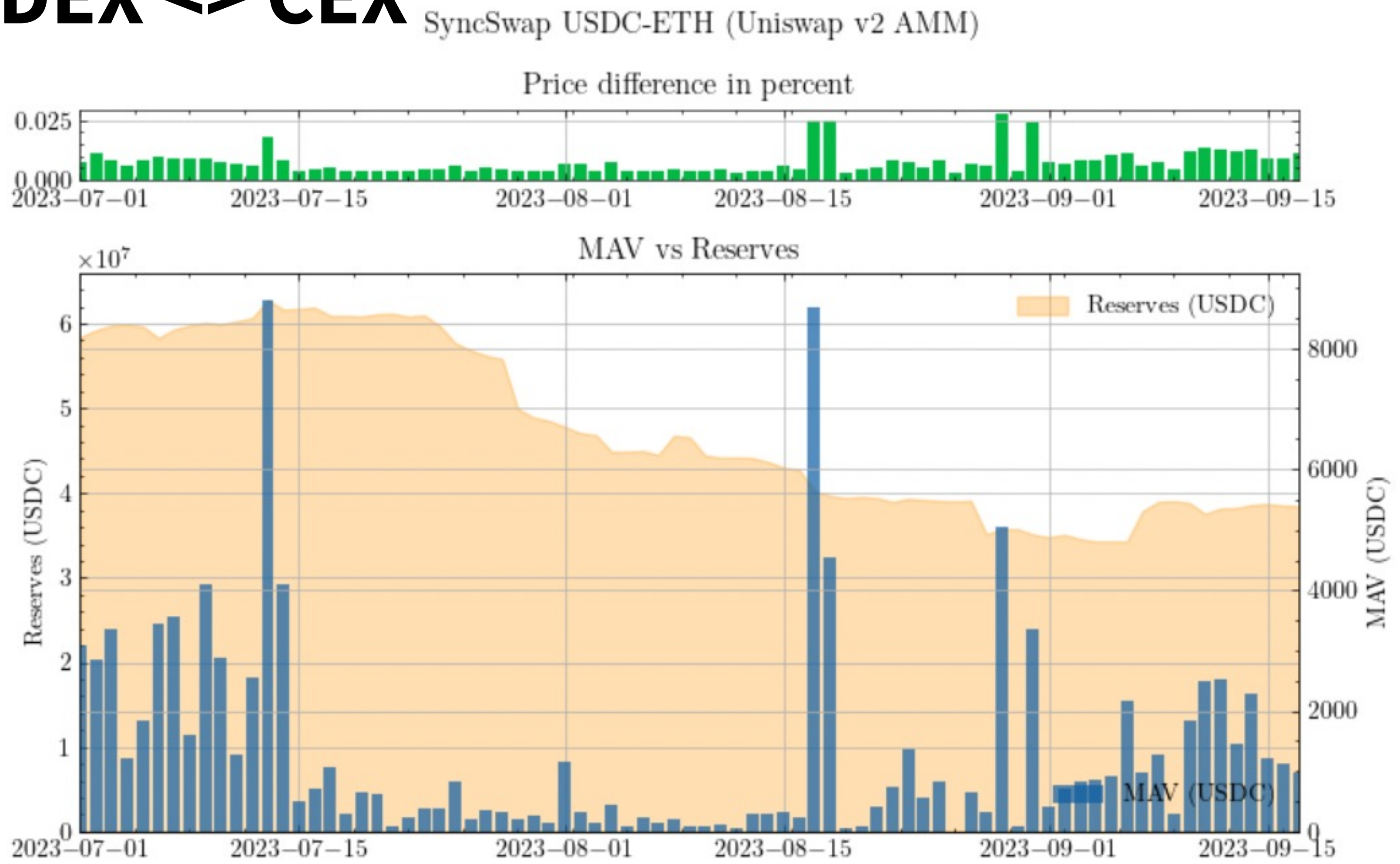


(a) Mean (relative) price difference. (b) Maximal Arbitrage Value in USD.

Comparison of ETH<>USDC Uniswap (v3) pools on Ethereum and its rollups

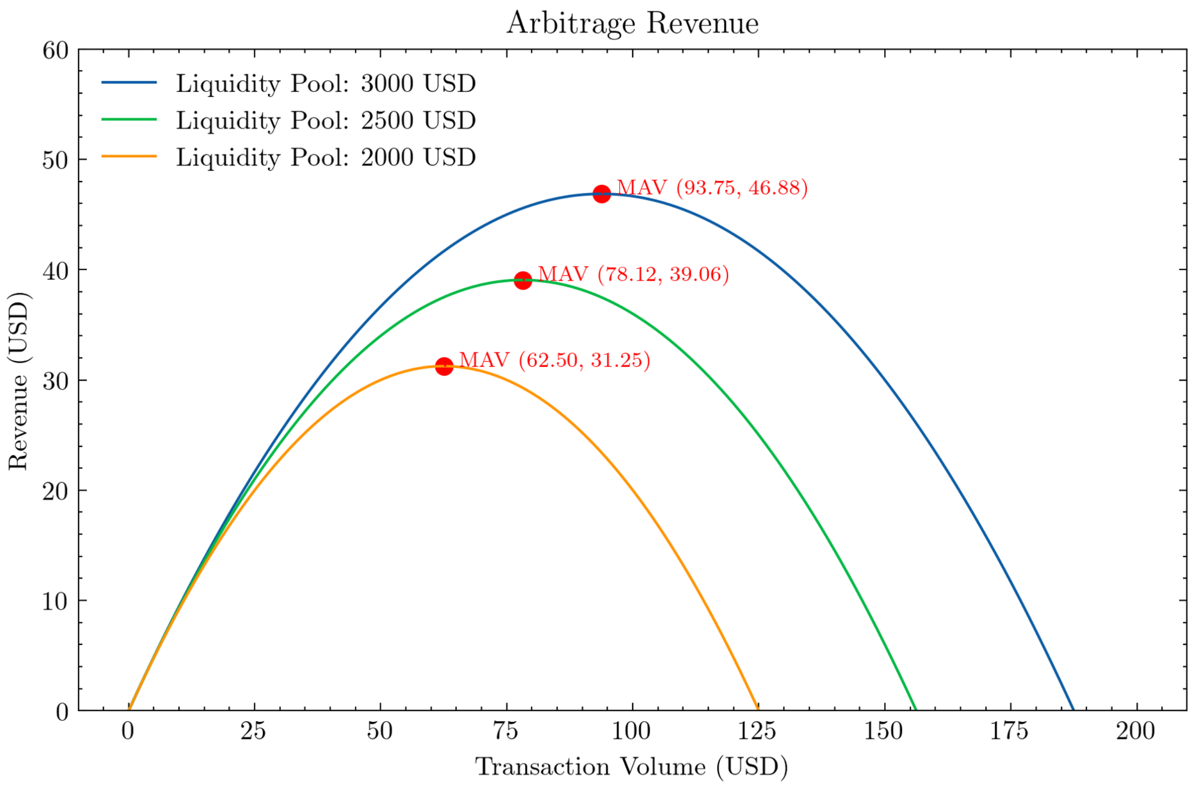
Tokens can be traded on various CEXs, DEXs and blockchains. Not always largest price difference corresponds to the highest arbitrage value.

Arbitrage DEX <> CEX



Arbitrageurs' profits depend on price difference and size of AMM liquidity pool

Volume of Arbitrage Transaction



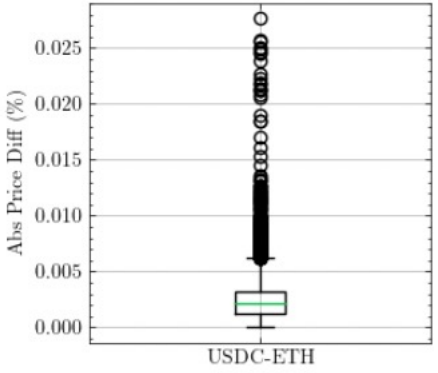
$$V_{max} = \frac{x * (P_a - P_c)}{2P_a}$$

$$MAV = V_{max} \frac{P_a - P_c}{2}$$

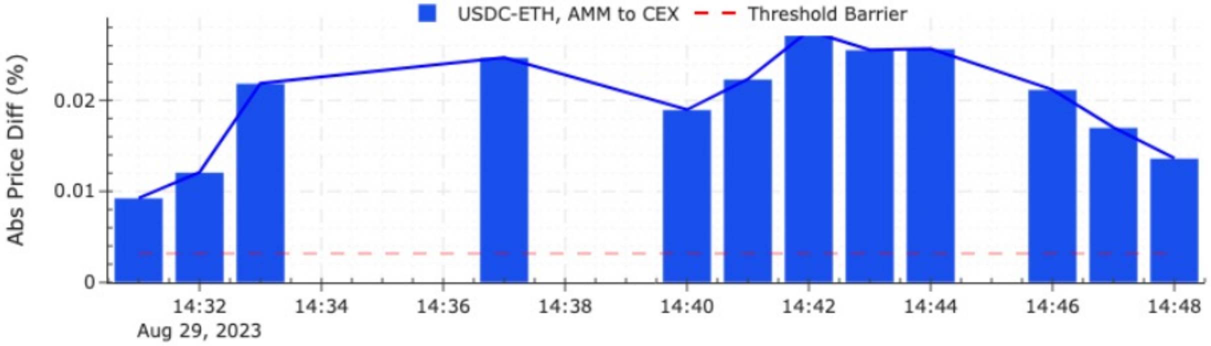
The maximum volume of the arbitrage transaction has a closed formula

Arbitrage Decay Time

(a) Time series of prices for USDC-ETH.

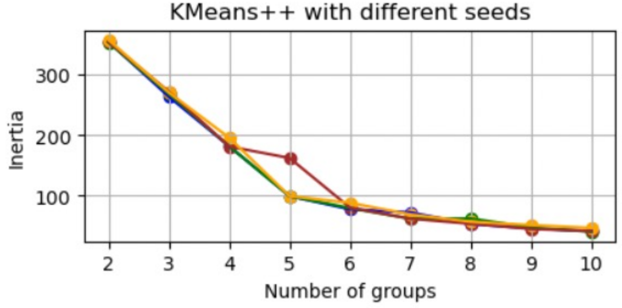


(b) Distribution of deltas.

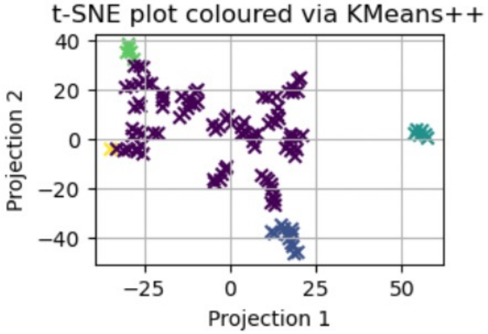


Price differences persists over a few blocks: multiple seconds, sometimes minutes

Factors Impacting Arbitrage



(a) Inertia plot pointing to best clustering.



(b) t-SNE projection of MAV events.

Group	time_decay	clean_MAV	avg_gas	Vmax_on_usage	n_points
0	2176.956522	321.755637	0.254151	27.518744	92
1	320.000000	346.367648	1.068779	19.182464	12
2	1500.000000	2762.368841	0.466423	45.899195	6
3	25032.000000	595.878215	0.166950	26.130199	5
4	180.000000	468.778719	0.821952	598.187780	1

(c) Average features for each cluster identified by KMeans++.

Dep. Variable:	y	**R-squared:**	0.190
Model:	OLS	**Adj. R-squared:**	0.172
F-statistic:	10.44	**Prob (F-statistic):**	8.42e-05

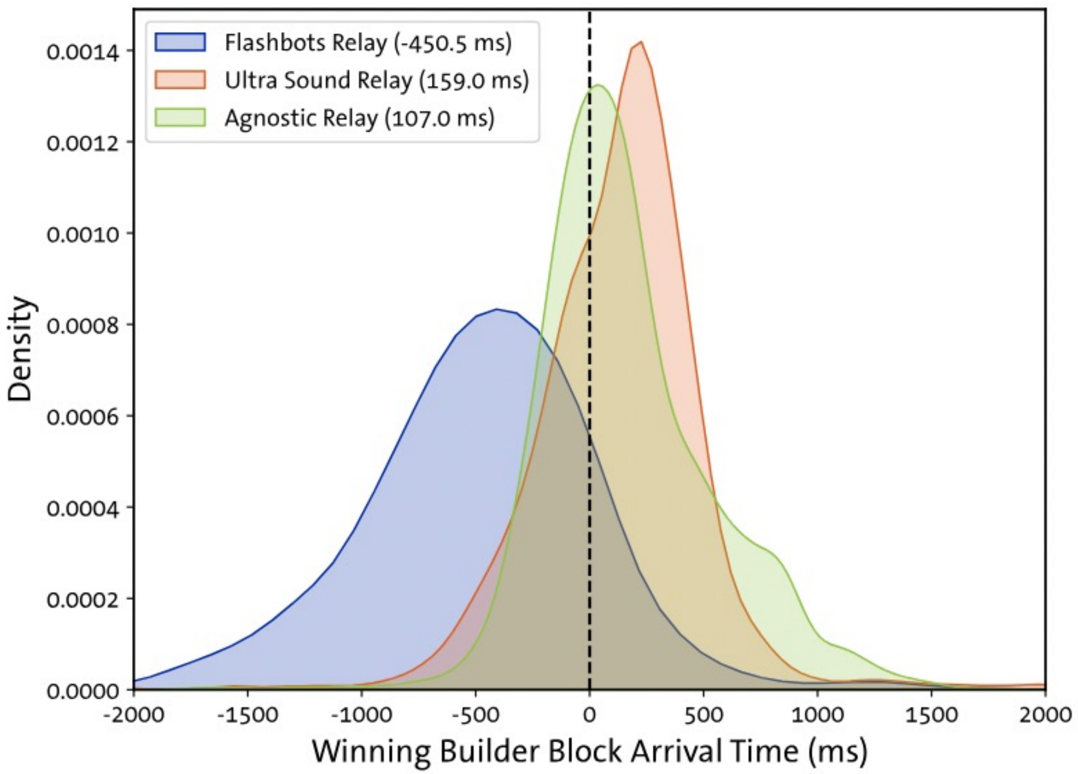
	coef	**std err**	**t**	**P> |t|**	**[0.025**	**0.975]**
x1	-418.7701	277.568	-1.509	0.135	-970.291	132.751
x2	1266.4030	277.568	4.563	0.000	714.882	1817.924
const	-3332.2671	1868.685	-1.783	0.078	-7045.304	380.770

Omnibus:	38.134	**Durbin-Watson:**	1.854
Prob(Omnibus):	0.000	**Jarque-Bera (JB):**	72.444
Skew:	1.682	**Prob(JB):**	1.86e-16
Kurtosis:	5.753	**Cond. No.**	56.0

Arbitrage is an almost risk-free opportunity for profit, arbitrageurs can be interested in collecting it despite its actual magnitude

Other Factors and Risks Arbitrage

- MEV (Maximal Extractable Value)
  - Transaction re-ordering attack within a block, e.g. front-running, for the winner of the MEV boost auction
- Rug-pull Attack
  - Sell off of the token by its creators after pumping its price



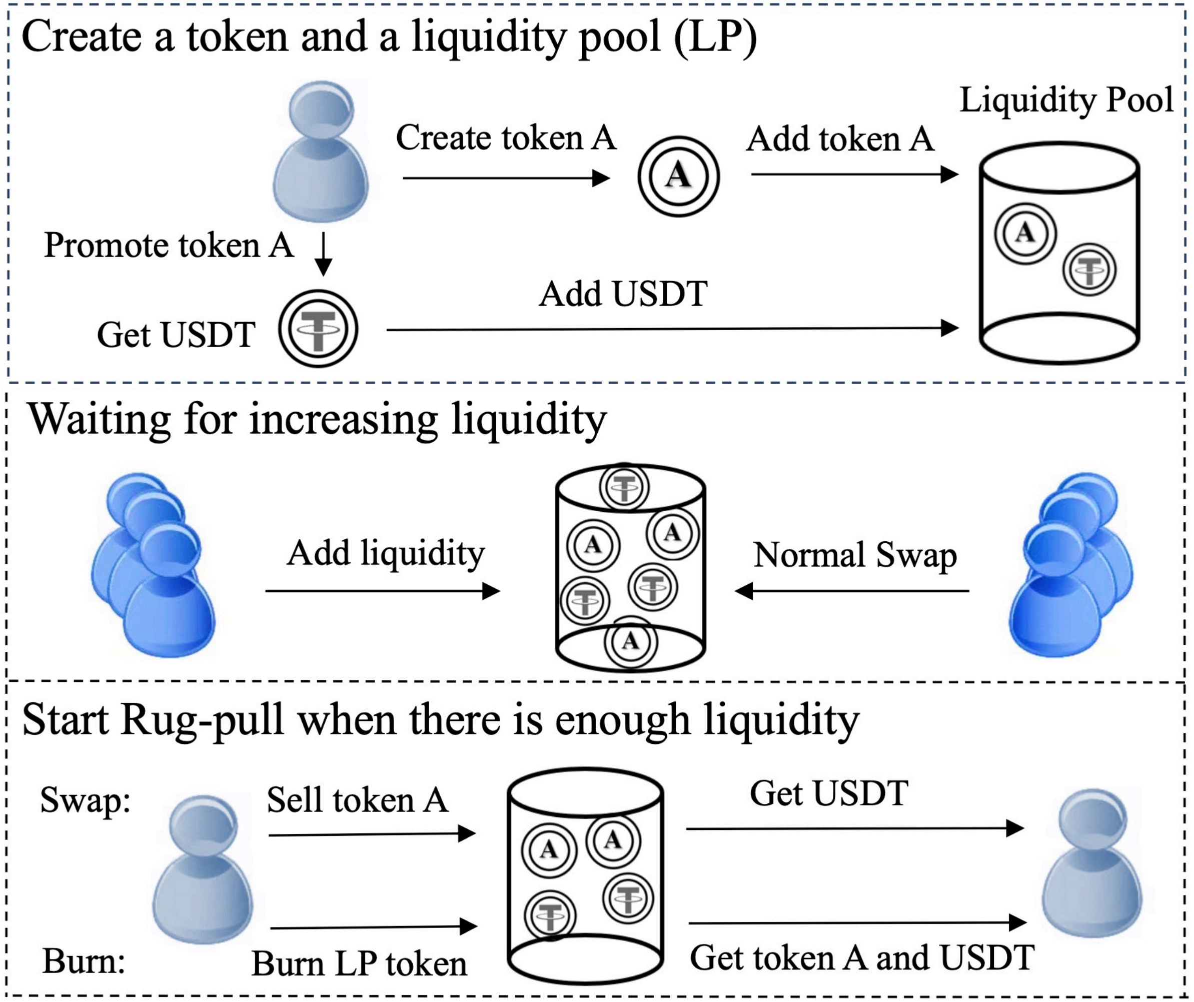
70% of MEV-transaction on Ethereum are related to arbitrage

Rug-pull Attacks

3

Processes of Rug-pull Attack

- Create a new token
  - Create a liquidity pool at DEX with this token
- Build trust to attract liquidity
- Drain the money abruptly
  - Sell your token
  - Close (“burn”) your liquidity position



Methods of Identifying Rug-pull Attacks

- *Step 1* Identify the balance anomaly event through the algorithm.

  balance change ratio r:

  $$r = \frac{\text{balance of a token after a transaction}}{\text{balance of that token before a transaction}}$$

  There is a balance anomaly if ratio < r .

- *Step 2* Optimize r.

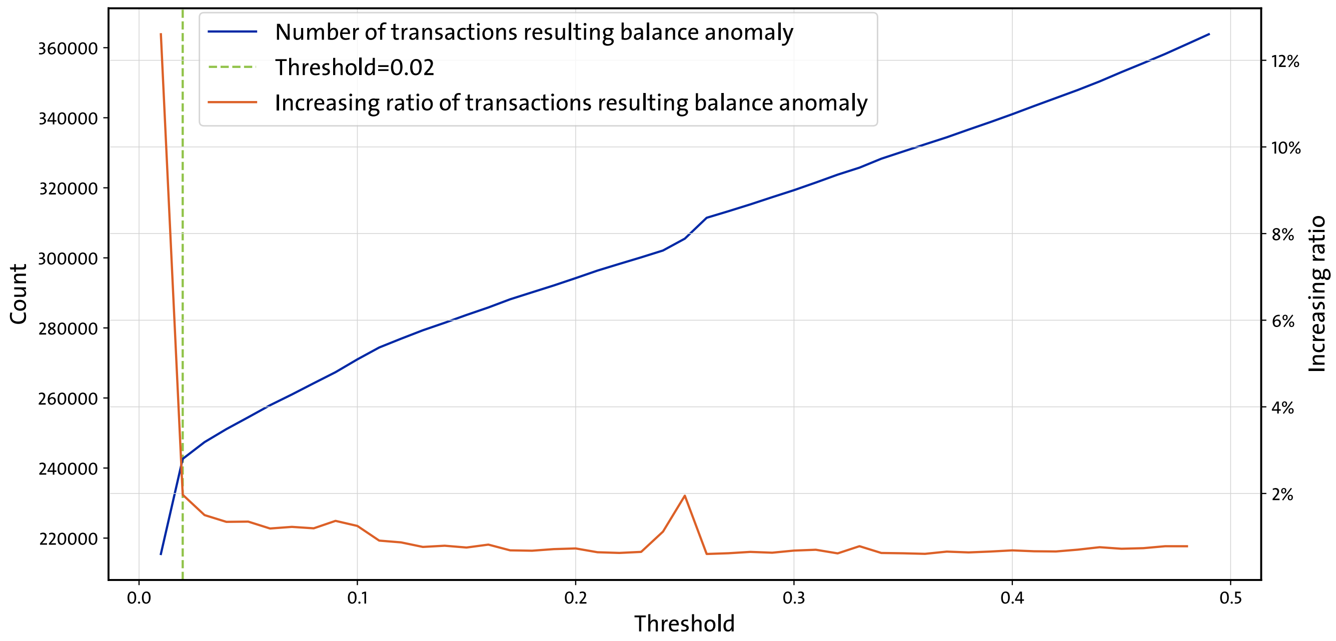
- *Step 3* There is a Rug-pull attack if:

Token creator=pair creator=transaction issuer

Algorithm 1: balance anomaly events detection for each liquidity pool

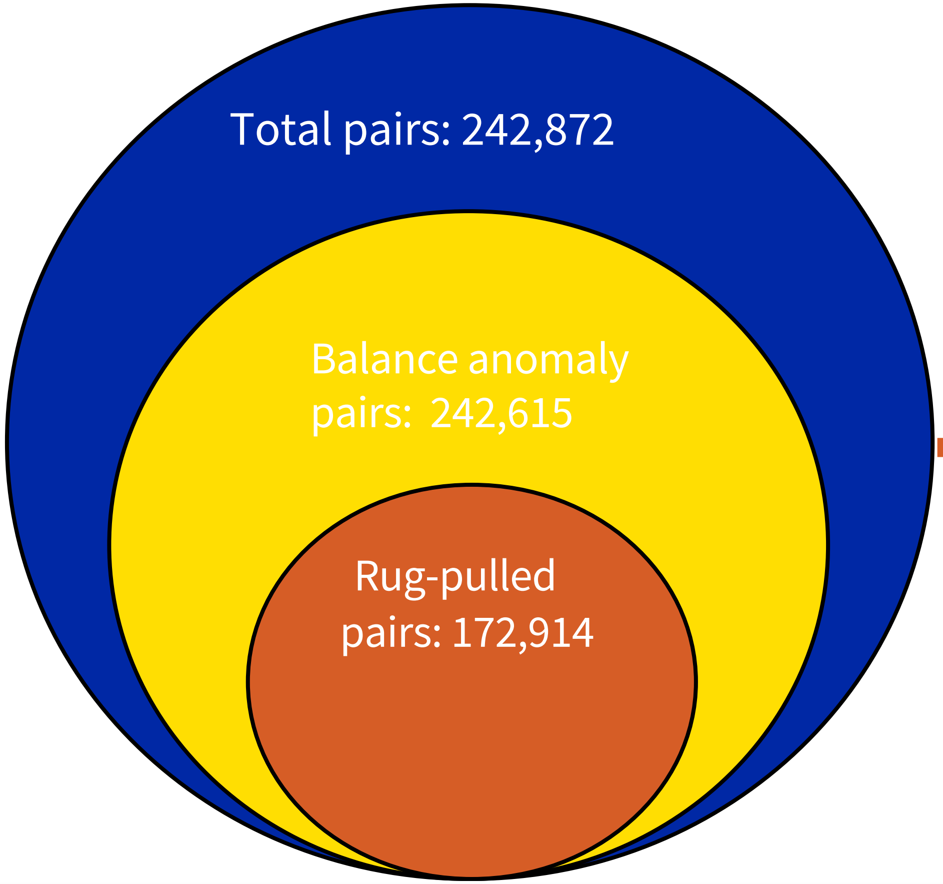
```
Input: Events sorted by time
Output: balance anomaly events events
Parameters: α is the threshold that measures change rate of token1's balance;
Definition: Token1 is one of WETH, USDT, USDC, and DAI for each liquidity pool;
current_amount1 = mint_events[0][amount1_minted];
token1_balance_before = current_amount1;
balance_anomaly_events = [];
for event in events do
    if event is Swap then
        token1_balance_after = token1_balance_before − amount1Out;
    else if event is Burn then
        token1_balance_after = token1_balance_before − amount1_burned;
    else
        token1_balance_after = token1_balance_before + amount1_minted;
    token1_balance_change = token1_balance_after/token1_balance_before;
    if token1_balance_change <= threshold then
        balance_anomaly_events.append(event);
return balance_anomaly_events
```

Parameter Optimization



The number of price anomaly events has the largest increasing speed when threshold equals 0.02

Result summary



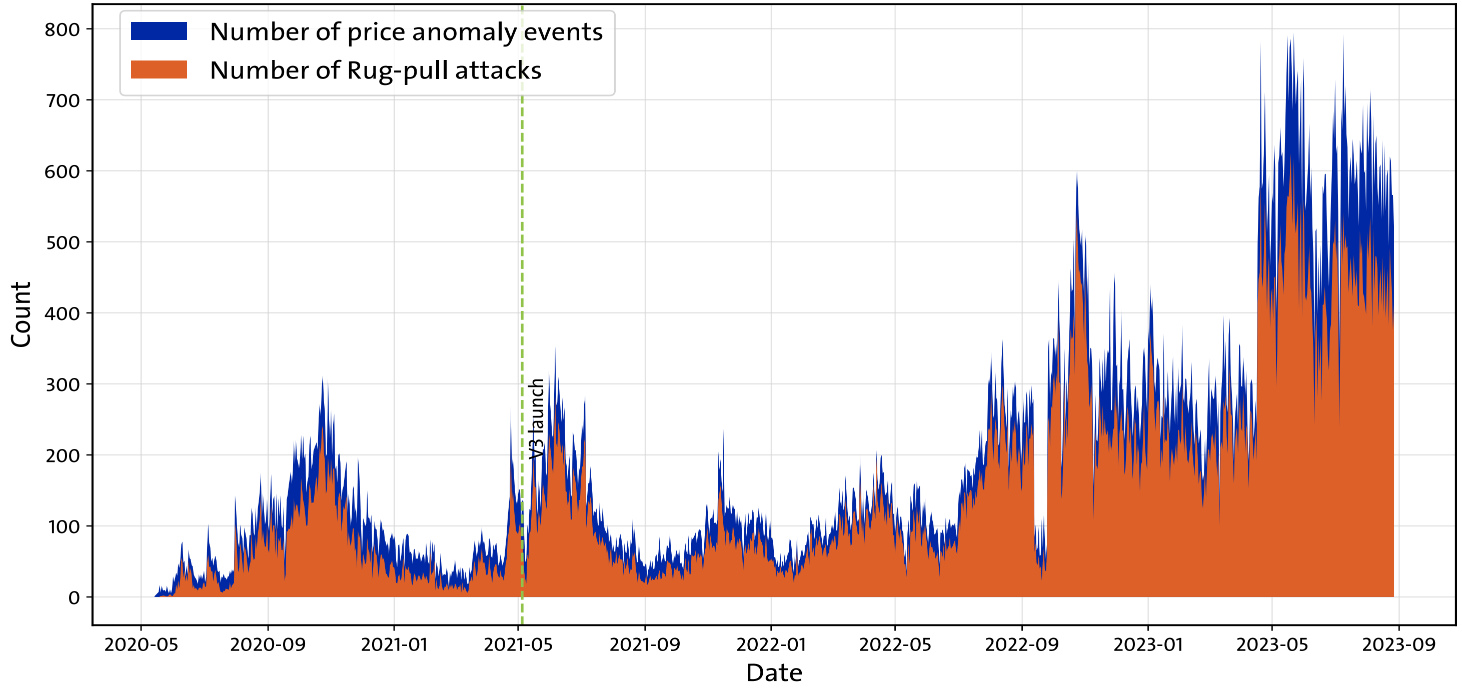
242,381 balance anomaly events

179, 640 Rug-pull attacks

154, 212 Rug-pull attackers

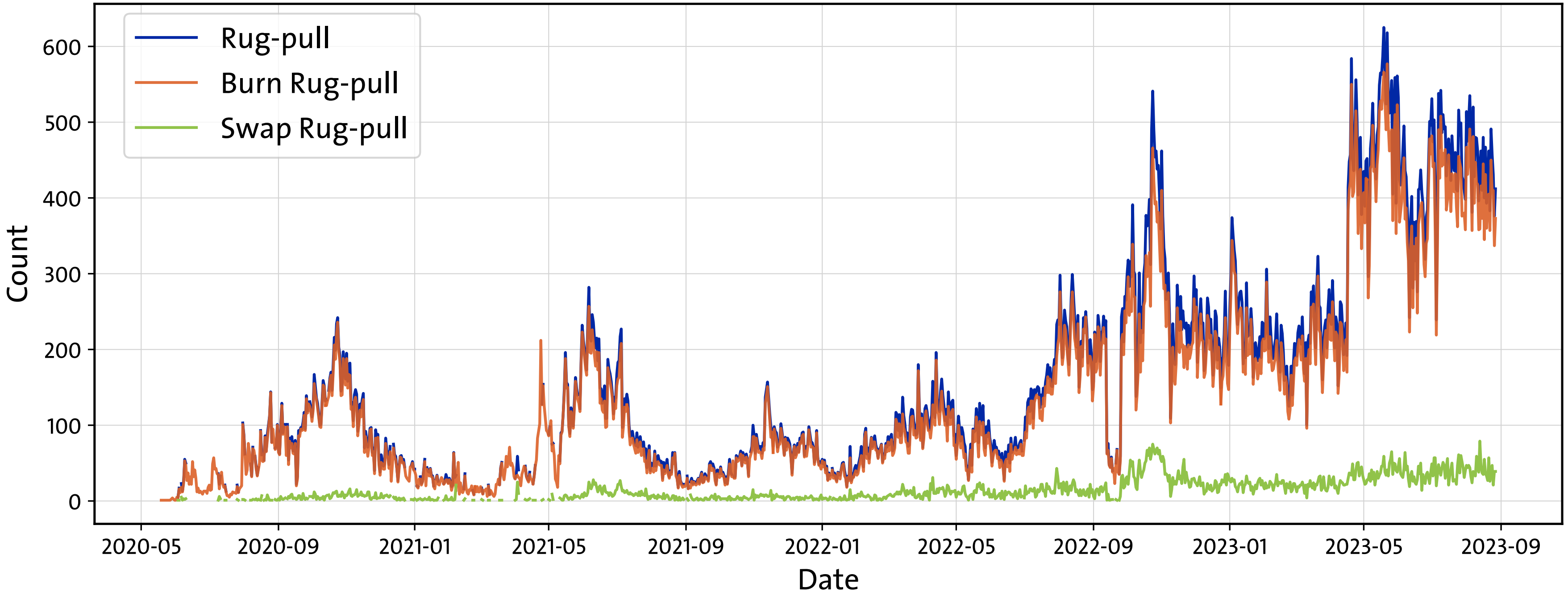
71.2% liquidity pools experienced Rug-pull attacks

Rug-pull Attacks Over Time



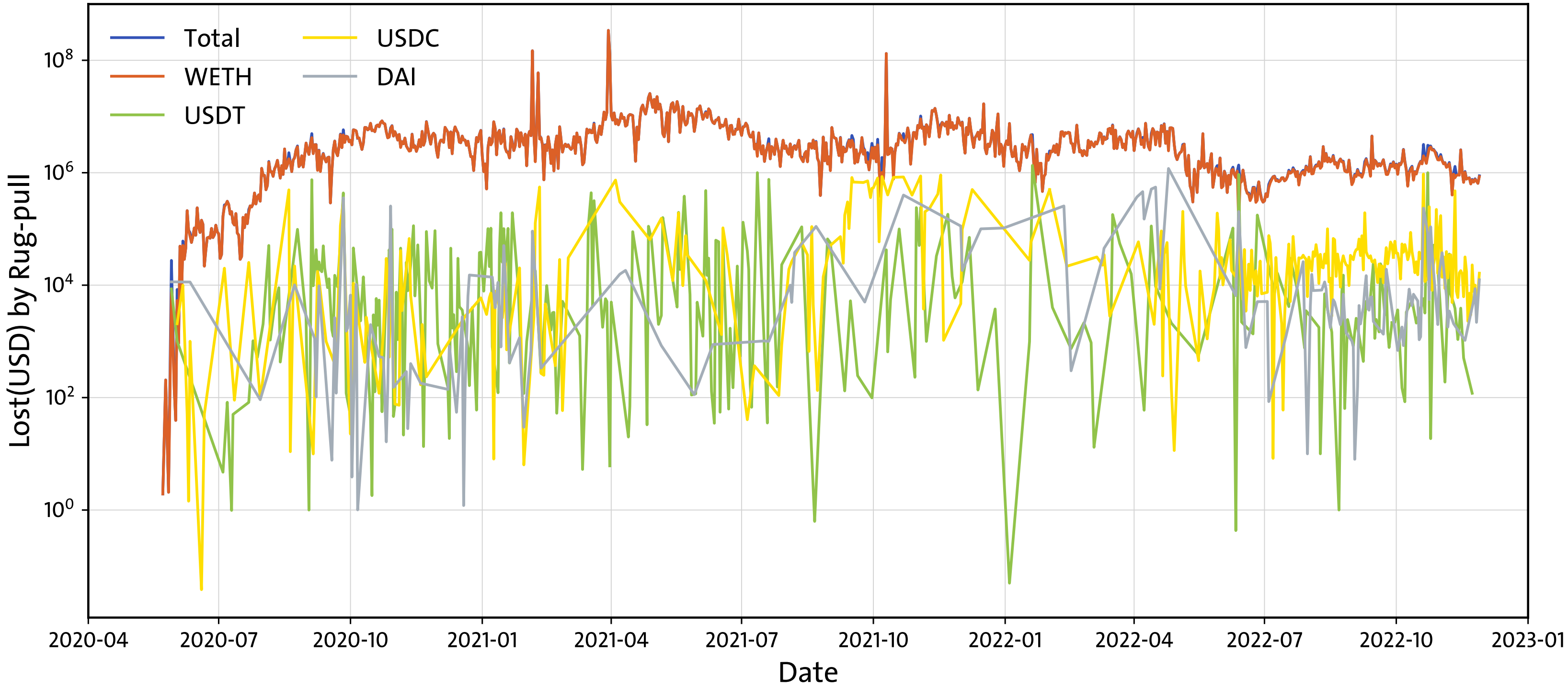
The number of daily rug-pull attacks shows a general upward trend on Uniswap V2, even with further notable increase after the launch of Uniswap V3.

Types of Rug-pull Attacks



Most of the Rug-pull attacks are the Burn Rug-pull attacks, while a small portion are the Swap Rug-pull attacks.

Rug-pull’s Effect on TVL



Rug-pull attacks result a large mount of TVL lost from Uniswap, around 4.5 million USD each day are lost by Rug-pull attacks.

Conclusions

4

Centralization patterns of Uniswap network

Despite its decentralized nature, the Uniswap market has shown Centralization patterns in terms of degree distribution, TVL centralization, and core-periphery structure.

More arbitrage opportunities with the longer path

The longer the cycle length, the more opportunities for profitable arbitrage.

Rug-pull attack is common on Uniswap

72% liquidity pools experienced Rug-pull attacks, and around 4.5 million USD each day are lost by Rug-pull attacks.

Contact

Prof. Dr Claudio J. Tessone

Professor of Blockchain & Distributed Ledger Technologies
UZH Blockchain Center, Chairman
+41 44 634 92 61
claudio.tessone@uzh.ch