IX Swap - Uniswap pools behavior analysis

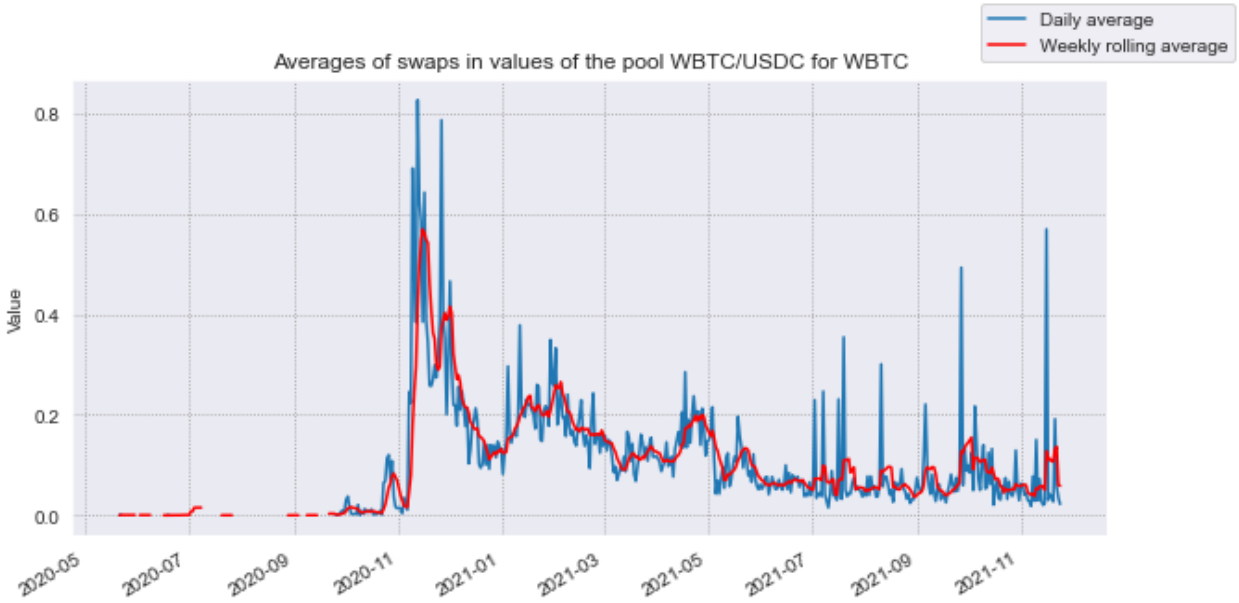
Introduction

Situation on the cryptomarket differs from one token to another, requiring analysis of the popular and long-living pools of the tokens from different industries that have different recognition on the market. For that current report contains information about 3 pool types:

- Classic tokens, representing popular blockchains, coins representing USD dollar equivalent, or business startups with blockchain;
- NFT, representing different platforms and areas;
- Meme-tokens, that are created as a market reaction to some important event, person, or to some joke. Those ones have the least predictable markets.

Pools analysis

WBTC/USDC



Picture 1: WBTC swapping in operations in the WBTC/USDC pool

Pool life cycle is characterized in most of the cases by an unclear picture in the beginning of the pool because of low trust and low interest of traders in the pool, after which comes a period of trades rise with further decrease of activity with stabilization of trades. Presented pool values distribution greatly demonstrates this concept. Another factor influencing the trades and required to review is price of involved tokens in the pool and in this case it is required to consider Bitcoin price distribution. For more comfortable and comparable price distributions

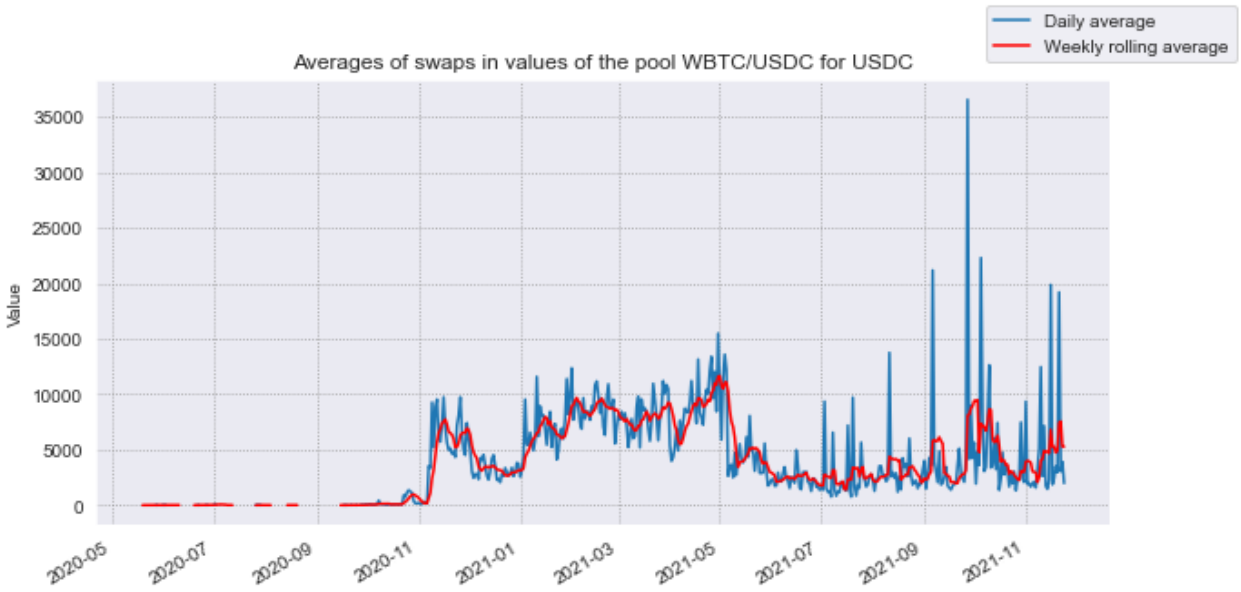
charts it is required to review token prices relative to US dollars taking into account that Uniswap recalculates prices, capitalizations and other trade metrics to US dollars.

Picture 2: BitCoin price distribution in the WBTC/USDC pool

Looking at the swapping in distribution of the WBTC keeping in mind the WBTC price distribution explains a lot about traders behavior. For example, the extreme rise of swapping in operations with WBTC in the time interval between November 2020 and March 2021 is caused by a great BitCoin price rise. The interesting moment is that the pool price for BitCoin is almost exactly matching the distribution that was registered on the market, meaning that pool token price distribution converges to the general-market price distribution with small deviations. Considering the rise of the BitCoin price many traders decided to change their BitCoins into USDC. After the “hot” trading moment, when extreme price rise caused extreme swapping in rise, traders were still trading WBTC higher compared to previous periods while the BitCoin price was rising. After March 2021, when BitCoin price stabilized, the traders behavior changed to lower swapping in operations, causing traders to keep their tokens waiting for better prices.

Picture 3: CoinDesk BitCoin price distribution chart

Distribution of the USDC swapping in operations also has a great rise during BitCoin price rise and has stabilized after first BitCoin price stabilization and second BitCoin price decrease. Small rise of swapping in operations for both USDC and WBTC in the September-November 2021 period was also caused by rise of the BitCoin price



Picture 4: USDC price distribution in the WBTC/USDC pool

The same rise of the token price caused a rise in the reserves of the WBTC/USDC pool. Conform distribution can be seen that the best part of the WBTC/USDC lifecycle was registered between November 2020 and May 2021. Liquidity providers get some profits from rising pool reserves, which explains reserves distribution: traders decided to take a max profit out of rise of the transactions frequency and values, removing their financial resources when pool behavior became less attractive for them.

In the previous graph the token price conform reserves daily updates distribution looks similar to the real-price distribution, but each swap has its own token price based on the current pool reserves value. There are many transactions happening during the day, changing reserves after each transaction, meaning that each transaction causes a price shift and reserves shift. Considering that, it was decided to perform a price distribution analysis of the estimated price per swap operation.

How to estimate the swap operations prices and find their increase rates

There are two data fields that will be used in analysis - amount_in and amount_out. Can be applied a formula using those data fields to find current token price:

$$Current\ token\ price\ = \frac{amount\ out}{amount\ in}$$

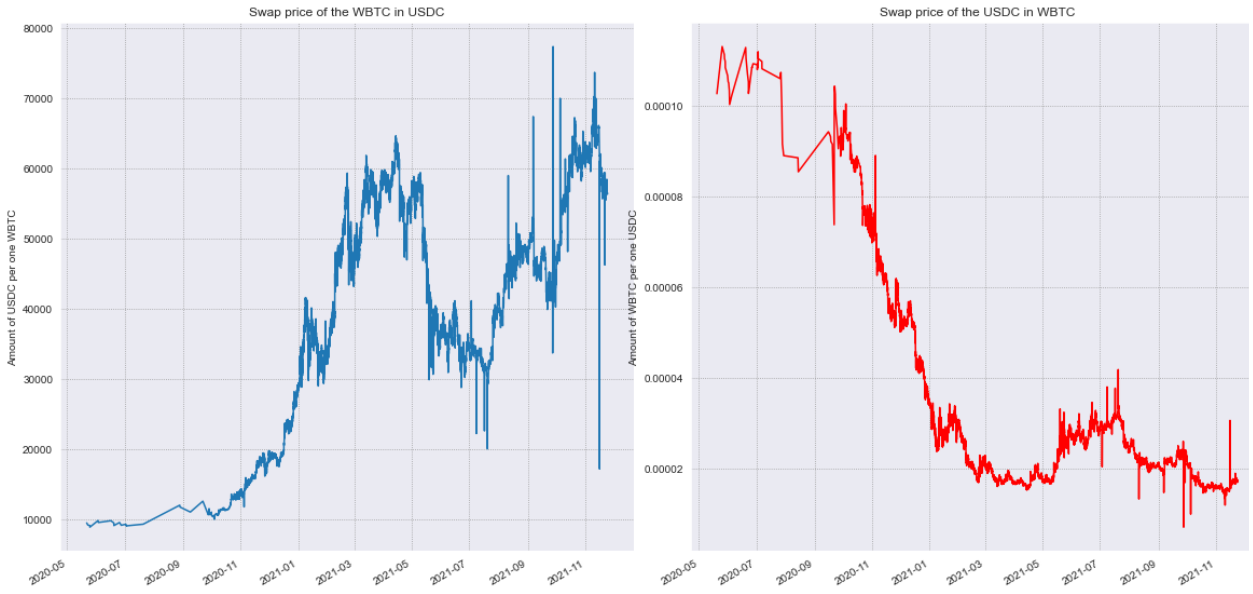
The *current token price* is representing the token_in price in the token_out equivalent. Using this method for each transaction can be found the current token price that was calculated on the Uniswap platform. Knowing current token prices can be found price change rate, which can be important in constructing prices change rates, using the formula:

$$Token\ price\ change\ rate\ = \frac{current\ token\ price - previous\ token\ price}{previous\ token\ price}\ *\ 100\ (\%)$$

Token price change rate will be represented in percentages.

How swap operations prices distribution differs from the reserve-based token prices

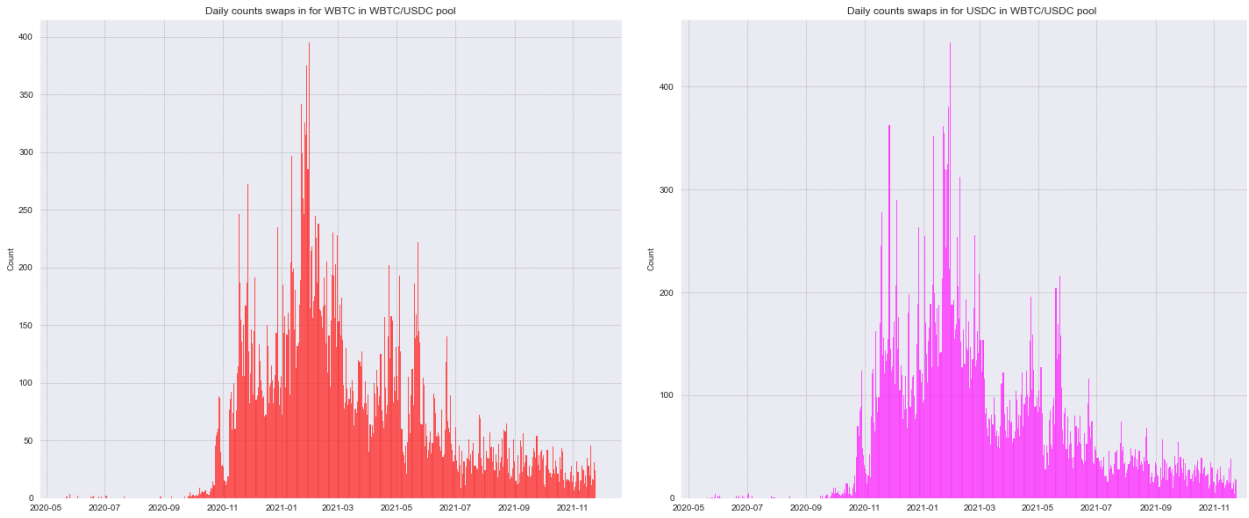
After visualizing the token price, estimated conform swap operations can clearly be seen the difference between reserve-based token prices and swap-based ones.



Picture 5: Swap price distributions for WBTC/USDC

Comparing the presented WBTC swap prices chart with WBTC reserve-based prices chart, it is observable that swap-based prices are a more ‘noisy’ analogue of the reserve-based ones. It happens due to the daily price changes happening because of exchange operations and that pool adapts to the current situation on the market. “Smoothing” the line will create an almost identical chart to the reserve-based one.

Daily prices deviations are different: in one cases the deviation is small (for example, the WBTC swap price deviation is smaller until May-June 2021) and in other there are anomalous price rises and drops (like August-November 2021 WBTC swap price changes). Keeping in mind swaps values can be observed that great price deviation is happening during low activity periods in the pools. The Authors’ opinion is that this phenomenon is happening due to the presence of the balancing algorithm during high-activity periods (TWAP-based one). To ensure that low swapping values in the picture 4 chart is explained by decrease of swapping operations below is presented the swap operations count histograms.

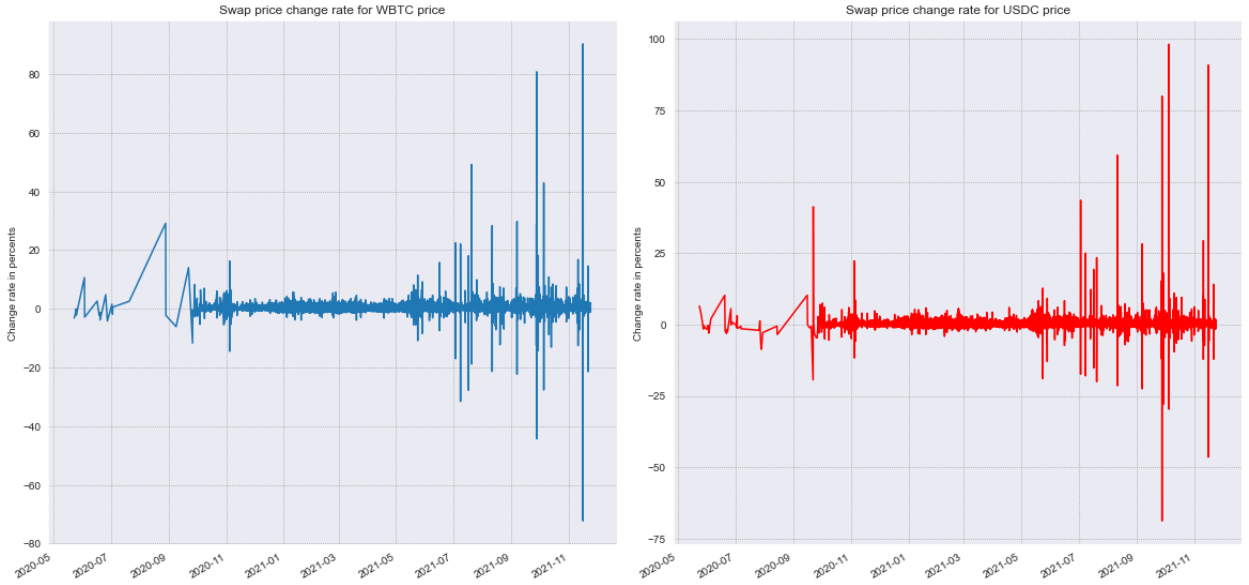


Picture 6: Daily swaps count distributions for the WBTC/USDC pool

The transactions count is almost identical to the transaction values per timestamps in the picture 4 graph, ensuring previously estimated theory and raising up the assumption about destabilization of transactions in low-activity periods.

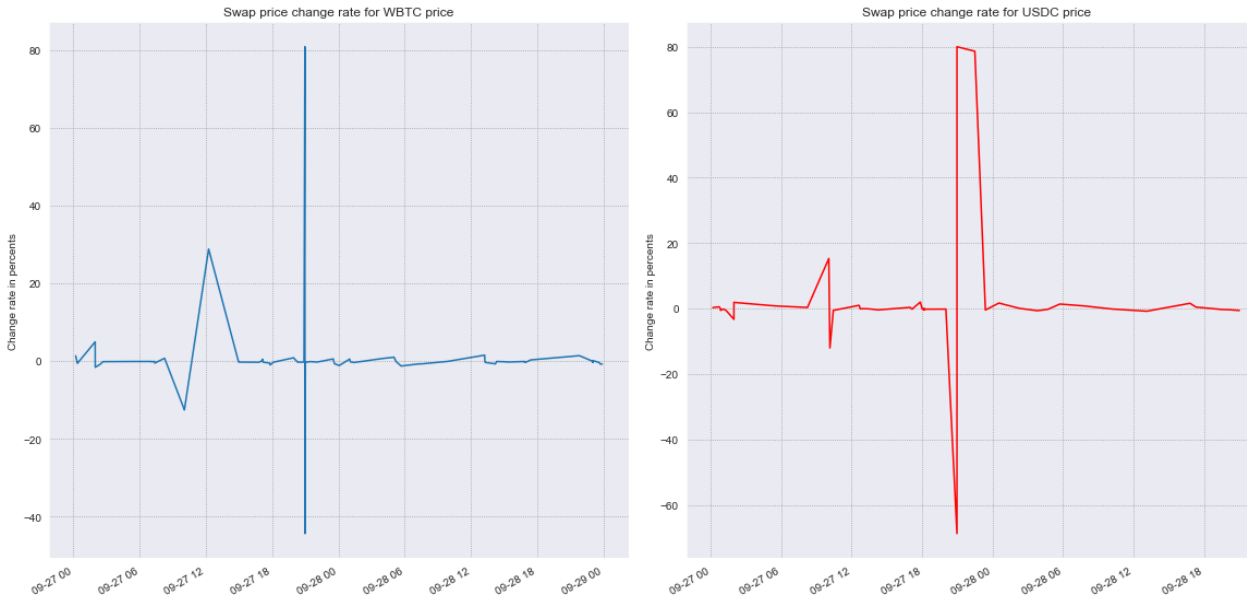
Strange moment or possible attack on the market (MEV)

To check how price deviation looks from the change rates perspective, the change rates distributions are presented below.



Picture 7: swap-based prices change rates distributions for the WBTC/USDC pool

During visual analysis authors were interested in a closer look into the period, when price change rates were around 60-80% (it is a too high price change), and authors created additional charts with closer look into 27-28 September 2021.



Picture 8: Swap-based price change rates for 27-28 September 2021 for the WBTC/USDC pool

Drop and next rise of the token price caused authors to pay attention to this situation.

	token_in	token_out	amount_in	amount_out	amount_usd	timestamp	first_to_second_price	price_change_rate
65603	USDC	WBTC	6000.000000	0.138634	6005.143255	2021-09-27 20:01:41	0.000023	220.049757
65607	WBTC	USDC	0.006960	297.845610	297.760491	2021-09-27 20:53:21	42791.511683	-44.694234
65608	USDC	WBTC	12797.000000	0.092386	12787.458570	2021-09-27 20:58:07	0.000007	-44.455047
65609	USDC	WBTC	976323.861321	12.689636	975595.915259	2021-09-27 20:58:07	0.000013	-44.027899
65610	WBTC	USDC	12.689636	981830.211723	981098.160132	2021-09-27 20:58:07	77372.604033	79.600818
66006	USDC	WBTC	5875.205194	0.059231	5878.316962	2021-10-05 09:00:00	0.000010	-49.563526

Picture 9: Swap transactions history fragment, covering presented rise and drop of the token price with strange pattern

Conform presented fragment can be seen transaction nr. 65608 where trader requested exchange of 12 797 USDC to WBTC. BitCoin price for 28 September is 42 247.36 USD. The reserve-based BitCoin price is almost the same (considering that USDC is a stable coin representing USD analogue on the crypto market and that pool balance converges to the real-market situation), but trader got 0.092386 WBTC instead of around 0.3 WBTC, which is ⅓ out of the real-price and around 6-8 thousand USD loss. The next operation changes almost 1 million USDC to the WBTC, getting 12.689636 WBTC and right after that performing reverse

operation, changing 12.689636 WBTC to USDC. As a result of those two operations, the trader got almost 6 thousand dollars profit, which is similar to the sum lost by the previous trader.

One important highlight is that by extracting the historical data through the uniswap subgraph, only the transaction timestamp is available (which is the same for all transactions within a block), meaning that the execution order of the transactions inside the block is lost. Because of this, these transactions were checked manually on Etherescan in order to get their execution order.

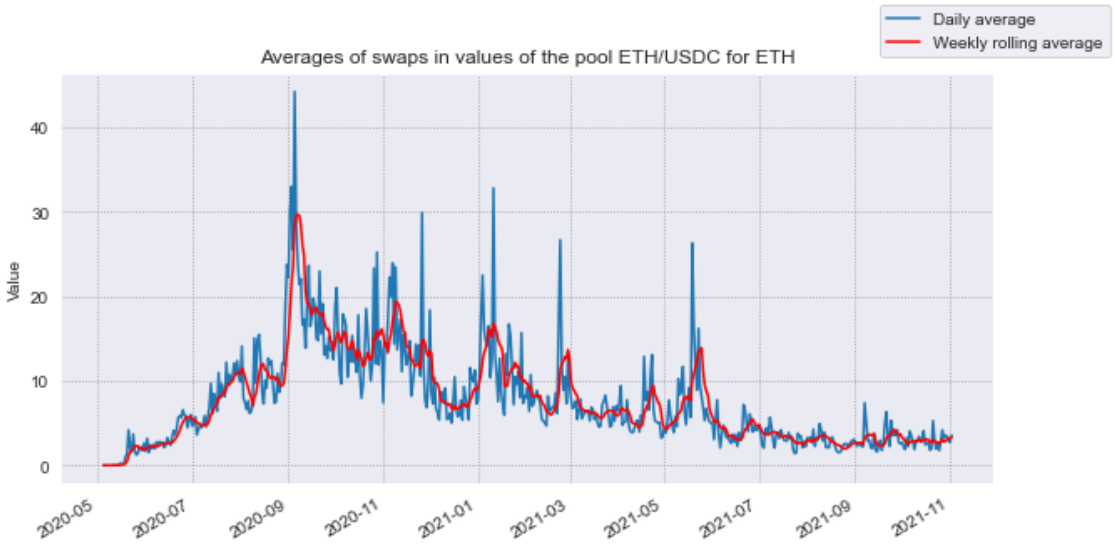
Picture 10: transaction history from Etherscan about possible MEV attack

Here (t1, t2, t3), it can be observed, how the swap transaction of the user got 'sandwiched' by the MEV-bot transactions. The execution order that would allow making the profit is ensured by bundling the transactions together (including the one sent by another user) and setting a high fee. This vulnerability cannot be exploited when the slippage parameter for the swap transaction is set or the reserves of the pools are very big (as it would require an extremely large transaction to cause a significant price impact).

This attack happened, due to the situation when the trader requested a too high transaction value compared to the available reserves in the pool. Conform reserves data for the current pool requested transaction is around ⅔ of available USDC token reserves in the pool, meaning that trader caused a strong change in token balance and therefore price.

ETH/USDC

The distribution of the ETH/USDC pool is more clear and readable, considering that distribution from the start has a great transaction frequency. Ethereum swapping in operations has a more stable and readable distribution compared to the WBTC one.



Picture 11: ETH swapping in distribution in ETH/USDC pool

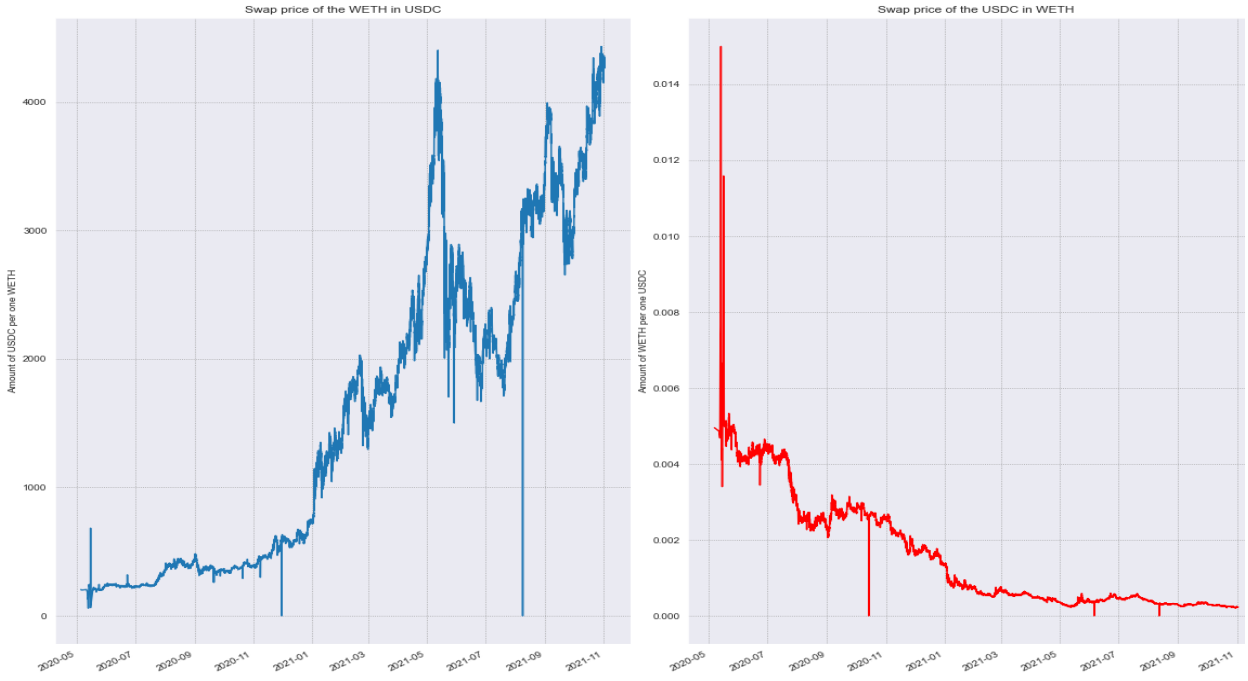
The Ethereum price in the WETH/USDC pool has a similar positive trend as WBTC price distribution, but relative rise and drops are much stronger in the current case. Percentage of changes is much higher.

Picture 12: WETH price distribution for WETH/USDC pool

Changes in the price of Ethereum inside WETH/USDC pool has the same rule as changes of the BitCoin price in WBTC/USDC pool - distribution of token price inside the pool converges to the general-market Ethereum price.

Picture 13: CoinDesk Ethereum price distribution

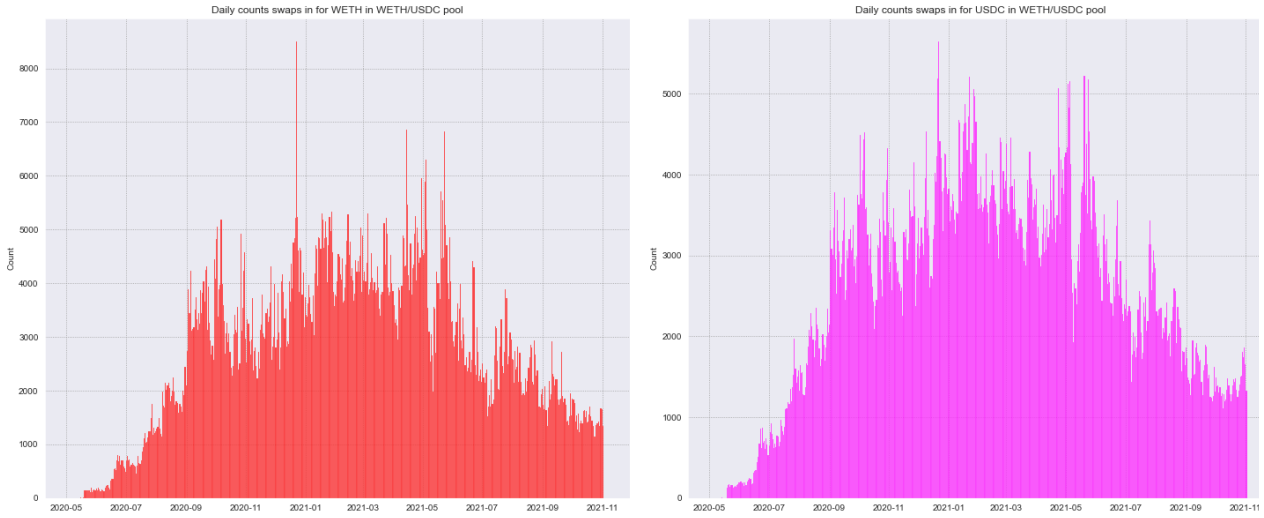
Comparing Ethereum price based on the reserves balance can be seen that there is a distribution similar to the real-market one. Considering that the previous pool had a big price deviation it was decided to compare swap-based prices with reserve-based ones.



Picture 14: swap-based price distributions for WETH/USDC

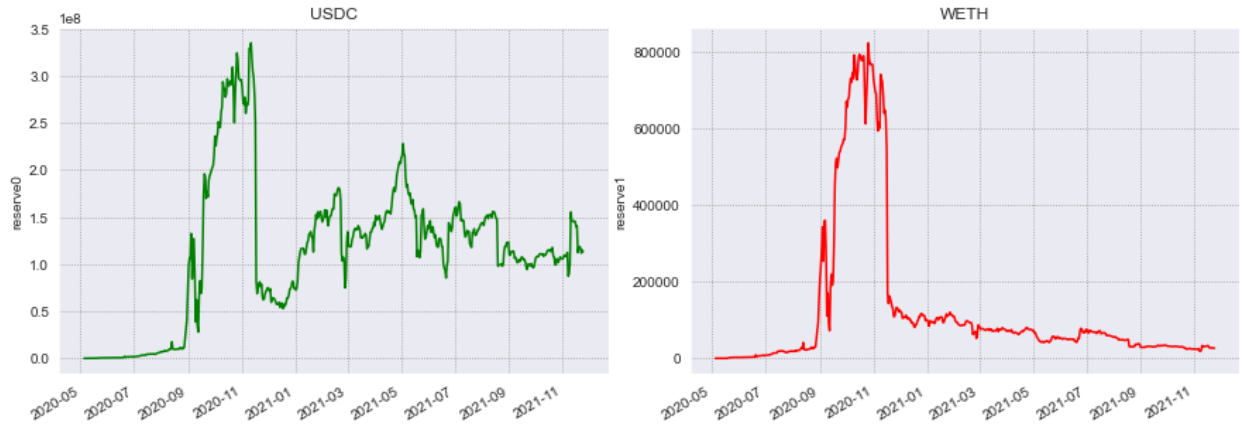
Price drops present in both charts are python errors that appeared during division processes, causing incorrect deviations present on the charts. Ignoring this error, there is still an observable high deviation of the price, but distribution is more stable compared to the previous case of WBTC/USDC pool. This difference can be explained by the higher transaction frequency and its distribution that is relatively high over the entire present time period. This causes more

stable and efficient work of the balancing algorithms, used to control transactions and reduce possibility of market destabilizing.



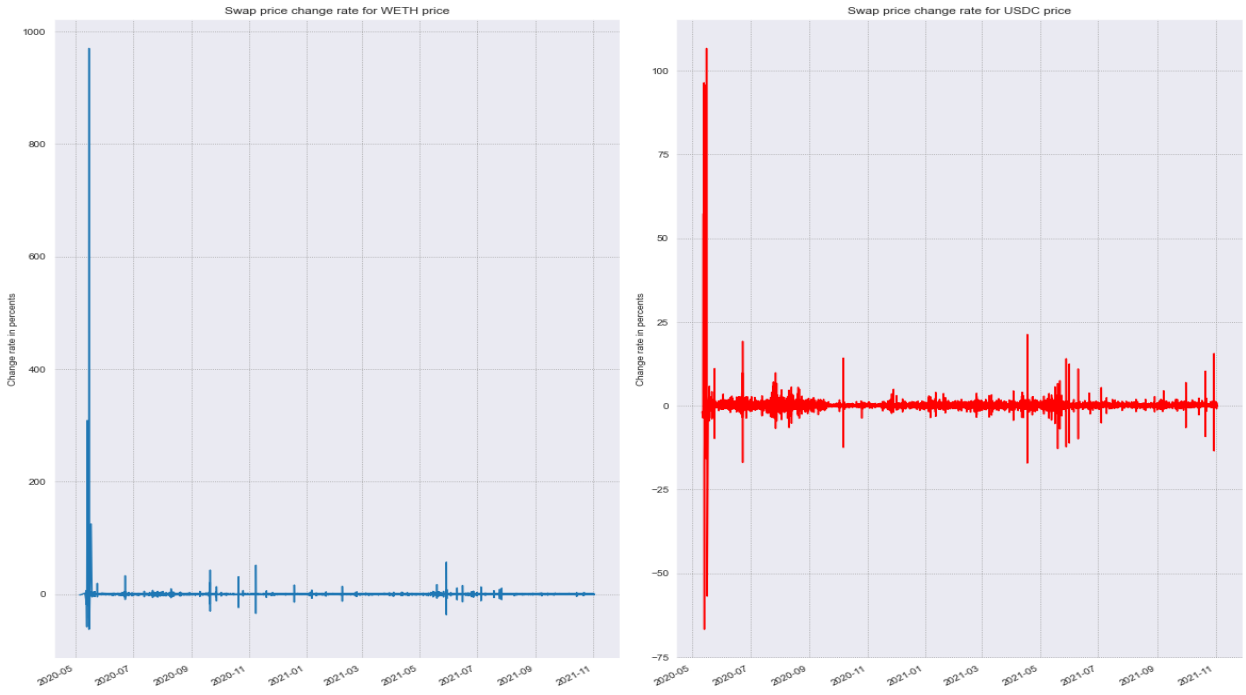
Picture 15: swaps count distribution

Compared to the WBTC/USDC pool there is only an initialization stage low activity period. It correlates with small reserves in the beginning of the pool lifecycle and only after September 2020 rise of reserves caused a rise in traders activity and therefore financial requirements required to perform MEV attacks are much higher.



Picture 16: Reserves distribution in the WETH/USDC pool

The distribution of the pool reserves has relatively higher values compared to the WBTC/USDC distributions. USDC reserves have high values and their distribution is more stable compared to the WBTC/USDC pool, there are higher values through the entire period and transaction frequency is higher, making it possible to set a TWAP-based mitigation mechanism control.

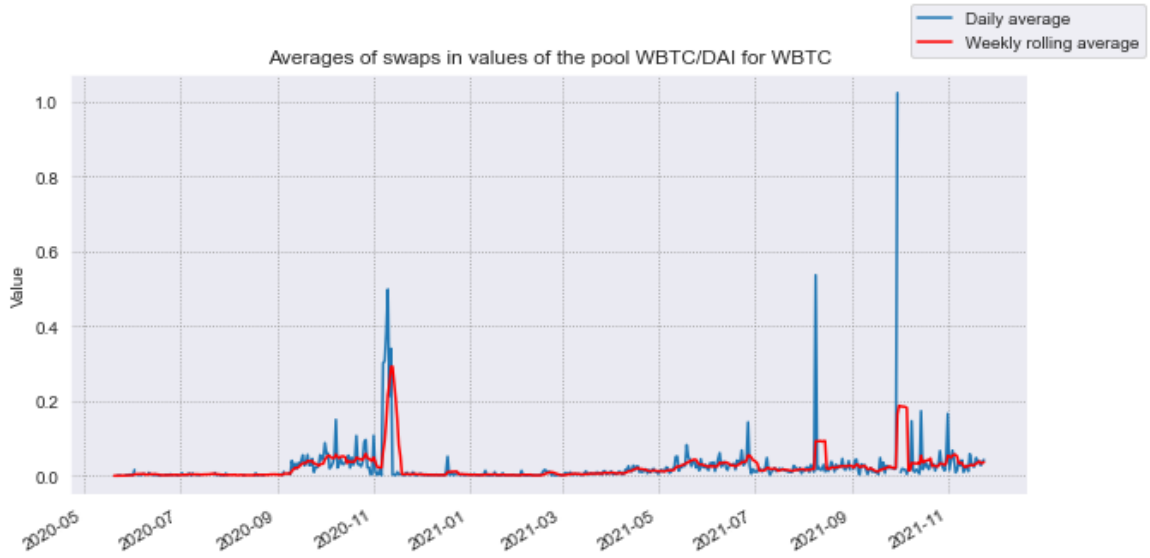


Picture 17: Swap prices change rates distributions for the WETH/USDC pool

In the beginning of the pool lifecycle there are present high changes in the token price, considering that pool activity is not balanced and there are still present high deviations, considering that users converge price distribution to the one presented on external markets and reserves are low meaning that sensitivity of those tokens prices is much higher. It is important to note that presented distributions were filtered from possible error deviations caused by python division results.

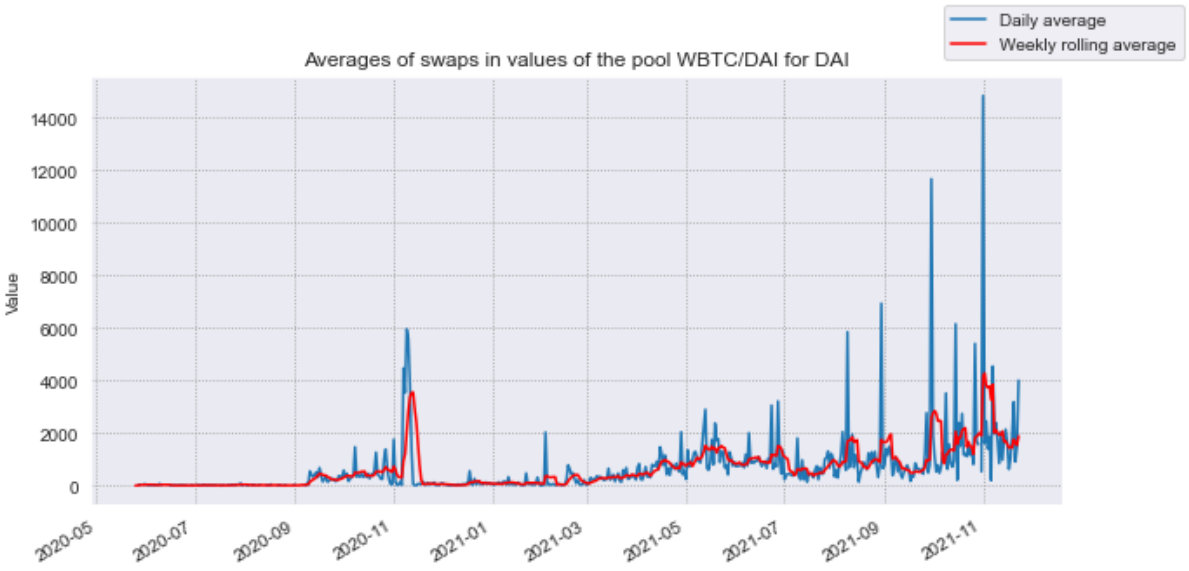
WBTC/DAI

Previously was reviewed behavior of the WBTC/DAI pool, containing USDC stablecoin. To show how different behavior can be in two different pools can be used a pool whereas stablecoin is used DAI token.



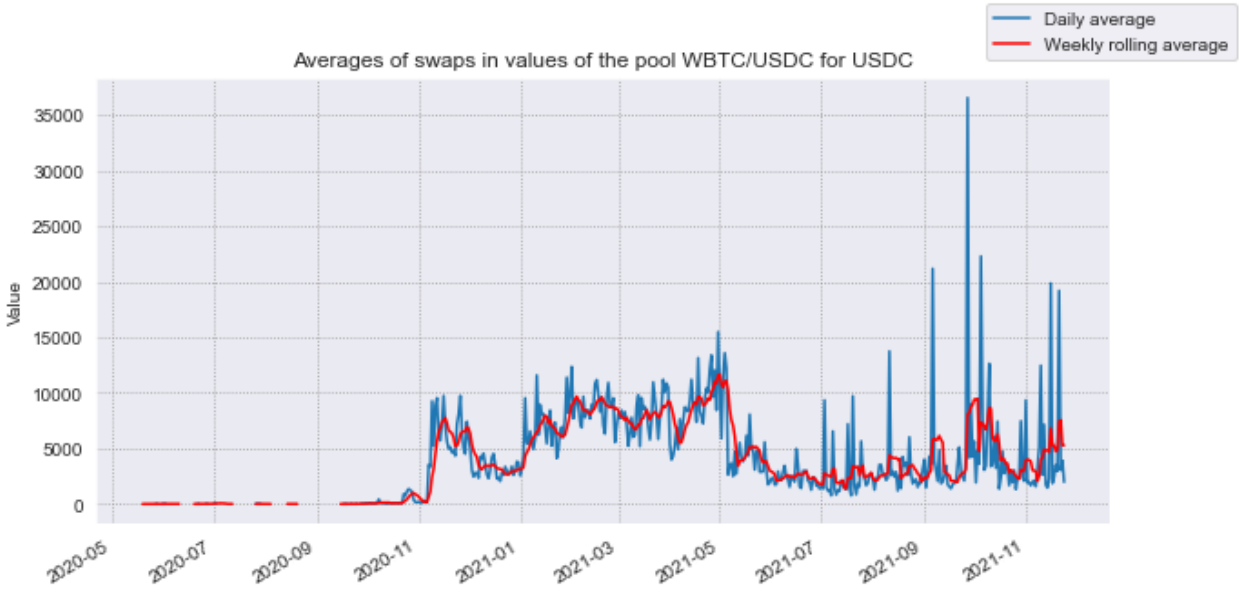
Picture 18: Swaps distribution in the WBTC/DAI pool for WBTC

The distribution of the swaps inside WBTC/DAI pool has a low activity even considering the price of WBTC. Daily values are not overcoming barriers of the 0.1 WBTC, meaning that daily swaps are not overcoming the 4-6 thousands of USD dollars, while WBTC/USDC pool had values overcoming 0.1 barrier and multiple cases of overcoming even 0.2 WBTC (and many cases of higher values). Current distribution has only two small periods of higher activity, reaching to the 0.2-0.4 WBTC during September-December 2020 and August-October 2021, corresponding to BitCoin price rise during respective periods.



Picture 19: Swaps distribution in the WBTC/DAI pool for DAI

DAI distribution of the daily swaps is not representing high activity of the pool. There are small rises happening during the rise of the BitCoin token price on the market, but the highest activity periods are not reaching medium activity values from the WBTC/USDC pool for USDC swaps.

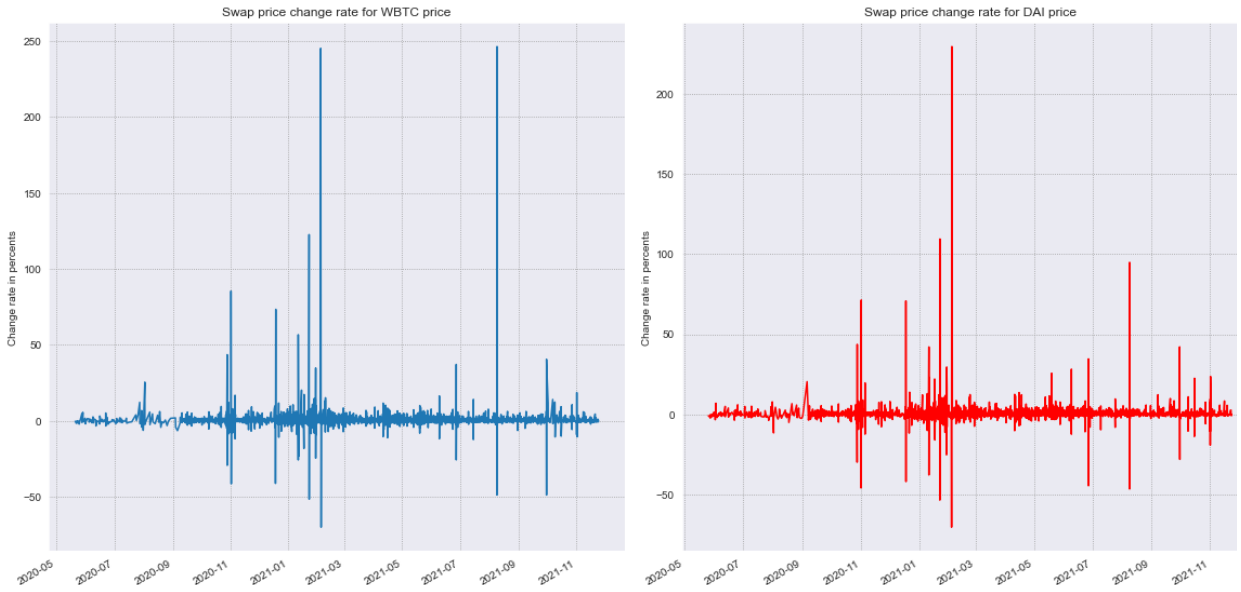


Picture 20: WBTC/USDC swaps distribution for USDC

Comparing these two pools activities can be seen how lower is activity in the WBTC/DAI pool, explaining extreme rises and drops in the swap price distribution.

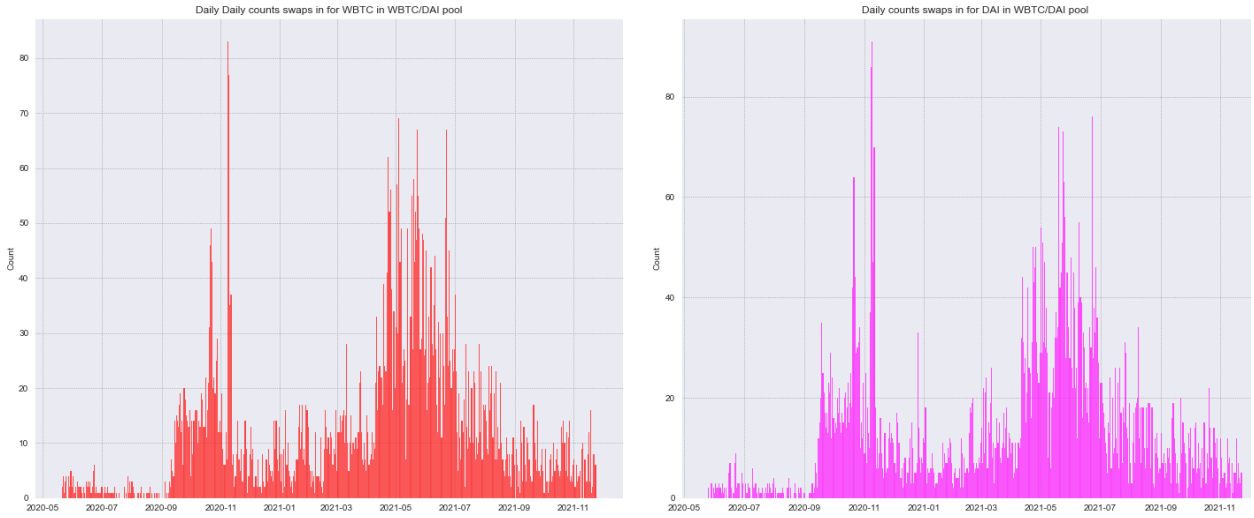
Picture 21: WBTC/DAI swap prices distribution

WBTC swap price distribution and DAI swap price distribution are unstable, having extreme price rises and drops, explainable by small pool activity, reducing deviation during high-activity periods.



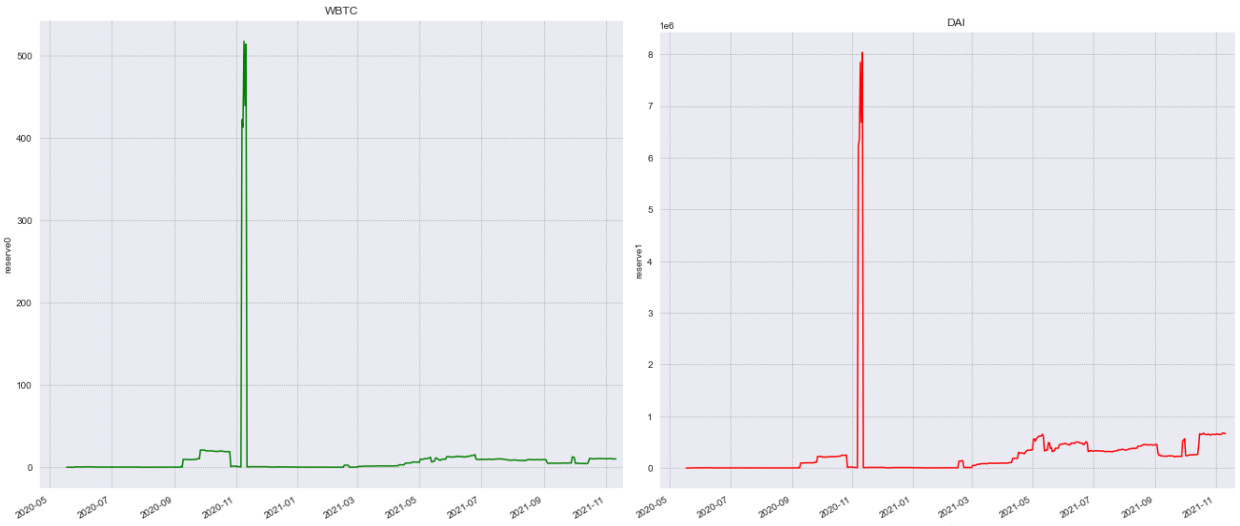
Picture 22: Swap price change rates for WBTC/DAI pool

Change rates are higher during low activity periods and one more proof of this phenomenon is present in the transaction count distributions.



Picture 23: Swap transaction count for WBTC/DAI pool

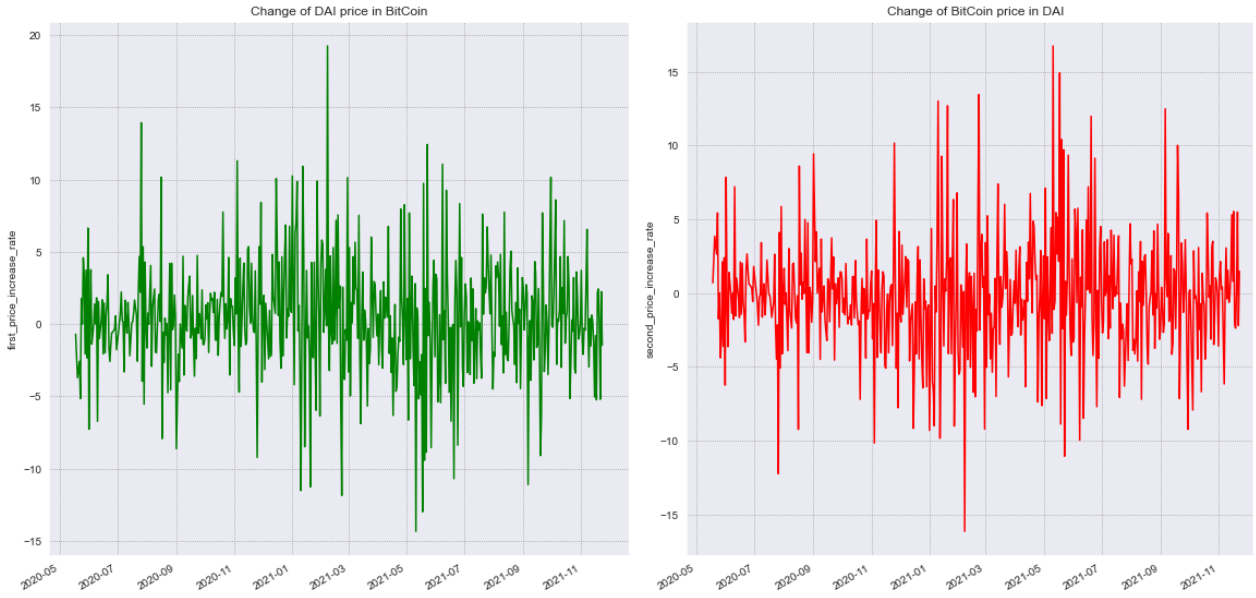
The high activity periods are covering time periods of smallest swap price change rates, meaning that balancing technologies are applied to the pool, while low activity periods are represented with higher swap price change rates.



Picture 24: reserves for WBTC/DAI pool

Conform presented distribution can be seen as another reason for high change rates during low activity periods - there are smaller pool reserves during those periods, meaning that high change rates are a result of several factors.

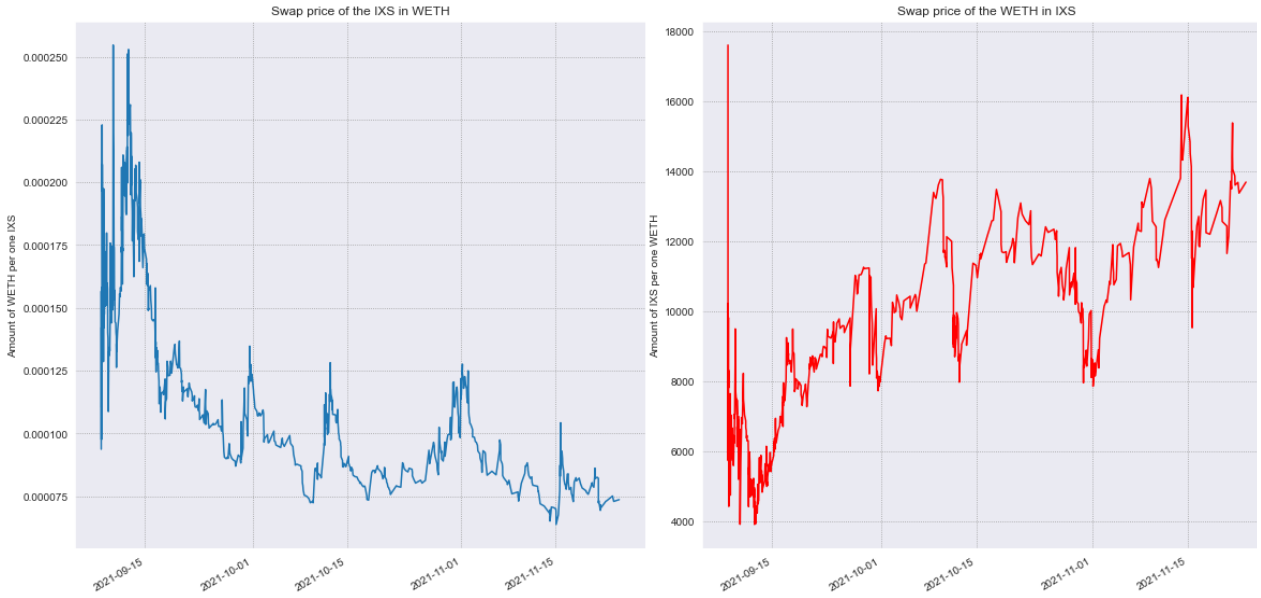
Due to the low reserves, bigger low activity periods and unstable behavior, reserve-based prices in this pool are also unstable.



Picture 25: reserve-based prices change rates for the WBTC/DAI pool

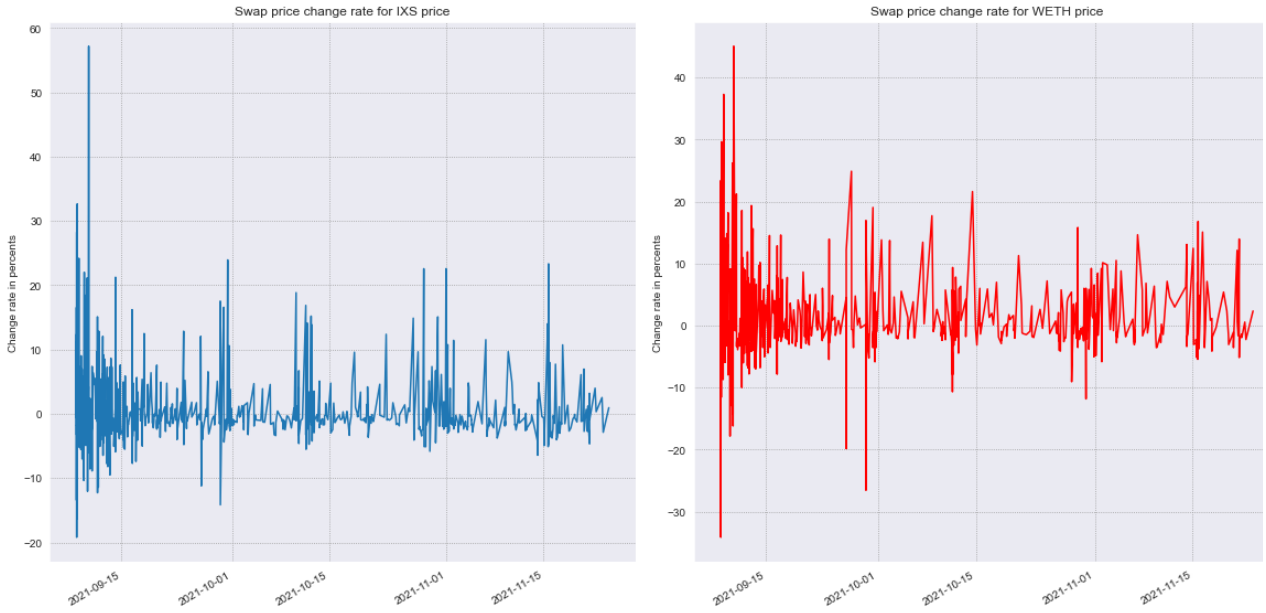
IXS/WETH or how first 2.5 months of token lifecycle look like

For checking the difference between behavior of different altcoins it was decided to pick the IXS/WETH pool.



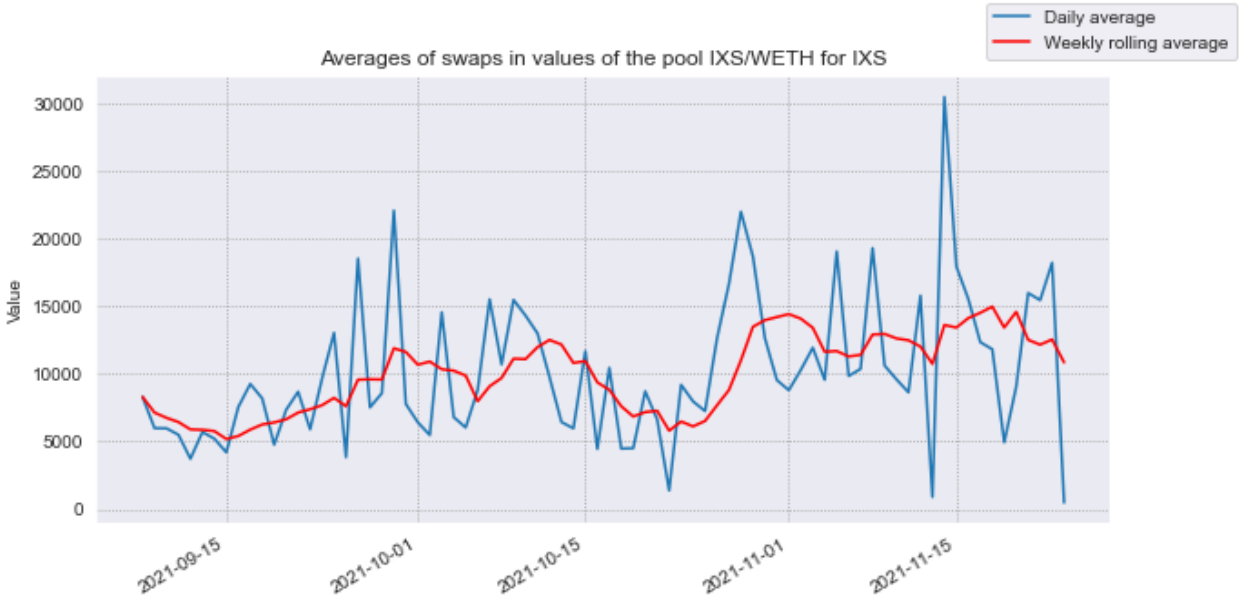
Picture 26: swap prices distributions for IXS/WETH pool

Compared to previously reviewed pools, swap price distributions have a better picture with relatively smaller price deviations, having only bigger changes in the beginning of the IXS/WETH pool lifecycle, but price distribution is still unstable.



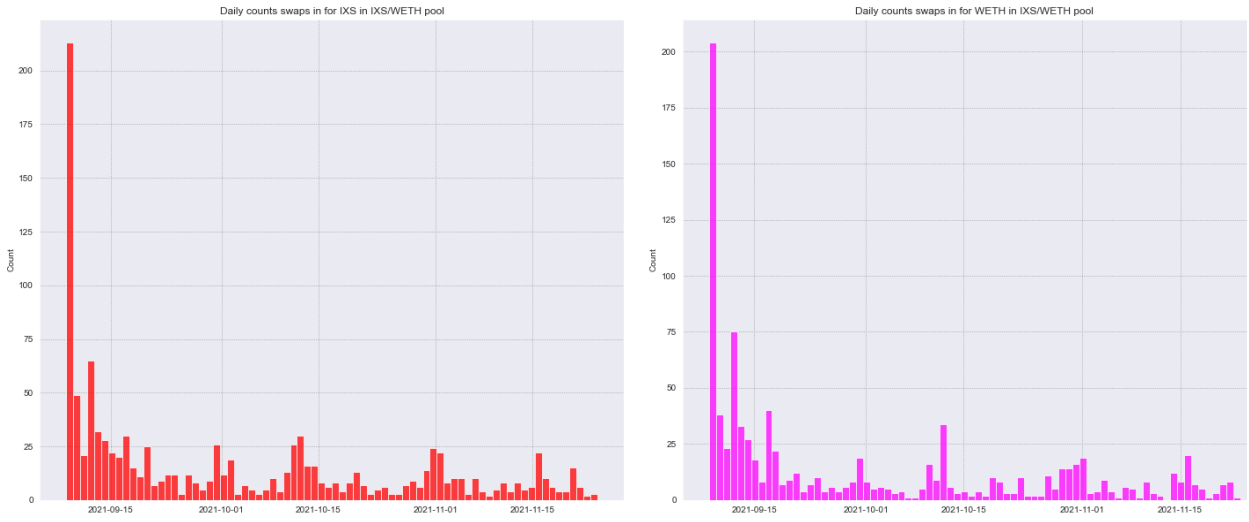
Picture 27: swap price change rates distributions for IXS/WETH pool

Conform presented distributions of the swap price change rates beginning of the pool lifecycle is a high-deviation period with big changes in the price. Increase of the transaction frequency decreases those deviations, but to check this moment it is required to check transaction frequency and pool size for the current pool.



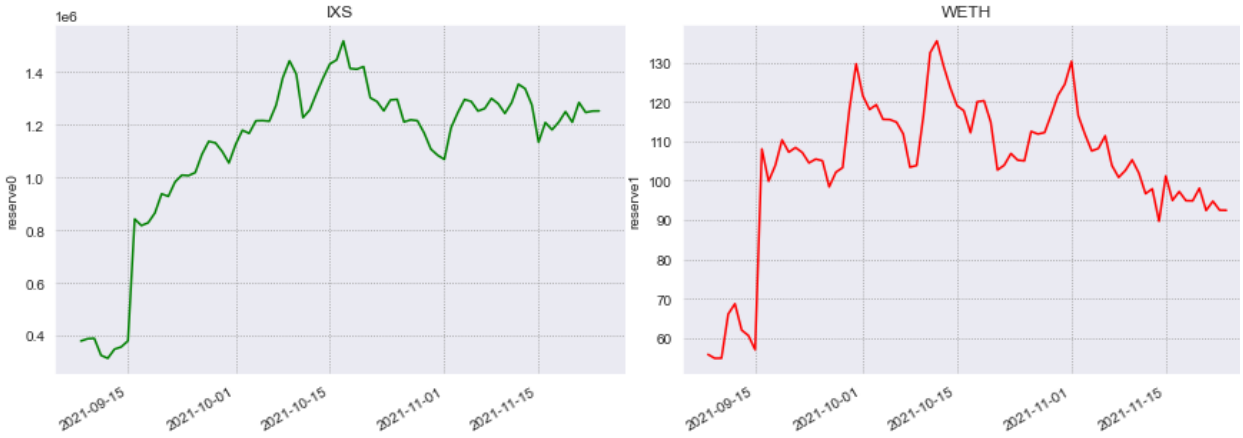
Picture 28: swaps distribution in IXS/WETH pool for IXS

Transaction activity is relatively low. To ensure it, below is the transaction frequency distribution.



Picture 29: swaps transaction count distributions for IXS/WETH pool

The distribution of the transactions count shows current low activity in the pool, but frequency is relatively stable. This stable transaction frequency causes more stable behavior, but distribution still requires stabilization.

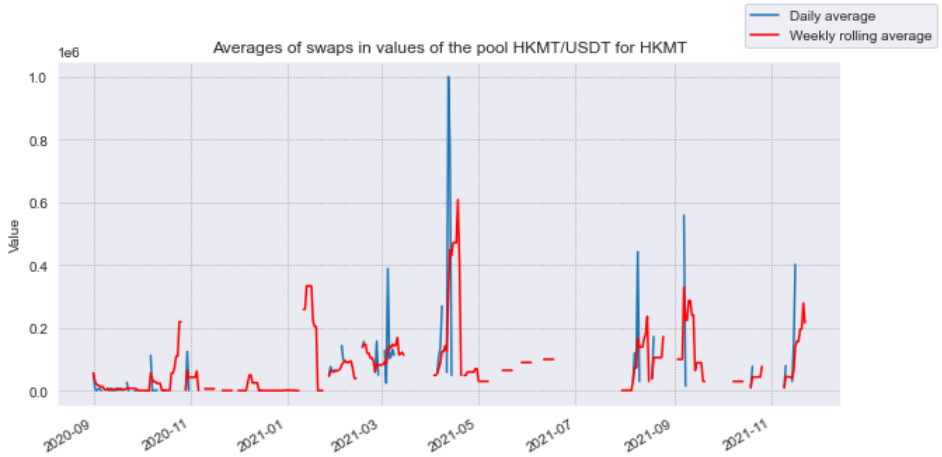


Picture 30: reserves for the IXS/WETH pool, left chart represents the IXS reserves, right one represents the WETH reserves

Another big reason that caused swap price stabilization is the increase of pool reserves, making the pool more stable. Variance increases are matching the moments of the reserves drops.

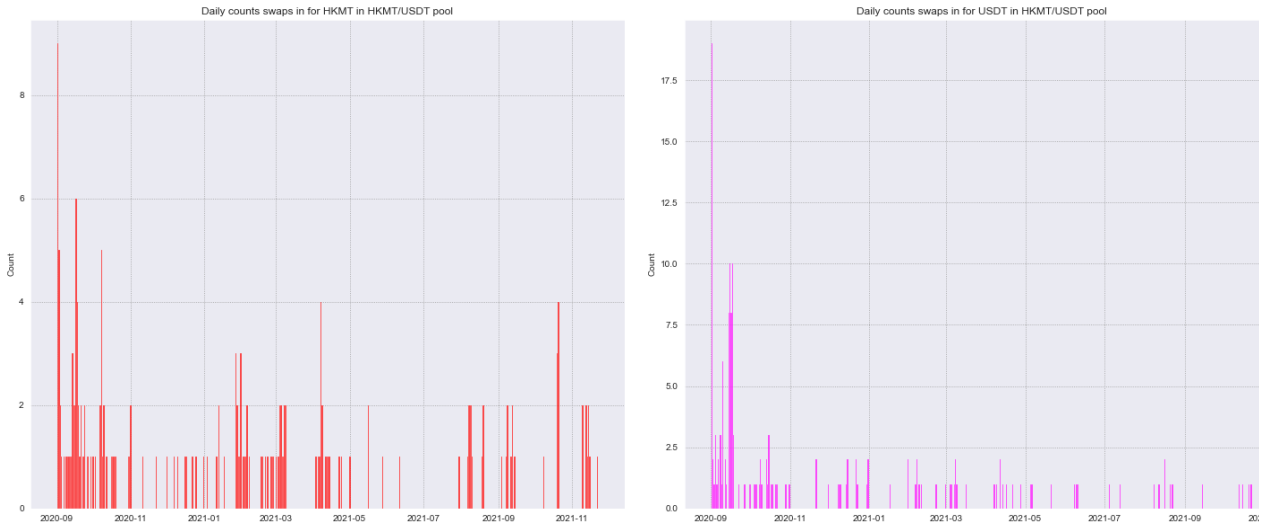
HKMT/USDT or case of low transaction frequency with giant reserves

Next pool chosen for the analysis was the HKMT/USDT pool. This is an interesting example of a low activity stable pool that had no extreme rises and drops.



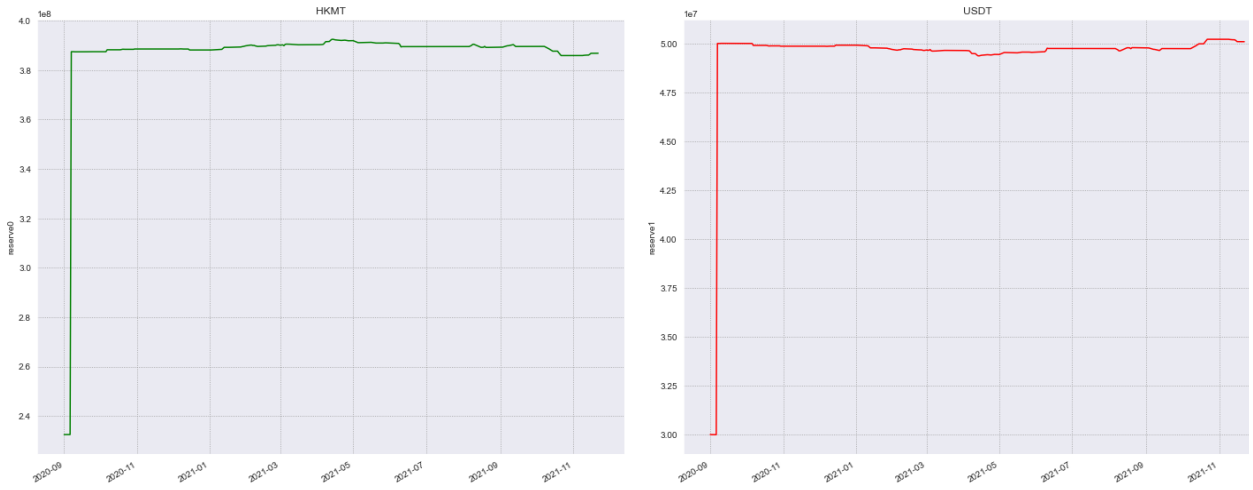
Picture 31: Swaps operations activity in the HKMT/USDT pool for HKMT

Conform presented chart, there are multiple time gaps in the swaps activity. This demonstrates a regular low activity in the pool. To ensure that, below is present the transaction count distribution.



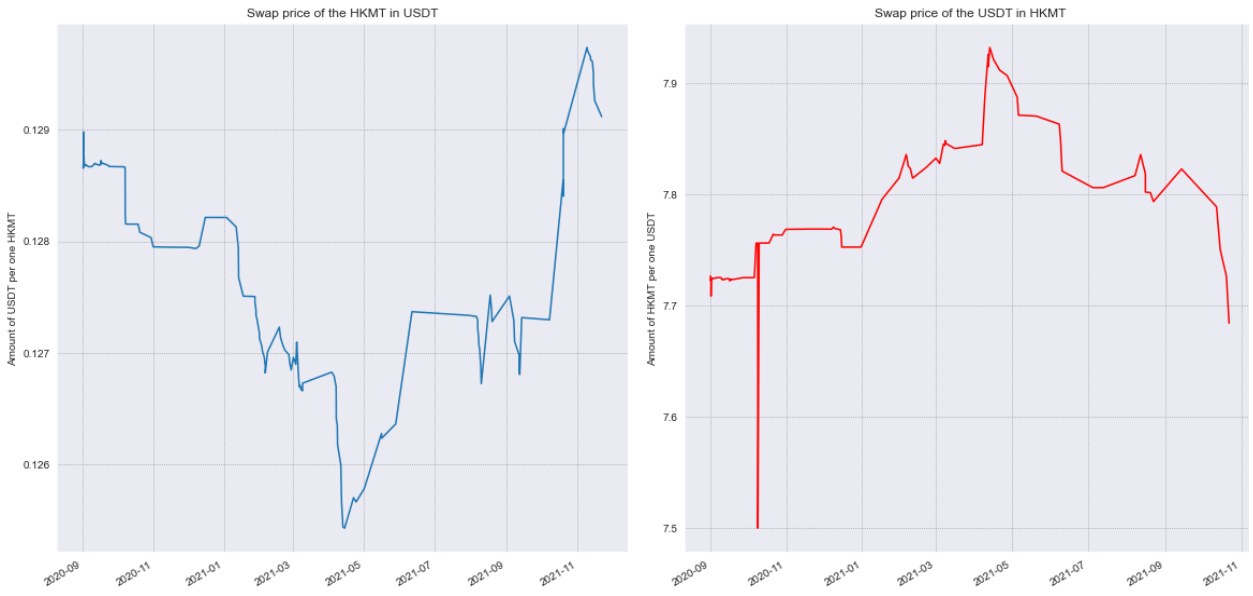
Picture 32: Swap transactions count for HKMT/USDT pool

Transaction count distribution demonstrates small transaction frequency. Current pool can become an efficient target for the MEV attack from this perspective, but it is necessary to check pool behavior from the pool reserves perspective.



Picture 33: Reserves of the HKMT/USDT pool

Reserves distribution lowers ability of performing efficient MEV attack, due to the high reserves values and their stable distribution, keeping almost the same through the entire 1-year period. In order to check if such an attack can happen or if there are unstable periods it is required to analyze swap price distribution and its change rate.



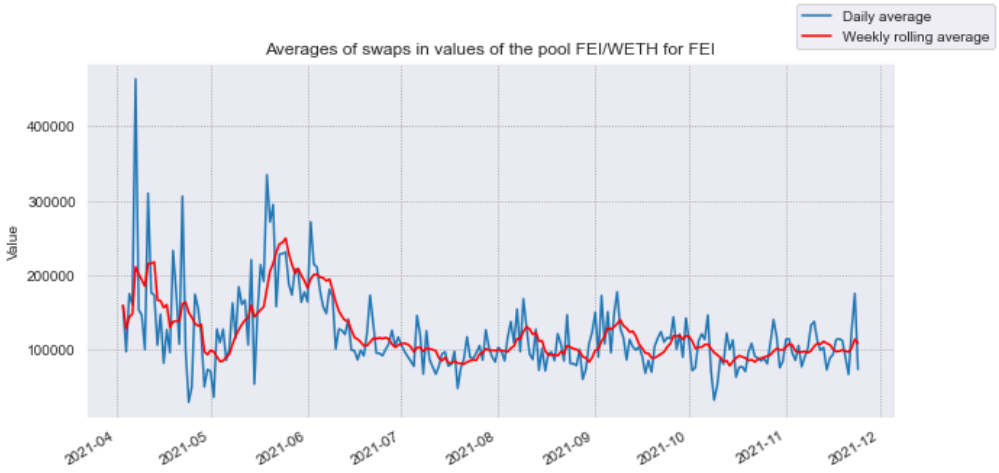
Picture 34: Swap price distribution of the HKMT/USDT pool

Conform price distribution can be seen that rises and drops are relatively small and there are not big rises/drops present in the distribution. This is an interesting case considering pool properties and low transaction frequency.

Taking into account the stable distribution of the reserves available in the pool, swap prices distributions have negative dependencies.

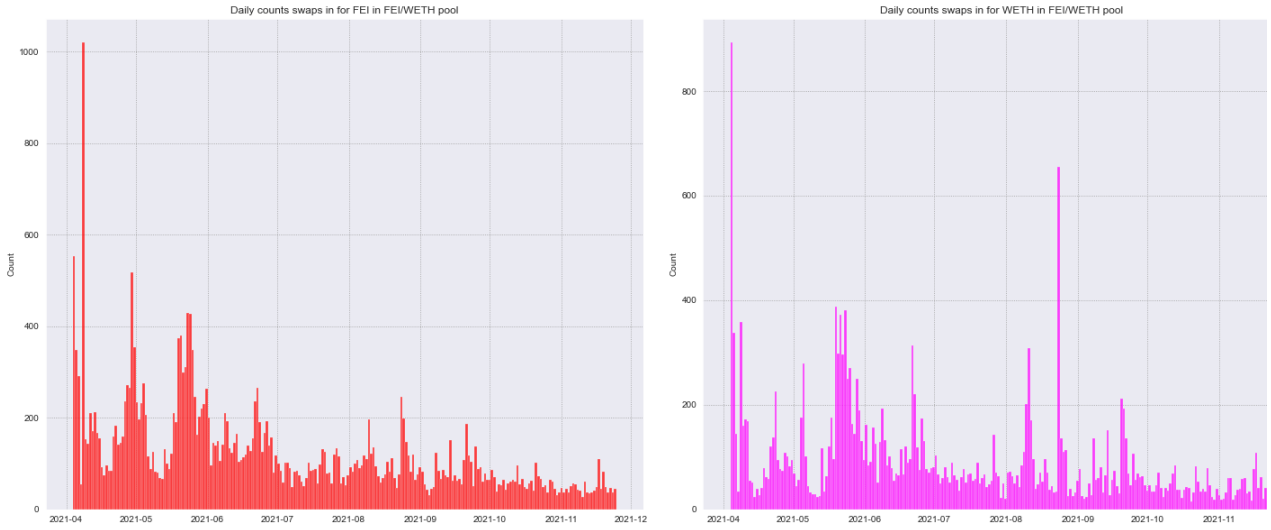
FEI/WETH

Another pool that will be used to compare its behavior relative to Ethereum is the FEI/ETH pool. FEI is a stablecoin, meaning that its distributions should have the same pattern as ETH/USDC pool, where Ethereum stablecoin was also attached to another stablecoin.



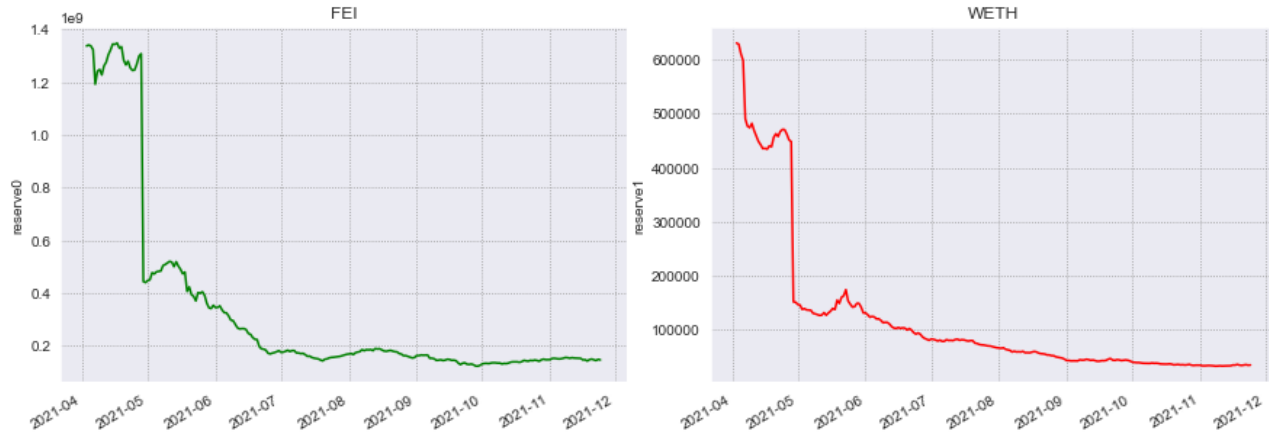
Picture 35: FEI/ETH swap transaction activity for the FEI

Swap transactions activity is higher compared to the ETH/USDC pool. Transaction values per day are higher, meaning higher transaction frequency and bigger token values used in transaction history.



Picture 36: swap transaction count distribution for FEI/ETH pool

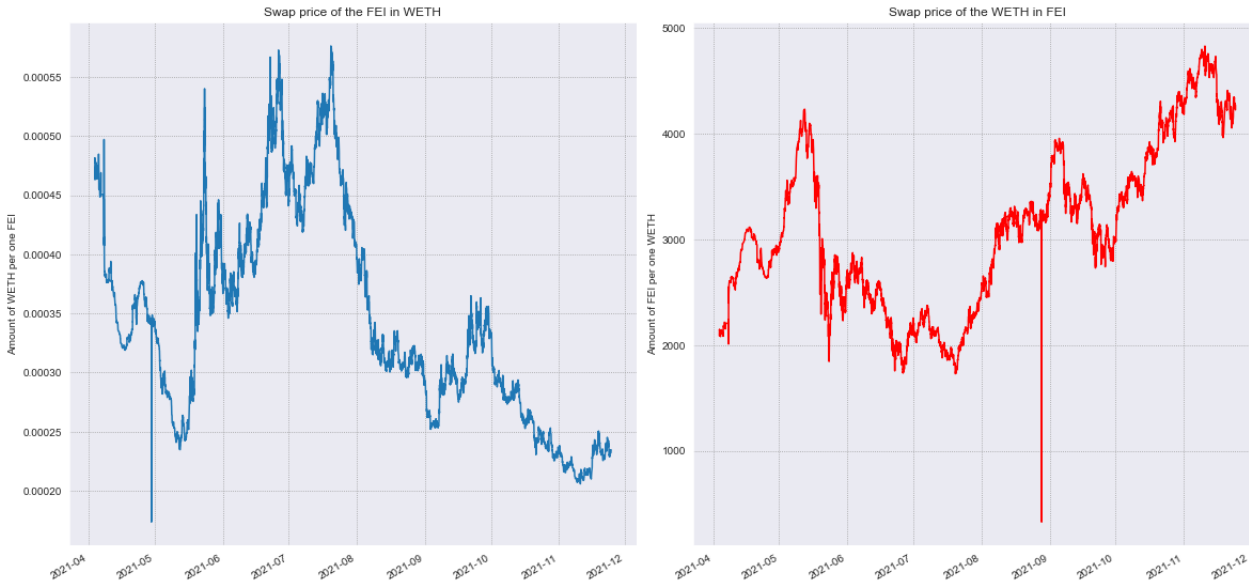
Transaction count demonstrates high transaction frequency and that there are anomalous periods of the transaction frequency rises, when transaction count rises in two, or more times. Presented distributions lower chances of performing frequent and efficient MEV attacks, but does not exclude such an opportunity.



Picture 37: reserves distribution for the FEI/ETH pool

Distributions demonstrate that the current situation of the pool is less attractive than before: amount of available resources has greatly decreased during the end of April-start of May 2021, and distributions were slowly decreasing till August 2021, when distributions stabilized. Even considering the negative trend in reserves distributions, reserves are high enough to protect

the pool from possible MEV attack. Still, if the negative trend continues, reserves could reach such small values that it would raise the danger of performing the MEV attack.



Picture 38: swap prices distribution for FEI/ETH pool

The swap prices distribution has normal deviations and overall distribution looks stable enough. The extreme drop present in the Ethereum price was caused by a strange drop of the price in the transaction presented below.

	token_in	token_out	amount_in	amount_out	amount_usd	timestamp	first_to_second_price	price_change_rate
39686	WETH	FEI	0.001	3.248770	3.243474	2021-08-28 09:16:41	3248.770000	0.216102
39687	WETH	FEI	0.001	3.248774	3.243331	2021-08-28 09:16:56	3248.773553	0.000109
39688	WETH	FEI	0.001	0.324877	3.243483	2021-08-28 09:21:48	324.877000	-90.000011

Picture 39: small transaction history fragment, covering a strange operation discovered in the pool

This operation is strange, because no mint/burn operation, no MEV-similar transactions were found close to this time period. Looking closer into the price can see that the amount_out value was shifted by one digit to the right (or like divided by 10). This can be an error present in the Uniswap history. This error creates “noise” in the real price history.

	token_in	token_out	amount_in	amount_out	amount_usd	timestamp	first_to_second_price	price_change_rate
39685	FEI	WETH	1985.876412	0.607615	1967.602022	2021-08-28 08:51:02	0.000306	-0.021607
39686	WETH	FEI	0.001000	3.248770	3.243474	2021-08-28 09:16:41	3248.770000	0.216102
39687	WETH	FEI	0.001000	3.248774	3.243331	2021-08-28 09:16:56	3248.773553	0.000109
39688	WETH	FEI	0.001000	0.324877	3.243483	2021-08-28 09:21:48	324.877000	-90.000011
39689	FEI	WETH	675.085714	0.206551	670.307283	2021-08-28 09:34:22	0.000306	-0.001645
39690	FEI	WETH	55447.930505	16.959115	55008.932388	2021-08-28 09:37:41	0.000306	-0.034819
39691	FEI	WETH	41410.764742	12.658133	41057.913311	2021-08-28 10:14:43	0.000306	-0.060177
39692	FEI	WETH	63307.251626	19.338709	62739.037399	2021-08-28 10:15:51	0.000305	-0.065000
39693	FEI	WETH	51356.475263	15.676892	50855.477426	2021-08-28 10:16:25	0.000305	-0.071184
39694	WETH	FEI	1.550000	5048.731674	5027.088786	2021-08-28 10:52:39	3257.246241	902.609062
39695	FEI	WETH	35508.129978	10.833920	35096.951096	2021-08-28 11:18:48	0.000305	-0.047638
39696	WETH	FEI	100.000000	325199.345732	323666.025517	2021-08-28 11:42:09	3251.993457	-0.161265

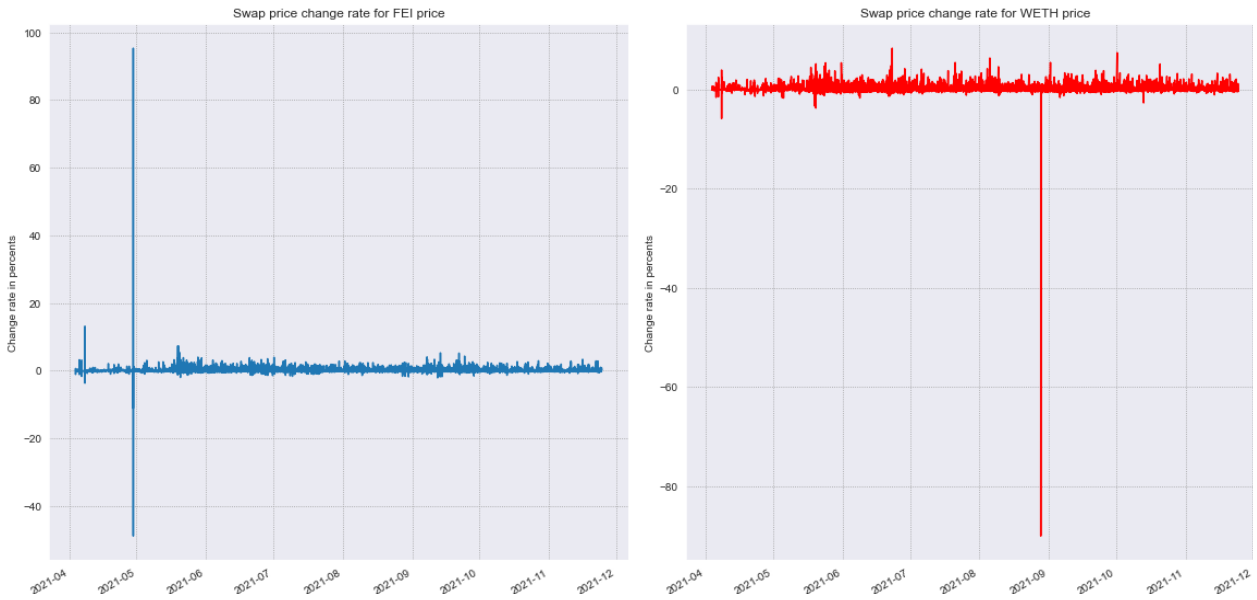
Picture 40: small transaction history fragment, covering a strange operation discovered in the pool and its influence over the transaction history

Conform presented transactions there are no MEV-like operations, but transaction history is now “noised” by this operation. To ensure that swap price has a similar distribution with the real price on the market below is presented a reserve-based price distribution.

As can be seen on the chart below, reserve-based price distribution is almost identical to the swap-based price distribution and similar to the real-market price evolution. Pool distributions converge and adapt to match a real-market situation.

Picture 41: reserve-based price distribution for the FEI/ETH pool

Price deviation from the percentages perspective demonstrates stable price distribution with some ‘error’ moments that were caused either by bugs in the system or by drops/rises caused by reserves changes. Some extreme rises and drops were also removed from the distribution (division errors and so on).

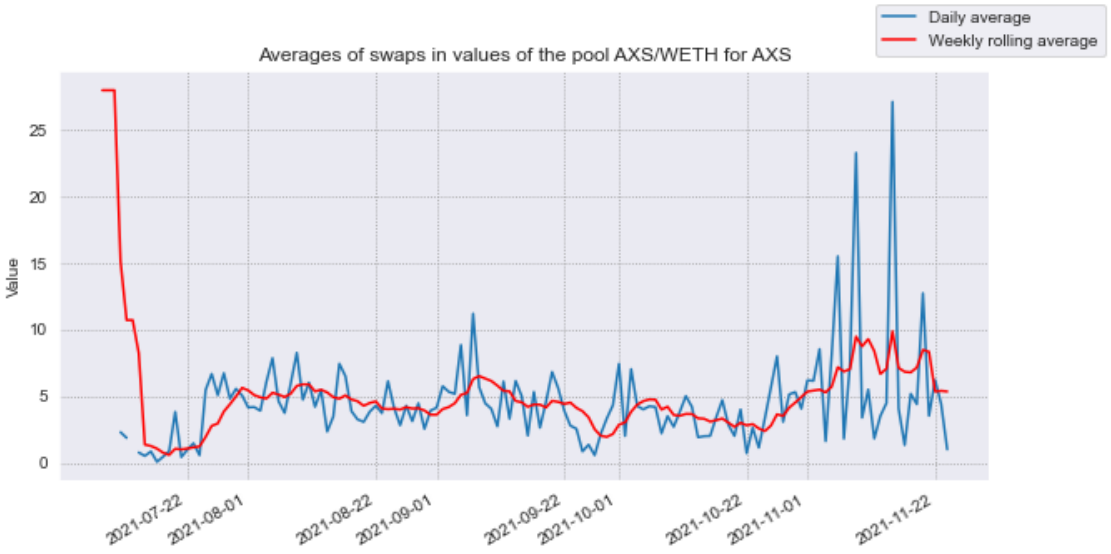


Picture 42: swap-based price change rates distributions for the FEI/ETH pool

AXS/WETH (NFT) or a bad case of unstable behavior of game token

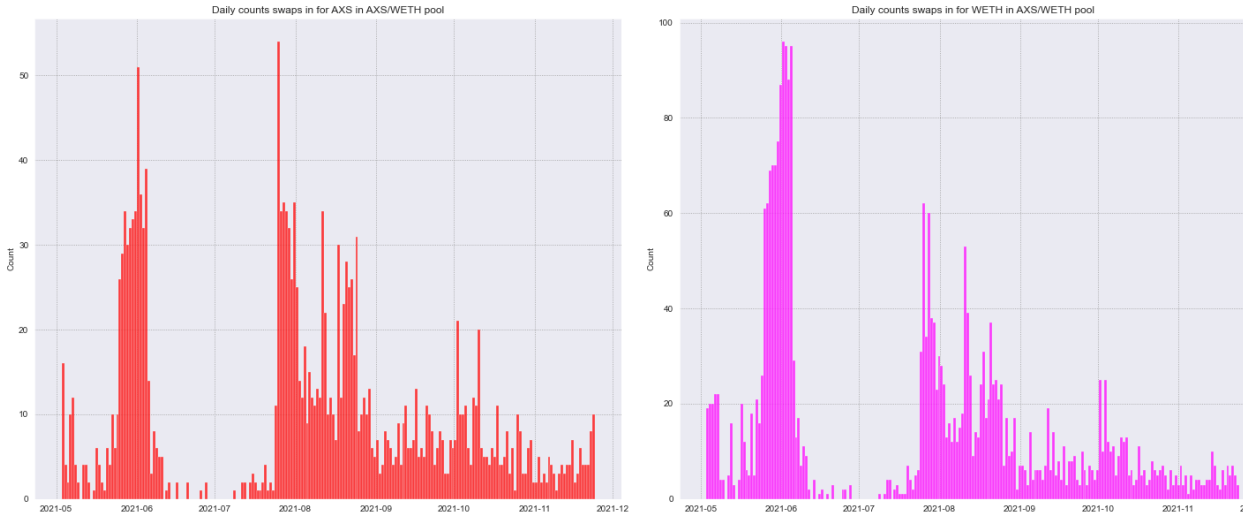
AXS token is an NFT token used in the Axie Infinity online game, where users (or players) need to purchase some creatures called “Axies” or to raise them, battle each other or to sell them. Axie Infinity inner economy is based on using NFT-based AXS (Axie Infinity Shards) or SLP (Smooth Love Potion). This game contains one of the most expensive NFT collections.

Authors discovered that this token is present on the Uniswap V2 as AXS/ETH pool and it was considered as a good option to check how this pool performed at Uniswap.



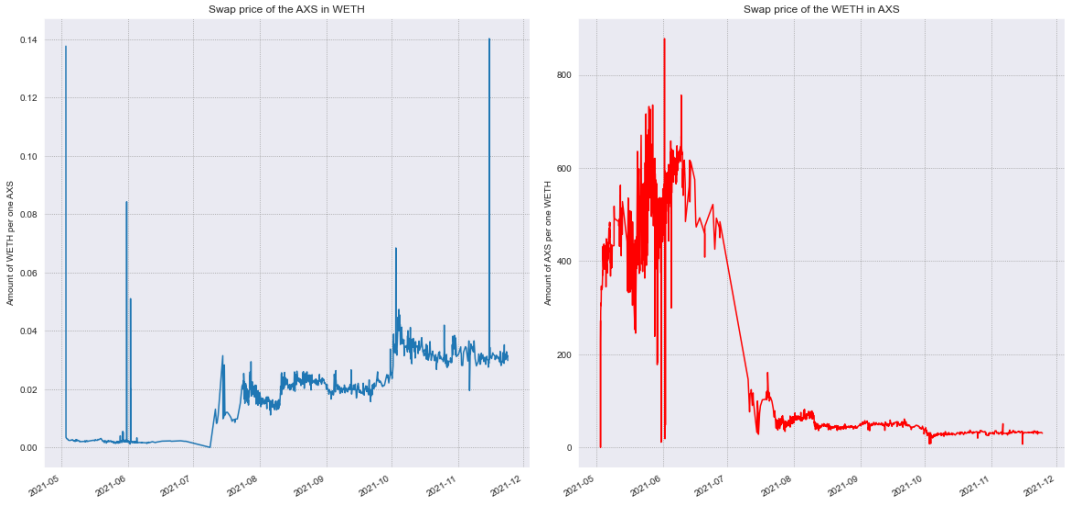
Picture 43: swap operations distribution for the AXS/ETH pool

Swap operations distribution is unstable in the AXS/ETH pool, considering that until August 2021 there were multiple gaps in the data, defining low transaction activity. Below is presented the transaction count distribution for the AXS/ETH pool.



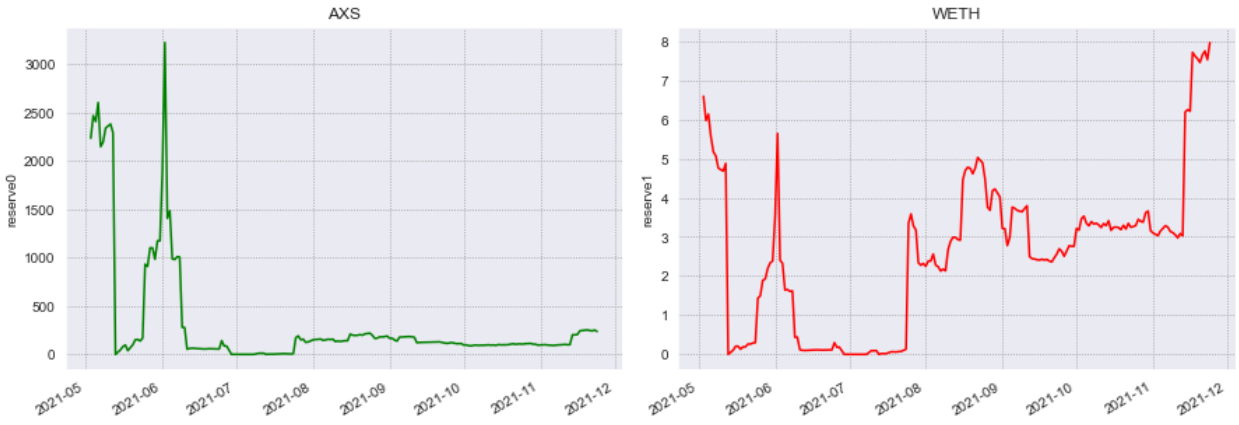
Picture 44: swap operations count distribution for the AXS/ETH pool

Swap operations count distribution show that there is an unstable behavior until August 2021, after which distribution has stabilized and behavior is more stable compared to the start of the pool lifecycle. The interesting moment is that looking at the swap price distribution chart without any changes shows a strange picture of extreme drops and rises in the token price, that can be explained by the reserves removal, which in the current case caused some anomalous changes in the distribution. Removal of those anomalies causes distribution optimization, with the next representation.



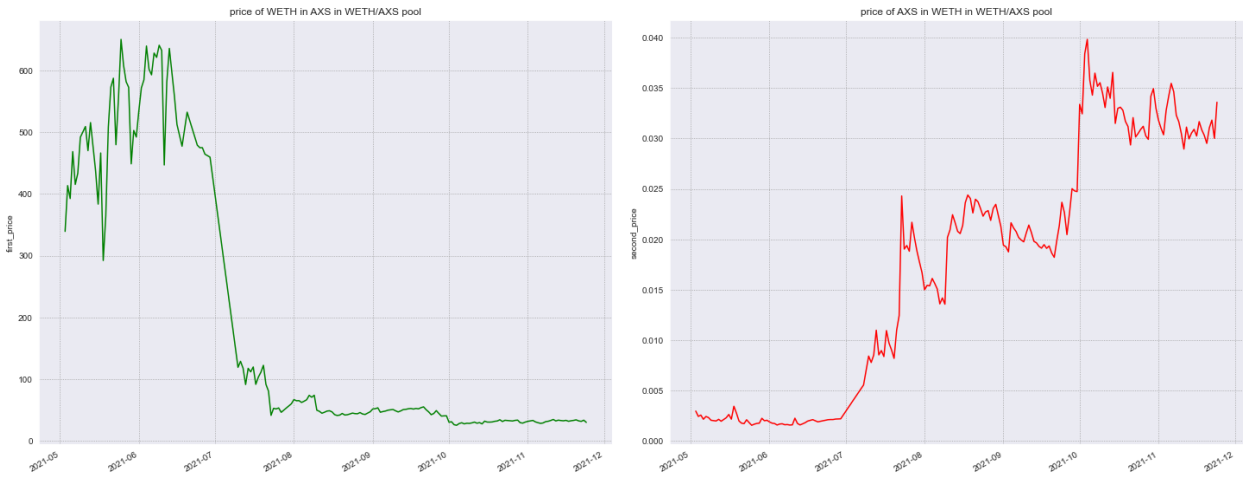
Picture 45: Swap price distributions of the AXS/ETH pool

Distributions show unstable and highly changeable behavior in the pool, which can be explained by the small transaction frequency in the beginning, but another suggestion is that there are big changes in the reserves distribution present during the extreme drops and rises.



Picture 46: AXS/ETH reserves distributions

Reserves distributions demonstrate previously estimated thought about possible extreme pool changes that caused drops and rises in the prices. Conform presented distributions can be seen that tokens balance had extreme drops in time intervals middle May - start of June 2021 and middle June - end of August 2021. Conform presented distributions the situation stabilized starting from August 2021.



Picture 47: reserve-based tokens price distributions in the AXS/ETH pool

Present price distributions form a more clear picture about price evolution through time and it is required to compare this price evolution with the situation on the market.

Picture 48: CoinCodex price distribution for AXS token

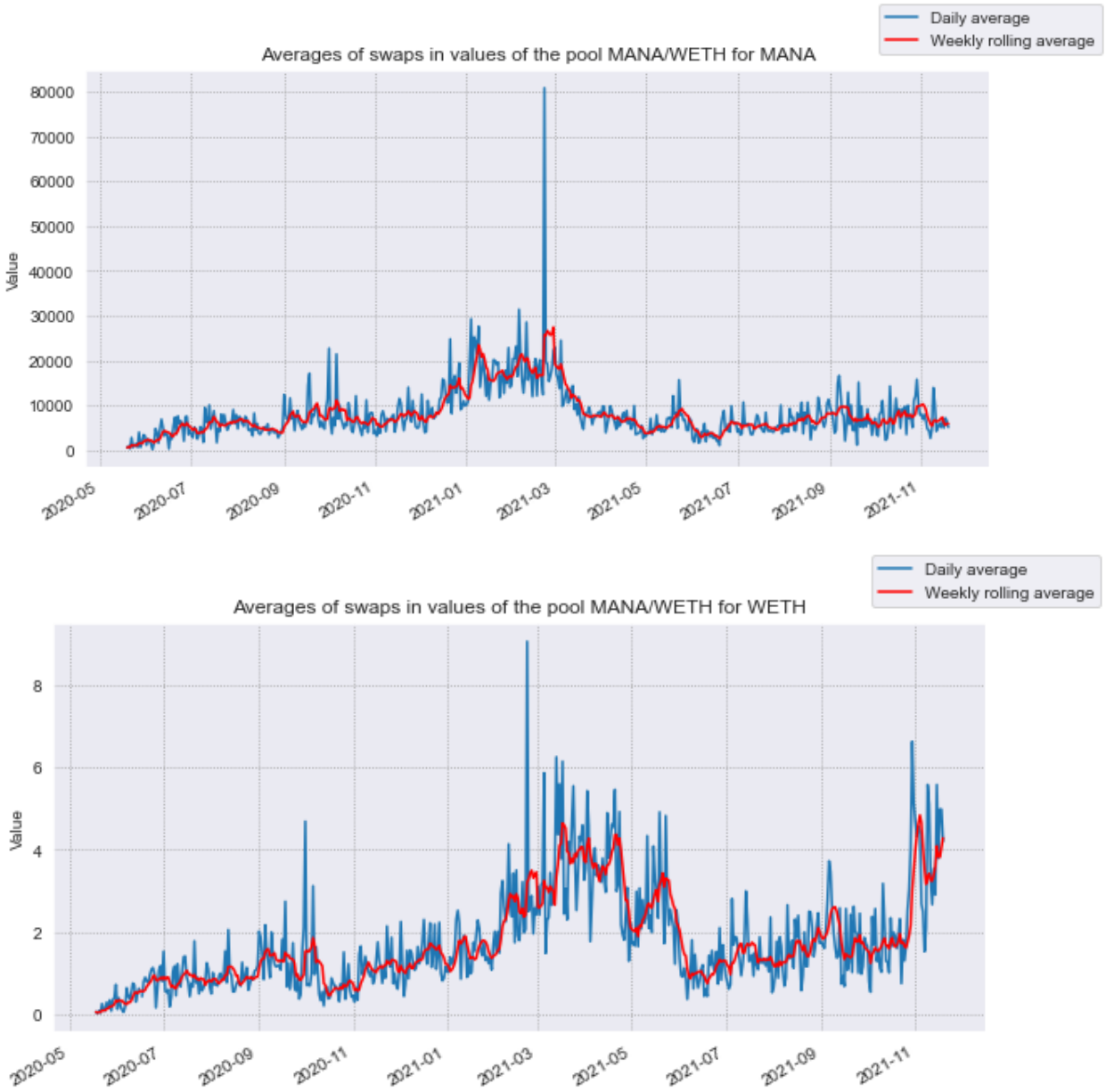
Real-market price distribution shows the same shape, tendency and shapes as the one present in the pool meaning that in this case pool also converges to the real-market price and distribution with possible deviations during pool lifecycle start and some anomalies.

MANA/WETH (NFT) or possible new trend

MANA token is a cryptocurrency used for performing trades inside the Decentraland meta-universe. This token is popular considering the current popularity of the meta-worlds and had a stable price distribution over the time, which can be seen in the chart below.

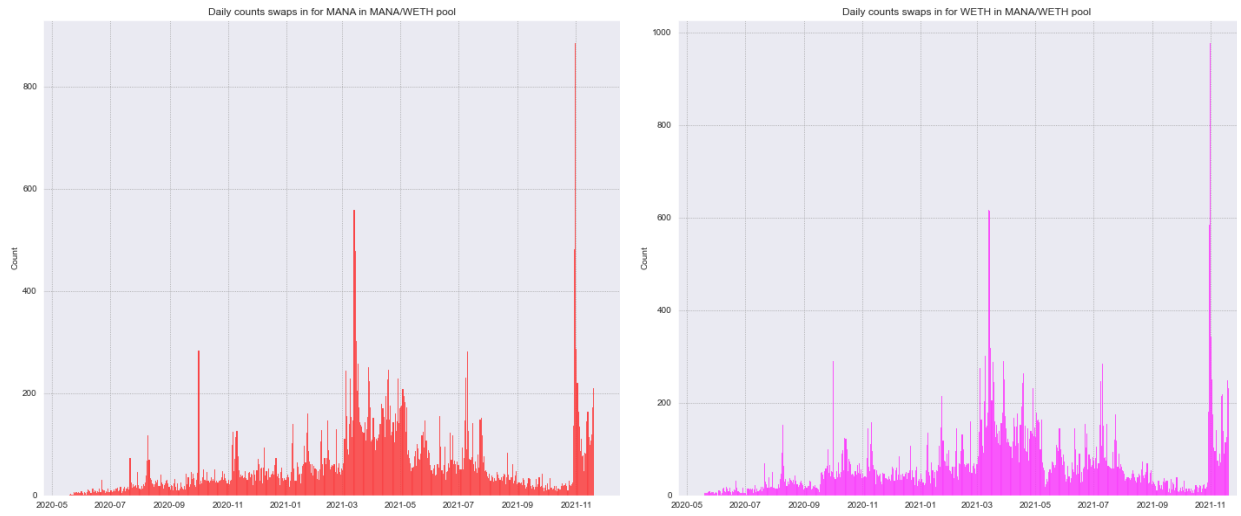
Picture 49: MANA to USD dollar price distribution for the last year taken from CoinBase

After the Meta-universe presentation from Facebook, popularity of the similar projects has greatly increased due to their already present implementations and their activity (in case of Decentraland it originally appeared in 2015 and publicly opened in February 2020). Considering such a great rise in NFT tokens popularity due to their use in such meta-worlds, it would be interesting to analyze behavior of the MANA/ETH pool.



Picture 50: Swap operations distributions in the MANA/ETH pool

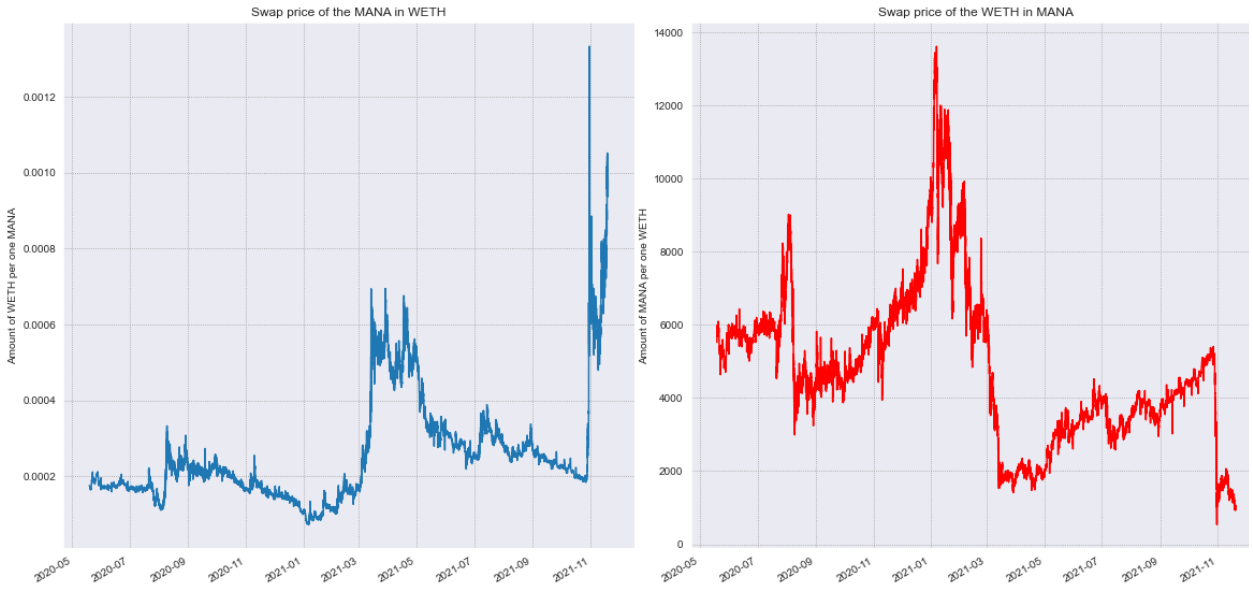
Distribution of swapping operations is stable, contains traceable trends and by the first look balancing algorithms should work properly with this pool, to check it below is reviewed transaction count distribution.



Picture 51: Swap operations count distribution in the MANA/ETH pool

Transaction count distribution forms a picture where transactions have great rises and drops. Here it can be seen that balancing algorithms could have problems in the time intervals of transaction frequency drops.

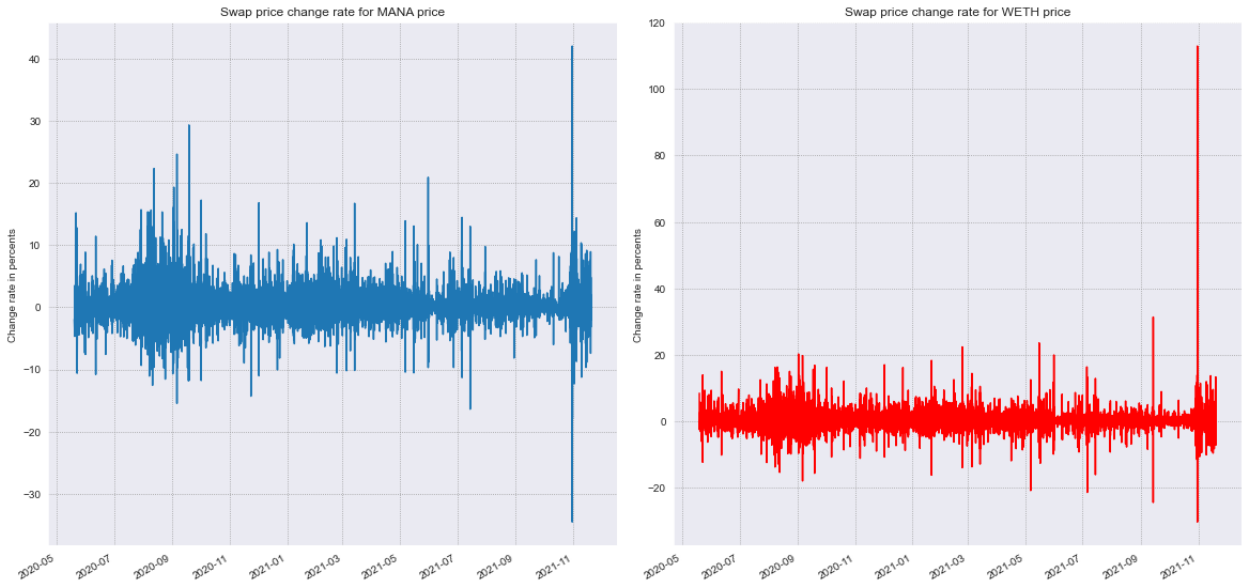
Swap-based prices shown in the distributions below have high deviations with extreme token price rises and drops. MANA distribution contains one strange price drop to 0 value.



Picture 52: swap-based price distribution for MANA/ETH pool

MANA distribution shows unstable behavior with extreme price rise in the end of the reviewed period, which is correlating with the WETH token price drop in the same period.

Deviation of the WETH token is more stable, but more clearly demonstrates negative price tendency.



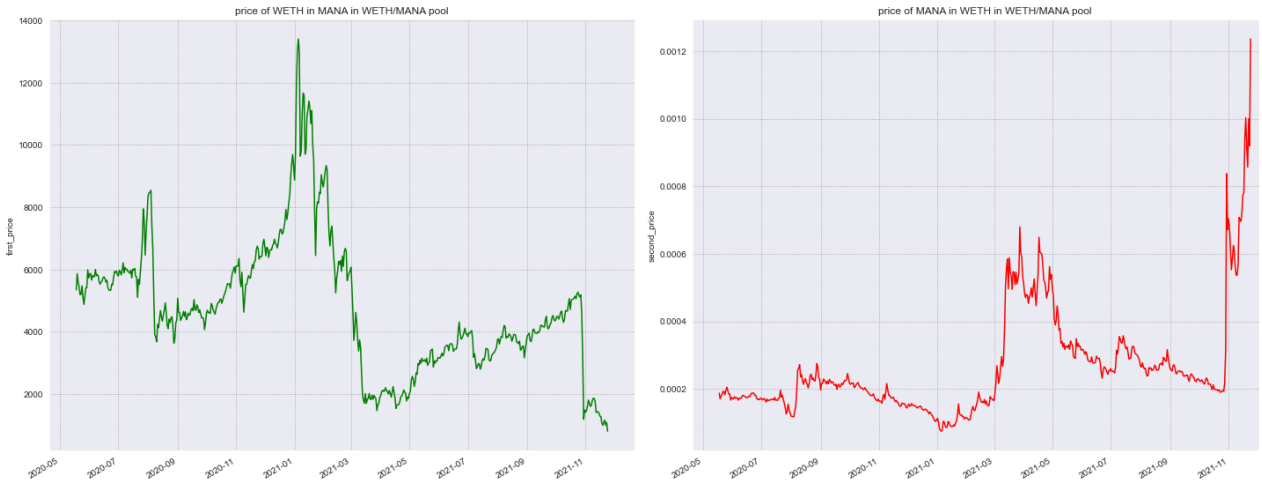
Picture 54: swap-price change rates distributions for MANA/ETH pool

There is a strange rise in the WETH price close to the end of the pool story. This strange rise is explained by the extreme rise of the MANA price several times. Can be observed that unstable price change rates deviation range becomes higher with destabilization of token price on external markets.

65432	MANA	WETH	15305.398848	14.349235	6.290683e+04	2021-10-31 01:19:14	0.000938	1.059439
65433	MANA	WETH	11828.063868	10.822690	4.744651e+04	2021-10-31 01:19:23	0.000915	-2.402775
65434	WETH	MANA	6.114025	6672.638237	2.680457e+04	2021-10-31 01:19:59	1091.365951	3.404224
65435	WETH	MANA	416.647577	322138.347555	1.826339e+06	2021-10-31 01:20:52	773.167457	-29.155985
65436	MANA	WETH	7133.002242	6.691679	2.933240e+04	2021-10-31 01:20:52	0.000938	2.527687
65437	WETH	MANA	29.120000	15716.287485	1.276450e+05	2021-10-31 01:20:52	539.707675	-30.195242
65438	MANA	WETH	322138.348763	429.238601	1.881530e+06	2021-10-31 01:20:52	0.001332	42.034423
65439	WETH	MANA	36.558669	42008.467382	1.599674e+05	2021-10-31 01:21:50	1149.069929	112.905983
65440	MANA	WETH	51207.000000	44.659091	1.957418e+05	2021-10-31 01:21:50	0.000872	-34.547807
65441	MANA	WETH	12400.864864	11.431987	5.010665e+04	2021-10-31 01:21:50	0.000922	5.703456
65442	WETH	MANA	0.728104	773.773337	3.185725e+03	2021-10-31 01:21:50	1062.724200	-7.514402
65443	WETH	MANA	21.140815	22948.207694	9.249896e+04	2021-10-31 01:21:50	1085.493025	2.142496
65444	MANA	WETH	10504.176570	9.739990	4.261609e+04	2021-10-31 01:22:24	0.000927	0.583501
65445	WETH	MANA	11.338632	12137.112588	4.961075e+04	2021-10-31 01:22:27	1070.421246	-1.388473

Picture 55: drop of Ethereum price relative to MANA token happening due to the MANA token price rise several times

To ensure that price distribution in the pool is similar with the real one below is presented reserve-based price distributions.



Picture 56: Reserve-based price distributions in the MANA/ETH pool

Price distribution in the pool looks similar to the real-market one, meaning that pool as in previous cases converges its price distributions to the real ones.

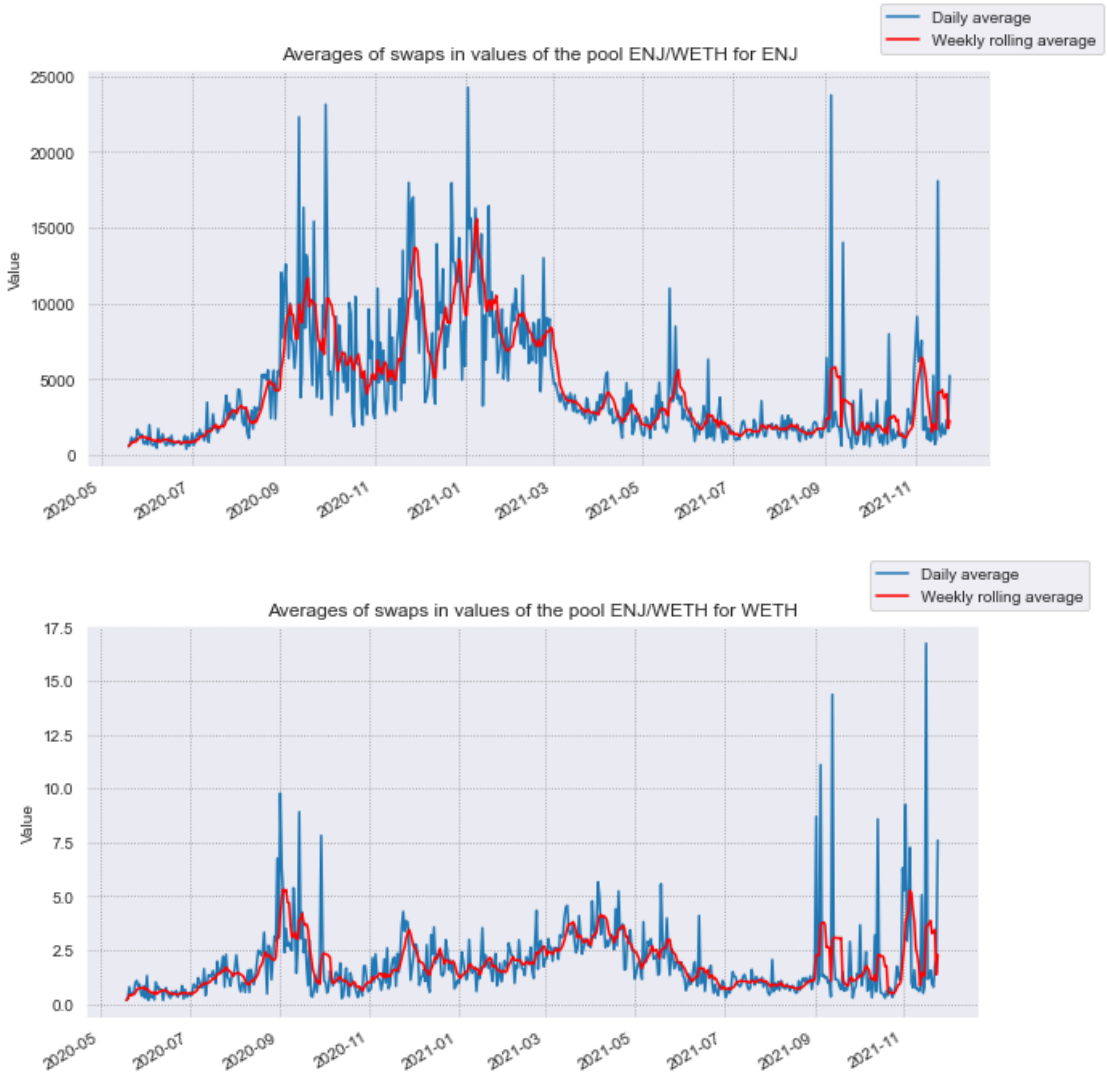
Previously presented transaction frequency distributions show that pool has a risk of facing a MEV attack and to check that it is required to check pool reserves.

Picture 57: Reserves of the MANA/ETH pool

Present reserves in the pool have a positive trend, meaning that reserves increase through time, increasing pool stability. There are present reserves drops and rises, causing pool destabilization.

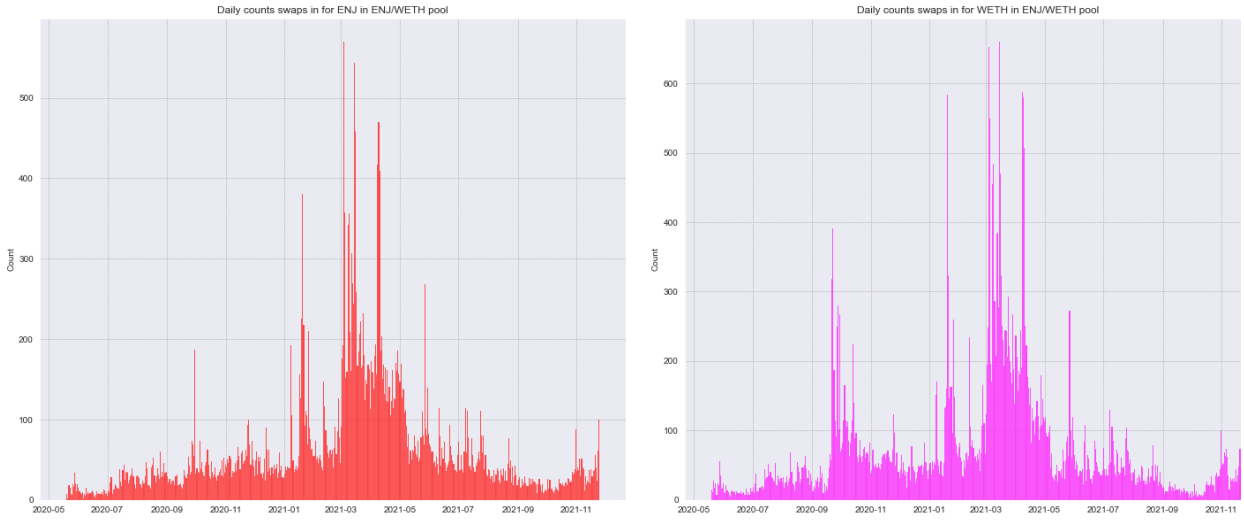
ENJ/WETH (NFT or STO) or how high popularity causes frauders bigger attention

ENJ token is the token used by an Enjin NFT platform that allows users to sell their digital goods on the market getting ENJ tokens for them. After that, those tokens can be exchanged for other tokens. From one perspective this can be considered as NFT token, due to its presence on the NFT platform, its use for selling or getting rights to different digital goods, but from another point of view this can be considered as the STO token, due to its use by a platform/organization on its NFT market. The token was released in June 2018. There was an ENJ/ETH pool present in the Uniswap V2.



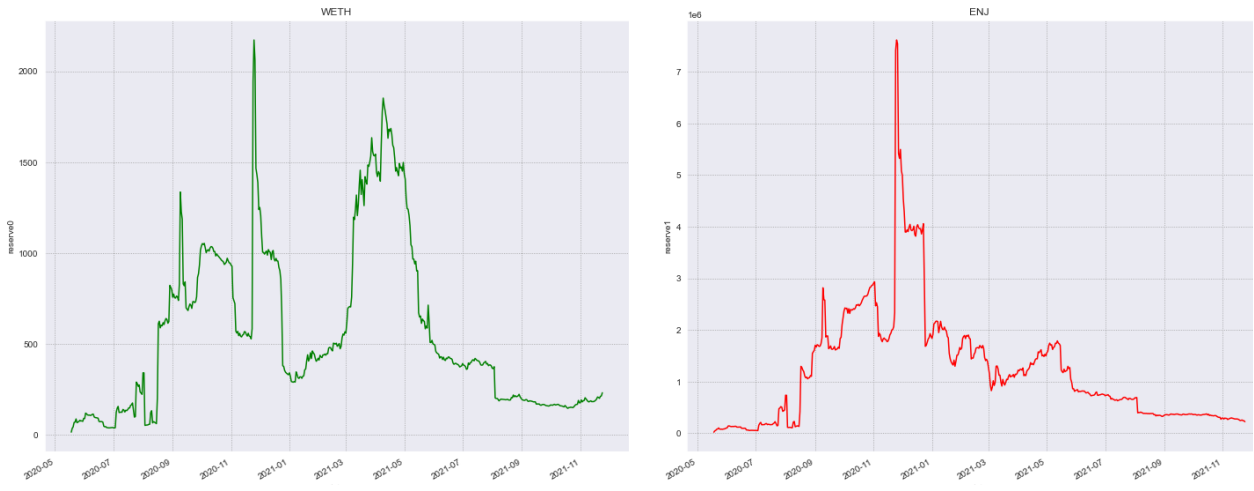
Picture 58: swap operations distribution for ENJ/ETH pool

Conform presented distribution pool had high activity between September 2020 and March 2021. Another small rise was registered between September and November 2021. Other periods have low transaction frequency.



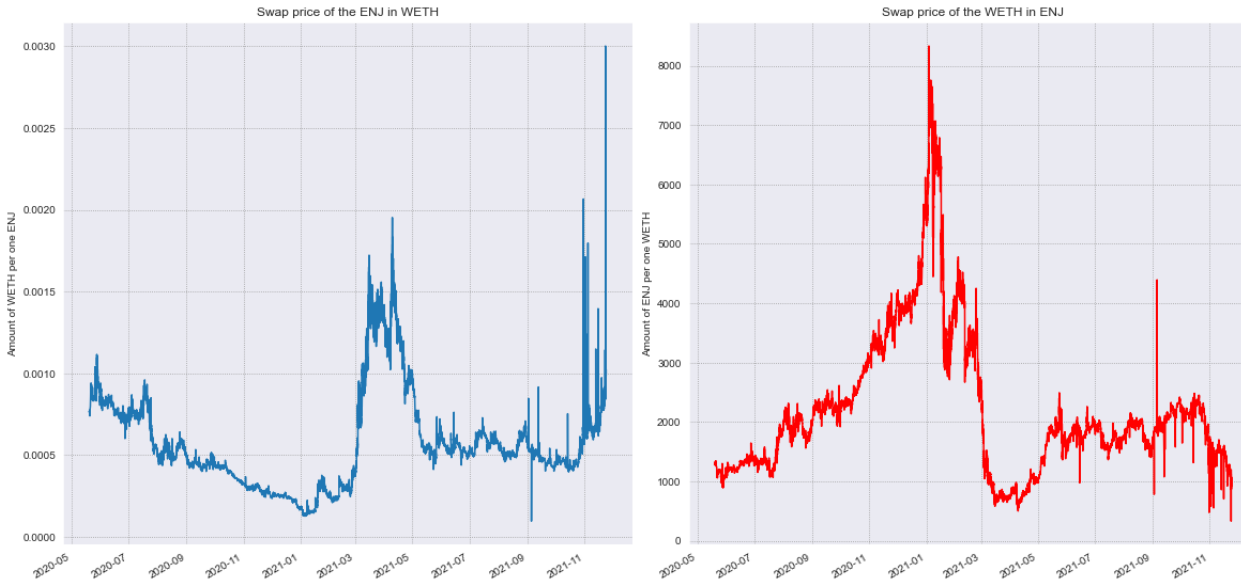
Picture 59: swap operations count distribution for ENJ/ETH pool

Transaction count also has unstable distribution. There is a high transaction frequency between February and May 2021. Considering transaction count, frequency is relatively high enough to consider pool safety from performing MEV attacks. To ensure this moment it is required to review pool reserves and tokens swap price distributions.



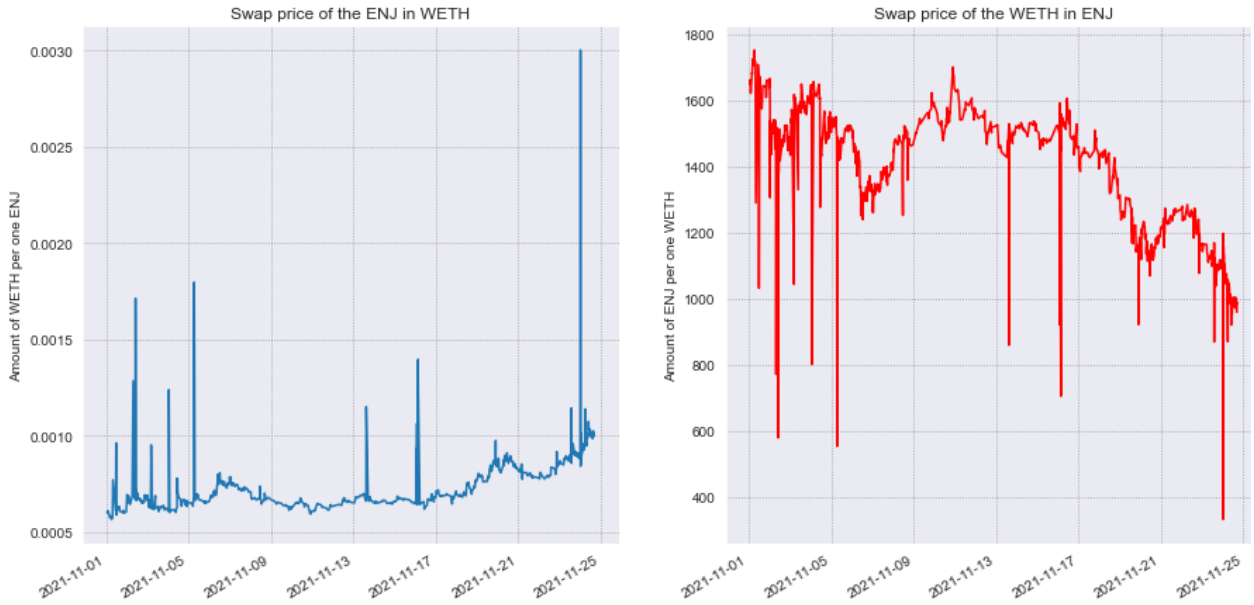
Picture 60: Reserves distribution in the ENJ/ETH pool

Distribution of the reserves has high rises and drops with unstable behavior. Reserves compared to previous pools is relatively low, meaning that currently the pool is unstable and price deviations should increase during last periods of pool history.



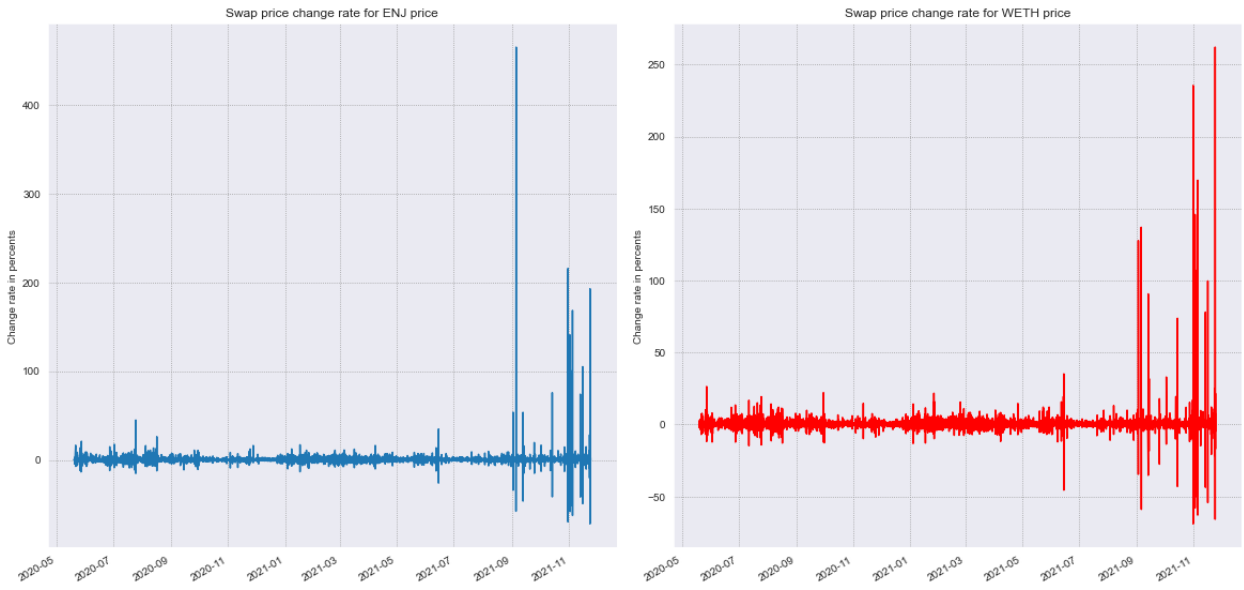
Picture 61: Swap price distribution in the ENJ/ETH pool

Price deviation during the start of the pool lifecycle and in the periods with big reserves available is smaller, compared to last periods, where reserves are much smaller and transaction frequency is smaller. During November 2021 there were high price rises that authors decided to look into.



Picture 62: Swap price distribution for ENJ/ETH pool during November 2021

To understand how strong were the price changes below is presented the price change rate distribution.



Picture 63: swap price change rate distribution for ENJ/ETH pool

There are anomalous increases in the price present in the distribution (rise of ENJ price by more than 400%). Below is a small transaction history fragment around this extreme price rise.

	token_in	token_out	amount_in	amount_out	amount_usd	timestamp	first_to_second_price	price_change_rate
70631	WETH	ENJ	1.552766	2878.020377	6092.616166	2021-09-05 15:09:16	1853.480325	-0.569779
70632	ENJ	WETH	474572.006540	109.616662	430127.429565	2021-09-05 15:09:16	0.000231	-56.410171
70633	WETH	ENJ	109.616662	481516.825905	430115.158190	2021-09-05 15:09:16	4392.733891	136.999219
70634	ENJ	WETH	10000.000000	0.975833	3829.093330	2021-09-05 15:09:16	0.000098	-57.752508
70635	ENJ	WETH	6922.774734	3.814684	14990.139483	2021-09-05 19:17:48	0.000551	464.680682
70636	WETH	ENJ	3.758762	6778.452031	14770.390903	2021-09-05 19:17:48	1803.373549	-58.946442
70637	WETH	ENJ	0.357279	656.105357	1407.173618	2021-09-05 19:39:04	1836.395730	1.831134
70638	WETH	ENJ	1.448645	2635.588884	5703.993978	2021-09-05 19:46:36	1819.347138	-0.928372
70639	ENJ	WETH	409.449076	0.225125	885.536575	2021-09-05 20:13:50	0.000550	-0.219327

Picture 64: transaction history fragment covering anomalous rise of the ENJ token price

Such a price deviation can be explained by the fact that pool reserves are small. Transactions nr. 70632 and nr. 70633 are another MEV attack. This can be seen due to the fact that transactions nr. 70631, 70632, 70633 have the same timestamp like they were executed in one block, price decrease for the 70631 is too big, while the person that performed transactions 70632 and 70633 has a much higher token price (almost 136% higher) leading to getting a profit equal to 14 000 USD dollars (attacker around 7000 ENJ tokens, while their price for 5 September 2021 was around 2 USD dollars). This attack caused strong price deviation that was stabilized only after the next 5-10 transactions.

MEV attack in this case was also performed due to the low pool reserves and low transaction frequency. Another reason why this pool was chosen - both Ethereum and ENJ tokens are popular ones that can be easily exchanged or sold on other platforms.

	token_in	token_out	amount_in	amount_out	amount_usd	timestamp	first_to_second_price	price_change_rate
72781	ENJ	WETH	4223.478413	2.765395	1.193130e+04	2021-10-31 08:09:56	0.000655	-1.918353
72782	WETH	ENJ	0.198250	305.217692	8.492489e+02	2021-10-31 08:44:51	1539.559608	5.799831
72783	WETH	ENJ	0.320000	491.263774	1.370114e+03	2021-10-31 08:55:39	1535.199294	-0.283218
72784	WETH	ENJ	406.412201	193519.686440	1.734995e+06	2021-10-31 09:23:04	476.166035	-68.983438
72785	ENJ	WETH	197625.424650	408.295164	1.743033e+06	2021-10-31 09:23:04	0.002066	215.532801
72786	ENJ	WETH	3782.493673	2.361826	1.006688e+04	2021-10-31 09:43:28	0.000624	-69.776951
72787	WETH	ENJ	1.741229	2781.632271	7.424980e+03	2021-10-31 09:45:57	1597.510990	235.494528
72788	WETH	ENJ	0.898985	1415.216577	3.830516e+03	2021-10-31 09:52:26	1574.237437	-1.456863
72789	WETH	ENJ	0.247812	387.649542	1.055465e+03	2021-10-31 09:53:16	1564.285667	-0.632164

Picture 65: transaction history fragment covering anomalous rises ENJ price and WETH price in ENJ/ETH pool

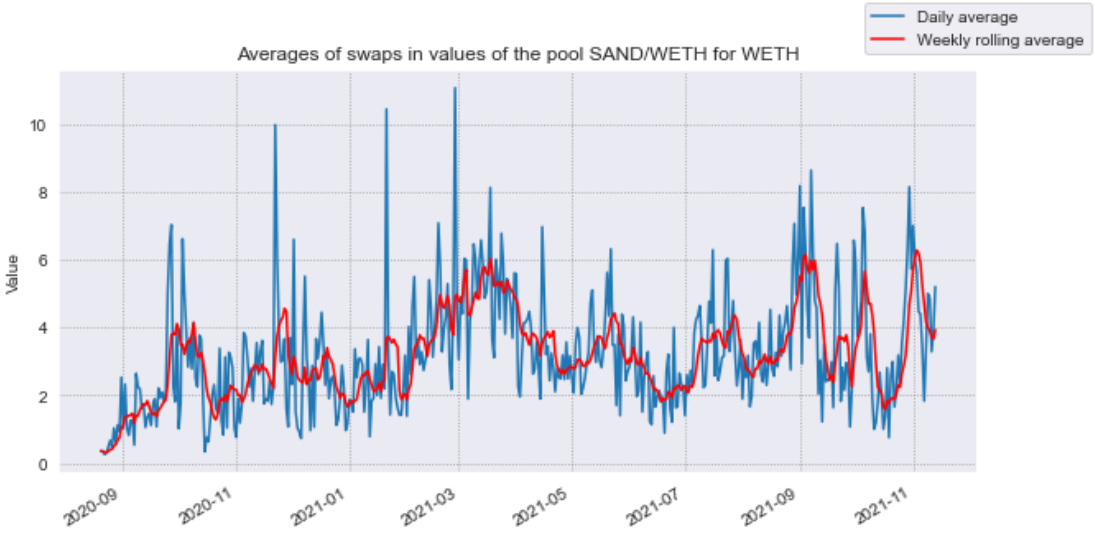
The presented transaction period is showing how small reserves allow big price deviations even from small transaction values. It is dangerous to perform swap operations in such pools considering that without setting a slippage factor a person is able to lose a lot of tokens due to change in token price.

Picture 66: reserves-based price distribution in the ENJ/ETH pool

Reserve-based price deviations are relatively high, showing how small pool reserves cause bigger price deviations. Considering that this pool contains popular tokens, small reserves and small transaction frequency there is a high chance of performing an efficient MEV attack.

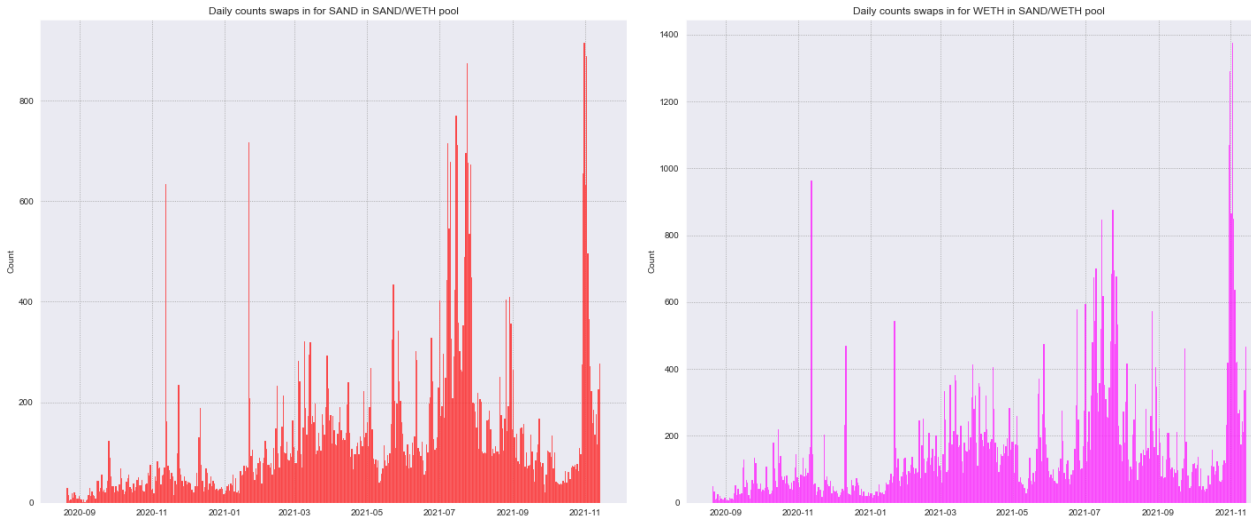
SAND/WETH (NFT) or a good case of NFT for art platform

SAND token is a NFT token used inside the Sandbox platform. This is a platform for creating voxel-based models that can be sold on this platform. This platform has its own metaverse that will be opened for each person during the end of November and December 2021. Considering the last moment, the token should have a price rise during this period and if the launch will be successful - after that. This token was found on the Uniswap V2 in pair with Ethereum.



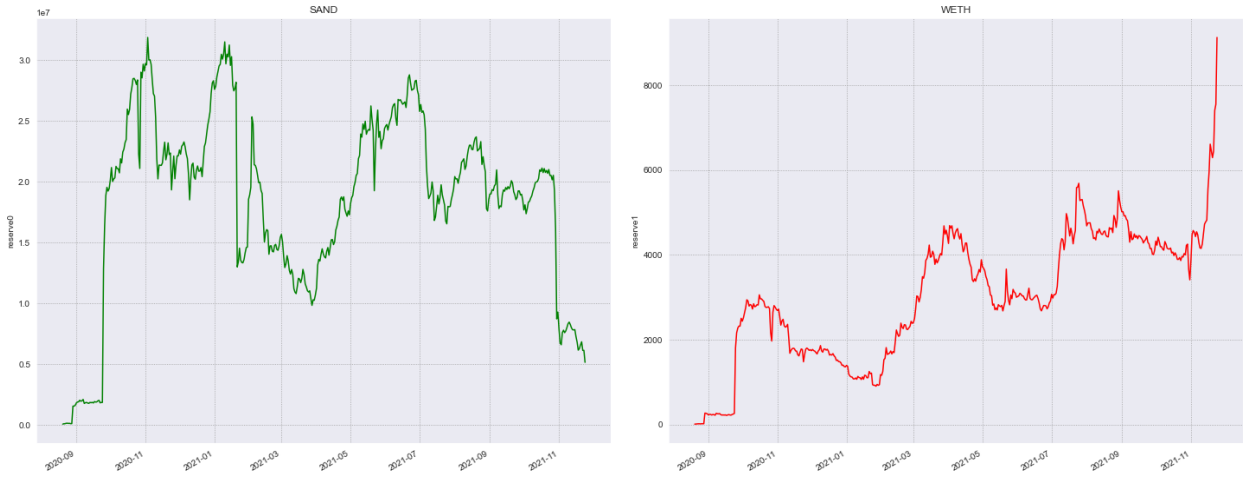
Picture 67: Swap operations activity in the SAND/ETH pool

The distribution of the SAND/ETH pool is relatively high and there are multiple high activity periods.



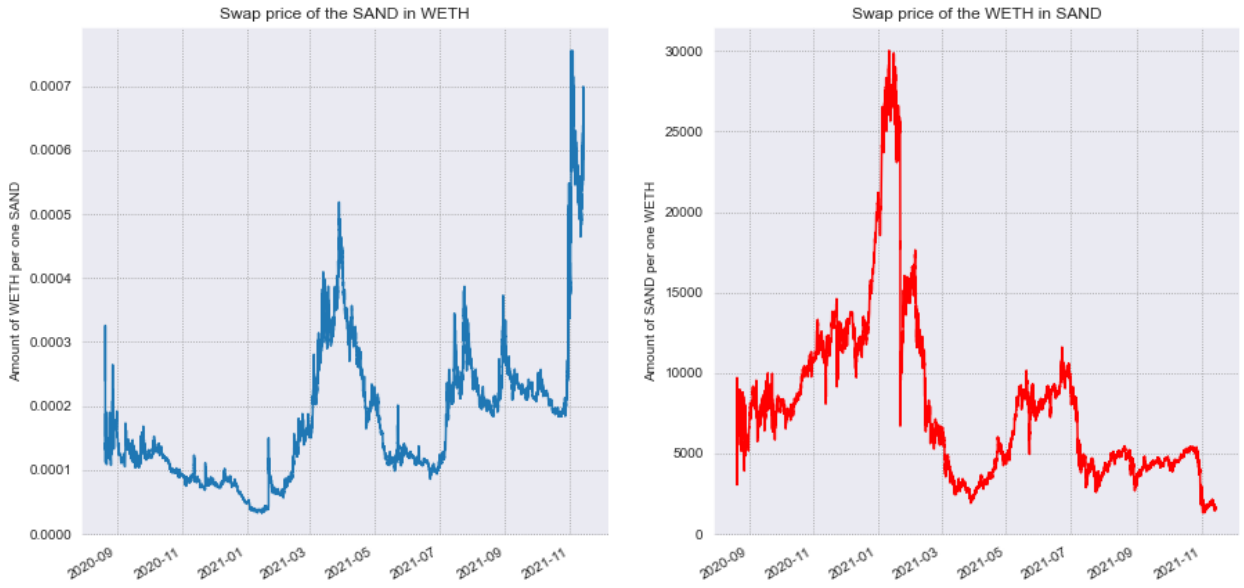
Picture 68: Swap transaction count distributions for SAND/ETH pool

First story half contains low transaction frequency, defining possible MEV attack. To check if this can be performed it is required to show reserves distribution.



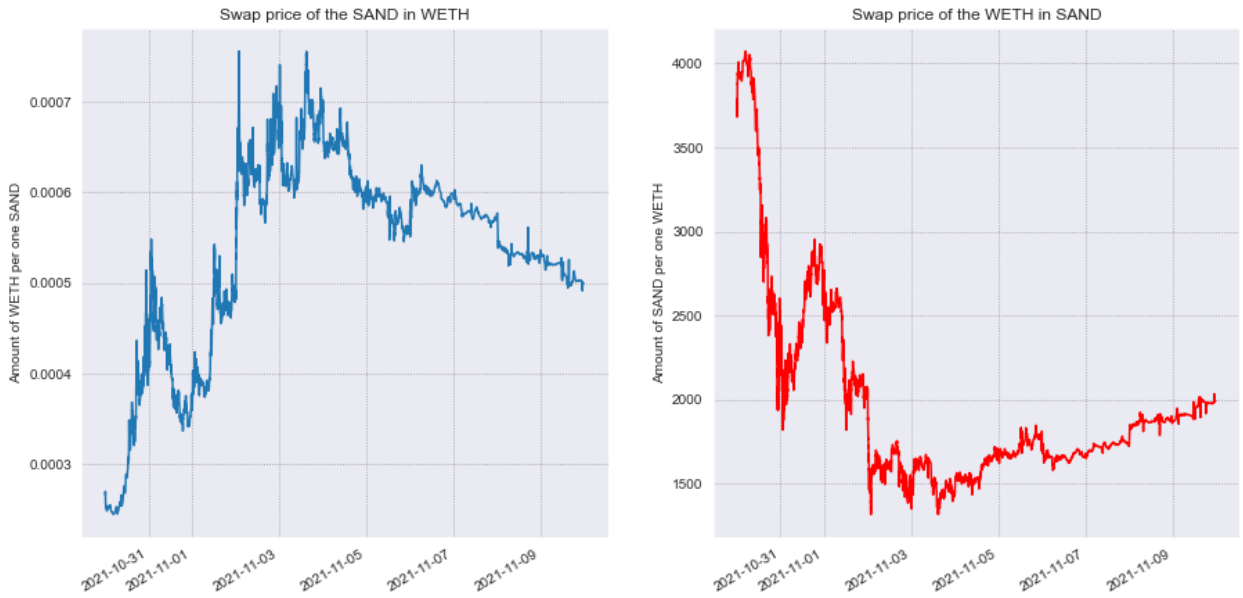
Picture 69: Reserves distribution in the SAND/ETH pool

Conform reserves distribution there is a low chance of performing an efficient MEV attack. This happens due to higher transaction values required for performing an efficient MEV attack, considering that a person should request an exchange that is able to break price distribution. To ensure that there was no MEV attack present in the pool, below are presented the swap price distribution and swap price change rates.



Picture 70: swap price distribution of the SAND/ETH pool

The presented price distribution shows anomalous changes in the SAND token price registered during the end of October and start of November 2021.



Picture 71: swap price distribution for end of October and start of November 2021 for the SAND/ETH pool

Distributions look stable, only SAND token has anomaly where SAND price drops to 0.

	token_in	token_out	amount_in	amount_out	amount_usd	timestamp	first_to_second_price	price_change_rate
117404	WETH	SAND	21.100019	44641.233396	92555.965801	2021-10-31 00:52:13	2115.696400	-1.911173
117405	SAND	WETH	5595.962492	2.652918	11637.116131	2021-10-31 00:52:13	0.000474	4.089153
117406	WETH	SAND	29.626893	61870.909727	129959.398479	2021-10-31 00:52:13	2088.336062	-1.293207
117407	SAND	WETH	44641.233858	21.293956	93406.680883	2021-10-31 00:52:13	0.000477	0.616957
117408	SAND	WETH	3916.743254	1.854685	8130.549345	2021-10-31 00:52:50	0.000474	-0.728411
117409	SAND	WETH	6561.684308	3.103175	13603.663758	2021-10-31 00:52:50	0.000473	-0.127535
117410	SAND	WETH	8251.727824	0.000000	0.000000	2021-10-31 00:53:14	0.000000	-100.000000
117411	SAND	WETH	2443.336608	1.154240	5060.441550	2021-10-31 00:53:14	0.000472	inf
117412	WETH	SAND	39.967903	85138.668516	174915.017002	2021-10-31 00:53:25	2130.176017	2.003507
117413	SAND	WETH	92157.729719	43.040572	188668.553513	2021-10-31 00:53:25	0.000467	-1.137114
117414	WETH	SAND	12.660852	26562.020660	55408.790528	2021-10-31 00:53:25	2097.964684	-1.512144
117415	WETH	SAND	17.121700	35726.873816	74964.823206	2021-10-31 00:54:24	2086.642904	-0.539655
117416	SAND	WETH	7839.143629	0.000000	0.000000	2021-10-31 00:54:24	0.000000	-100.000000
117417	SAND	WETH	2321.170427	1.101217	4821.514055	2021-10-31 00:54:24	0.000474	inf
117418	SAND	WETH	91566.427665	43.325763	189695.425244	2021-10-31 00:54:29	0.000473	-0.265784
117419	SAND	WETH	7447.186981	0.000000	0.000000	2021-10-31 00:54:29	0.000000	-100.000000
117420	SAND	WETH	2205.112064	1.031506	4516.294486	2021-10-31 00:54:29	0.000468	inf
117421	WETH	SAND	11.261579	23867.430591	49306.731400	2021-10-31 00:55:02	2119.368118	1.568319

Picture 72: transaction history fragment with strange drops in token prices

There are strange transactions happening in shown transaction history, considering that there are some swaps, where the amount of our token is equal to 0, breaking the price evolution.

	token_in	token_out	amount_in	amount_out	amount_usd	timestamp	first_to_second_price	price_change_rate
117501	WETH	SAND	2.700287	5178.375269	11832.059300	2021-10-31 01:10:19	1917.712864	2.934607
117502	WETH	SAND	22.643621	43155.494032	99265.781694	2021-10-31 01:10:28	1905.856578	-0.618251
117503	SAND	WETH	7074.861385	0.000000	0.000000	2021-10-31 01:10:28	0.000000	-100.000000
117504	SAND	WETH	2094.866455	1.098376	4815.092901	2021-10-31 01:10:28	0.000524	inf
117505	WETH	SAND	1.880000	3563.456345	8241.600121	2021-10-31 01:10:28	1895.455503	-0.545743
117506	SAND	WETH	25000.002277	13.074511	57316.433696	2021-10-31 01:10:37	0.000523	-0.255081
117507	SAND	WETH	6721.118792	0.000000	0.000000	2021-10-31 01:10:37	0.000000	-100.000000
117508	SAND	WETH	1990.123273	1.037190	4546.866459	2021-10-31 01:10:37	0.000521	inf
117509	WETH	SAND	1.626885	3068.409774	7132.541043	2021-10-31 01:11:04	1886.064141	-0.495467
117510	WETH	SAND	12.000000	22557.883510	52610.039293	2021-10-31 01:11:04	1879.823626	-0.330875
117511	WETH	SAND	22.568046	42817.679177	98942.148901	2021-10-31 01:11:04	1897.270113	0.928092
117512	WETH	SAND	5.609624	10500.000000	24597.428130	2021-10-31 01:11:14	1871.783303	-1.343341
117513	SAND	WETH	88109.608000	46.326718	203164.553079	2021-10-31 01:11:44	0.000526	0.885728

Picture 73: transaction history fragment with strange drops in token prices

There are strange transactions that have the same 0 value of out_token similar to the previous shown transaction history fragment.

There were no MEV attacks detected, defining that transaction frequency and reserves does not allow performing efficient MEV attacks. This is a stable pool with positive trends. Considering news mentioned in the subchapter beginning will cause additional price rise and positive distribution trend.

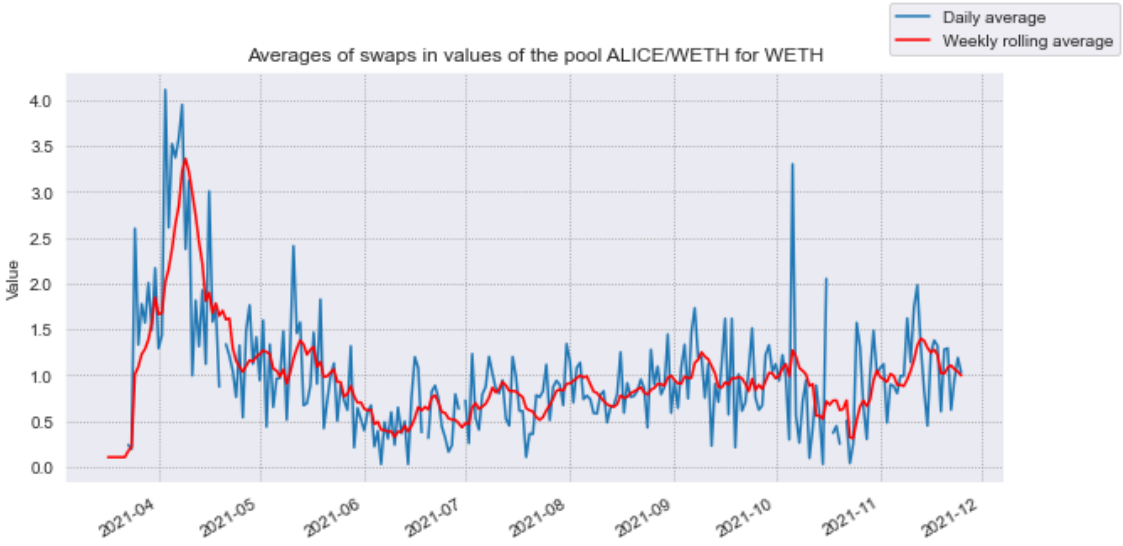
Picture 74: reserve-based price distribution of the SAND/ETH pool

This is the only case when reserve-based price was different from the real-market one. In the current SAND price distribution can see an anomalous rise between March-May 2021, while real price had a small rise compared to present rise in the pool. After this period the distribution looks similar to the real one.

Picture 75: real-market price evolution of the SAND token conform coinmarketcap.com

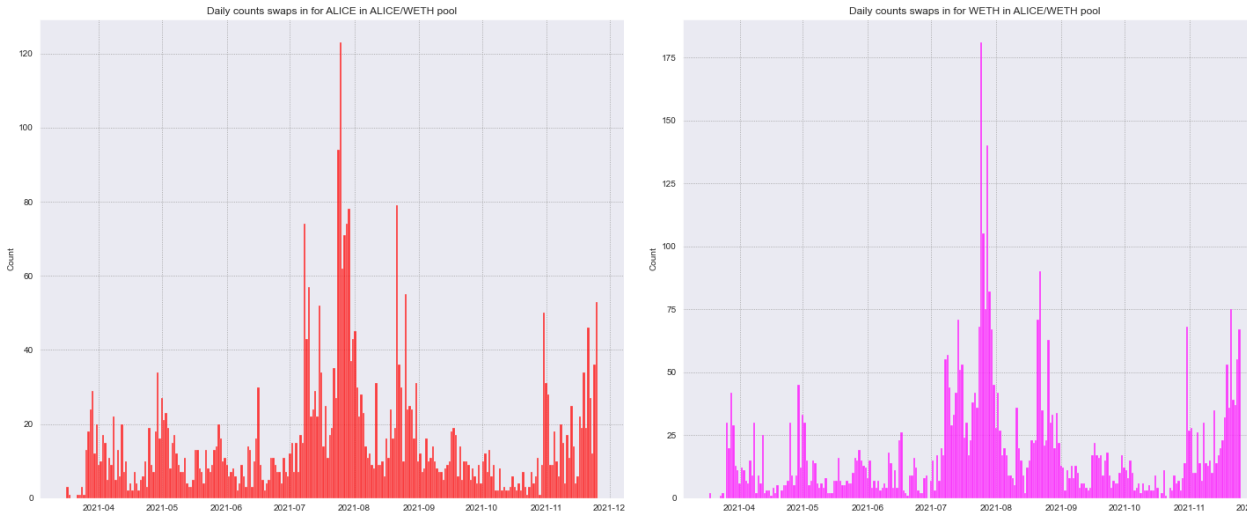
ALICE/WETH (NFT) or how unstable game tokens can be

There are multiple farming simulators on the gaming market that are popular and generate great profits to owners of those projects. This popular gaming direction also arrived to NFT, as “My Neighbor Alice” project, which is a farming/building game. ALICE token is used as an “in-game” currency for purchasing goods. This currency was found on the Uniswap V2 as a part of the ALICE/ETH pool.



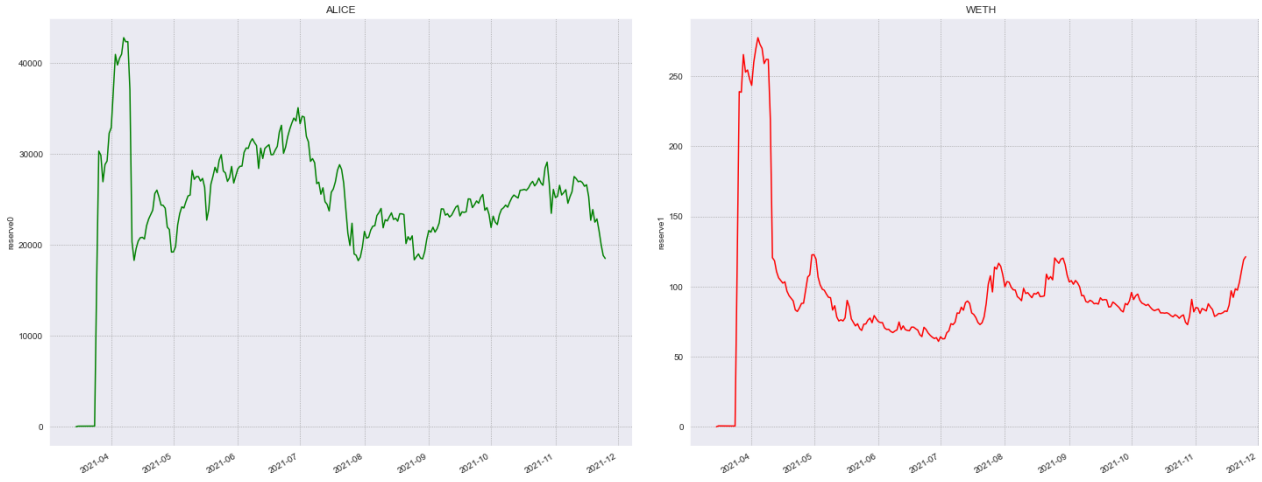
Picture 76: Swap operations activity in the ALICE/ETH pool

Activity present in the ALICE/ETH pool is relatively low, compared to the other pools, due to low capitalization of trades per day, meaning that there are either small values in transactions, or that there is a low transaction frequency.



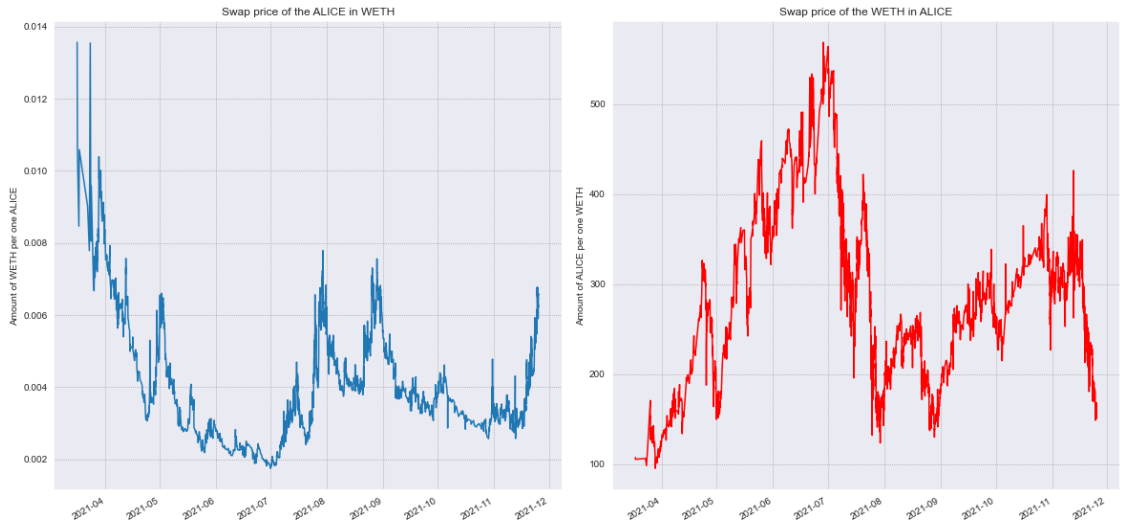
Picture 77: swap transaction count distribution in the ALICE/ETH pool

Transaction frequency is low with great transaction count rise between July-September 2021. During this period transaction history is relatively high but in other periods there is a small transaction count. Considering that it is important to check pool reserves and possible presence of MEV attacks.



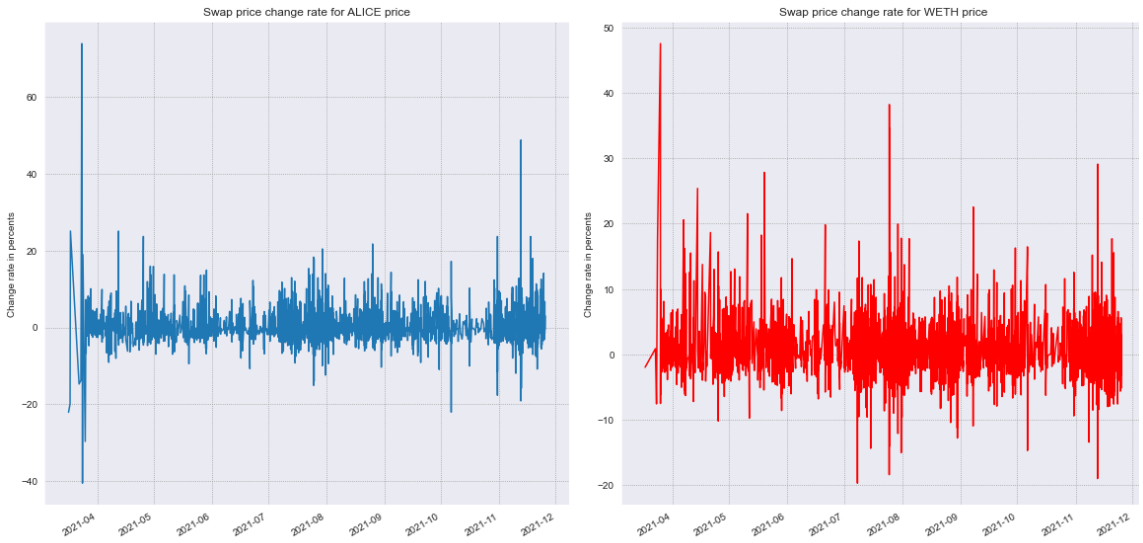
Picture 78: Reserves distribution for ALICE/ETH pool

Reserves present in the pool are relatively small and even considering their stable distribution their values are small to ensure safe trading without MEV attacks. To check their presence below are presented swap price distributions and swap price change rates.



Picture 79: swap price distributions in the ALICE/ETH pool

Conform present distributions there are no strange extreme drops or rises in the token prices, but the price deviations are relatively high, making distributions unstable. Considering that, below is the swap price change rates distribution.



Picture 80: swap price change rate for ALICE/ETH pool

The noise present in the distribution and its high values show how unstable the current pool is. It means that this pool can be an easy target for heavy MEV attacks, but the reason why this pool is not attacked by the MEV is that the pool is not popular. Amount of transactions is more-less stable, but transaction frequency is small, present tokens are not widely popular compared to previous ones. Still, with the rise of popularity and token price, the current pool can become an easy target for performing MEV attacks.

DOGE/WETH (Meme-token) or how joke became a serious project

Easy to get, easy to lose, hard to forget

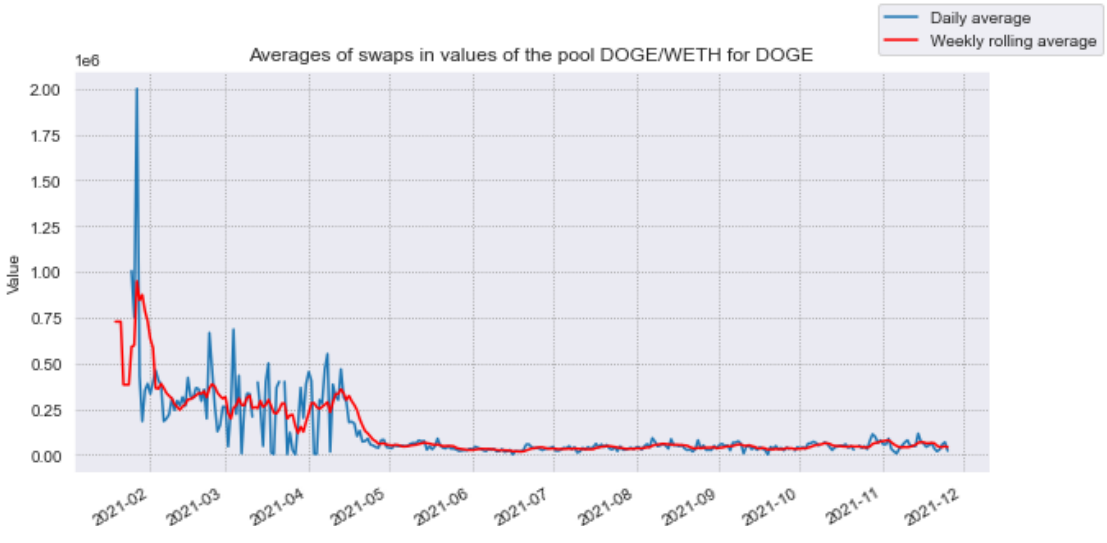
All previous cases represented pools of altcoins, NFT and stablecoins. Those tokens represent complex cases, when behind the token are some organization, communities, companies, start-ups, complex media or even meta-worlds. But there is another case of tokens, one that contains the most unstable, unpredictable and strange behaviors - meme tokens.

Meme tokens are created to hype around some popular memes and their price is almost in all of the cases speculative, meaning that their prices are based on supply and demand. This supply and demand is not controlled. Due to those market properties meme-tokens are an easy way to get big profits in a short time, but from another point of view this is an easy way to lose financial resources due to unpredictable fast token price drops or other unique market situations.

Due to presence of the MEV attacks, some transaction frequency drops that cause TWAP mitigation mechanisms inactivity in previous cases it is important to consider such cases and analyze their behavior. Each pool will be reviewed also from the history perspective to understand why some distribution changes have occurred.

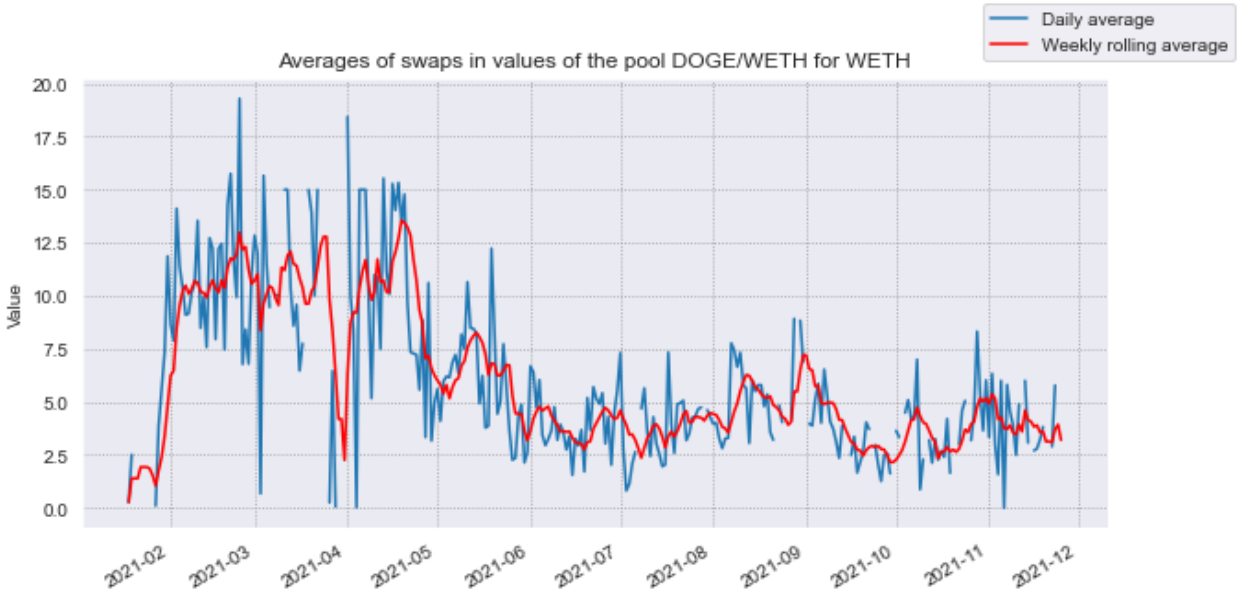
How Twitter activity and Reddit communities are able to rise and drop token price

As a first meme-token for analysis was chosen a DOGE coin - a project that was launched in December 2013 as a “joke” by two software engineers. Pool DOGE/WETH was found on the Uniswap V2 and below are presented the swaps transactions distributions.



Picture 81: swap operations distribution of the DOGE/WETH pool for DOGE

Until the middle of April 2021 there are higher transaction token values. After the middle of April 2021 happened a big decrease of swap activity and distribution became stable, but token values are much smaller.

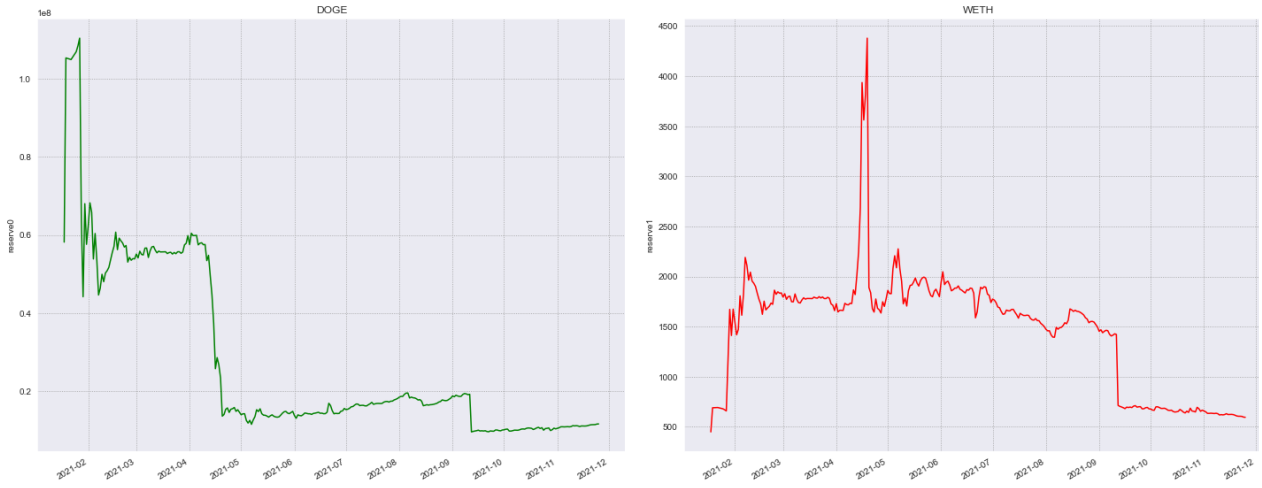


Picture 82: swap operations distribution of the DOGE/WETH pool for WETH

Swap operations distribution for WETH token has higher values, considering the WETH token price capitalization of the pool keeps relatively high, but the distribution is dropping starting from the middle of April 2021.

Considering those market changes authors decided to check what changes caused such drops in distributions. Starting from 2019 this token has been actively mentioned by many popular persons, like Elon Musk, Snoop Dogg, Jin Simmons and many other popular persons, mentioning their either interest in this token or showing that they have some tokens in their wallets. During the Spring 2021 token price has greatly increased after multiple tweets from Elon Musk (also about the fact that he bought some coins for his son), when SpaceX decided to “send this coin to the moon”, when Dallas Mavericks became the first NBA club that started selling tickets for DogeCoin, and when a popular traders group “WallStreetBets” (responsible for one of the biggest share price pumps with GameStop shares) opened for a short time discussions about DogeCoin (links: 1, 2, 3, 4, 5, 6). Such an interest in token raised a token price, causing multiple changes not only on the market but also in the current pool.

Drop in the swap distribution is caused by the token price raise, causing people to perform swap operations with smaller token values. Another moment is that token price changes caused burns in pool reserves, presented below.



Picture 83: reserves distributions for DOGE/WETH pool

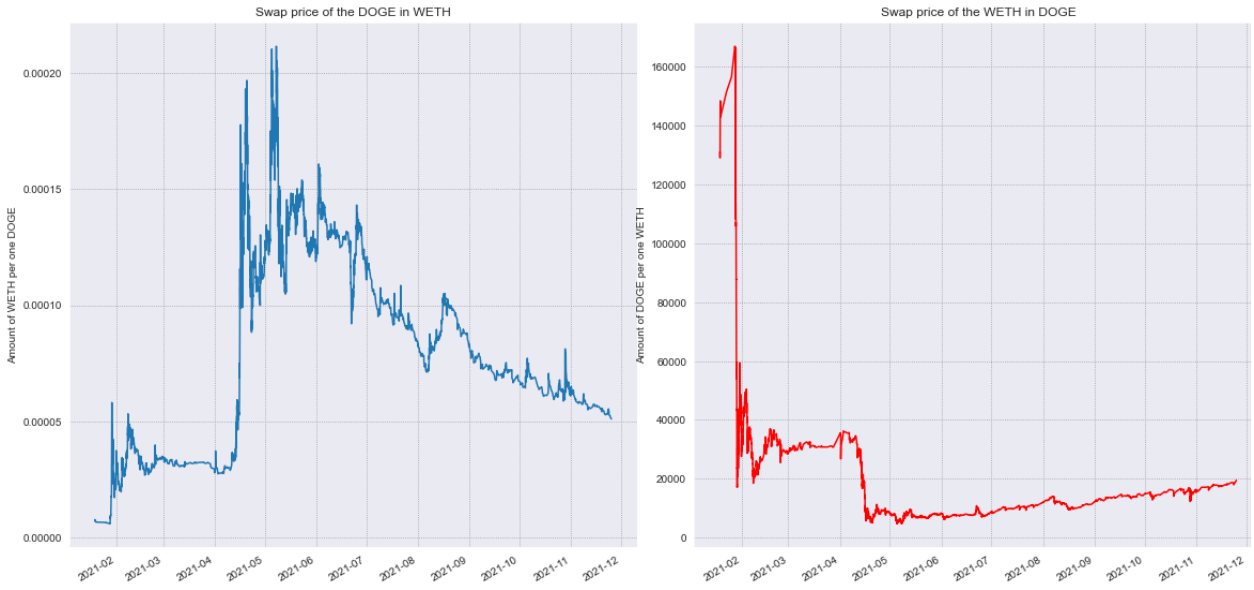
Conform presented distributions there was a great drop in reserves around the middle of April 2021. There is an additional drop of the reserves around the middle of September 2021.

Picture 84: DOGE coin price distribution for last year taken from CoinDesk

Conform presented price distribution DOGE had a drop around September 2021, causing decrease of reserves. One of the reasons why the price decreased is some critique coming from popular persons, raising questions about current token operation fees, asking for their decrease to ease token operations (link).

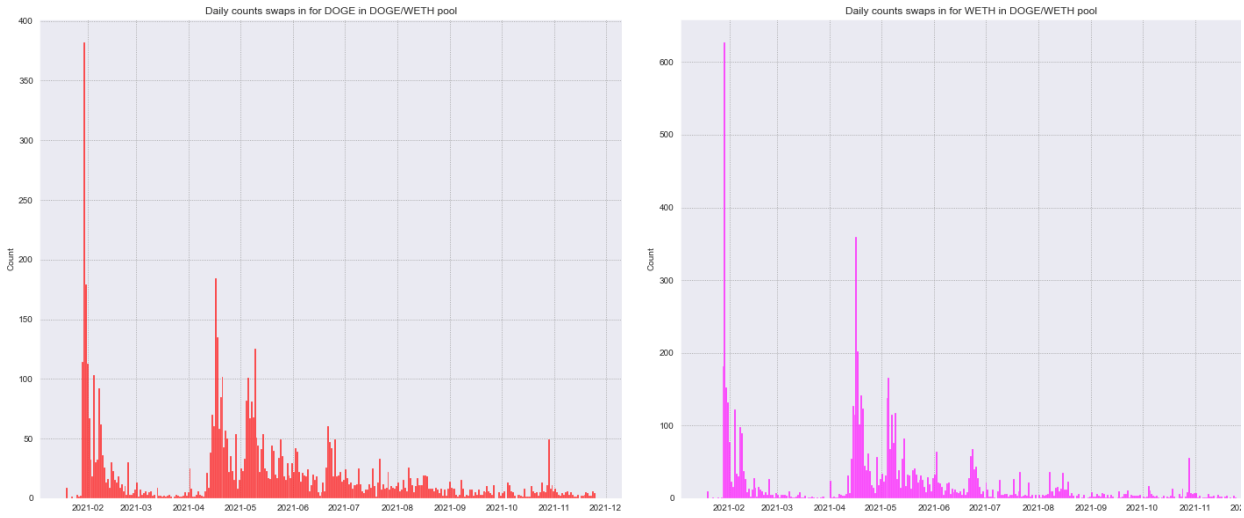
Picture 85: reserve-based price distributions in the DOGE/WETH pool

The price distributions of the pool have some differences compared to the real-market price distribution. DOGE price had a peak around May and start of July 2021, but starting from the September 2021 pool-based price is slowly decreasing while real price had local rise during October and small decrease around November.



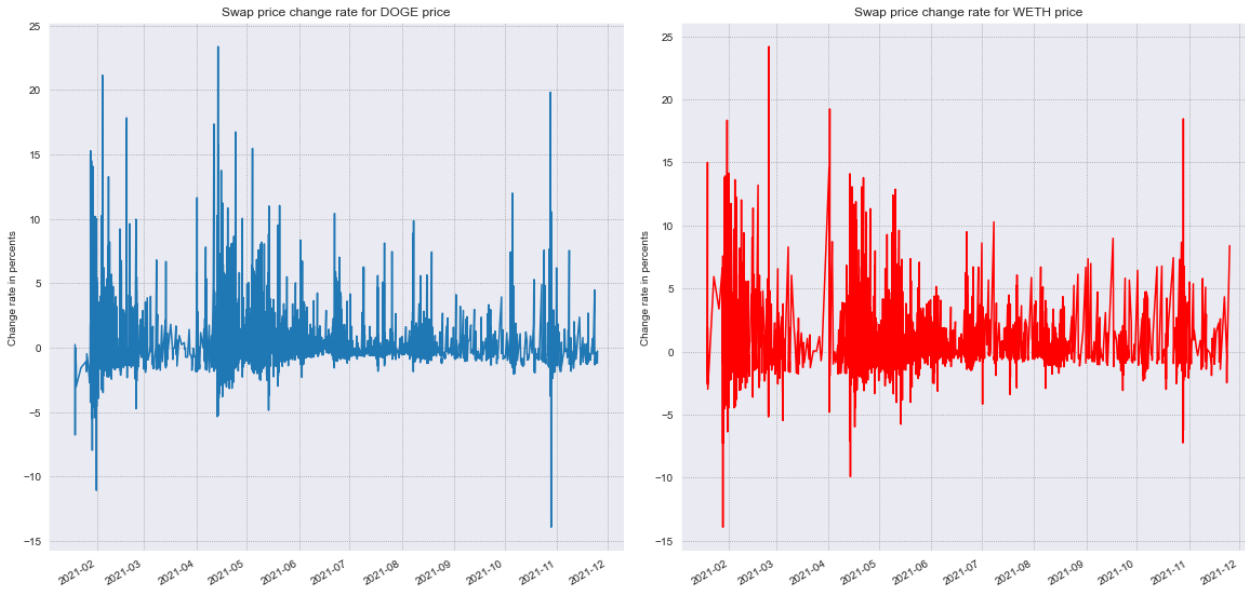
Picture 86: swap-based price distributions for the DOGE/WETH pool

Presented distributions demonstrate high deviation of values around high-activity periods, showing high traders interest and their desire to exchange the tokens. After anomalous price rise distribution becomes stable and there are no extreme deviations in token price. To ensure that this is caused by high transaction frequency below is presented the transaction count distributions.



Picture 87: transaction count distributions for the DOGE/WETH pool

Conform presented distributions there are some transaction frequency rises. Most of the time transaction count is small and therefore there is an option of performing MEV attack over the pool, considering the possibility of too big time gap between transactions, but according to the presented swap-based token prices distributions there were no MEV attacks.



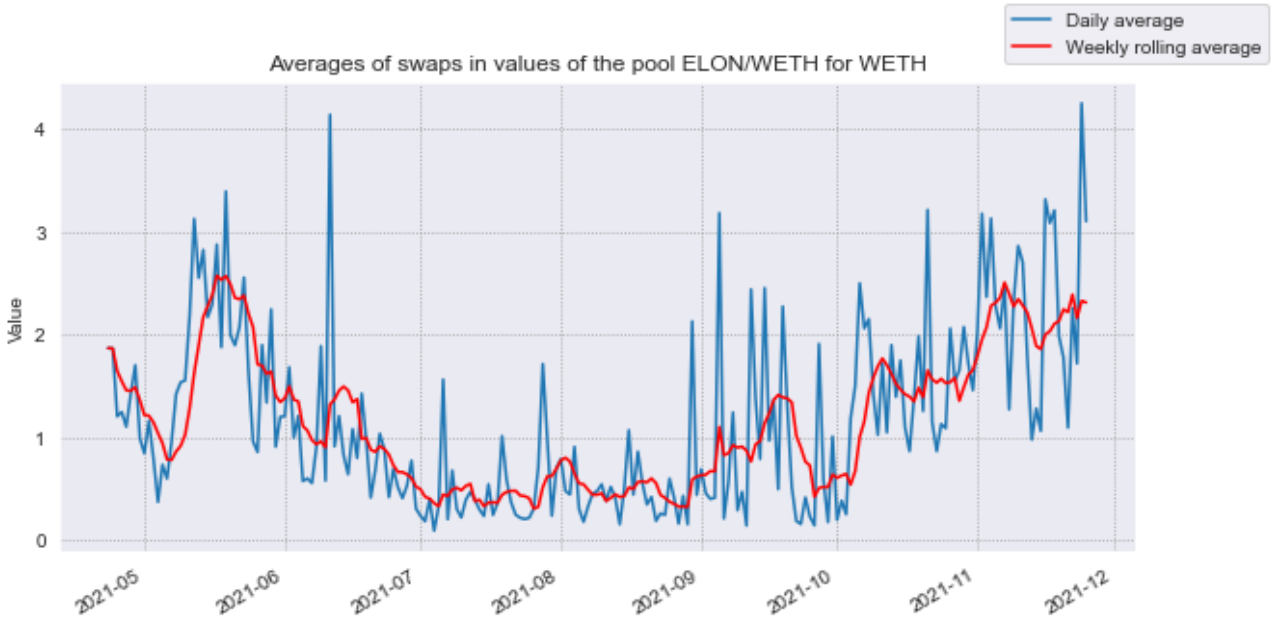
Picture 88: swap-based token price change rates for DOGE/WETH pool

Conform presented charts there were no anomalous price changes that would demonstrate the MEV attack pattern. It does not mean that such an attack will not happen in the future. Small reserves, small transaction frequency and token popularity can cause attackers attention to this pool.

ELON/WETH (Meme-token) or how unstable memes can be

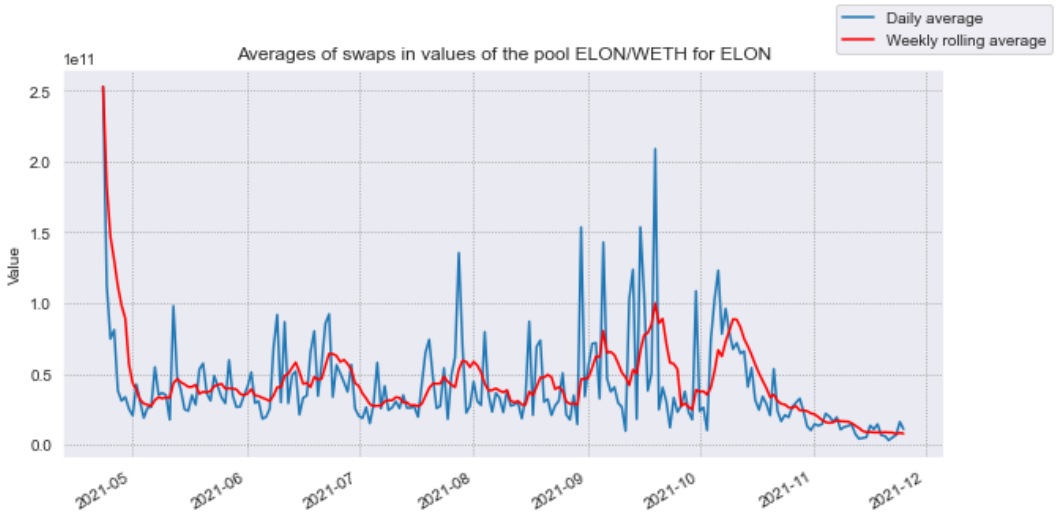
After multiple Dogecoin market changes caused by the Elon Musk tweets and activity there appeared a new token named Dogelon (ELON token), which is another meme-token. It appeared this year and its price is always changing. Considering that this is a relatively new token and its appearance right from the beginning in the Uniswap V2 platform as a part of ELON/WETH pool it was decided to dive deeper into its analysis.

Due to the low token price of ELON below is presented the WETH swap distribution over ELON/WETH pool, where it can be seen that the amount of operations happening per day is relatively small. Higher pool activity was registered between May-June 2021 and between September-November 2021 and it keeps rising up.



Picture 89: swap operations distribution of the ELON/WETH pool for WETH

ELON swap distributions keep on almost the same level for entire registered token history and rolling week average demonstrates wave-like distribution of the swap operations.



Picture 90: swap operations distribution of the ELON/WETH pool for ELON

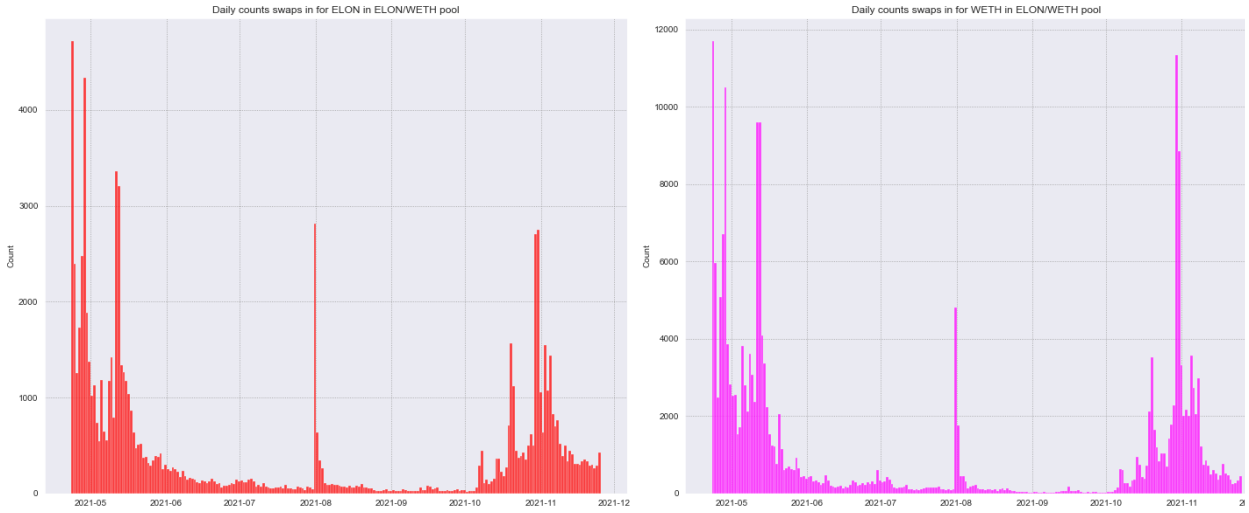
The interesting moment is that transaction count in the current pool has anomalous rises and drops that can be seen in the distributions presented below. There were registered 3 rises:

- Between end of April and middle of the May 2021;
- Start of August 2021;
- Between the start of October and the start of November 2021.

The same high activity periods were registered for the WETH side of the ELON/WETH pool. This distribution corresponds with real-market changes of the ELON token price meaning that each rise of the token price caused a rise of the swap activity. In the last period can be seen a drop of the swap activity related to token price decrease and stabilization.

Picture 91: ELON token price evolution taken from Crypto.com

Transaction count distribution clearly demonstrates how popular meme-tokens can be and how many transactions can happen during high-activity phase.



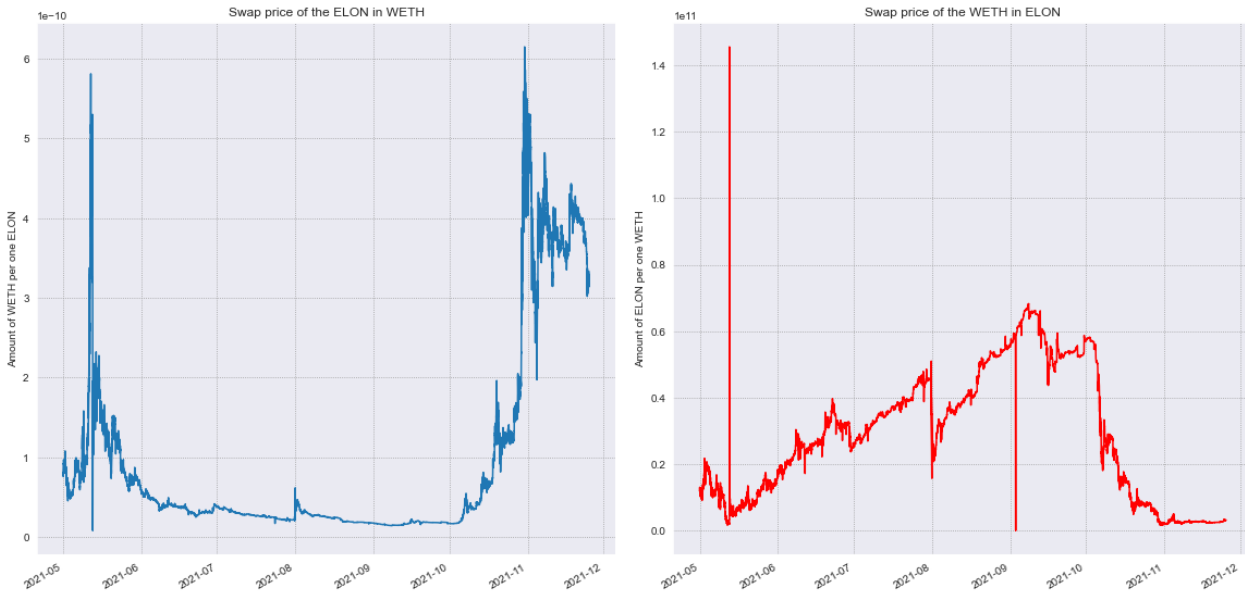
Picture 92: transaction count distribution for ELON/WETH pool

Transaction frequency during small activity periods show that there is an option of performing MEV attack. In order to check the possibility of performing such an attack it was decided to check pool reserves.

Picture 93: reserves distribution for ELON/WETH pool

ELON reserves distribution shows slow increase of available tokens until last registered anomalous rise that caused big token burn. WETH reserve shows rise of liquidity during May 2021 after which comes a low reserves period, defining low trust to this token pair, after which comes anomalous rise of WETH tokens in the pool, defining great rise of traders interest to the

token. Due to big changes in reserves and big transaction frequency rise and drops it is required to check swap price distribution for the current pool.



Picture 95: swap-based price distribution for ELON/WETH pool

Distribution of the swap-based price starting from May 2021 shows that ELON token price had two giant rises during May 2021 and starting from October 2021. There are two anomalous changes in the token price from the WETH token price side, that look like MEV attacks. After deep pool history analysis was the only one strange transaction, price for which greatly increased, while there was no registered reserves drop or any big changes.

	token_in	token_out	amount_in	amount_out	amount_usd	timestamp	first_to_second_price	price_change_rate
201473	WETH	ELON	1.322041e-02	7.811944e+08	4.939528e+01	2021-09-03 01:08:31	5.909002e+10	-3.443978e-02
201474	WETH	ELON	9.000268e-03	5.318127e+08	3.362562e+01	2021-09-03 01:11:34	5.908854e+10	-2.502673e-03
201475	ELON	WETH	5.457151e+09	9.179362e-02	3.427337e+02	2021-09-03 01:19:07	1.682079e-11	5.973902e-02
201476	ELON	WETH	3.569799e+10	6.000000e-01	2.238869e+03	2021-09-03 01:53:39	1.680767e-11	-7.804131e-02
201477	ELON	WETH	1.933268e+09	3.247048e-02	1.221740e+02	2021-09-03 02:50:43	1.679564e-11	-7.153145e-02
201478	WETH	ELON	1.000000e-18	1.000000e-18	3.771929e-15	2021-09-03 03:17:31	1.000000e+00	-1.000000e+02
201479	WETH	ELON	2.200650e+00	1.299231e+11	8.360580e+03	2021-09-03 04:07:53	5.903853e+10	5.903853e+12
201480	ELON	WETH	5.027630e+09	8.485039e-02	3.237747e+02	2021-09-03 04:37:52	1.687682e-11	4.832956e-01
201481	WETH	ELON	4.700149e-01	2.767094e+10	1.791605e+03	2021-09-03 04:57:30	5.887248e+10	-2.812665e-01
201482	WETH	ELON	7.000000e-01	4.115662e+10	2.669034e+03	2021-09-03 05:00:46	5.879516e+10	-1.313210e-01

Picture 96: transaction history fragment with strange transaction, where was registered anomalous price change

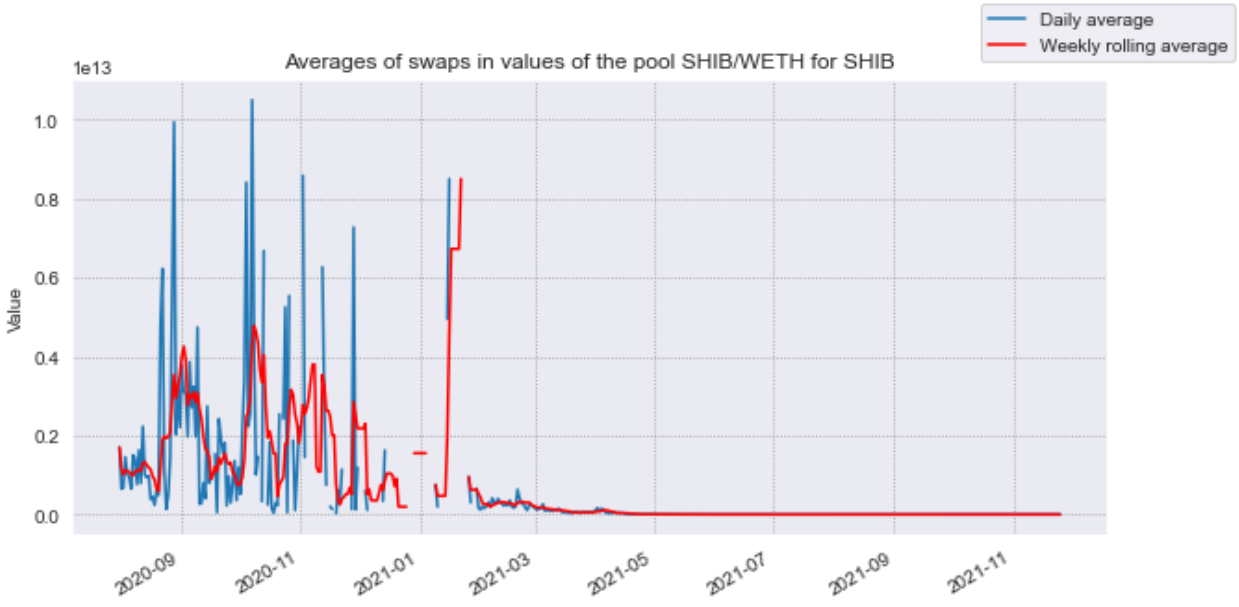
There was no MEV attack detected during the pool analysis. While transaction frequency opens an option for performing a MEV attack, reserves values are relatively high compared to previous pools, meaning that an attacker must obtain a large financial power to perform an

attack, meaning that there is a very small chance of performing such an attack. Still, considering small token lifecycle and that this is a meme-token, distribution of which much depends on the news related to this token, this pool may be unstable and there can be multiple token changes in the future, causing distribution drops and rises.

SHIB/WETH (Meme-token) or unstable token case

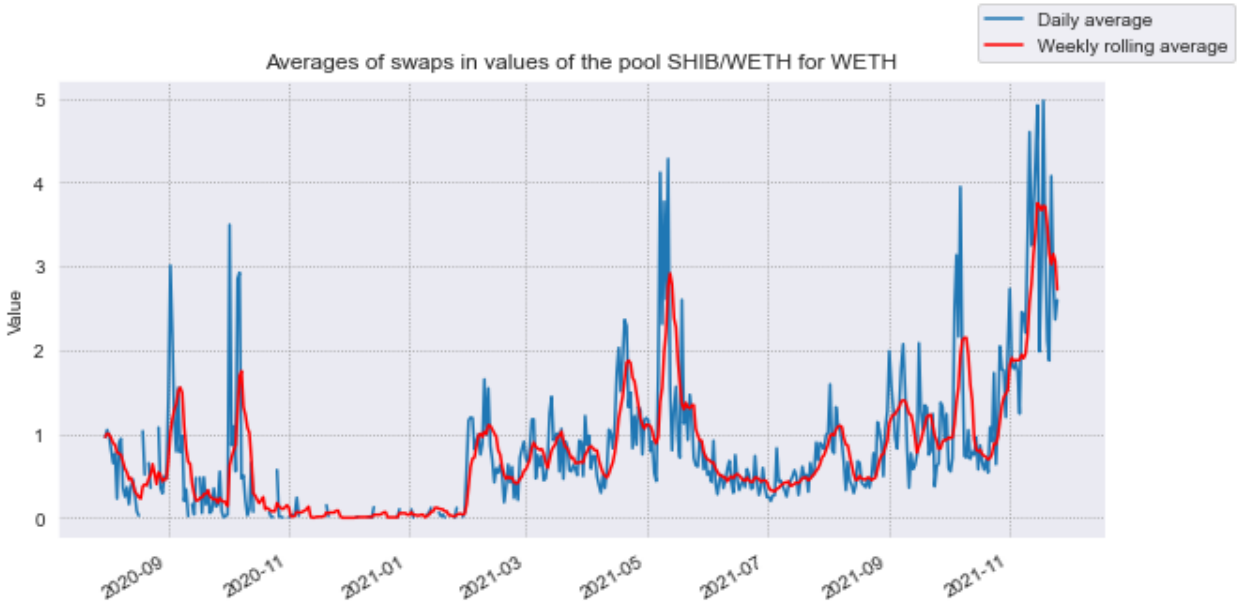
How one token phenomenon can cause appearance of another one

The Dogecoin phenomenon caused higher interest to the meme-tokens, increasing community interest in the meme-coins. Those changes caused the appearance of some coins like ELON (Dogelon), but the current case is a little bit different. Shibu Inu token is a token that appeared at the August 2020 as a "Dogecoin killer" making this token an unique case of the token launched as another token killer. There is one strange moment about this token - the goal of the token is to beat a Dogecoin capitalization without crossing the 0.01 USD dollar threshold price. One of the inspirations for creating this project was the case of the WallStreetBets group that raised GameStop share price. On the 4-th October 2021 there was a token price rise that happened due to the tweet from Elon Musk about this token. Another interesting moment is that this token almost reached the desired capitalization value (to overcome Dogecoin capitalization, links: 1, 2, 3).



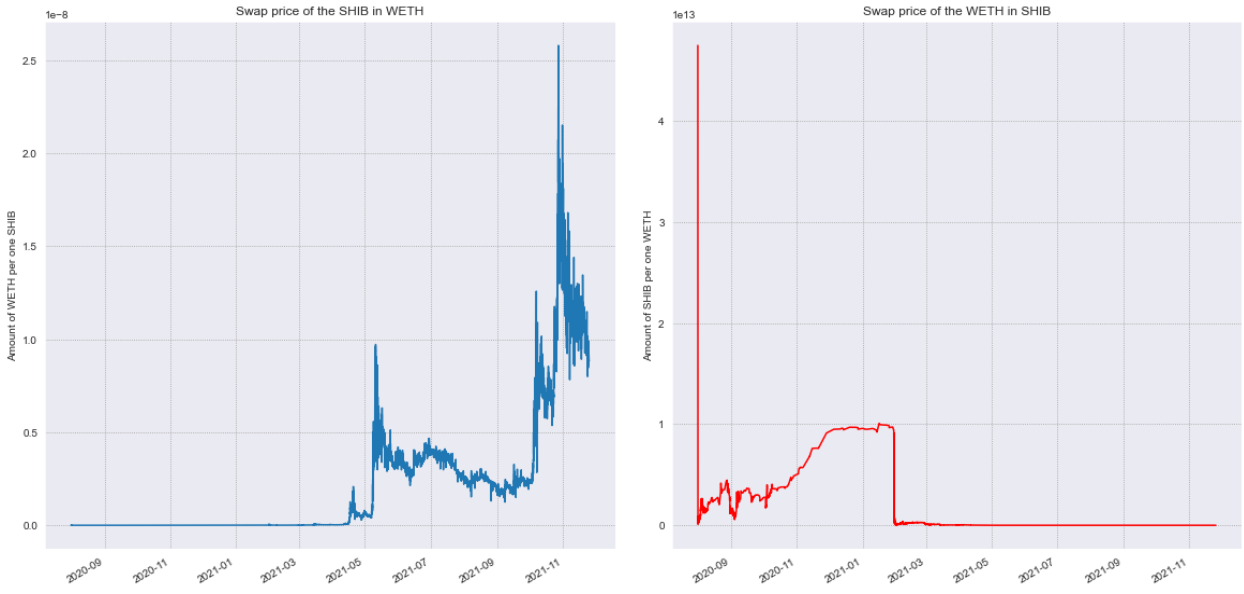
Picture 97: Swap operations distribution of the SHIB/WETH pool for SHIB token

Swap operations distribution looks unstable until February 2021, after which happened a distribution stabilization with smaller transaction values for current token. This could happen due to the Shibu Inu token price rise and this moment will be reviewed later.



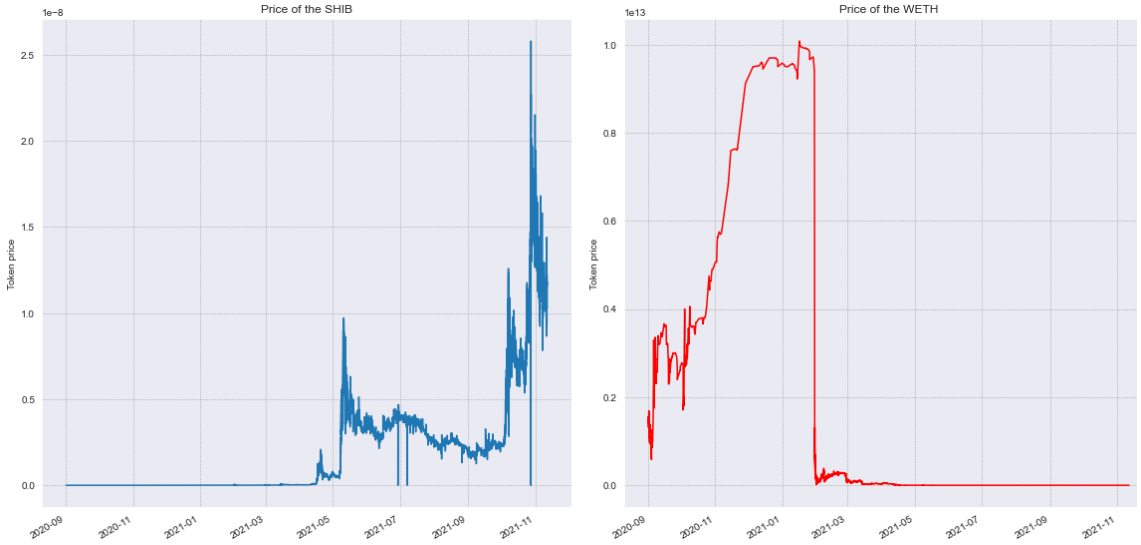
Picture 98: swap operations distribution of the SHIB/WETH pool for WETH

Pool swapping operations distribution from the WETH side looks more representative considering the rise of the transaction values starting from February 2021. To ensure that such a swapping activity is related to the token price below are presented swap-based price distributions and real-market based ones.



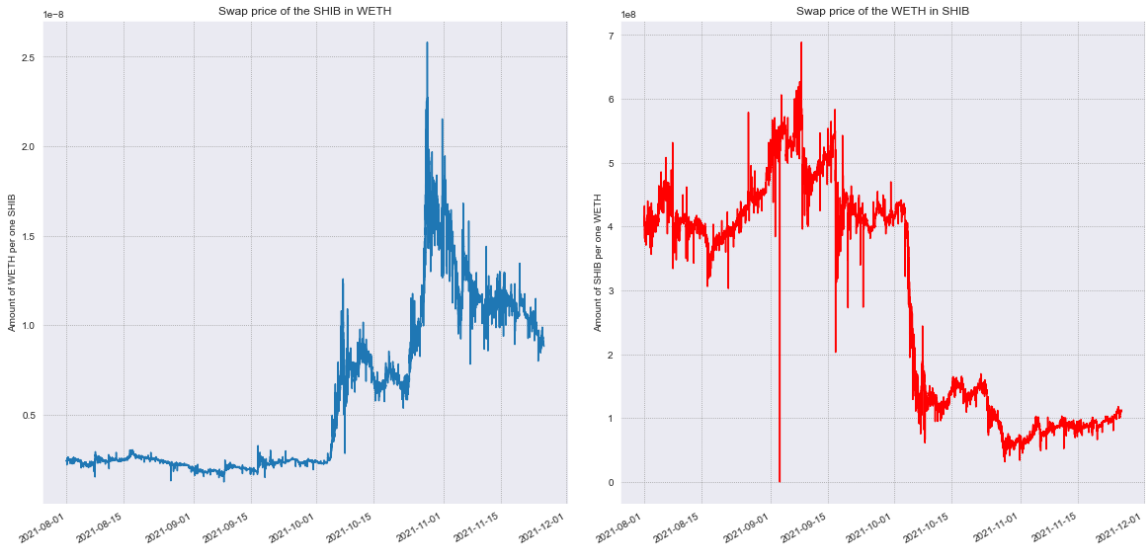
Picture 99: swap-based token price distributions for SHIB/WETH pool

Conform presented swap-based prices Shibu Inu token price had a great rise. Considering that first transactions have anomalous changes in prices distributions it was decided to move chart periods starting from September 2020 and distributions have become more readable.



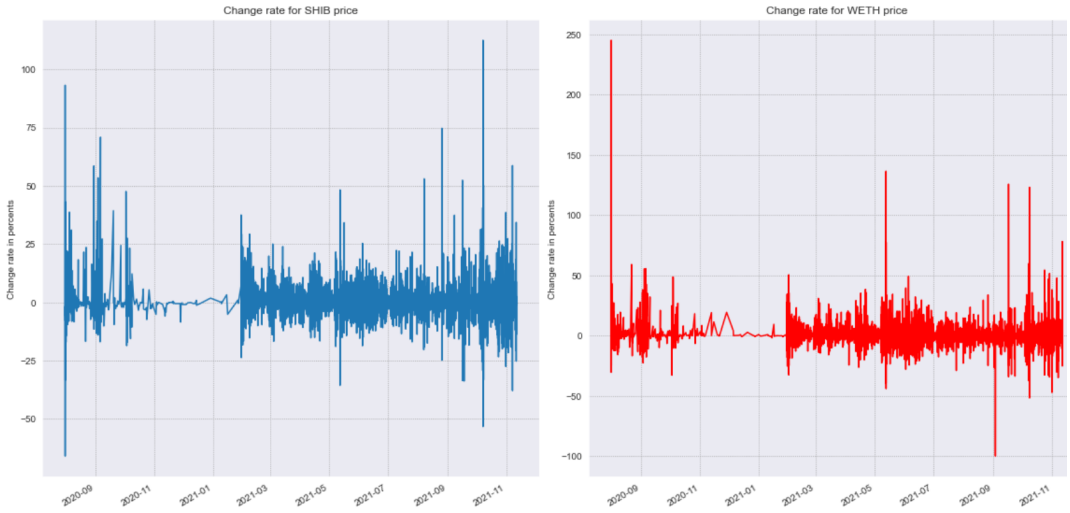
Picture 100: swap-based price distributions for the SHIB/WETH pool starting from the September 2020

Until the middle of April 2021 the SHIB price was keeping on very low values after which started anomalous token price rises. During those high activity periods token price deviations were high and there were some strange token price falls. Considering such a big token price rise it was decided to look for the last 3 months price distribution.



Picture 101: swap-based token price distributions for SHIB/WETH pool from the August 2021

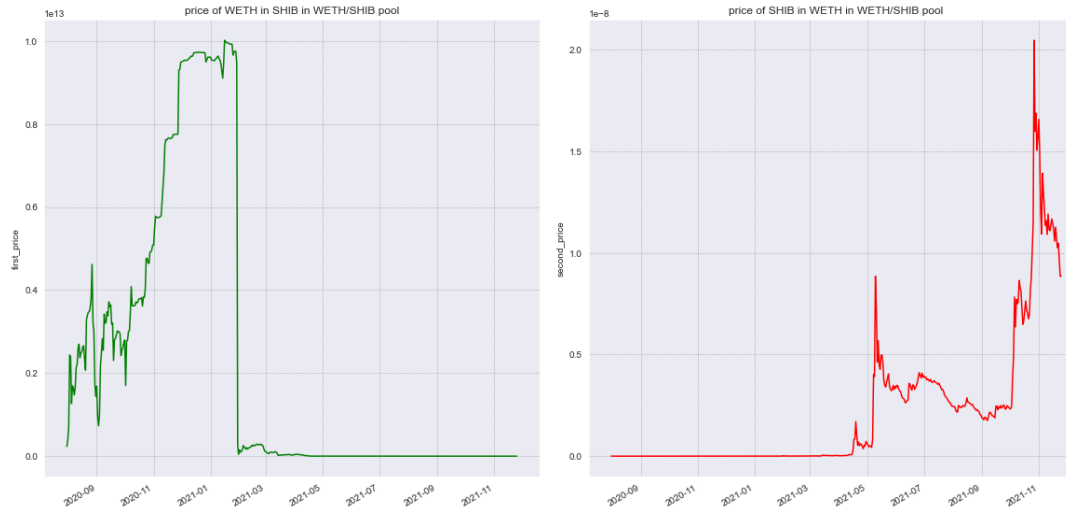
Price distributions are unstable, containing some extreme rises of the token price for the SHIB side and extreme drops for the WETH side which should be verified and analyzed from the change rates perspective.



Picture 103: swap-based price change rates distributions for SHIB/WETH pool

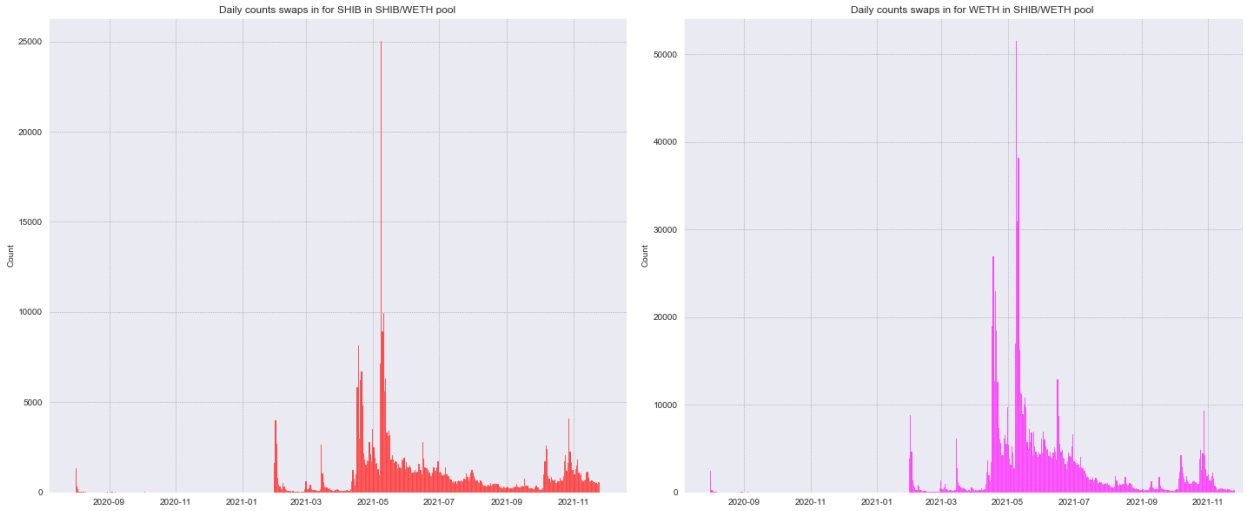
Conform presented distributions can be seen that the pool is unstable, prices for SHIB have high deviation and it is hard to predict which price value will token have in the future. The same unstable picture can be seen in reserve-based prices. Still, SHIB has a positive price trend and WETH has a negative trend referred to the SHIB token. Deviations in the token price reduce attractiveness of the pool for investors, considering that drops and rises are relatively big, compared to altcoins examples.

When reserves are weak, but transaction frequency is high



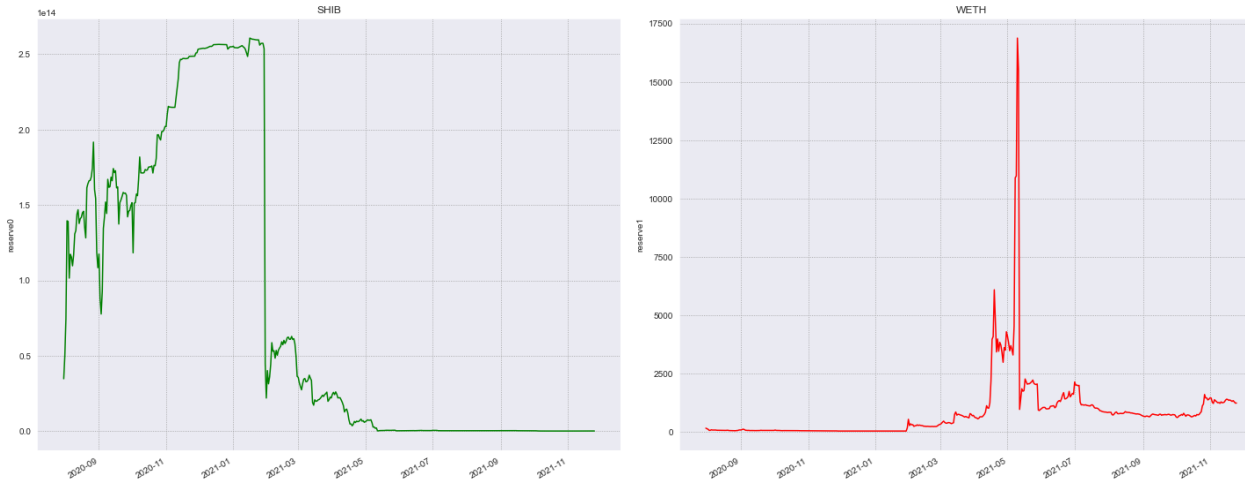
Picture 104: reserve-based price changes in the SHIB/WETH pool

Price distribution is unstable even from reserves perspective. Considering those high price deviations it is required to check for possibility of performing MEV attacks.



Picture 105: swap transactions count distribution for SHIB/WETH pool

Conform presented distribution pool activity was almost around 0 between September 2020 and February 2021, but after that pool activity had an anomalous rise of pool activity and high transaction frequency is keeping through the entire remaining time of 2021. There are multiple drops, but considering present values frequency is still relatively high.



Picture 106: reserves in the SHIB/WETH pool

Presented values in reserves of the SHIB/WETH pool were relatively high in the time interval between April 2021 and June 2021 making possible MEV attacks hard to implement. But in other periods the amount of required financial power to perform attacks is much lower and

the only factor protecting the current pool from performing such an attack is TWAP mitigation mechanism.

SQUID/WETH or how fraud with one token influences another one

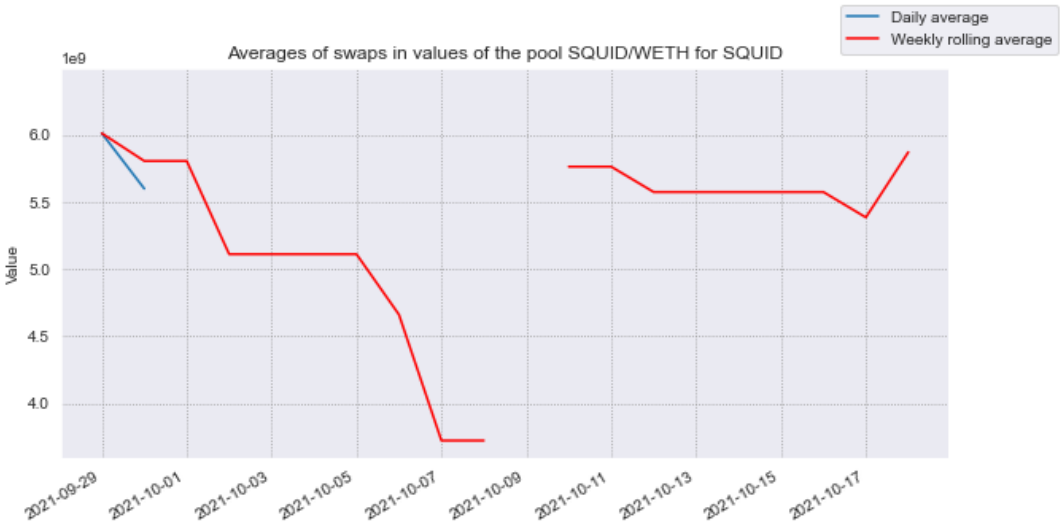
Why is this an interesting case?

Authors decided to take a look at an interesting case that happened with one of the new tokens, that was dedicated to the new TV-series made by Netflix called the “Squid Game”. The token was named SQUID and it was launched on the 20-th October 2021. After getting to the high price (around 3 000 USD dollars), the token was massively sold. Conform original concept, the principle behind the token was to have access to buying the token and winning selling option via web-games dedicated to this specific token (founders web-games). Trader was able to sell the token only after winning any “SQUID” game, but at the moment of token launch there was no web-page available for mentioned games. Conform transaction history that can be found on the Etherscan founders of the SQUID token changed several times the contract for the token (they left a specific window in the original contract in order to be able to change its behavior) and before selling the tokens massively founders changed the contract, opening selling option for the founders.

This led to the massive price drop from around 3 000 USD dollars to less than 1 USD dollar. This token is currently considered as a “scam” token (there were predictions from several sources about the “scam” scheme of this token) and founders extracted around 3 million USD dollars (sources: 1, 2, 3, 4).

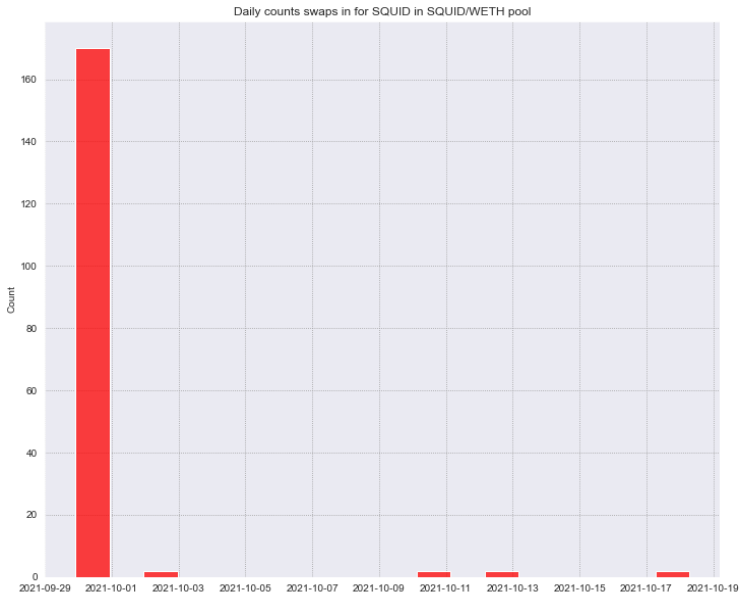
What connection can be between SQUID from SQUID/ETH pool and the “scam” one?

There was a token registered in the Uniswap V2 starting from the end of September 2021, which means that SQUID token reviewed in this section is not the “scam” based one, but reputational damage that was received by all the “Squid Game” theme may sign a soon end of the SQUID/ETH lifecycle.



Picture 107: Swaps transaction history of SQUID/ETH pool for SQUID

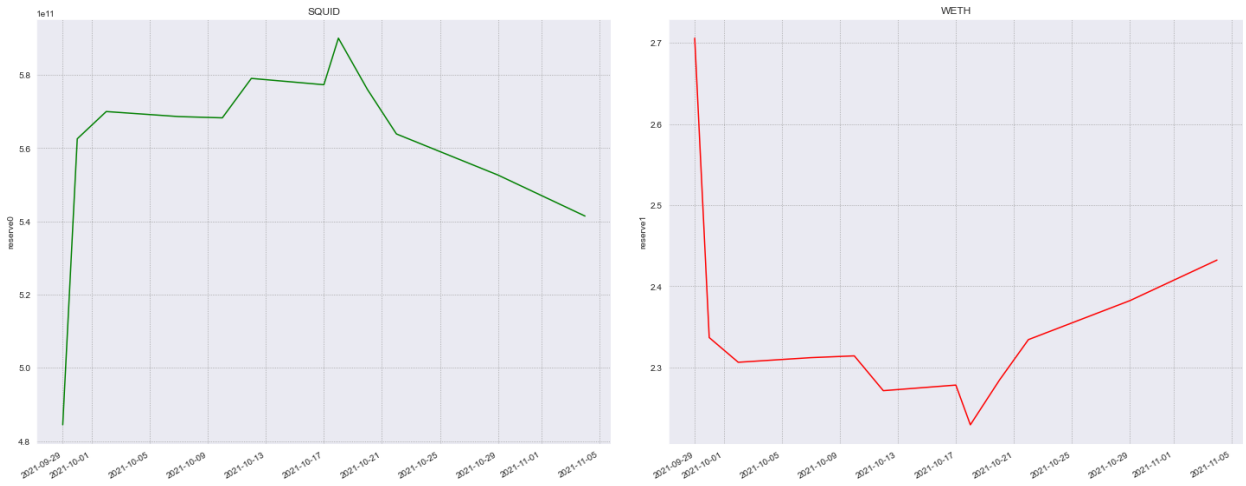
During even such a small lifecycle the pool activity is extremely low and distribution shows small transaction frequency.



Picture 108: SQUID/ETH swap transactions count

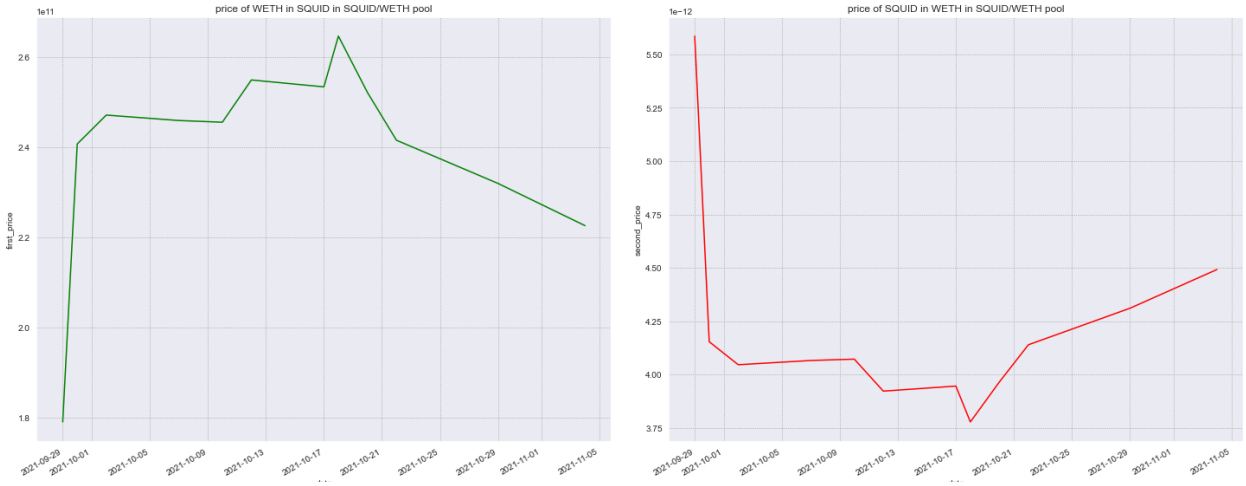
Why is the weak pool not always a target for MEV attack?

Here it can be clearly seen that SQUID token is not a popular one and there is a small activity period during the start of the pool lifecycle. This pool can be an easy target for any attack, but the problem of the pool is in its low attractiveness, that can be seen through reserves amount and prices.



Picture 109: SQUID/ETH pool reserves

While the SQUID reserve has a weak positive trend, WETH reserve has a negative trend, defining decrease of user interest in the current pool. The WETH token is a popular one and its distribution better establishes the current situation on the market with this pool.



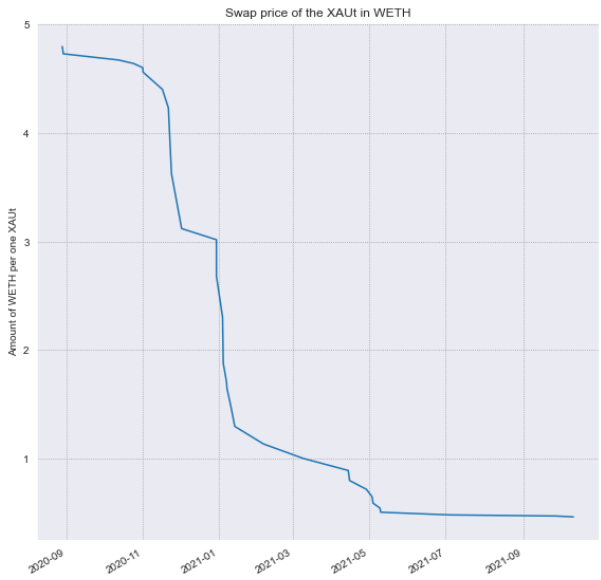
Picture 110: SQUID/ETH pool reserve-based prices

Conform price distributions the SQUID token is dropping from the initial moment, when the price is raised at pool initialization stage. There is no attention to the market, reducing the option of performing MEV attacks.

The important moment that requires mentioning is that the “scam” SQUID token used a scheme conform which no trader was able to perform sell operation over the token, causing only a price increase of the token. If the market wants to protect participants it would be required to consider such cases and pay attention to the behavior of such tokens.

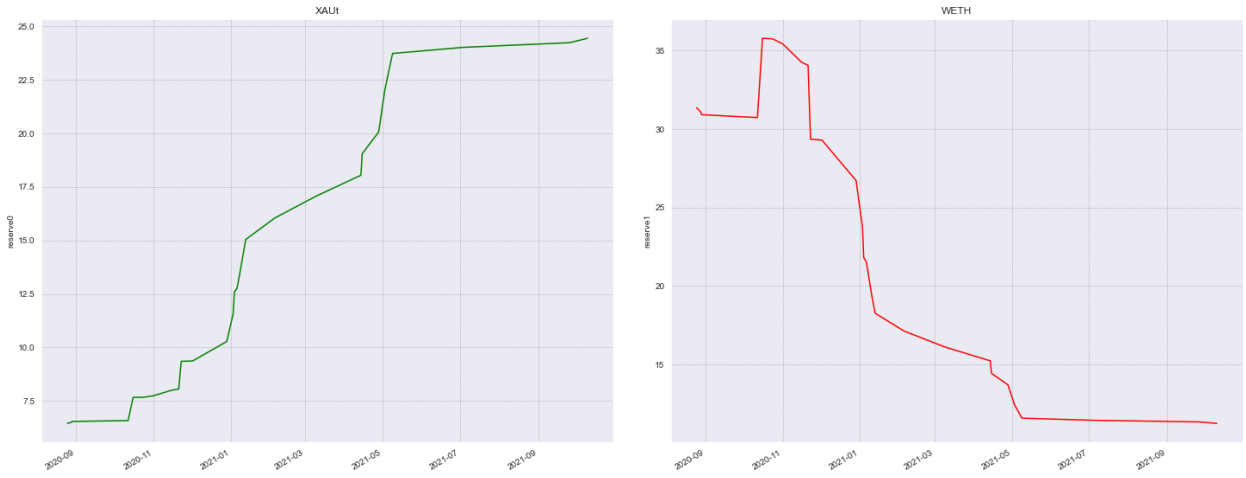
XAUt/WETH (STO) or how STO is used only to get access to altcoin

Tether gold is a digital asset that is offered by TG Commodities Limited. One full XAUt token represents one troy fine ounce of gold on a London Good Delivery bar. The principle behind the token is to have gold ownership avoiding drawbacks associated with physical gold, such as high storage costs and limited accessibility (links: 1, 2). Authors took Uniswap V2 history of this token and below is presented the token history.



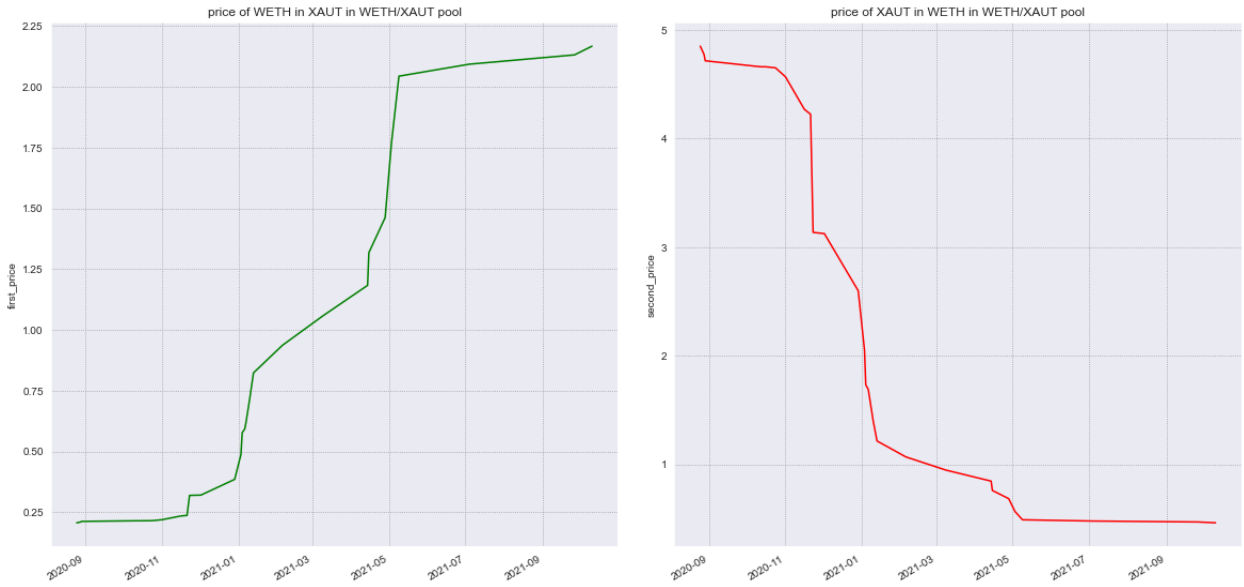
Picture 111: swap-based XAUt token price in the XAUt/WETH pool

There were no swap transactions from WETH to XAUt setting such a situation when XAUt token price is decreasing. Reserve-based XAUt token price distribution looks similar to the swap-based one.



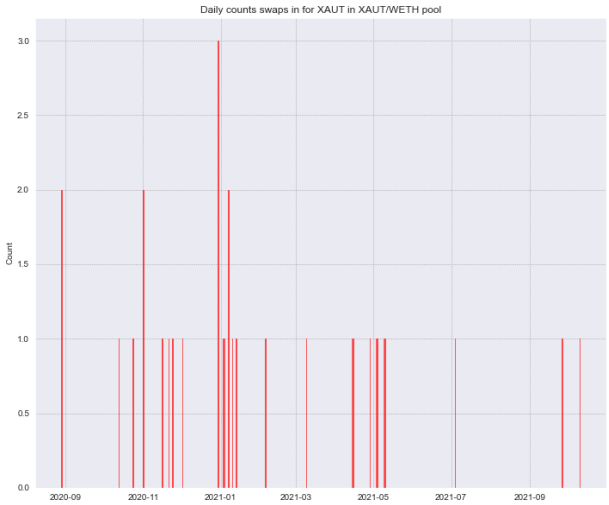
Picture 112: reserves distributions in the XAUt/WETH pool

Conform presented distributions can be seen that reserves of the pool are slowly increasing from the WETH side and decreasing from XAUt one.



Picture 113: reserve-based price distributions of the XAUt/WETH pool

The problem behind this pool is in its small reserves and relatively high transaction values, decreasing price so much that reserves increase in the current case just cause a smaller decrease of the XAUt token price.



Picture 114: swaps transaction count for XAUt in the XAUt/WETH pool

The situation in the current pool is relatively bad, considering that reserves are small, transaction rate is small and therefore MEV attack can be easily performed. Additional factor

about possible MEV attacks is that both tokens in the pool are popular, meaning that their attractiveness is higher for attackers compared to the other pools.

The last important observation about this pool is that the price taken from the start of the pool lifecycle is not matching the real one. At the start of pool lifecycle the price set for one XAUt was around 5 WETH. WETH token price was around 420-430 USD dollars while XAUt price was around 1900 USD dollars. Ethereum price was rising through the entire time taken. This pool looks like a good source of getting Ethereum at a smaller price compared to the real-market one. Therefore, this pool does not have at all swaps of WETH to XAUt due to the bad price.

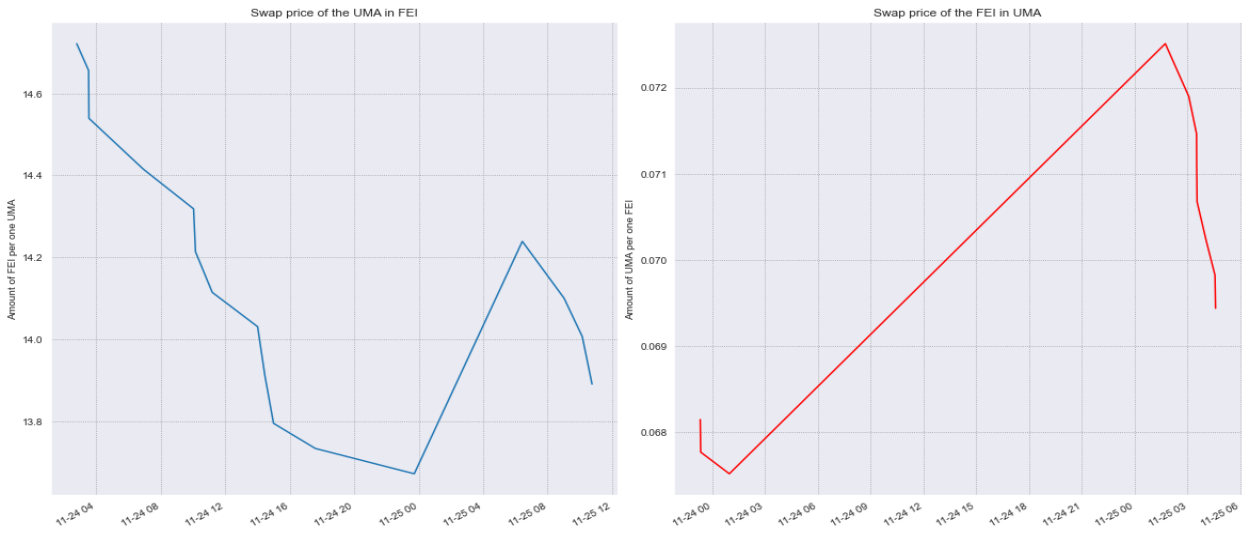
Picture 115: XAUt token price for the last year distribution taken between end of November 2020 till end of November 2021

Considering that this pool became a good source of getting Ethereum at a smaller price it is hard to say if this pool further will become a complete one with exchanges on both sides.

UMA/FEI (STO)

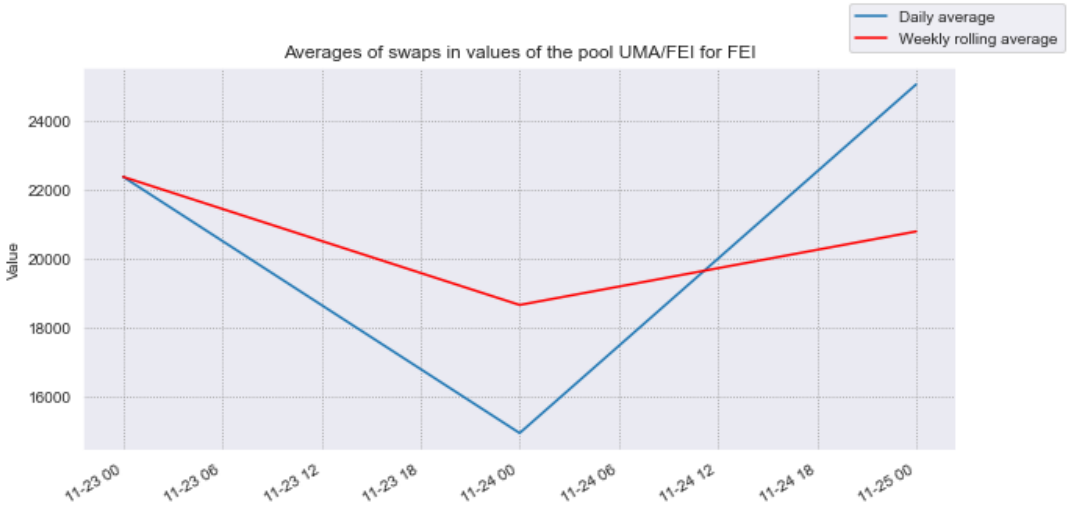
UMA is an Universal Market Access token that was launched in December 2018. UMA gives the option of digitizing any real-world derivatives like futures, contracts for difference, swaps and so on. The reason why this idea appeared was that there are limitations and high financial barriers present on the financial market and authors of the UMA wanted to give an option for any person to become a part of this market (Link: 1).

UMA/FEI is a relatively new pool on the Uniswap V2 that has a history of only several days and therefore charts will not represent a clear distribution picture. For better understanding it is required to have a bigger picture, but even basing on the current time interval something can be estimated.



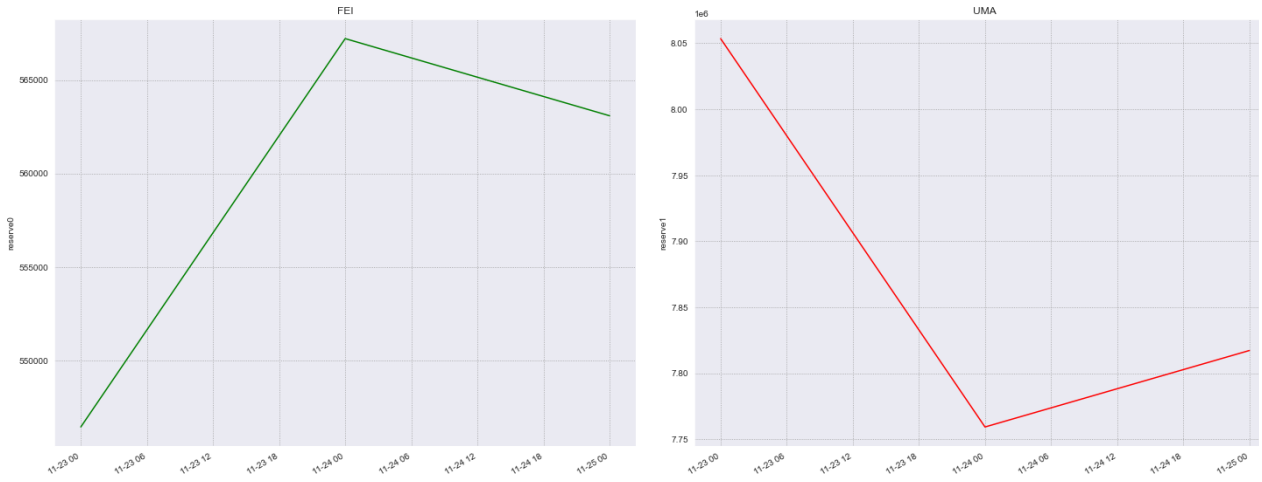
Picture 115: swap-based prices distributions of the UMA/FEI pool

Conform presented distributions can be seen that the time window is relatively small and UMA token was slowly decreasing during the first day and had a small rise during the second day. The FEI token price is increasing but during the second day this token was decreasing. Those distributions show people's interest in changing the UMA token to the stablecoin one.



Picture 116: swaps activity distributions in the UMA/FEI pool

Conform present charts can be seen that there is a relatively small activity, but with further pool evolution it can become a popular and reliable pool.



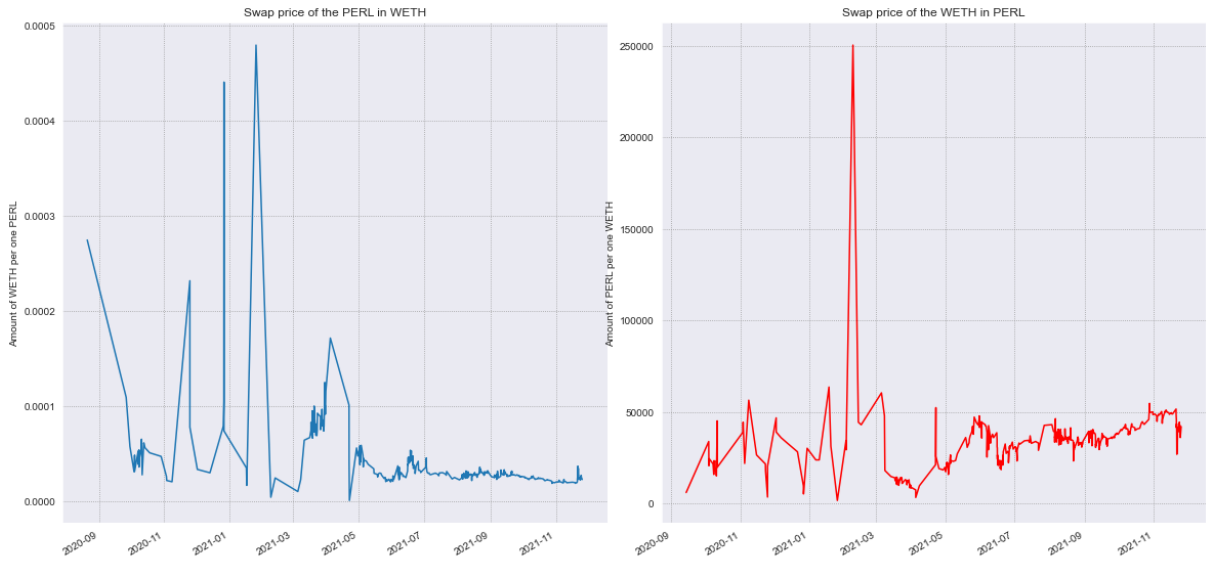
Picture 117: reserves distributions of the UMA/FEI pool

Conform presented pool reserves can be seen that the pool is relatively stable and attackers would require a high financial power to perform this attack and transaction frequency (even for such a small time window) is relatively high. Therefore, it would be difficult to perform a MEV attack on that pool.

To perform a more efficient and better overview of the pool distributions, to find patterns in the data and find general trends it would be useful to get a bigger time window and therefore to get a better history.

PERL/WETH (STO) or how mint transactions could save a pool

PerlinX is a decentralized finance interface platform that allows users to trade assets of any kind with each other through incentivized liquidity mining and synthetic asset generation. Pools on that platform are powered by the Balancer protocol and use UMA protocol to generate synthetic assets (link: 1). This token was found inside the PERL/WETH pool on the Uniswap V2.



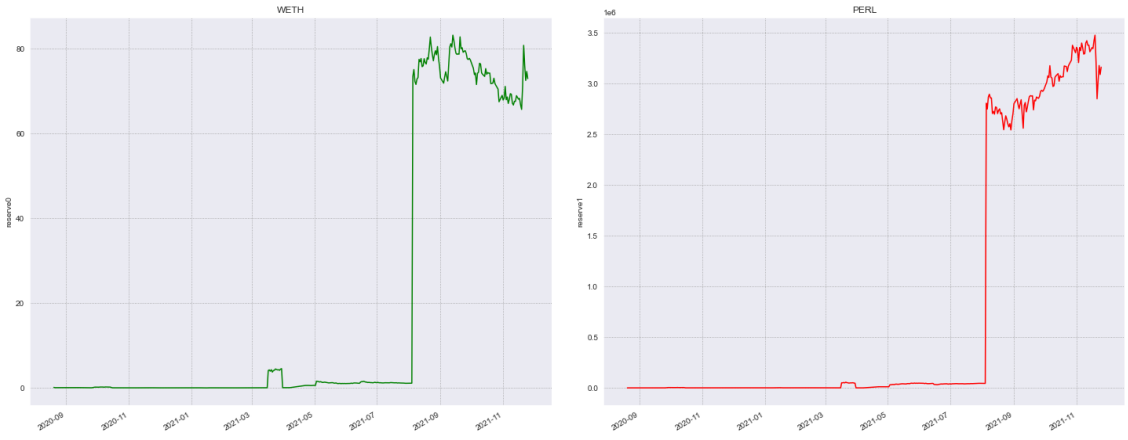
Picture 118: swap-based price distributions of the PERL/WETH pool

Swap-based prices have unstable and hard to predict behavior with stabilization of the price deviation at the specific moment after May 2021. Thai can happen if either pool reserves have increased and therefore each transaction value has a smaller impact over price changes or transaction values have dropped, causing smaller price impacts.

	token_in	token_out	amount_in	amount_out	amount_usd	timestamp	first_to_second_price	price_change_rate
7	PERL	WETH	408.979034	1.546745	312.551851	2020-08-20 07:44:09	3.781967e-03	1528.124912
8	WETH	PERL	0.010000	39.812766	2.020848	2020-08-20 07:53:39	3.981277e+03	22180.594590
69	PERL	WETH	901.362451	0.209247	63.801716	2020-11-24 20:25:34	2.321456e-04	1020.592464
102	PERL	WETH	1316.251394	0.631761	450.743442	2021-01-25 12:17:45	4.799698e-04	2734.041390
104	WETH	PERL	0.001461	50.000000	1.000974	2021-02-02 03:04:53	3.423146e+04	1852.842586
213	WETH	PERL	0.277616	424153.138076	357.593123	2021-04-22 13:25:58	1.527841e+06	7099.831468
214	WETH	PERL	0.001372	43680.787426	1.766648	2021-04-22 13:25:58	3.184822e+07	1984.523861
218	PERL	WETH	600.370614	0.030088	38.991787	2021-04-28 09:44:12	5.011490e-05	4547.285878

Picture 120: transactions with biggest price change rates

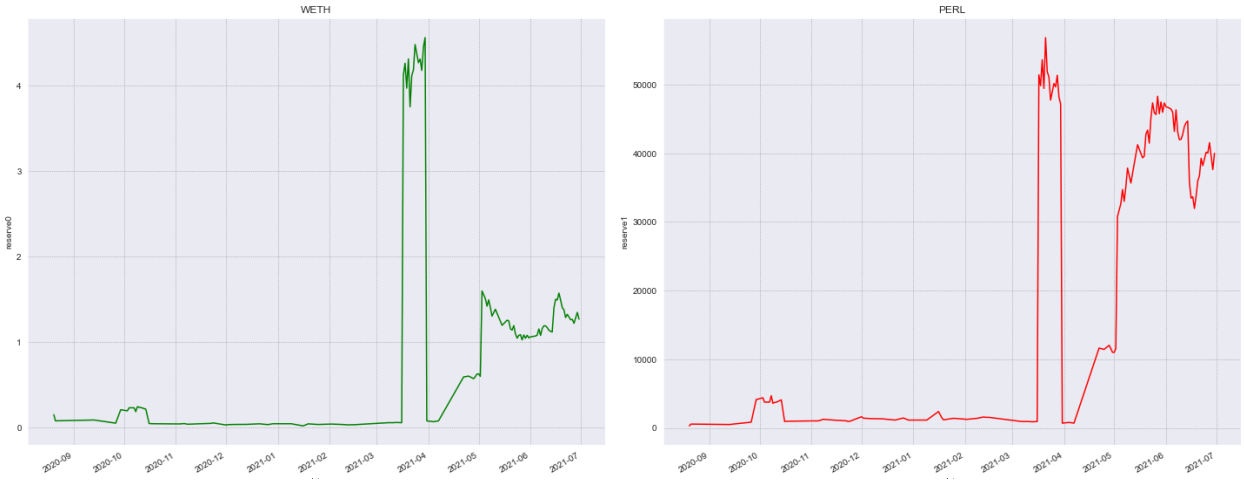
Presented transactions have a high increase rate. Taking into account transaction capitalization they are relatively small and considering the price impact reserves of the pool are too small to make distributions stable.



Picture 121: reserves distributions for the PERL/WETH pool

Conform presented reserves distributions there were very small reserves amount until middle of August 2021, meaning that even relatively small transactions would cause big price changes. After the middle of August 2021 there is an anomalous rise of pool reserves. In order to ensure that price change rates were caused by small reserves it was decided to look into transaction history.

Below can be seen a mints transaction history, conform which first reserves inserted in the pool are around 450 of PERL and around 0.1 of WETH.



	amount0	amount1	timestamp
0	0.100000	4.500000e+02	2020-08-20 07:31:20
1	0.184215	2.819900e+03	2020-09-29 17:26:24
2	0.002946	6.350000e+01	2020-11-06 17:48:44

	token_in	token_out	amount_in	amount_out	amount_usd	timestamp	first_to_second_price	price_change_rate
3	WETH	PERL	0.111533	2.000000	22.576193	2020-08-20 07:37:55	17.931936	-12.868540
4	PERL	WETH	2.058032	0.113905	23.020060	2020-08-20 07:41:29	0.055346	NaN
5	WETH	PERL	0.122975	2.197419	24.871883	2020-08-20 07:43:44	17.868808	-0.352045
6	PERL	WETH	9.435072	0.002192	0.442872	2020-08-20 07:44:09	0.000232	-99.580298
7	PERL	WETH	408.979034	1.546745	312.551851	2020-08-20 07:44:09	0.003782	1528.124912
8	WETH	PERL	0.010000	39.812766	2.020848	2020-08-20 07:53:39	3981.276636	22180.594590
9	WETH	PERL	0.010000	33.276398	2.018745	2020-08-20 07:55:58	3327.639778	-16.417770

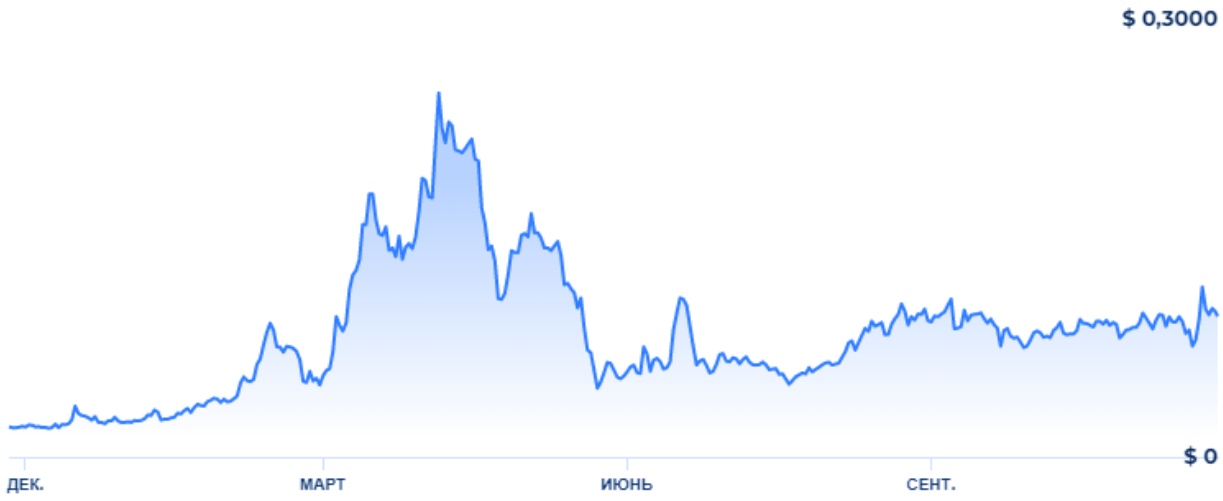
Picture 122: reserves distributions in the PERL/WETH pool with first three mints history and swap transactions history fragment, where anomalous price rise was registered

Presented transaction history demonstrates that anomalous price rise happened due to the small reserves values. Initial PERL reserves in the pool are around 295 PERL tokens and in the same date was registered a mint transaction that raised PERL token value by 450 PERL tokens having in result around 745 PERL tokens. As a result, swap of the 408 PERL tokens in the transaction nr. 7 causes drop of the 54.77% of pool reserves. Such a drop causes extreme change in the token price.

	reserve0	reserve1	reserveUSD	dailyVolumeToken0	dailyVolumeToken1	date	first_price	second_price
0	0.153498	2.958885e+02	62.347684	3.435517	1.087056e+03	2020-08-20	0.000519	1927.631252
1	0.081605	5.573478e+02	33.663391	0.071893	2.614593e+02	2020-08-21	0.000146	6829.813170
2	0.091605	4.966680e+02	33.233211	0.010000	6.067977e+01	2020-09-13	0.000184	5421.836328
3	0.054551	8.350475e+02	19.107331	0.037054	3.383795e+02	2020-09-26	0.000065	15307.637112

Picture 123: reserves distributions in the PERL/WETH pool

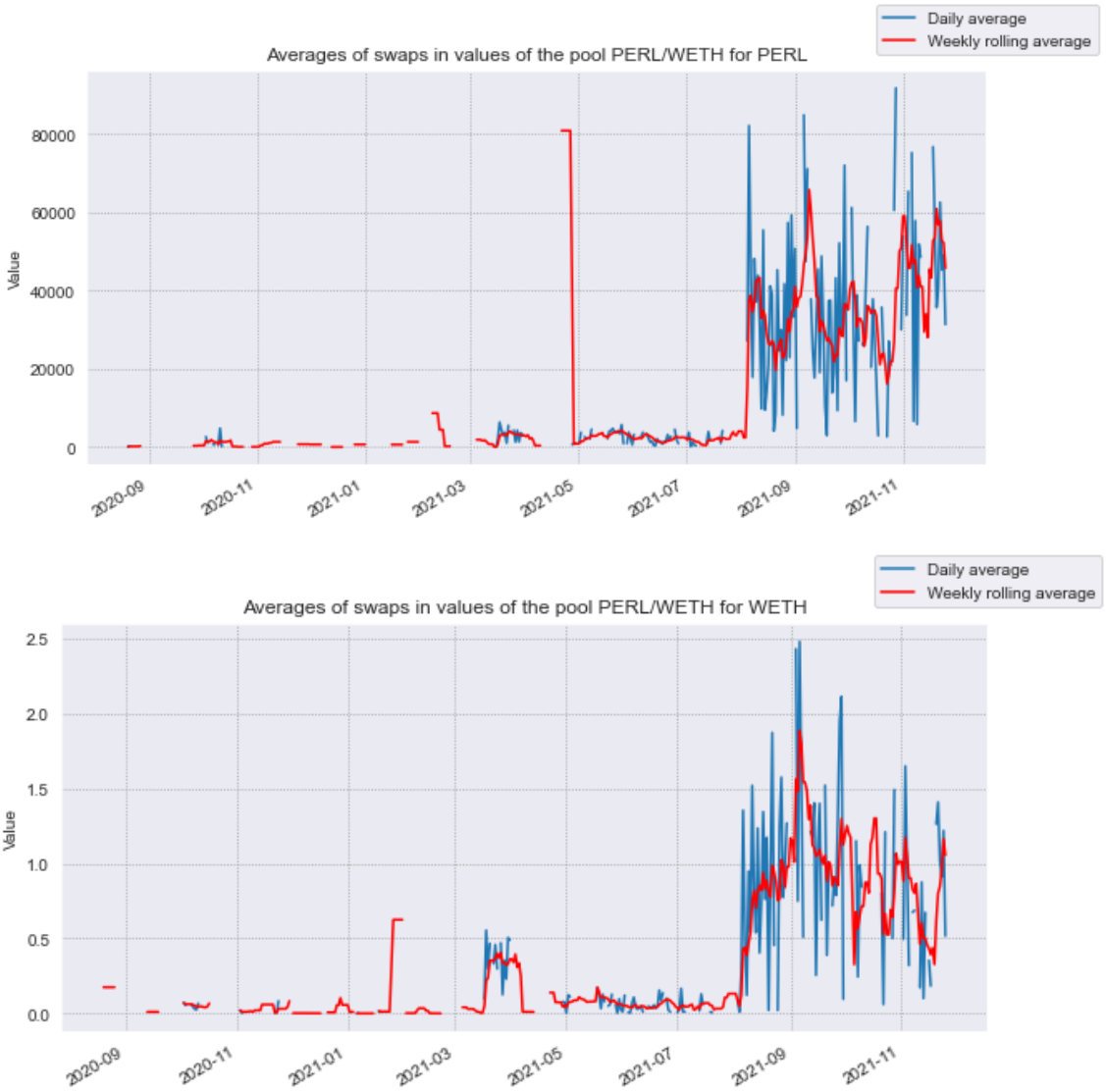
Another interesting observation is that all extreme price changes were registered before anomalous reserves mint. The strange thing about those mints is that in most of the cases they are happening with positive token price changes that signal to investors about possible further high activity of the pool.



Picture 124: PERL price in USD dollar changes taken from the coinranking.com for time interval between end of November 2020 till end of November 2021

Conform presented distributions there should be mints transactions (either with high values or many of them) while anomalous mints were registered in the first half of August 2021. Authors suggest that anomalous mints were caused by the desire of token founders to save the presented pool. Another strange moment is that transaction count before anomalous mints is only

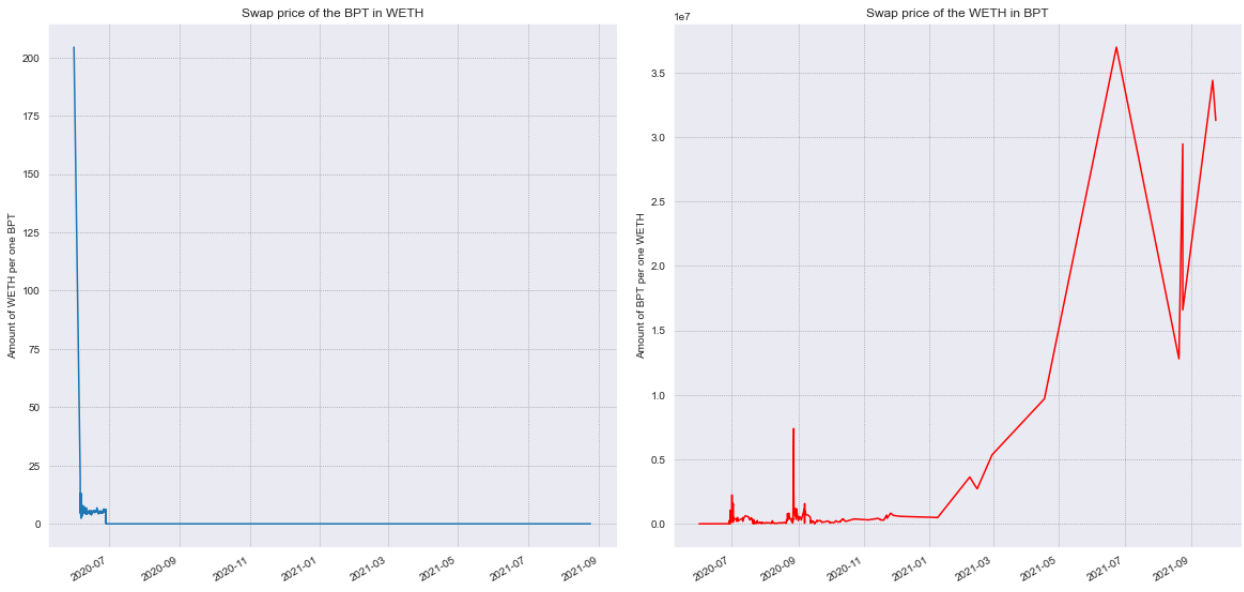
⅓ of transaction history, while after reserves mints transaction count is ⅔ of transaction history. More than 1000 of the 1500 transactions happened during the last 3 months while before that only 500 transactions happened in 8.5 months. This can be seen even on the swap activity charts.



Picture 125: swaps activity charts for PERL/WETH pool

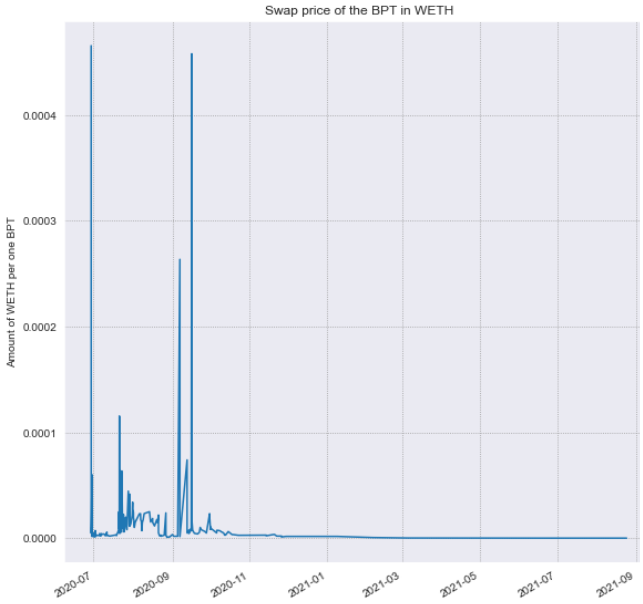
BPT/WETH (STO) or how incorrect pool prices can lead to pool death

BPT tokens are Balancer Pool tokens created for Balancer Platform. This is a community-driven protocol, automated portfolio manager, liquidity provider, and price sensor. The tokens are representing a share of a specific pool and in case of losing BPT token, the person loses its share of mints in the invested pool (links: 1, 2).



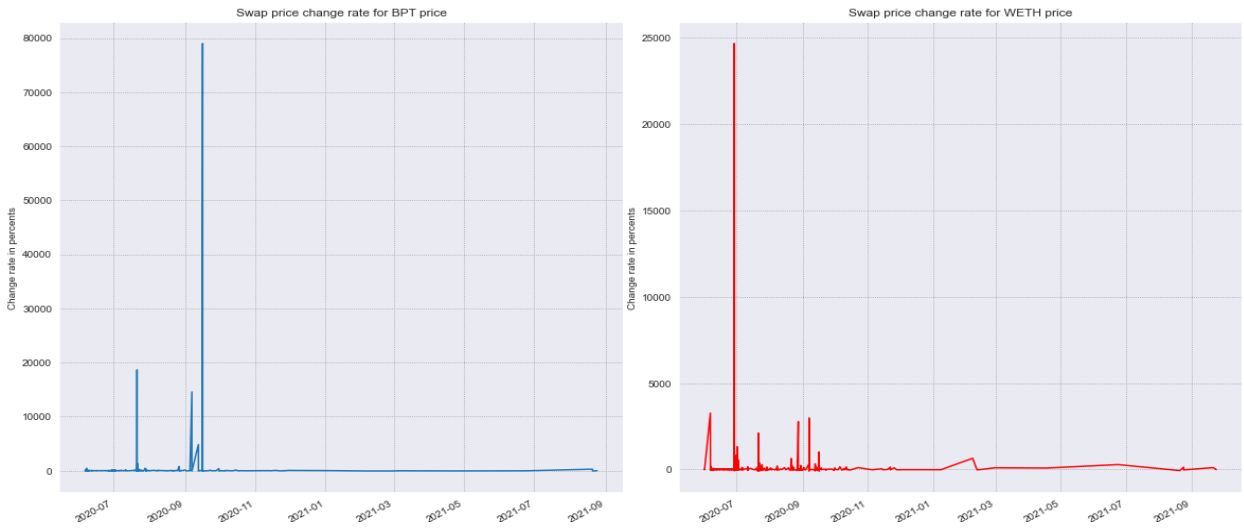
Picture 126: swap-based price distributions in the BPT/WETH pool

Presented flat line in the distribution may be a much smaller price that due to the small prices it looks as a flat line on the distribution. The distribution was taken from June 2020, but distribution was still flatlined and it was decided to take all transactions whose price was smaller than 0.002.



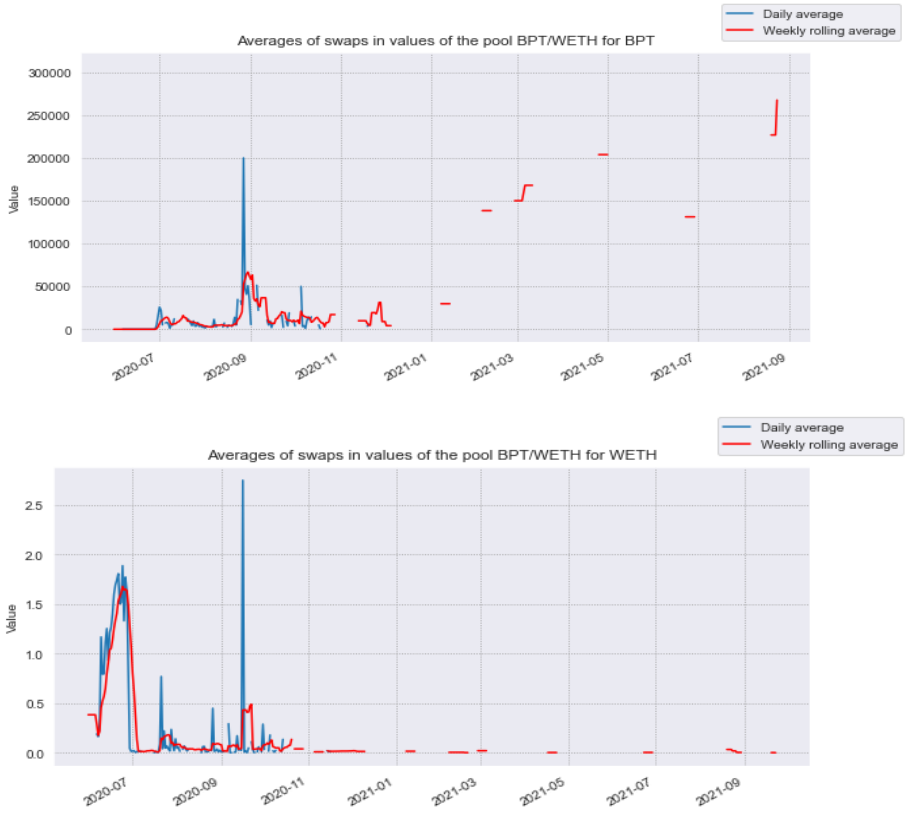
Picture 128: swap-based token price in the BPT/WETH pool where token price is smaller than 0.002

The price changes are too high. Therefore it was decided to find price change rates distributions in the BPT/WETH pool.



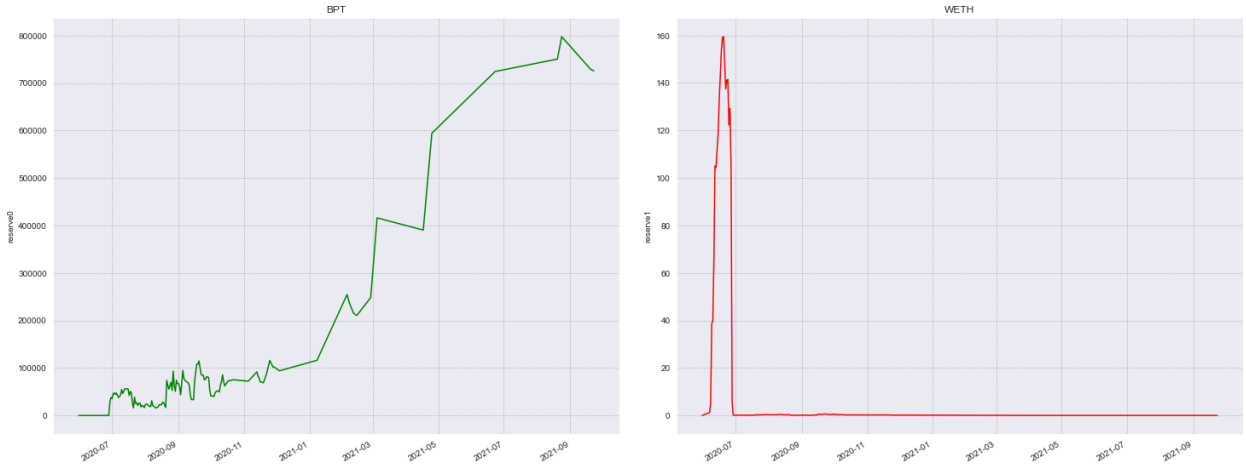
Picture 129: swap-based price change rates in the BPT/WETH pool

The strange moment about both of the presented distributions is that there are many changes present in the time interval between June 2020 till middle of October 2020. It means that the high swap activity period was in the same time period. This can be seen on the distributions shown below.



Picture 130: swap activity in the BPT/WETH pool

In order to check why price changes dropped it was decided to check pool reserves presented below.



Picture 131: BPT/WETH pool reserves distributions

Conform presented distributions another reason why price changes have stabilized is due to the reserves increase over the time. Price could stabilize with increase of reserves, but while BPT reserves greatly increased the WETH reserves came to almost zero. Therefore it is important to check distributions closely.

Looking at the swaps operations tokens movement it was decided to check what was the WETH token movement during 28th June 2020, after which pool started to lose almost all WETH tokens.

```
print(bpt_weth_df[(bpt_weth_df.index > 1679) & (bpt_weth_df.index < 1977) & (bpt_weth_df.token_in == 'BPT')]['amount_out'].sum())
print(bpt_weth_df[(bpt_weth_df.index > 1679) & (bpt_weth_df.index < 1977) & (bpt_weth_df.token_in == 'WETH')]['amount_in'].sum())
```

✓ 0.4s

```
227.1167151118571
138.73205975724926
```

Picture 132: WETH token movement inside BPT/WETH pool where first number represents token moving out of the pool and the second one represents token moving into the pool

During transactions between numbers 1700 and 1850 there was removed around 80.12 WETH token. Conform reserves records for the start of 28th June there were around 105 WETH token reserve. It means that using swap operations there was removed around 76.3% of WETH token pool reserves.

	amount0	amount1	amountUSD	liquidity	timestamp
0	0.038184	5.250594	2461.568018	0.447214	2020-05-31 21:06:15
1	0.417425	2.000000	945.674491	0.887479	2020-06-13 10:07:00
2	0.119339	0.582595	275.554580	0.256009	2020-06-13 16:50:17
3	3.280877	16.797741	7885.957027	7.204152	2020-06-14 10:14:07
4	2.659988	11.818349	5190.763404	5.436221	2020-06-15 06:32:10
5	2.575563	13.775960	6217.870796	5.772561	2020-06-15 17:54:35
6	0.007609	0.038823	17.953201	0.016500	2020-06-22 02:10:53
7	2.714016	13.339686	6494.472194	5.771805	2020-06-22 18:27:18
8	0.228369	1.126151	543.369184	0.485606	2020-06-23 16:38:16
9	4.187742	20.707012	9628.537045	8.880001	2020-06-25 16:48:59
10	2.254845	12.293817	5621.547012	5.000000	2020-06-27 06:19:54
11	1.890473	10.326405	4735.810114	4.195795	2020-06-27 08:04:21
12	2.249246	12.730518	5563.581778	5.074951	2020-06-28 06:24:14
13	19926.757513	0.107702	23.803892	39.372188	2020-06-29 14:26:50
14	813.791060	0.002403	0.539017	1.078611	2020-07-03 01:26:21

Picture 133: Burns transactions in the BPT/WETH pool

Considering that after transactions there were removed 80.12 tokens out of the pool and that after that there were burns on the total sum of around 23.06 tokens, meaning that at the end of 28 of June there remained only around 2 WETH tokens. One person performed swaps changing getting as much WETH tokens as possible and extracted

	token_in	token_out	amount_in	amount_out	amount_usd	timestamp	sender	to	txd	first_to_second_price
1721	BPT	WETH	0.004215	0.024040	5.424104	2020-06-28 15:58:01	0x7a250d5630b4cf539739df2c5dacb4c659f2488d	0xe644ae0d7640ed2838e97a3a0689e9bf50627eab	0xba5acdb334e420ed9dbaa469fbbb226ef2bdaeee98e8...	5.704031
1722	BPT	WETH	0.267191	1.500000	335.551931	2020-06-28 16:08:49	0x7a250d5630b4cf539739df2c5dacb4c659f2488d	0x7a250d5630b4cf539739df2c5dacb4c659f2488d	0x22e6869b5d7a895bcaa6b75d6b00378699ef9ea5ec54...	5.613970
1725	BPT	WETH	0.121490	0.680867	153.222975	2020-06-28 17:11:22	0x0000000000025d4386f7fb58984cbe110aee3a4c4	0x0000000000025d4386f7fb58984cbe110aee3a4c4	0x43a7469912b079520f99f8699866bcb03145a2c37d16...	5.604305
1726	BPT	WETH	0.157132	0.866407	194.780662	2020-06-28 17:12:07	0x860bd2dba9cd475a61e6d1b45e16c365f6d78f66	0x860bd2dba9cd475a61e6d1b45e16c365f6d78f66	0x1c387372410b4226910b5bac6a9bf5ccbf613990a562...	5.513875
1729	BPT	WETH	0.474830	2.845818	634.537659	2020-06-28 17:57:22	0x860bd2dba9cd475a61e6d1b45e16c365f6d78f66	0x860bd2dba9cd475a61e6d1b45e16c365f6d78f66	0x9e5b29aee88011c038cdd0c23f2ce8b3913816af555a...	5.993346
1730	BPT	WETH	0.301881	1.711233	383.648371	2020-06-28 17:57:45	0xf164fc0ec4e93095b804a4795bbe1e041497b92a	0xf164fc0ec4e93095b804a4795bbe1e041497b92a	0x0b5ca2ad19858642b2e5712cd52b97d61602c1524c1b...	5.668570
1731	BPT	WETH	0.076169	0.441519	99.642952	2020-06-28 17:57:45	0x693c188e40f760ecf00d2946ef45260b84fbc43e	0x693c188e40f760ecf00d2946ef45260b84fbc43e	0x91b907040b92a61c3b5065dbbe935129faf4f402477f...	5.796583
1733	BPT	WETH	494.784081	92.193342	10763.617011	2020-06-28 18:03:14	0x860bd2dba9cd475a61e6d1b45e16c365f6d78f66	0x860bd2dba9cd475a61e6d1b45e16c365f6d78f66	0xe71b7ec874808805f1fd39106ebba7acc6b7533151c9...	0.186330
1735	BPT	WETH	30.867565	2.265044	464.643724	2020-06-28 18:03:23	0x860bd2dba9cd475a61e6d1b45e16c365f6d78f66	0x860bd2dba9cd475a61e6d1b45e16c365f6d78f66	0xe739f130dd8c0e3a86fdc966a6adbb0688319f101992...	0.073379
1739	BPT	WETH	15.656916	1.572610	335.606901	2020-06-28 18:03:43	0x860bd2dba9cd475a61e6d1b45e16c365f6d78f66	0x860bd2dba9cd475a61e6d1b45e16c365f6d78f66	0x1a572ef61d8cd249ec7e020d6f6282b7987a9e737db2...	0.100442
1743	BPT	WETH	26.152808	2.648828	544.493173	2020-06-28 18:04:23	0x860bd2dba9cd475a61e6d1b45e16c365f6d78f66	0x860bd2dba9cd475a61e6d1b45e16c365f6d78f66	0xe9e36815602bcb36cb7823d0d3913fd8e93a722cd123...	0.101283
1746	BPT	WETH	14.735481	1.534026	327.869574	2020-06-28 18:05:09	0xf1ad4bfdf8829d55ec0ce7900ef9d122b2610673	0xf1ad4bfdf8829d55ec0ce7900ef9d122b2610673	0x0376d703ea15409a14927ef51715241a2671f32ff71e...	0.104104
1749	BPT	WETH	16.235134	2.150065	453.345085	2020-06-28 18:05:23	0x860bd2dba9cd475a61e6d1b45e16c365f6d78f66	0x860bd2dba9cd475a61e6d1b45e16c365f6d78f66	0xb1085e37d2d3c347c6d36242058c4112c1ed5413311d...	0.132433
1750	BPT	WETH	24.636451	3.677403	744.456818	2020-06-28 18:05:52	0x860bd2dba9cd475a61e6d1b45e16c365f6d78f66	0x860bd2dba9cd475a61e6d1b45e16c365f6d78f66	0x3d99bc68155084f53d746522ec892915adc00f22875e...	0.149267
1752	BPT	WETH	5.880017	1.177136	257.446498	2020-06-28 18:05:52	0x860bd2dba9cd475a61e6d1b45e16c365f6d78f66	0x860bd2dba9cd475a61e6d1b45e16c365f6d78f66	0xb9581b4c79edfe8d74edf09d366eb7c7fd8a5d4a97f8...	0.200193
1754	BPT	WETH	8.841230	2.093689	449.085127	2020-06-28 18:05:52	0x860bd2dba9cd475a61e6d1b45e16c365f6d78f66	0x860bd2dba9cd475a61e6d1b45e16c365f6d78f66	0xe7c59e47bdd22d593ba784f4a11ee59d0177b383d96c...	0.236810
1758	BPT	WETH	23.434218	3.867703	783.223947	2020-06-28 18:06:20	0x860bd2dba9cd475a61e6d1b45e16c365f6d78f66	0x860bd2dba9cd475a61e6d1b45e16c365f6d78f66	0x775c82e4dd4c07bb252916aaa27a480fcf4703eac9d8...	0.165045
1760	BPT	WETH	30.216991	4.705933	929.318917	2020-06-28 18:06:20	0xf1ad4bfdf8829d55ec0ce7900ef9d122b2610673	0xf1ad4bfdf8829d55ec0ce7900ef9d122b2610673	0x9bec95d223f9f7d3523fbfdb79154404a91d83483d30...	0.155738
1761	BPT	WETH	9.755480	1.675504	360.796701	2020-06-28 18:06:34	0x860bd2dba9cd475a61e6d1b45e16c365f6d78f66	0x860bd2dba9cd475a61e6d1b45e16c365f6d78f66	0x300cda736d4d412e084bbe21993ff7e2de9dd82b8c1e...	0.171750
1767	BPT	WETH	3.820315	0.696245	154.236021	2020-06-28 18:07:33	0x860bd2dba9cd475a61e6d1b45e16c365f6d78f66	0x860bd2dba9cd475a61e6d1b45e16c365f6d78f66	0xd47dde5110c372f0c638589c7f2ce16897afd6897461...	0.182248
1768	BPT	WETH	7.968059	1.391044	302.064463	2020-06-28 18:07:33	0xf1ad4bfdf8829d55ec0ce7900ef9d122b2610673	0xf1ad4bfdf8829d55ec0ce7900ef9d122b2610673	0xfdd27dc289bae7ea9eb163ffa7a67e70021e900db4c6...	0.174578
1771	BPT	WETH	3.400352	0.625601	138.880647	2020-06-28 18:08:09	0x693c188e40f760ecf00d2946ef45260b84fbc43e	0x693c188e40f760ecf00d2946ef45260b84fbc43e	0x0b58564311aaf580ba00295c1bbaca81818066be8016...	0.183981

Picture 134: transaction history catching 4 transactions during which one person extracted almost all of the tokens in the BPT/WETH pool

Considering this extraction of all tokens out of the pool it is required to check pool-based token prices with real-market ones. Conform information on 28-th June 2020 taken from the

coinmarketcap.com the BPT token price is around 12.03$, while WETH token price is around 231$. It means that one WETH token is equivalent to 19.2 BPT tokens (or BAL token).

Picture 135: BPT token price distribution for the last year taken from coinmarketcap.com

Transaction history shows that BPT token is equal to around 5.7 WETH tokens, which is not corresponding to the real-market price. Some attackers discovered that token prices are not corresponding to the real-market ones and there is a possibility of extracting all precious tokens using the less precious token. This is a perfect illustration of why token price should correspond or to be close to the real-market price. Otherwise some persons could try extracting all precious tokens using their less precious equivalents in the pool.

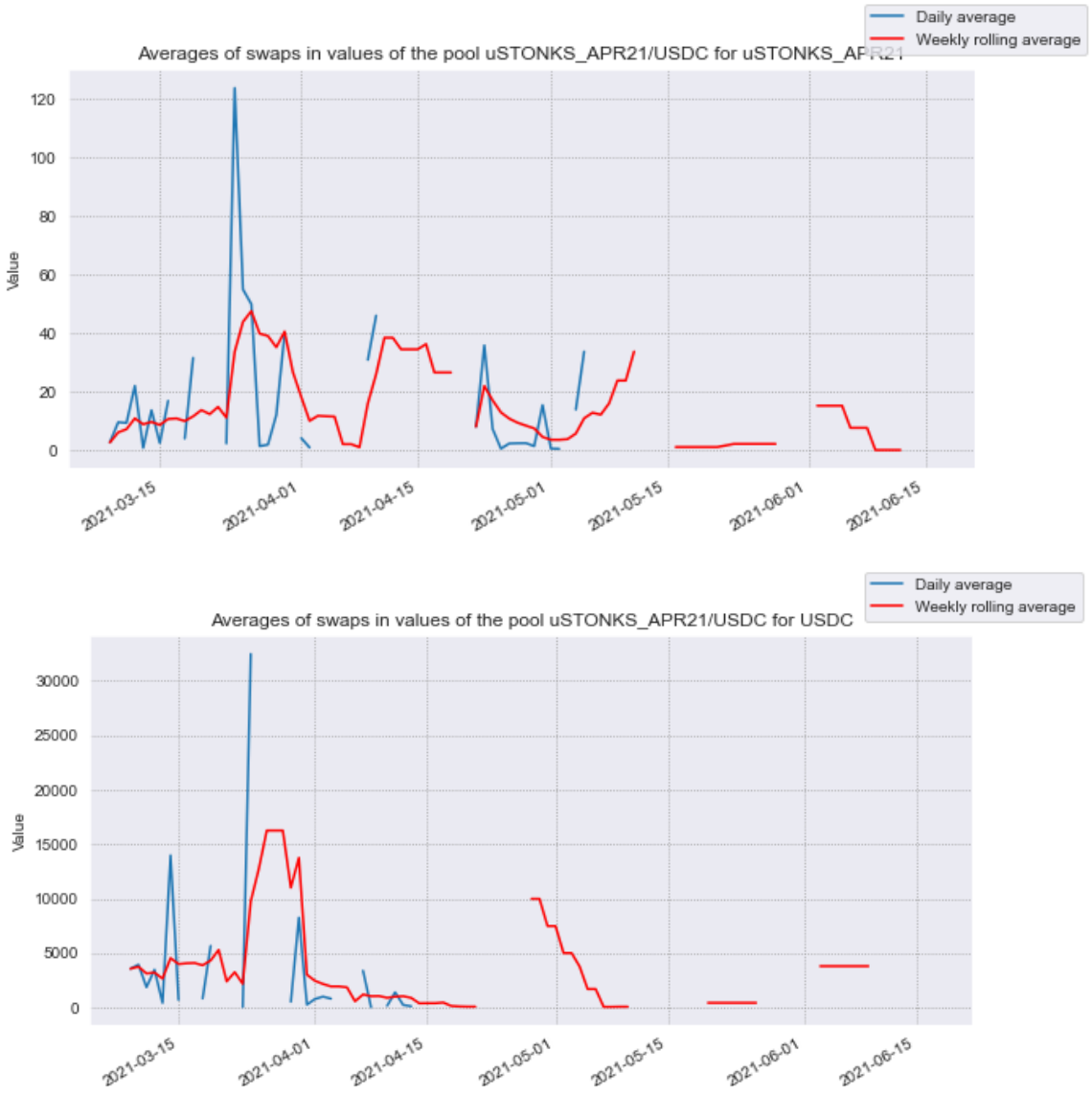
Another reason why this case is a unique one - for performing this attack a person used 567 BPT tokens that are equal to the 870$ which is a very small financial power required for performing this attack. Person extracted WETH token equal to the around 23 100$ meaning that person extracted and got around 22 230$ of profit from this situation.

After performing this attack on the pool there is almost no activity registered, meaning that pool died after extreme price changes and people see no reason for changing tokens inside this pool.

uSTONKS_APR21/USDC (STO) or small pool with bad activity

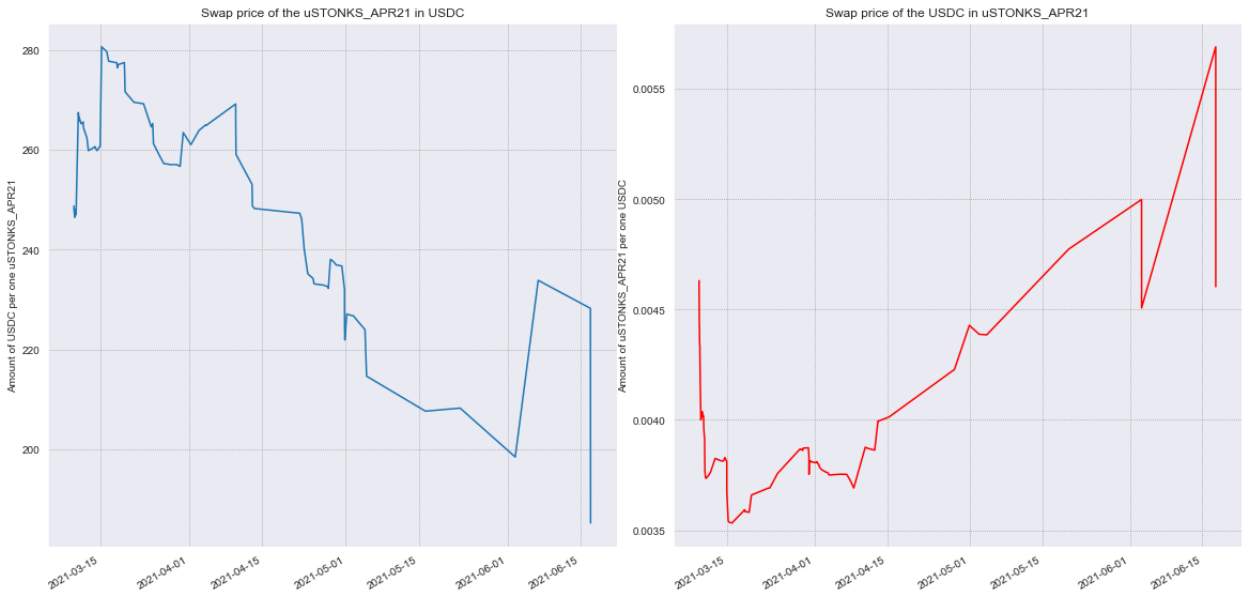
uSTONKS_APR21 token is a synthetic that tracks the ten most “bullish” Wall Street Bets stocks and captures sentiment of this community. This is a result of collaboration of the UMA project with YAM Finance to develop a suite of innovative DeFi derivatives (links: 1, 2). The

problem about this token was that authors were not able to find token price distributions and therefore in the current chapter will be reviewed only information taken from Uniswap V2.



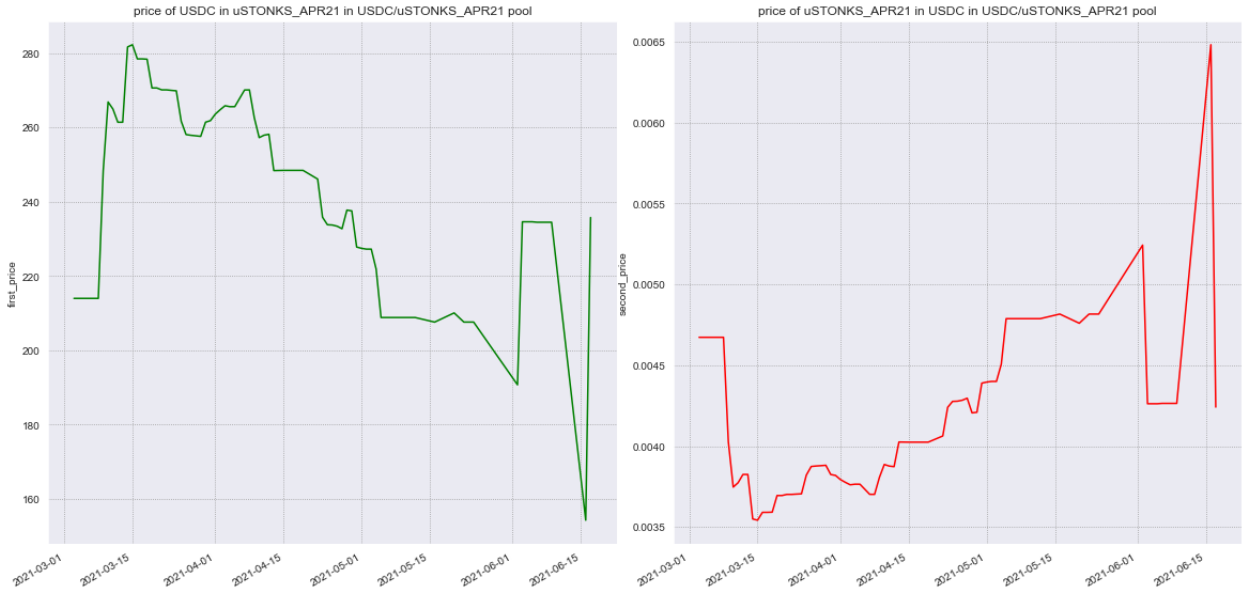
Picture 136: swap operations activity of the uSTONKS_APR21/USDC pool

Swap activity is relatively low and there were two periods of some present activity - during March 2021 and during the end of April 2021. The lack of price information makes it difficult to find out the reason for such activity drops and there is no option of checking if those changes were caused by bad token prices. Therefore it is required to dive deeper into the present data and compare swap-based prices and reserve-based ones.



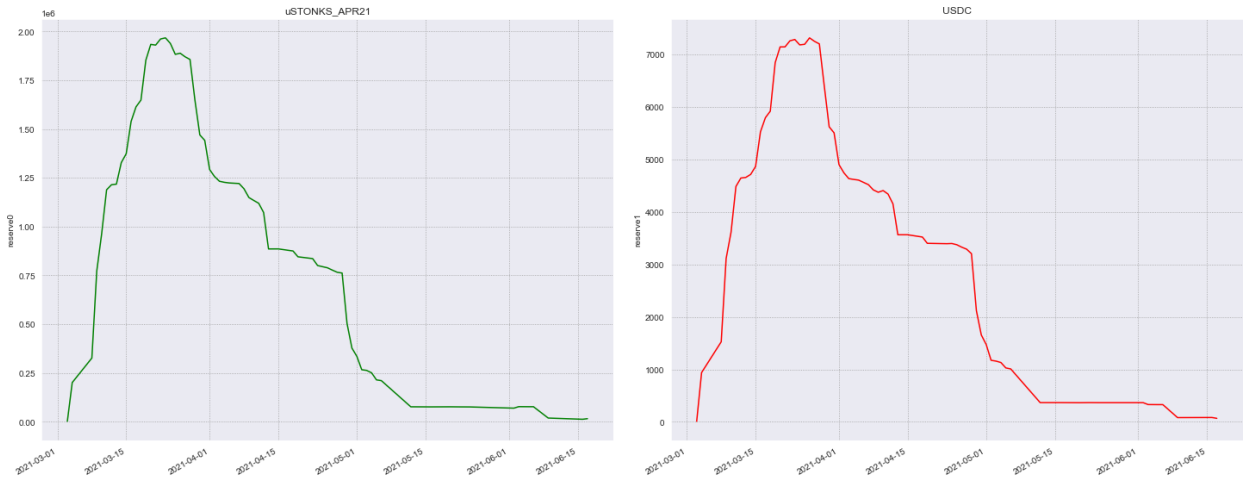
Picture 137: swap-based token price distributions of the uSTONKS_APR21/USDC pool

uSTONKS_APR21 price is slowly dropping with small local rises of token price, while USDC token price is slowly increasing. In the current case pool price changes are not caused by the both token prices changes due to use of stablecoin in pair with STO.



Picture 138: reserve-based token price distributions of the uSTONKS_APR21/USDC pool

General shapes of distributions look similar and swap-based prices are less stable compared to the reserve-based ones and the general price pattern is similar. The problem about the current pool is that there is a small overall transaction count, representing low pool activity and that pool data has multiple gaps.



Picture 139: reserves distributions of the uSTONKS_APR21/USDC pool

Presented distributions demonstrate that prices in the pool were more stable during high-reserves values. Also transaction frequency during this period was higher compared to the period with smaller reserves. This change can be caused by the user's desire to exchange tokens in more stable and large pools than in ones that are less stable. Conform analyzed distributions there were no extreme changes that would represent frauds or some attackers activity while pool had both small reserves and small transactions frequency, meaning that presented tokens in the pool are not popular ones.

Current pool state is looking like a “dead” pool that has almost no present activity, where reserves are extremely low and where prices are unstable with negative trends.

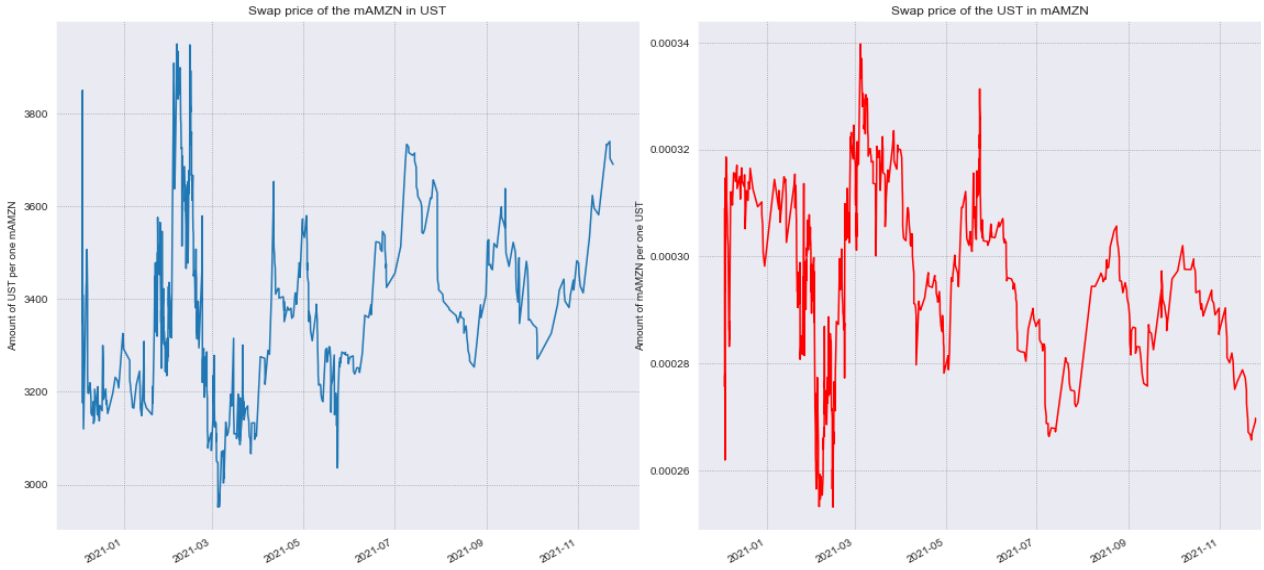
mAMZN/UST (STO)

mAMZN (or Mirrored Amazon) is a synthetic asset tracking the price of an Amazon stock. mAMZN exists as CW20 and ERC20 versions which can be traded on the Terraswap and Uniswap respectively (links: 1, 2). It can be minted on the Mirror protocol, which references on-chain prices provided by Band Protocol’s decentralized network or oracles.

This pool also contains TerraUSD token (shortly called UST) which is a decentralized and algorithmic stablecoin of the Terra blockchain. It is a scalable, yield-bearing coin that is value-pegged to the USD dollar. It was launched in September 2020 (link: 1).

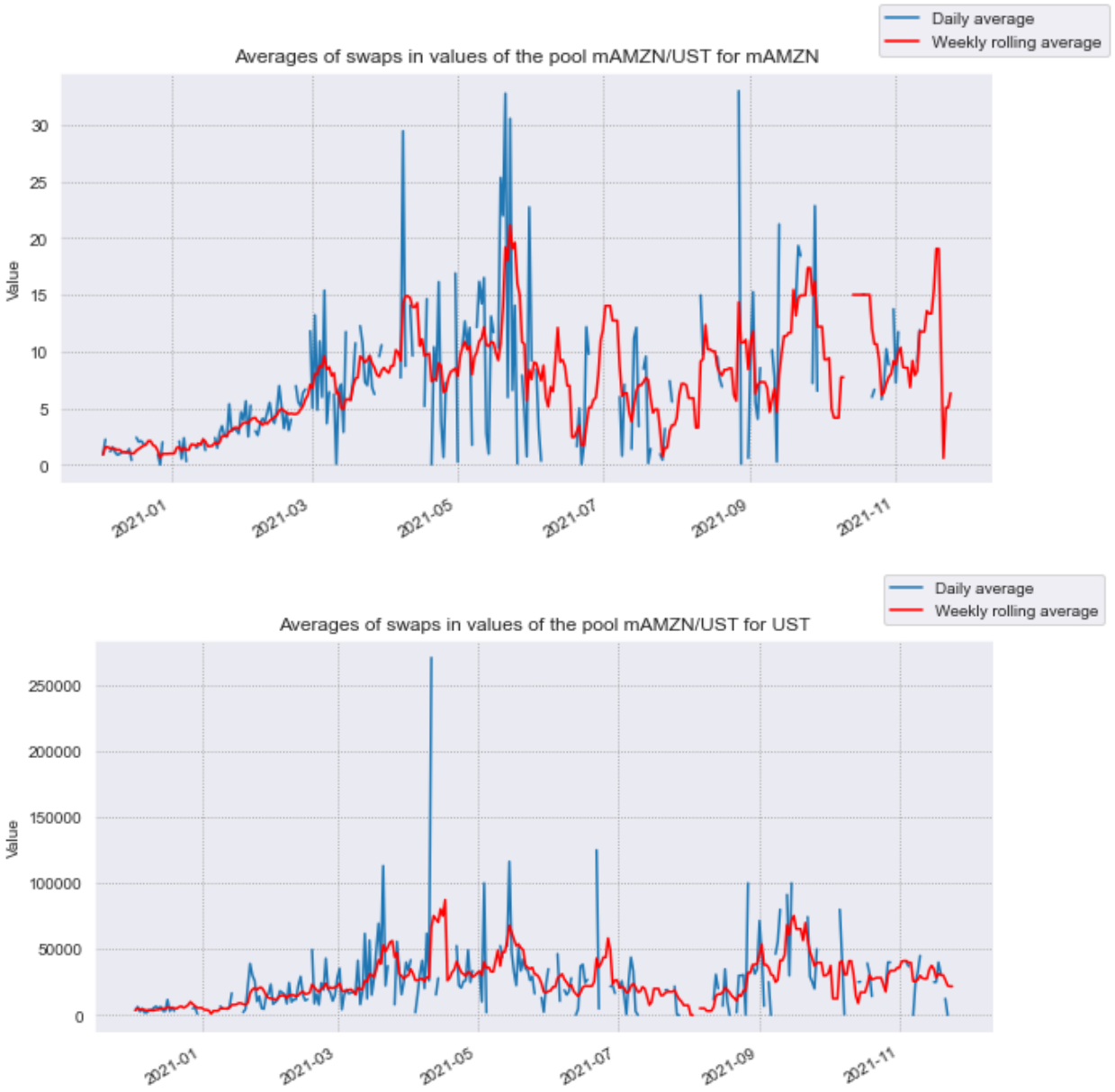
Picture 140: mAMZN token price first chart and UST token price second chart for last year taken from CoinMarketCap.com

There were only two drops of the stablecoin price, meaning that price changes in the distribution could happen in the beginning of the 2021 and during the end of May 2021.



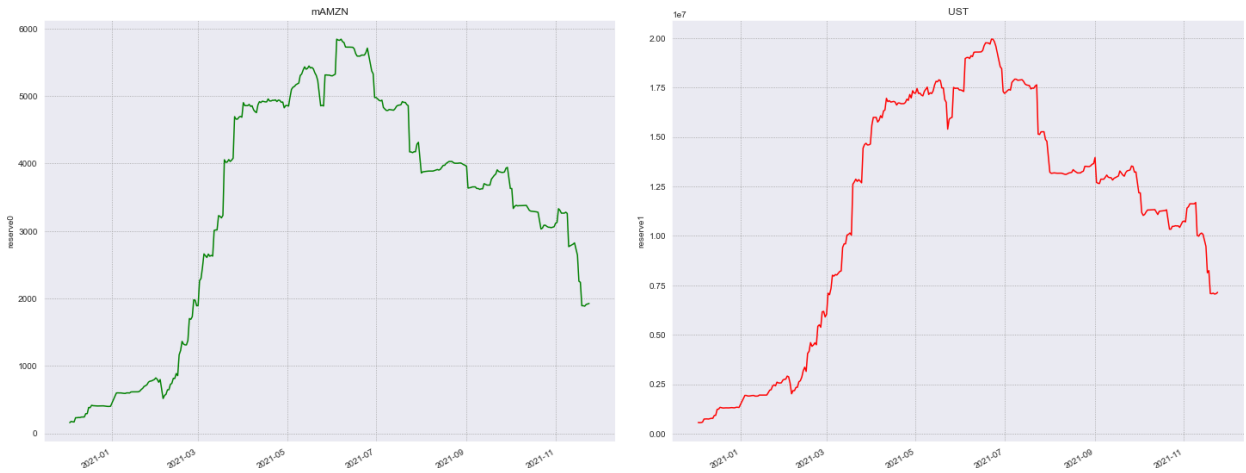
Picture 141: swap-based price distributions for the mAMZN/UST pool

During the start of the pool, the life cycle has “noisy” distribution, meaning that there is either small transaction frequency reducing “balancing” or small reserves in the pool.



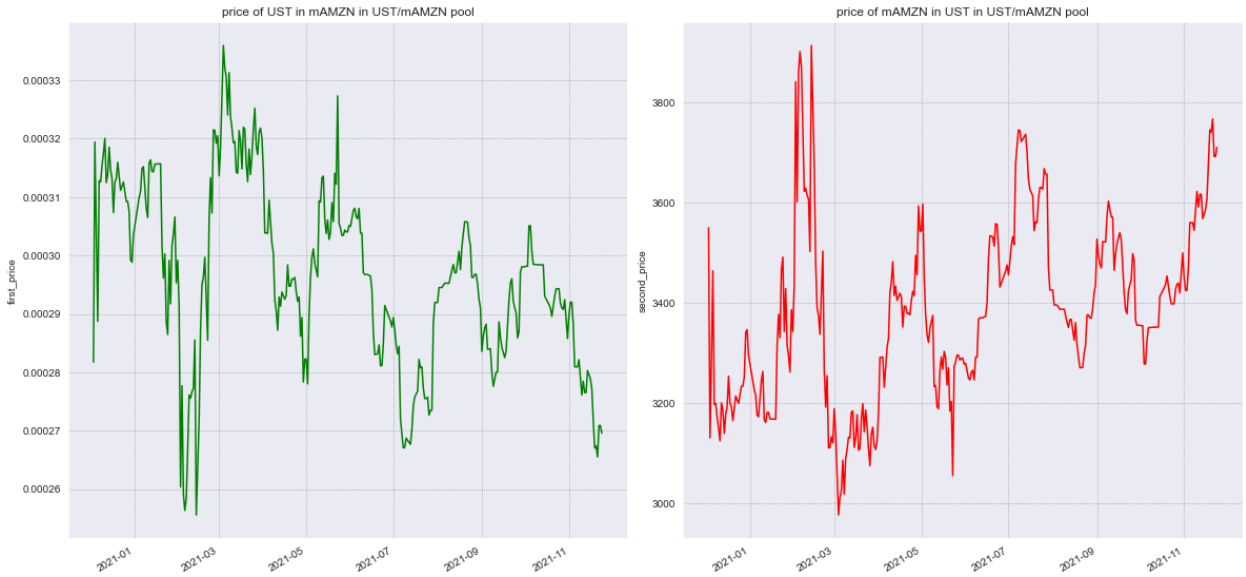
Picture 142: swap transaction activity in the mAMZN/UST pool

There were drops in transaction frequency starting from July 2021. Till that moment transaction frequency is relatively high, meaning that “noisy” price distributions in the first half and clearer distributions in the second half are caused by drop of the transaction frequency and therefore it is required to check pool reserves distributions.



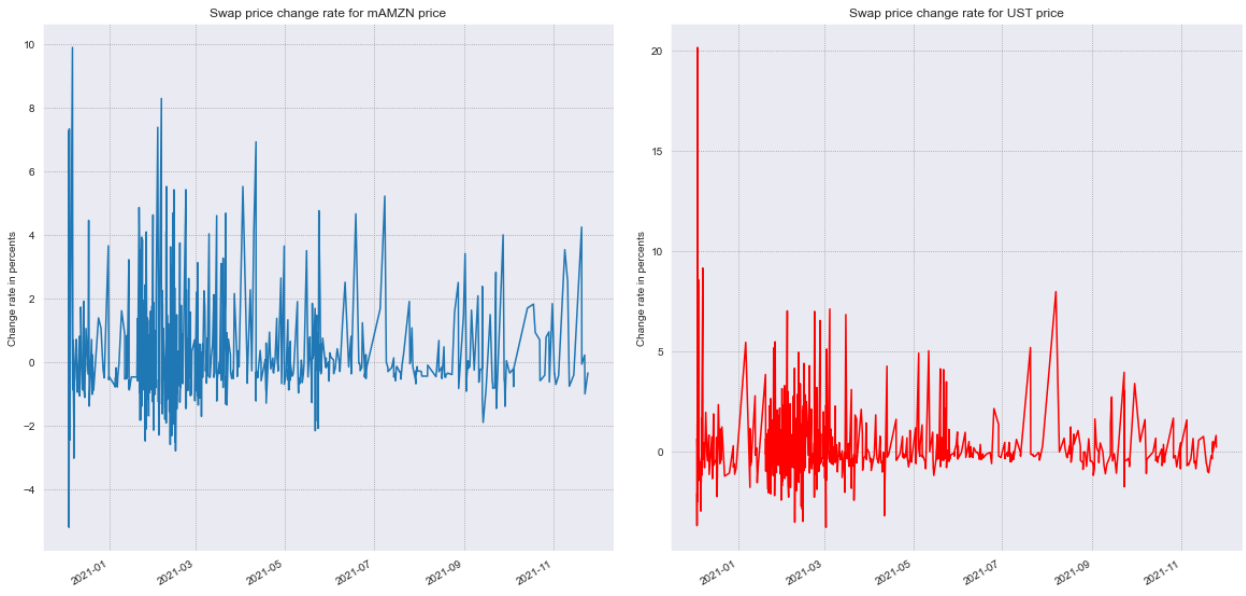
Picture 143: reserves distributions in the mAMZN/UST pool

Reserves in the pool were fastly increasing during the first half of the year and after that started a slow decrease of the token price. Transaction frequency had a great drop while pool reserves were increasing. This behavior is strange. Another strange moment is that mAMZN reserve-based token price has bigger rises and drops compared to the real market price distributions.



Picture 144: reserve-based price distributions in the mAMZN/UST pool

Considering that pool represents relatively popular tokens with big capitalization and high mAMZN token price it is important to dive deeper into pool price changes.



Picture 145: swap-based price change rates distributions in the mAMZN/UST pool

Swap-based price change rates look stable compared to the other ones, meaning that there were not registered extreme rises and drops in token prices. Conform distributions can be seen that there are higher change rates present during the beginning of the pool life cycle with smaller pool reserves and higher transaction frequency.

mBABA/UST (STO)

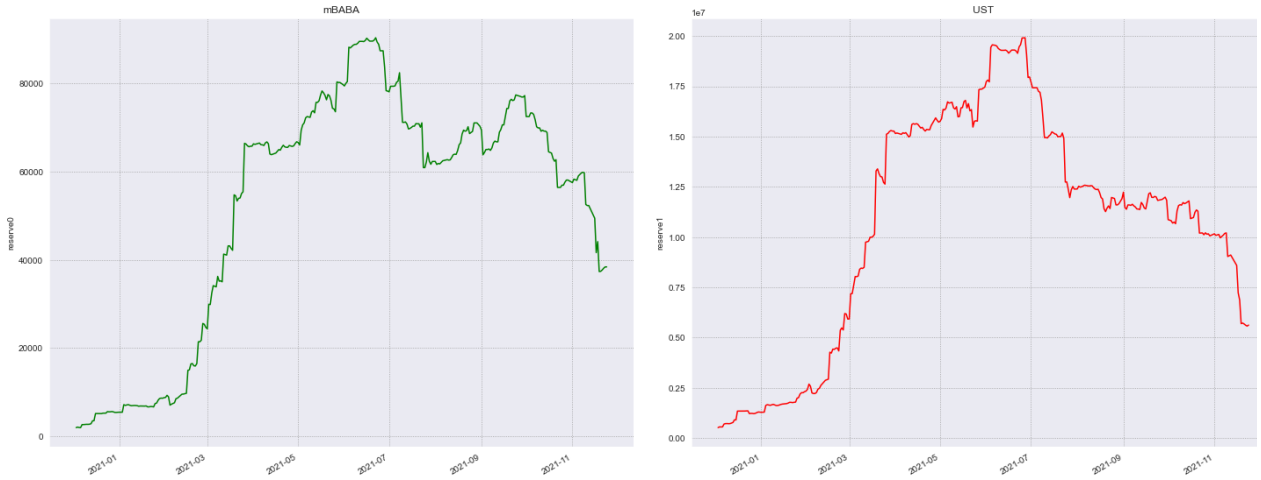
Mirrored Alibaba (or mBABA) is a token that works by the same principle as mAMZN token and represents Alibaba shares prices.

Picture 146: mBABA token price distribution taken from the CoinMarketCap.com

mBABA price is slowly decreasing and both swap-based and reserve-based token prices should correspond to the real-market price distribution.

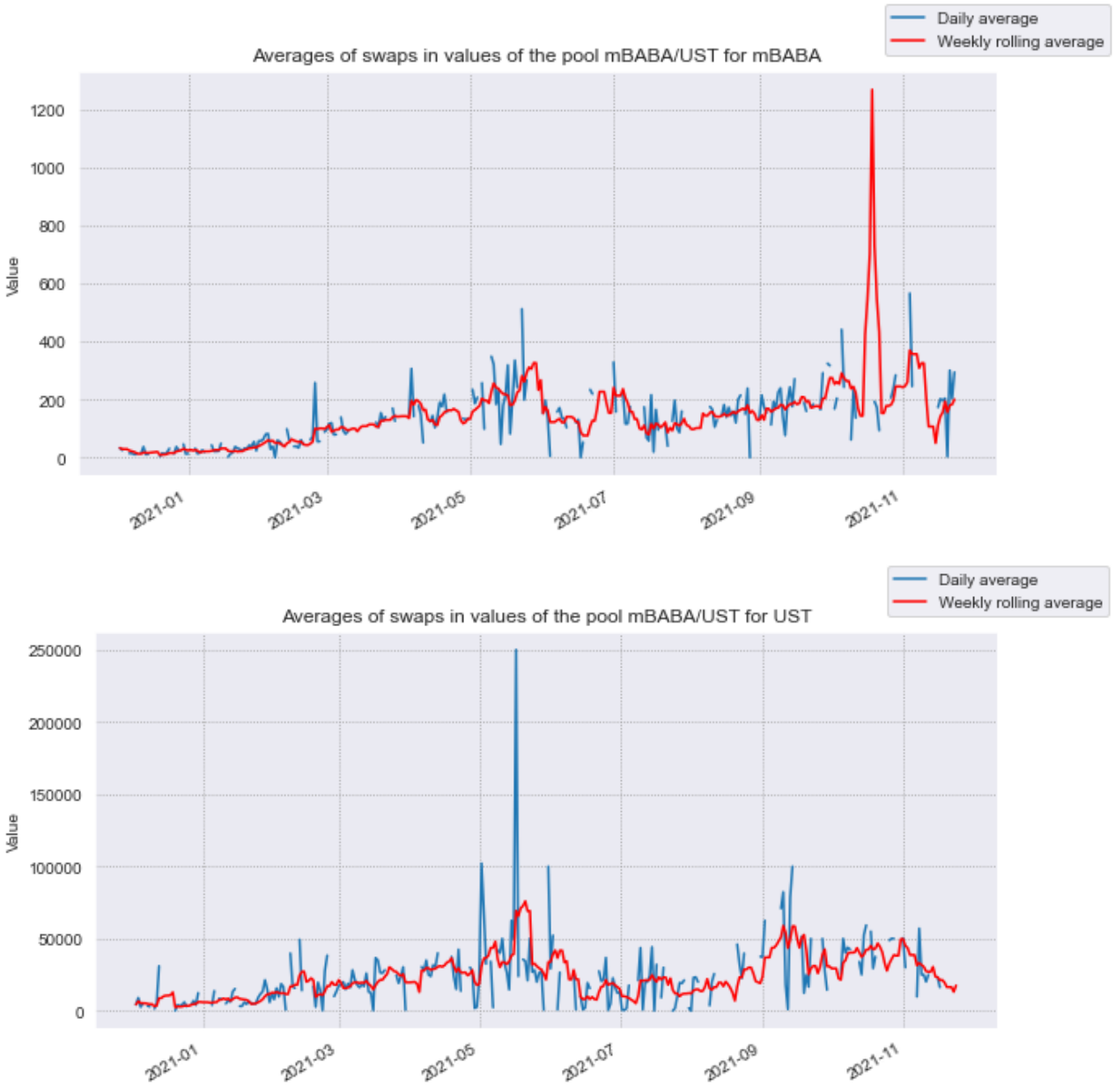
Picture 147: swap-based token prices distributions for the mBABA/UST pool

During the start of the pool life cycle there is a "noise" in distributions that represent either small transaction frequency or small reserves in the pool. After the first 3 months of pool activity distribution became more stable.



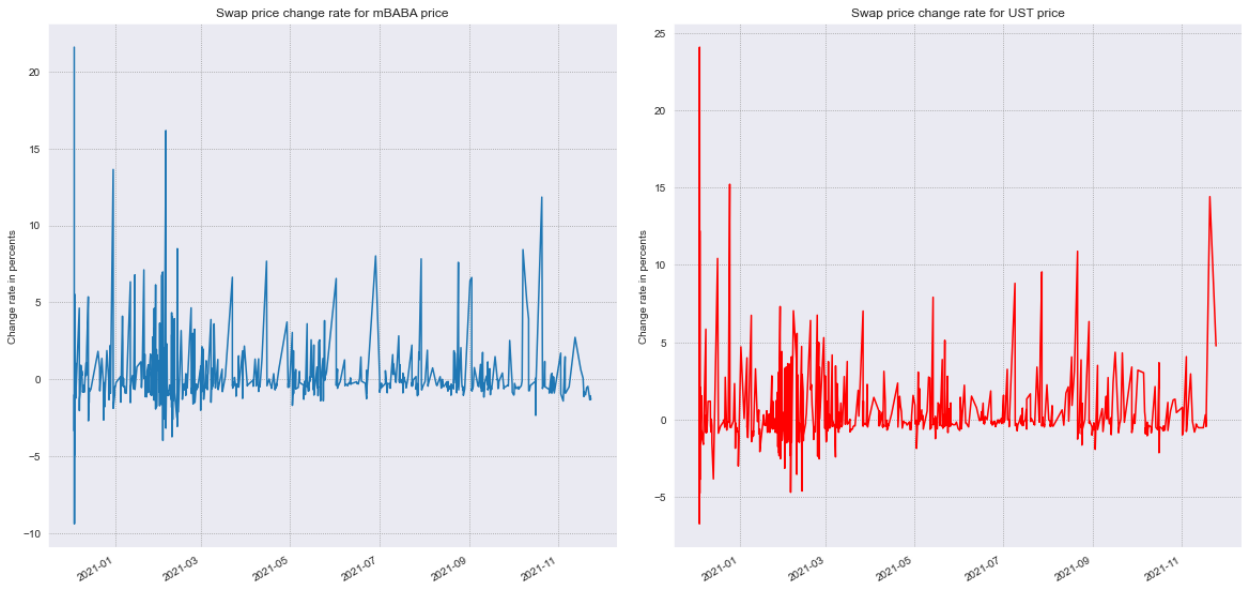
Picture 148: reserves distributions in the mBABA/UST pool

During the first half of the pool life cycle "noise" present in the distributions is caused by small reserves present in the pool.



Picture 149: swap transactions activity in the mBABA/UST pool

Presented distributions show relatively stable activity with medium-level activity size. There should be no extreme drops and rises of the tokens prices, considering that pools are relatively big and transactions frequency is enough to hold prices from extreme changes.



Picture 150: swap-based price change rates in the mBABA/UST pool

There are no extreme price changes present in the distribution meaning that there were no frauds or MEV attacks performed over the pool. Still, transaction frequency keeps an option for attackers with high financial power to perform such an attack.

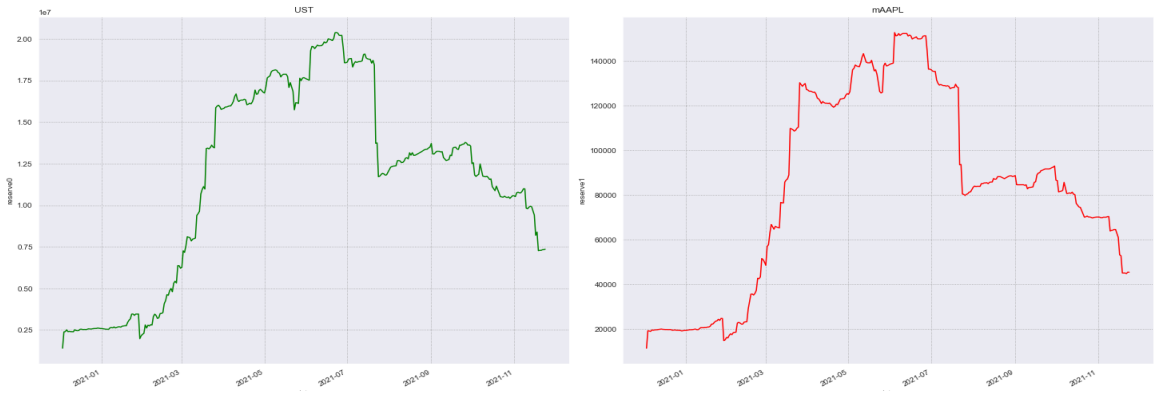
mAAPL/UST (STO)

mAAPL is working with the same principle as mBABA and mAMZN tokens and mirrors Apple company share price. Compared to the previous "mirrors" this pool has the biggest transaction history.

Picture 151: mAAPL token price distribution taken from the CoinMarketCap.com from the left and mAAPL swap-based token price from the right

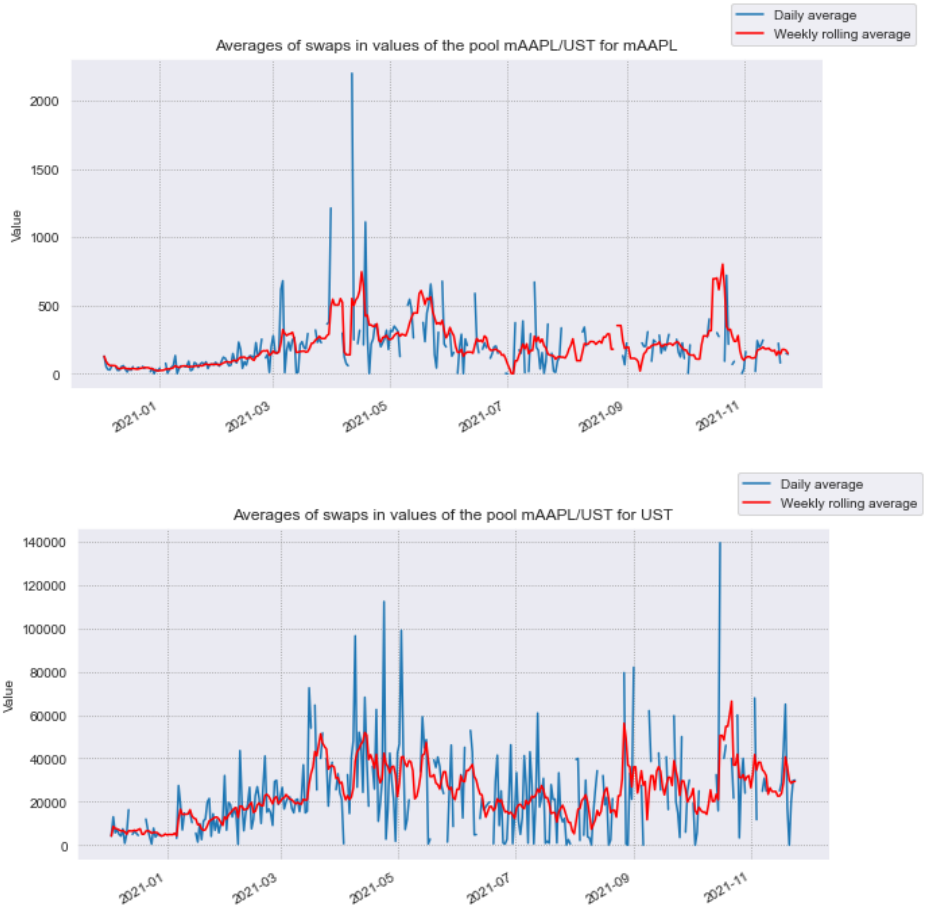
Pool-based token price and real-market based one have similar distributions and therefore pool converges to the real market distributions. mAAPL token price is "noisy" meaning that pool

reserves increased at the stage of smoothing the distribution. This can be seen on the distributions presented below.



Picture 152: reserves distribution for the mAAPL/UST pool

This pool is less likely to become a target for MEV attack or for extraction of all presented tokens, considering that there are high financial resources required for performing an attack and high transaction frequency.



Picture 153: swap transactions activity in the mAAPL/UST pool

The last important moment about this pool is that transaction frequency is relatively stable.

DOG/WETH (fractionalized NFTs)

What fractionalized NFT is, comparison with traditional NFTs

NFTs have specific limitations related to how NFT works:

- ***Speculative market*** - value of NFT is purely based on supply and demand, token recognition and popularity. Therefore, if the token is an unpopular and unrecognized one, then there is a risk that there will be no option of selling such a token;
- ***Regulation and copyright issues*** - NFTs are not regulated and their sells are based on trust of the buyer to this token or specific desire to purchase it;
- ***Lack of security protocols*** - NFTs have been the target of some security breaches from actors who do not believe that those tokens are "real" investments;
- ***Storage*** - this is the most specific, but also the most interesting moment about NFT. In order to sell NFT it is required to use a marketplace (like OpenSea, Mintable, Rarible) to create, list and sell NFTs. If this platform will somehow shut down then all those NFTs can be lost forever.

The principle behind fractionalized NFTs is that the owner of a fractionalized NFT has an ownership of a part of the asset behind those NFTs. Fractionalized NFTs give fractional ownership and it is an efficient way to invest in high-priced assets. The NFT owner divides ERC-721 token into multiple ERC-20 tokens meaning that each new ERC-20 token is a fractional NFT of the original ERC-721 asset. Those tokens create some benefits:

- ***Price discovery*** - using this token it is easy to access the market value of NFT for example via selling 10-20% of the ownership on the market;
- ***Enhanced Liquidity*** - in case of simple NFT price may be too big to find traders ready to perform such purchase. Fractionalized NFTs have much smaller prices and there will be more traders ready to perform such trades.
- ***Democratizing Investment*** - fractionalized NFTs open purchasing options for small and medium investors;

- ***Curator fees*** - the original NFT owner who dividers the NFT into fractionalized NFTs stand to receive a curator fee annually and the cost is capped at a maximum price set by the governance to prevent high fees;
- ***Easy monetization*** - artists are able to more easily monetize their assets compared to the original NFT.

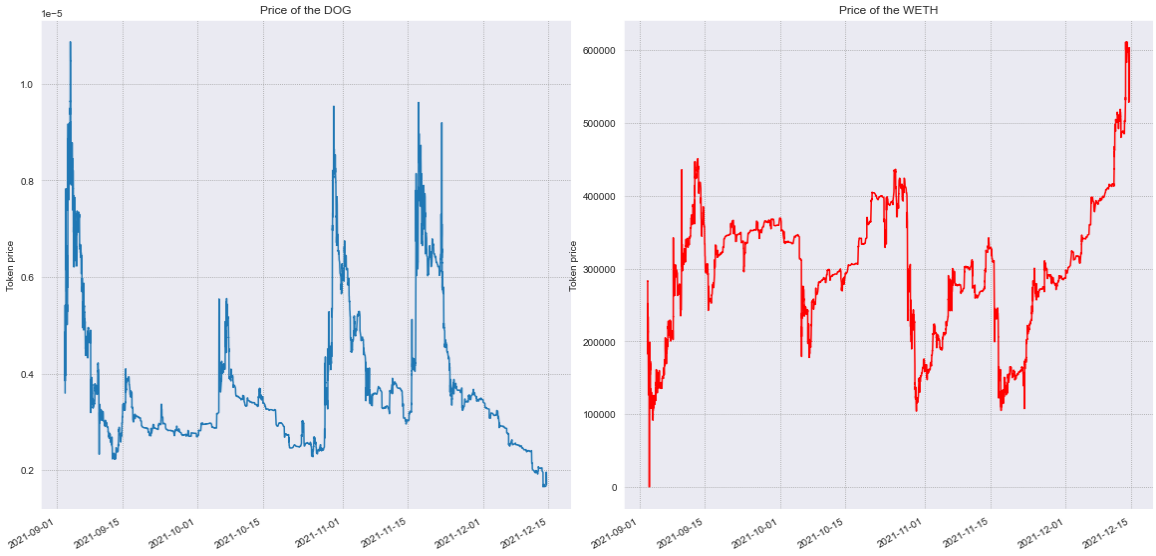
Taking into account fractionalized NFTs properties, their advantages and how they can be used, it is important to consider this token type in performing crypto market research. Those NFTs were not found on the Uniswap platform and therefore extracted transaction history from the SushiSwap platform.

Popular meme-picture becoming a fractionalized NFT leader

Doge is a popular and iconic meme. Picture of this dog was transformed into NFT and then fractionalized to be owned by anyone by Atsuko Sato, owner of the dog. Conform Coinmarketcap information trades of this token started from 3 September 2021.

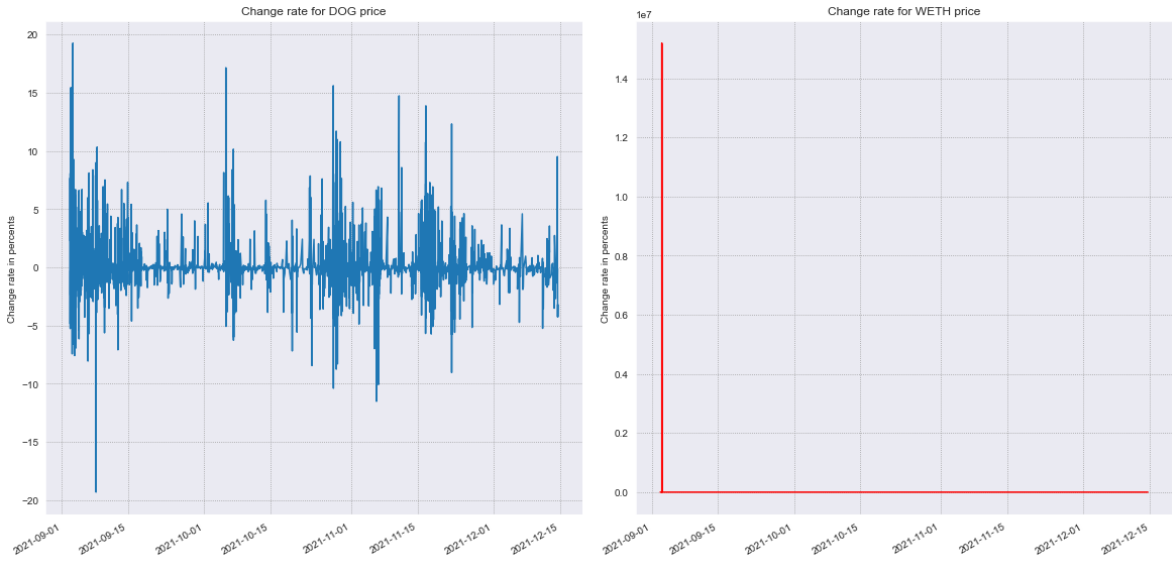
Picture 154: DOG price distribution taken from CoinMarketCap

DOG price is limited by the 0.04 USD upper price limit and token price has big deviations, meaning that the market currently is unstable about this token.



Picture 155: Price distributions of the DOG/WETH pool

DOG price distribution is almost perfectly matching the external markets price distribution, meaning that pool distributions are converging to the real prices, but from the WETH side can be observed anomalous price drop in the start of September 2021. To ensure that the observed case is representing possible attack below is presented price change rates distributions.



Picture 156: price change rates distributions of the DOG/WETH pool

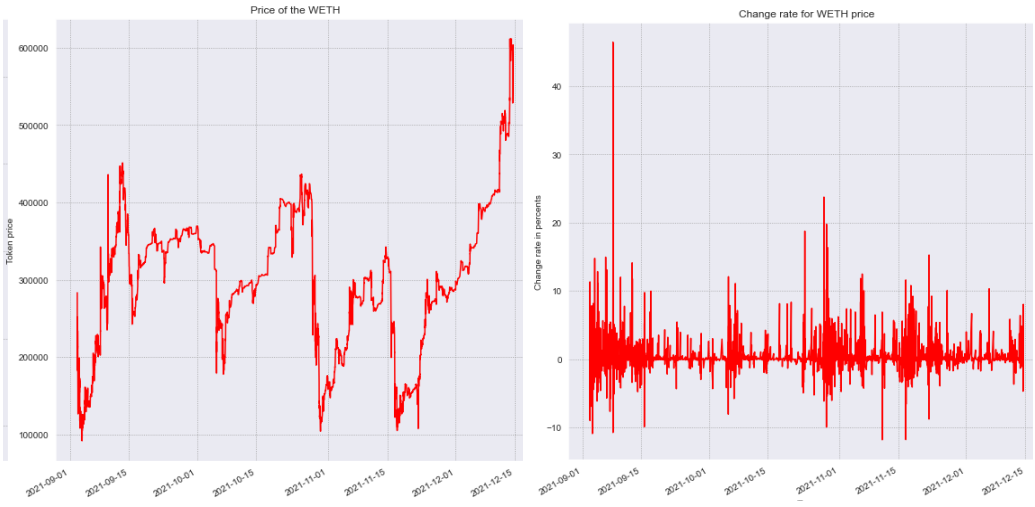
DOG price change rates distribution has big changes in price, but WETH side has one strange moment that entirely breaks the distribution and it looks like there was some market manipulation.

1791	WETH	DOG	2.000000e-01	3.040509e+04	7.537366e+02	2021-09-03 03:12:47	152025.453581	3.151124e-02
1792	WETH	DOG	3.469375e-02	5.272499e+03	1.308105e+02	2021-09-03 03:14:06	151972.599905	-3.476633e-02
1793	WETH	DOG	9.256591e-01	1.406421e+05	3.490815e+03	2021-09-03 03:16:15	151937.293557	-2.323205e-02
1794	WETH	DOG	1.000000e-18	1.000000e-18	3.772845e-15	2021-09-03 03:17:31	1.000000	-9.999934e+01
1795	WETH	DOG	7.321611e-01	1.111979e+05	2.762330e+03	2021-09-03 03:18:14	151876.274830	1.518753e+07
1796	DOG	WETH	8.525832e+04	5.580274e-01	2.105383e+03	2021-09-03 03:18:37	0.000007	1.531304e-01
1797	DOG	WETH	6.832238e+04	4.470701e-01	1.686752e+03	2021-09-03 03:19:46	0.000007	-2.442136e-02
1798	WETH	DOG	5.000000e-02	7.651800e+03	1.886451e+02	2021-09-03 03:20:48	153036.004588	7.636017e-01

Picture 157: transaction history fragment with strange token price rise

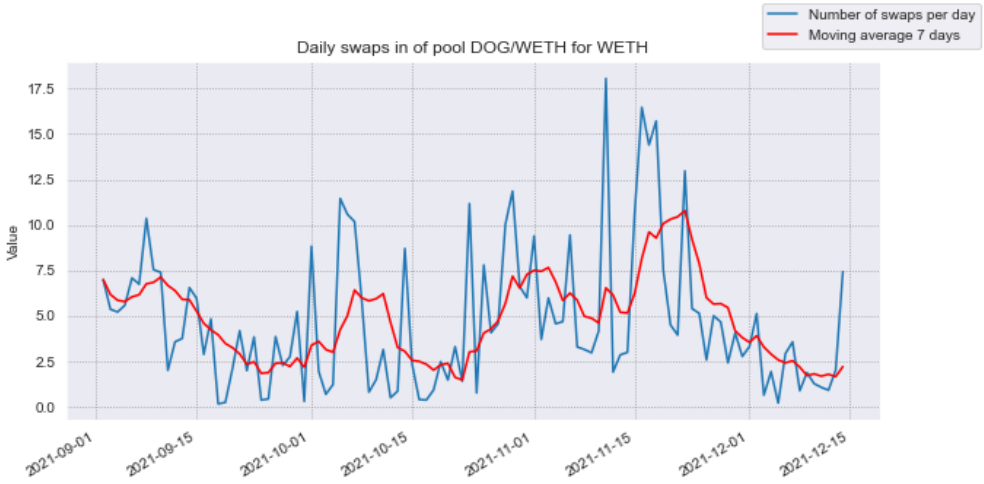
There are too small values set for both WETH and DOG sides. Most probably there was a calculational error caused by too small value of exchanged token in transaction. Another moment that ensures this assumption is that there are no big value transactions happening around specified price drop, which could have been a good chance of performing another trader's losses extraction attack.

It is required to remove this extraction from the charts in order to get an understandable picture of the WETH price deviation. Below are presented changed distributions with ignored anomalous transaction impact. There is still one big price positive change observable from the WETH side that happened 8 September 2021 between 06:10 and 06:13 AM. There was one transaction where trader performed swap of $1.6 * 10^8$ of DOG tokens greatly increasing DOG tokens reserve and decreasing WETH token reserve, causing big price change.



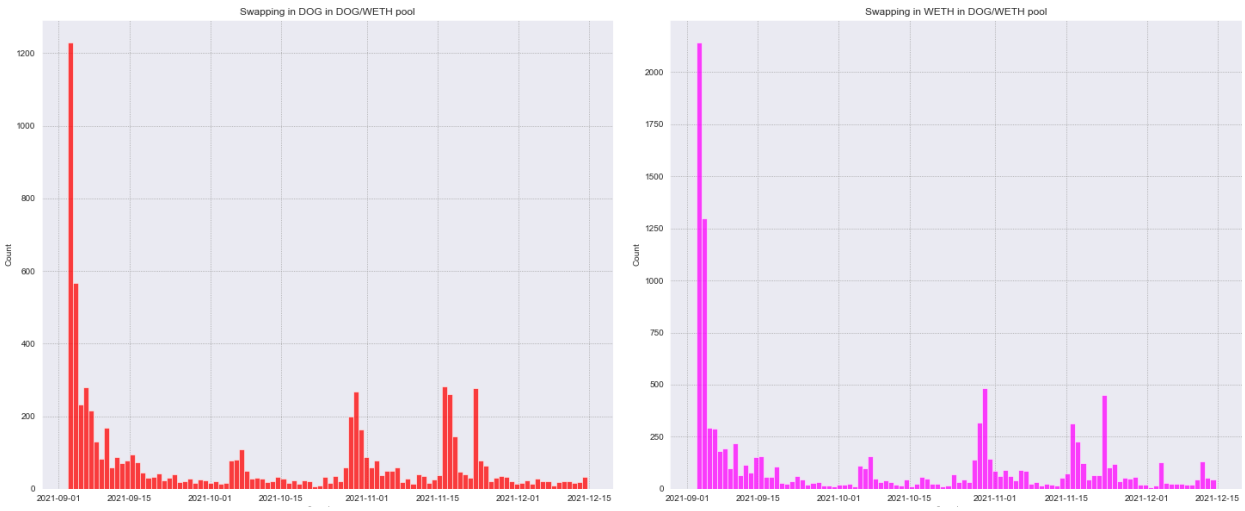
Picture 158: WETH price distribution and WETH price change rates distribution for DOG/WETH pool

Daily mean and weekly rolling average distributions for WETH side of DOG/WETH pool demonstrates big pool activity and that it is popular. It is efficient to perform trades on such a pool.



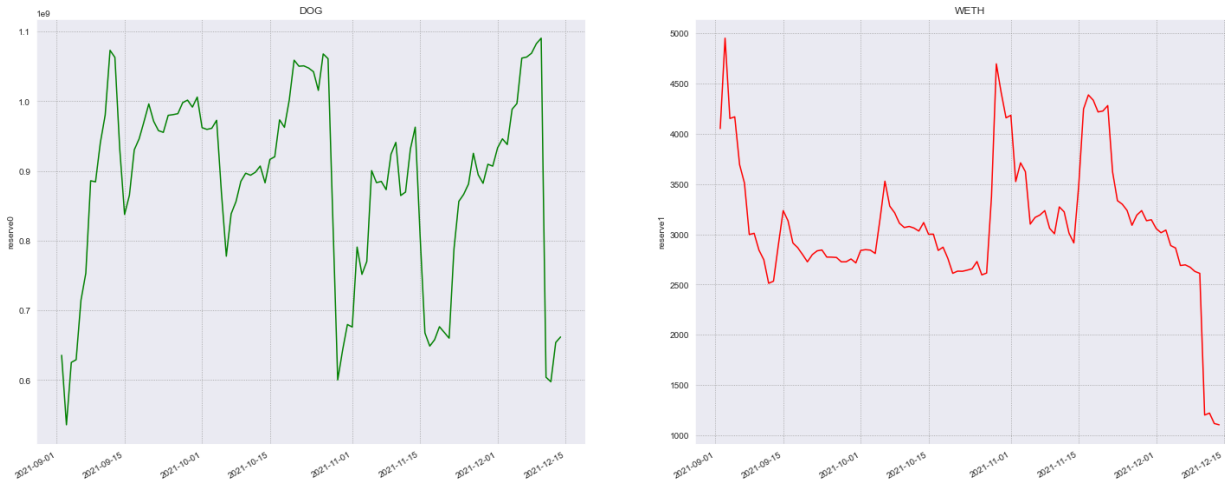
Picture 159: WETH side swap activity for DOG/WETH pool

To understand distribution of the transaction frequency below is presented transaction count distributions.



Picture 160: transaction count distribution for DOG/WETH pool

Start of the pool lifecycle can be characterized by high transaction frequency and high activity. After that there were three transaction frequency rises while during all other periods there was low activity. Considering those pool properties can be estimated that high capitalization is caused more by bigger transaction values.



Picture 161: DOG/WETH pool reserves distributions

Reserves of the pool were relatively big, meaning that the pool was protected against MEV attack, requiring the attacker to have high financial power. From the start of December 2021 there was registered decrease of WETH side reserves which is corresponding with rise of DOG reserves amount, meaning that pool ratio has greatly changed, but high pool capitalization is still present.

General observations

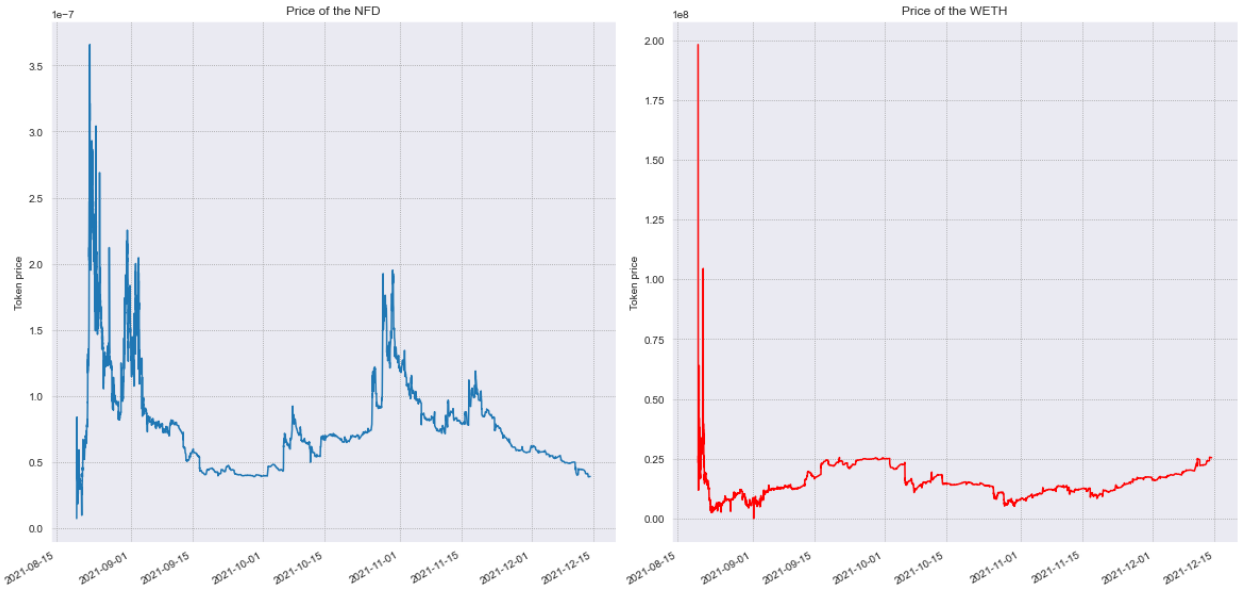
The presented pool is a good example of a popular token and popular market, where high capitalization and medium-level unstable transaction frequency define possible further profit extraction either by speculating on supply and demand or by token price rise over time. DOG token price is unstable, highly depending on popularity of the Doge meme and recognition of this token, defining anomalous price rises. General DOG price tendency does not look positive or negative.

NFD/WETH (fractionalized NFTs) or who said doppelganger?

NFD represents a fractionalized piece of the original Doge NFT auction on Zora using “Fractionalized.art”. The token appeared on the 24 August 2021, little before launch of the DOG token and token price is much smaller than DOG one. This is also one of the most popular fractionalized NFTs present on the markets and therefore distributions should also demonstrate high pool activity.

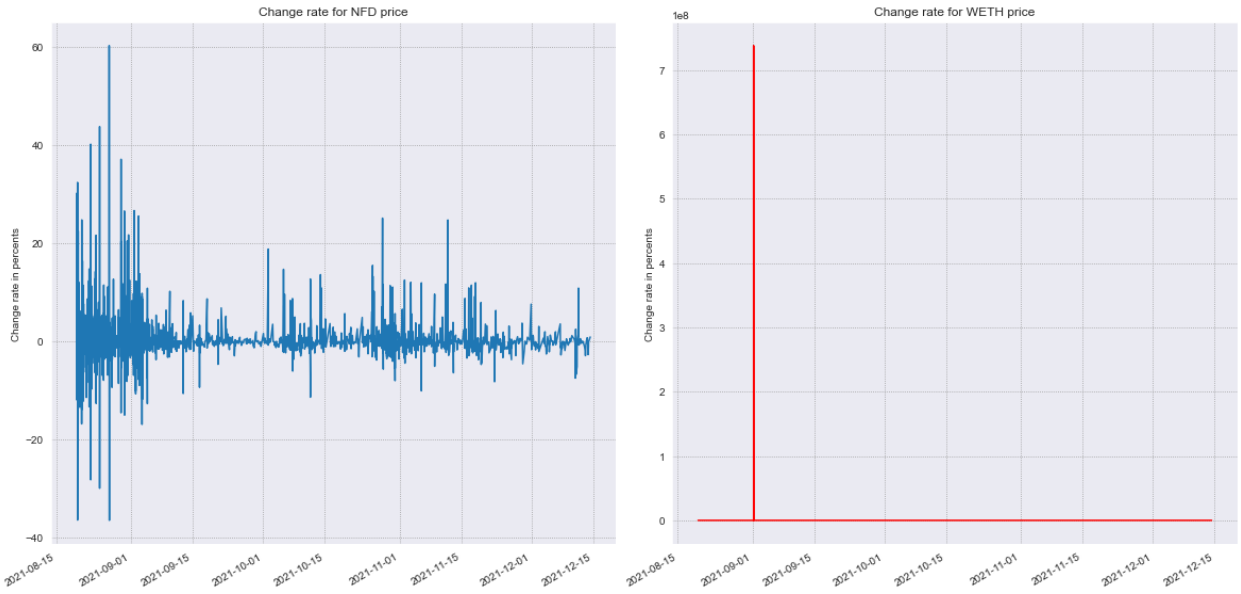
Picture 162: NFD token price distribution taken from CoinMarketCap

Distribution differs from the DOG one and there are only two great price rises. The NFD token price distribution is not breaking the 0.0008 USD upper limit. The presented below token prices distributions in the NFD/WETH pool are matching the external markets price distribution.



Picture 163: tokens prices distributions of the NFD/WETH pool

Deviations of the NFD price distribution are high during the start of the pool lifecycle. Price is also highly deviating from the WETH side during the start of pool lifecycle. There is one strange observation from the WETH side, where the price dropped to almost zero value in the beginning of September 2021.



Picture 164: tokens prices change rates for the NFD/WETH pool

Prices change rates distributions demonstrate anomalous WETH token price rise in the same period as the one observed for the previous pool of DOG/WETH. Considering the known time period of price drop in the previous case and requirement of removing possible outliers to see a better picture of change rates distributions, it is required to dive deeper in this case.

Registered extreme price rise was registered with a transaction happening on 1 September 2021 at 6:45 AM. Considering the strange price change it is required to review the transaction history fragment containing this strange transaction.

	token_in	token_out	amount_in	amount_out	amount_usd	timestamp	first_to_second_price	price_change_rate
13572	WETH	NFD	2.710541	20000000.0	9537.998213	2021-09-01 06:45:22	7.378600e+06	7.378599e+08

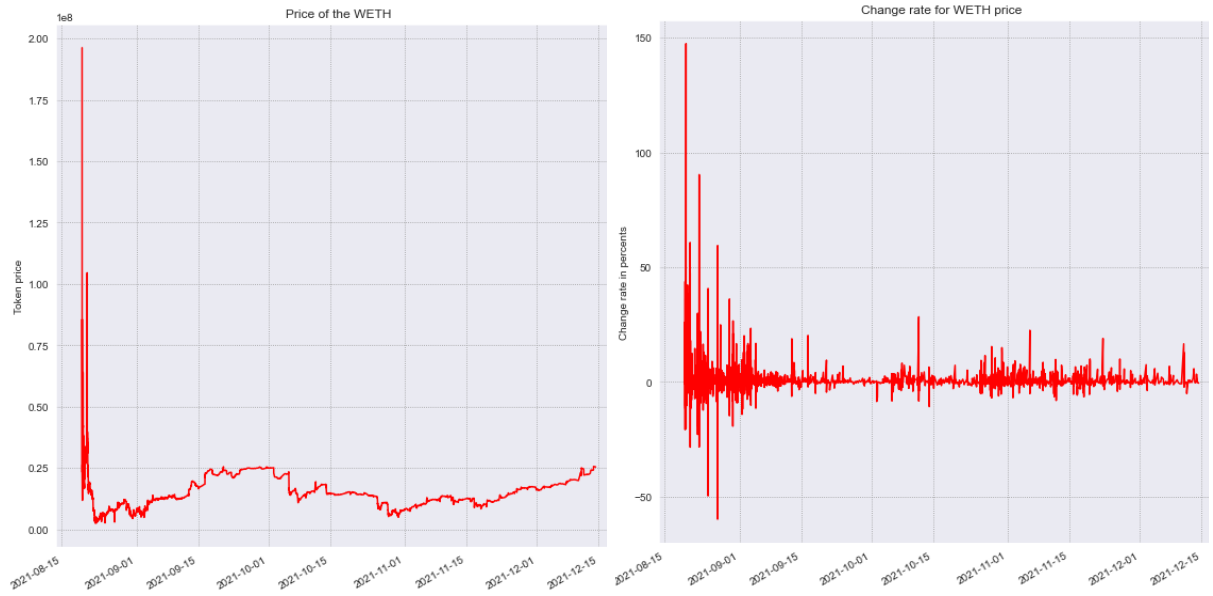
Picture 165: strange transaction

The drop is similar to one in the previous reviewed pool. There are also too low transaction values, but there are no extreme transaction values around, meaning that this case is also not representing attack or a market speculation. Prices before and after the strange transaction are similar, meaning that strange drop was not used for extracting profit.

	token_in	token_out	amount_in	amount_out	amount_usd	timestamp	first_to_second_price	price_change_rate
13561	NFD	WETH	5.091563e+07	6.534754e+00	2.276703e+04	2021-09-01 05:16:27	1.283447e-07	2.780126e+00
13562	WETH	NFD	6.483100e+00	5.091563e+07	2.258706e+04	2021-09-01 05:16:27	7.853594e+06	-1.789453e+00
13563	WETH	NFD	3.000000e+00	2.304244e+07	1.045197e+04	2021-09-01 05:16:27	7.680815e+06	-2.200001e+00
13564	WETH	NFD	5.559957e+00	4.316226e+07	1.949529e+04	2021-09-01 05:49:30	7.763056e+06	1.070741e+00
13565	NFD	WETH	8.347105e+06	1.080082e+00	3.787178e+03	2021-09-01 05:49:35	1.293960e-07	8.191124e-01
13566	WETH	NFD	5.640345e-01	4.338124e+06	1.978064e+03	2021-09-01 05:50:37	7.691239e+06	-9.251177e-01
13567	WETH	NFD	5.271339e+00	4.000000e+07	1.852758e+04	2021-09-01 05:53:08	7.588204e+06	-1.339633e+00
13568	WETH	NFD	3.000000e+00	2.233462e+07	1.056523e+04	2021-09-01 06:00:42	7.444873e+06	-1.888875e+00
13569	NFD	WETH	7.742061e+06	1.038356e+00	3.656824e+03	2021-09-01 06:00:42	1.341188e-07	3.649863e+00
13570	WETH	NFD	1.417488e-01	1.052724e+06	4.985336e+02	2021-09-01 06:37:03	7.426690e+06	-2.442355e-01
13571	WETH	NFD	1.000000e-18	1.000000e-18	3.516481e-15	2021-09-01 06:42:52	1.000000e+00	-9.999999e+01
13572	WETH	NFD	2.710541e+00	2.000000e+07	9.537998e+03	2021-09-01 06:45:22	7.378600e+06	7.378599e+08
13573	WETH	NFD	5.639545e+00	3.960985e+07	1.985895e+04	2021-09-01 06:55:02	7.023591e+06	-4.811339e+00
13574	WETH	NFD	6.780500e+00	4.896822e+07	2.387668e+04	2021-09-01 06:55:02	7.221919e+06	2.823743e+00
13575	NFD	WETH	4.896822e+07	6.910437e+00	2.433424e+04	2021-09-01 06:55:02	1.411209e-07	5.220790e+00

Picture 166: transaction history fragment with strange transaction

Considering how this transaction changes price and price change rates distributions it is required to remove it from plots to see a better picture.



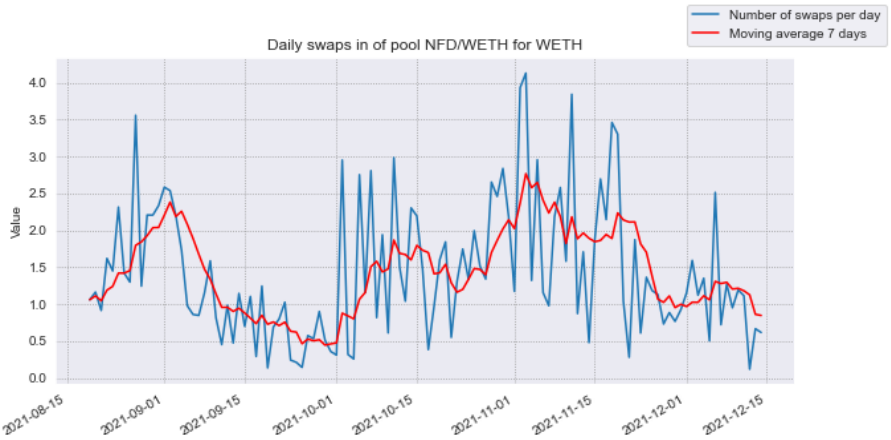
Picture 167: price and price change rates distributions of the WETH token in NFD/WETH pool

In the beginning of the pool lifecycle can be observed extreme deviation of the WETH price and some strange changes like around 150% token price rise. While this 150% price change was caused by swapping high NFD tokens and therefore causing WETH token price rise, there was another interesting moment which demonstrated a successful MEV attack.

423	WETH	NFD	1.680792e+00	4.624475e+07	5304.294044	2021-08-19 21:00:47	2.751366e+07	-3.012374
424	WETH	NFD	1.543720e+01	3.387241e+08	48717.061605	2021-08-19 21:02:04	2.194207e+07	-20.250295
425	WETH	NFD	1.914300e+00	3.355713e+07	6041.190827	2021-08-19 21:02:04	1.752971e+07	-20.109102
426	NFD	WETH	3.387241e+08	1.599973e+01	50492.291856	2021-08-19 21:02:04	4.723528e-08	32.413679
427	WETH	NFD	3.000000e-02	7.751712e+05	94.672233	2021-08-19 21:02:55	2.583904e+07	47.401373

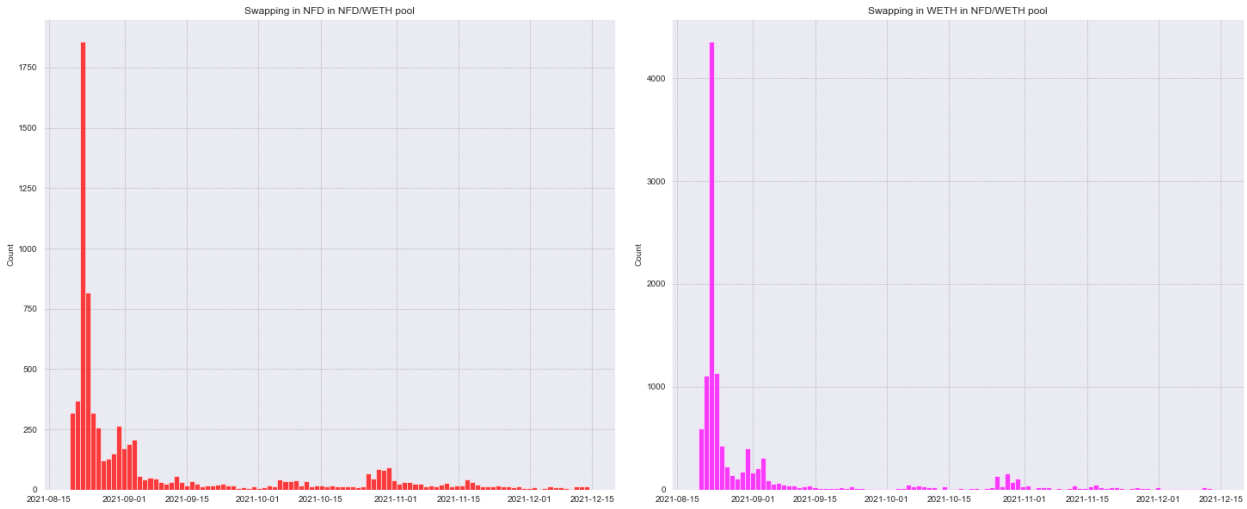
Picture 168: MEV attack on the NFD/WETH pool

Can be observed that there were two transactions in one block happening with exactly the same values of out token in the first transaction and in token in the second transaction. Between those two transactions is a relatively big transaction, but due to big reserves of the pool (presented below) price change was relatively small. Because of this property the attacker extracted only around 1800 USD profit out of the attack (profit is almost equal to the victim's loss).



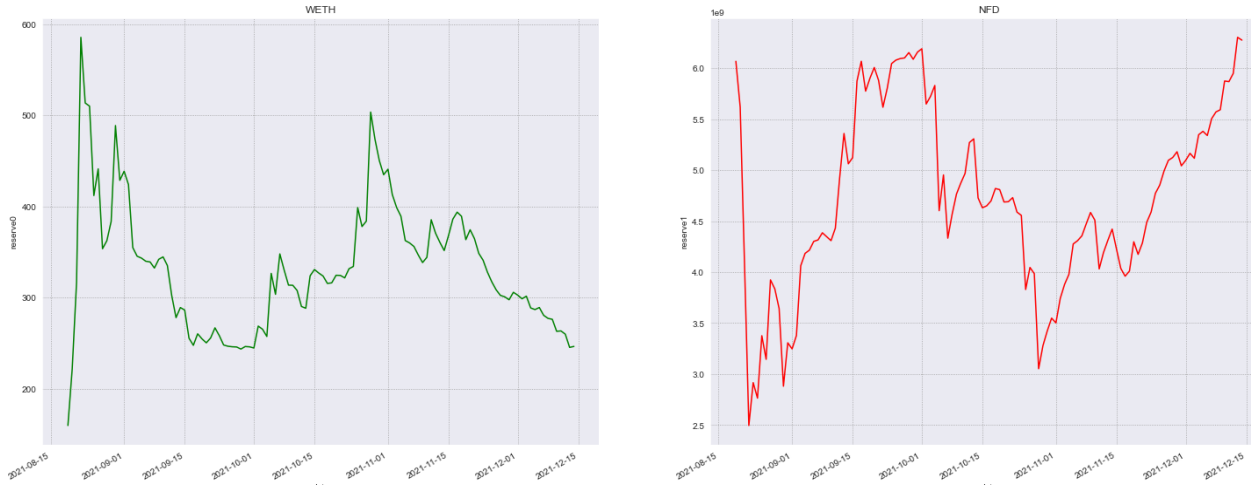
Picture 169: swap activity of the WETH side in NFD/WETH pool

The activity in the pool is smaller compared to the previous case and to ensure that this is not caused only by smaller transaction values below is presented the transaction count distributions.



Picture 170: transaction count distributions for different sides of the NFD/WETH pool

There was high activity registered in the time interval between middle of August 2021 till 4-5 September 2021. After this period of pool lifecycle beginning activity dropped to small transaction activity. Considering this it is possible to perform a MEV attack.

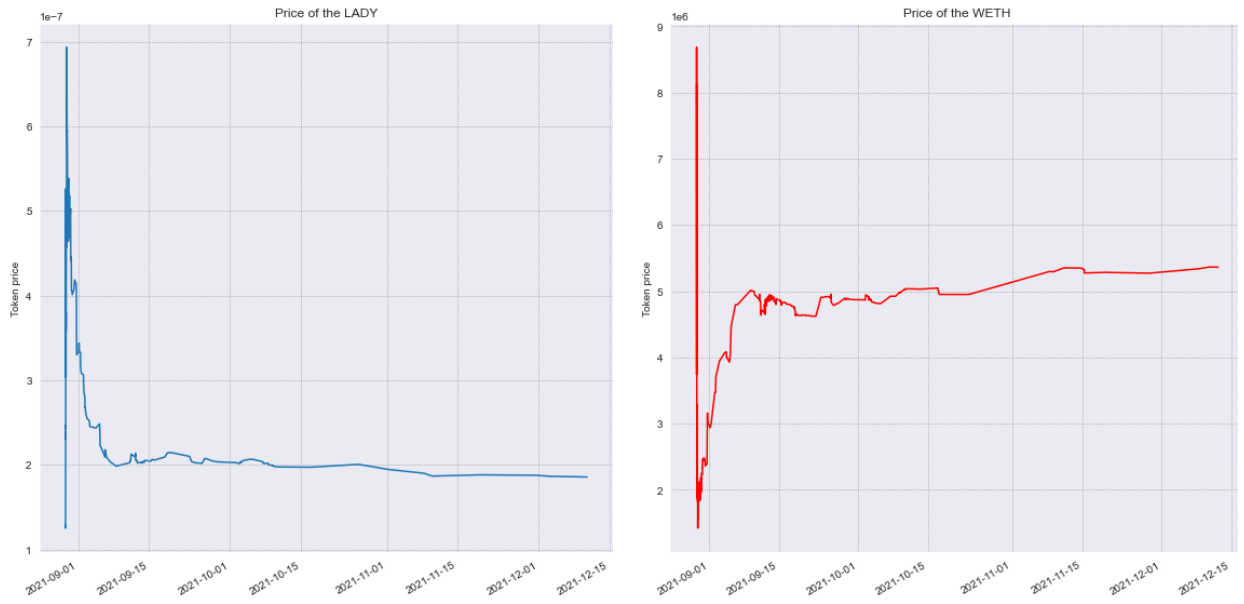


Picture 171: reserves distribution in the NFD/WETH pool

Pool reserves are relatively high, meaning that small price deviations during observed MEV attack were caused by big pool reserves, smoothing the attack impact on the prices.

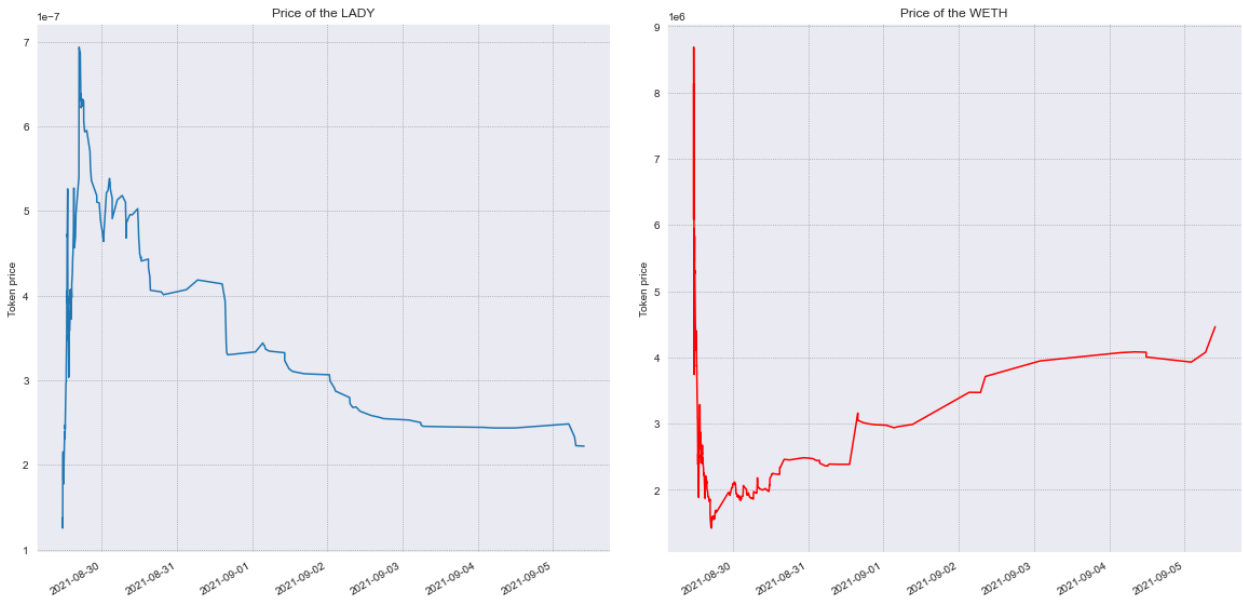
LADY/WETH (fractionalized NFTs) or short living pool extreme start

There is a “ladypunk” token created on “fractionalized.art” with market overall token activity and popularity smaller than previous DOG and NFD cases. The interesting moment about the presented case is that there is an extreme price change observed during the start of LADY/WETH pool lifecycle on SuchiSwap.



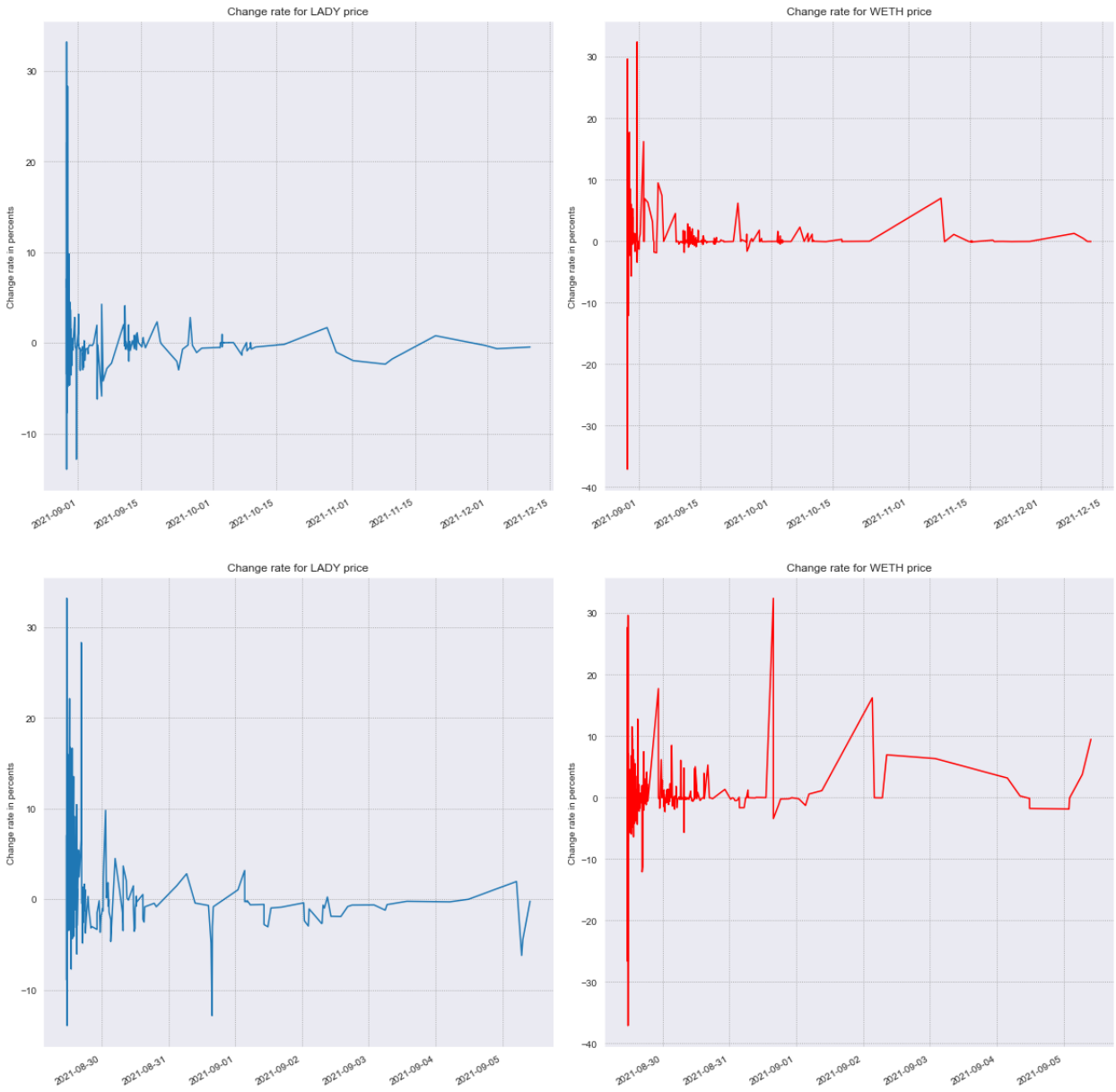
Picture 172: prices distributions in the LADY/WETH pool

Conform presented charts beginning of the pool lifecycle was characterized by extreme price changes. In order to dive deeper into the data below is presented a closer look into this price change.



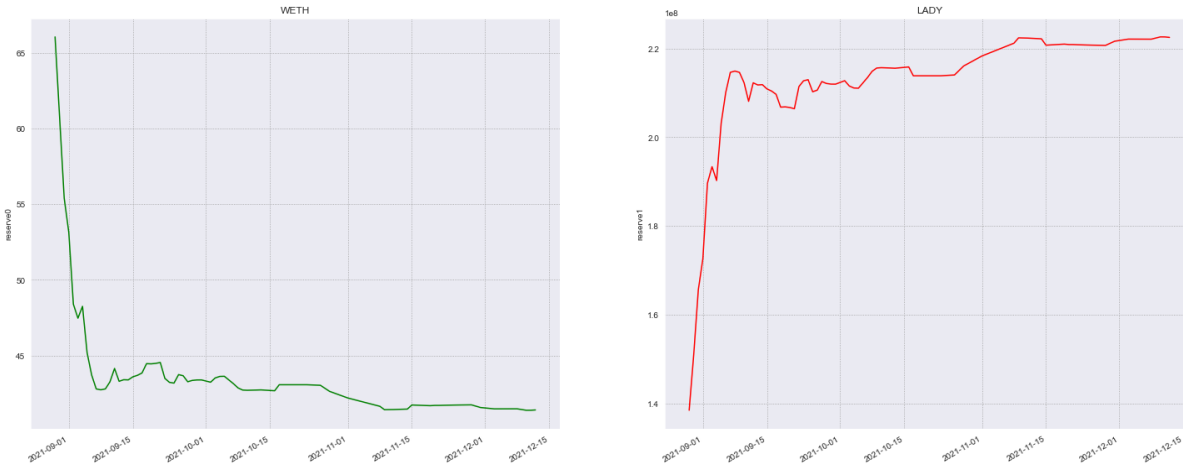
Picture 173: prices distributions in the LADY/WETH token before 6 September 2021

The price changes are big enough to attract attention to verify for presence of MEV attacks or some market speculations.



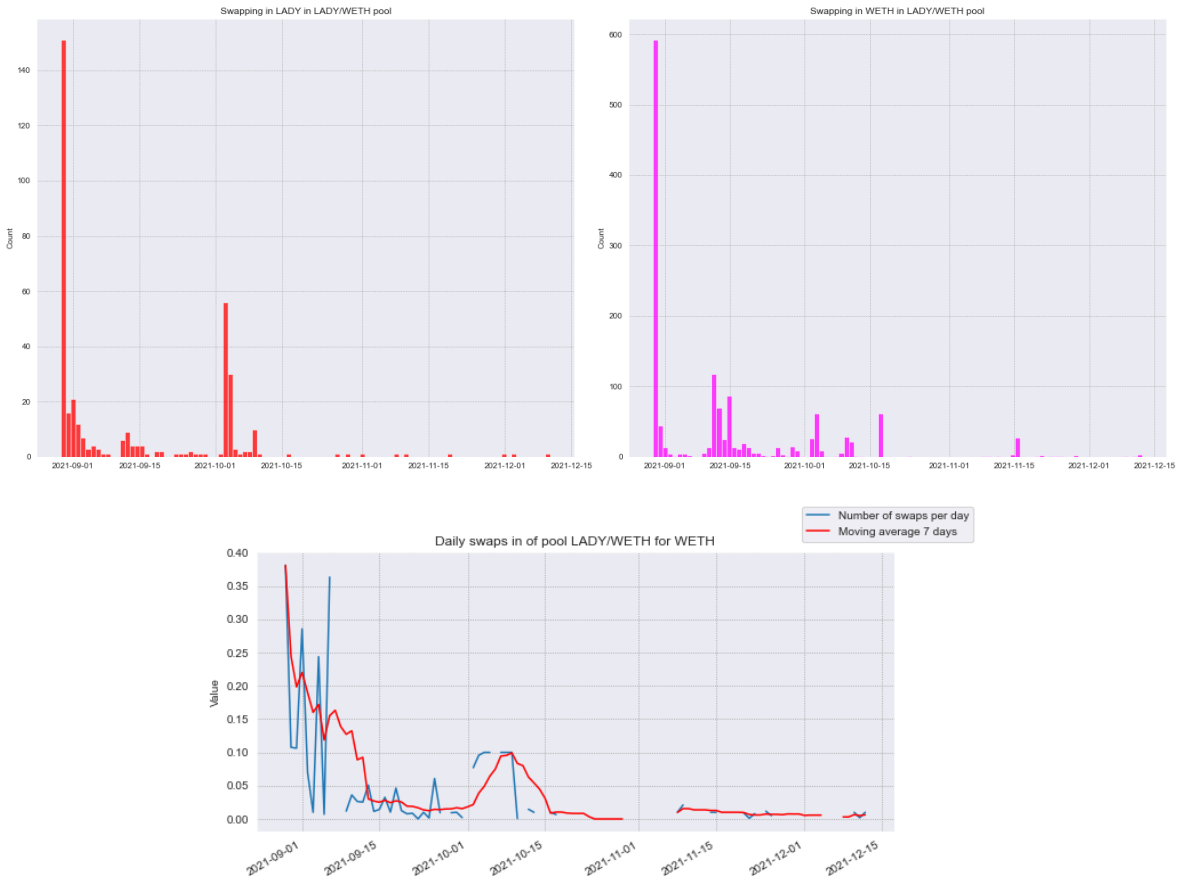
Picture 174: price change rates distributions for entire period and till 6 September 2021 for LADY/WETH pool

Start of the pool lifecycle can be characterized as an unstable one with further stabilization. Suggestion is that there is a connection between pool reserves and price change rates, meaning that there was possibly incorrect initial pool reserves established and traders performed trades to make price distributions converge to prices on external markets, but there were not found any mentionings of this token on other platform (therefore, there was no option of comparing pool prices with external ones).



Picture 175: reserves distributions in the LADY/WETH pool

WETH reserves had almost 30% drop while LADY reserves had almost 50% rise. Reserves distribution stabilizes after the first two weeks of pool lifecycle and there are small changes, which considering pool reserves sizes demonstrate decrease of pool activity.



Picture 176: swap activity in the LADY/WETH pool for WETH side and transaction count distributions for LADY/WETH pool

Swap activity of the pool is small with small rises and extreme initial activity. Looks like activity was present while tokens relative prices were profitable for traders and when prices stabilized activity dropped. The problem of this case is that it is not possible to ensure the fact of incorrect initial pool values that were used by traders.

	token_in	token_out	amount_in	amount_out	amount_usd	timestamp	first_to_second_price	price_change_rate
31	LADY	WETH	1.704775e+06	3.671787e-01	1175.158268	2021-08-29 11:35:58	2.153825e-07	9.424711
32	WETH	LADY	1.000000e+00	4.550603e+06	3198.676772	2021-08-29 11:37:43	4.550603e+06	-5.772733
33	WETH	LADY	1.000000e-02	5.899570e+04	31.984126	2021-08-29 11:37:46	5.899570e+06	29.643694
34	WETH	LADY	1.000000e-01	5.916212e+05	319.841261	2021-08-29 11:37:46	5.916212e+06	0.282095
35	WETH	LADY	1.028308e-01	6.115380e+05	328.895243	2021-08-29 11:37:46	5.947030e+06	0.520906
36	LADY	WETH	3.170277e+07	6.119274e+00	19573.578911	2021-08-29 11:37:46	1.930202e-07	-10.382600
37	LADY	WETH	4.609734e+07	9.893984e+00	31645.044338	2021-08-29 11:37:51	2.146324e-07	11.196873
38	WETH	LADY	5.000000e-01	1.870353e+06	1599.206305	2021-08-29 11:37:51	3.740705e+06	-37.099605
39	WETH	LADY	9.761349e+00	4.609734e+07	31220.823300	2021-08-29 11:37:51	4.722436e+06	26.244524
40	WETH	LADY	1.000000e+00	5.370542e+06	3198.396037	2021-08-29 11:38:14	5.370542e+06	13.723992
41	LADY	WETH	5.867906e+06	1.083816e+00	3466.472847	2021-08-29 11:38:14	1.847024e-07	-13.944796
42	WETH	LADY	1.039001e+00	5.867906e+06	3323.138167	2021-08-29 11:38:14	5.647639e+06	5.159573
43	WETH	LADY	1.000000e-01	5.512833e+05	319.826243	2021-08-29 11:39:37	5.512833e+06	-2.386945

Picture 177: transaction history fragment with MEV attack

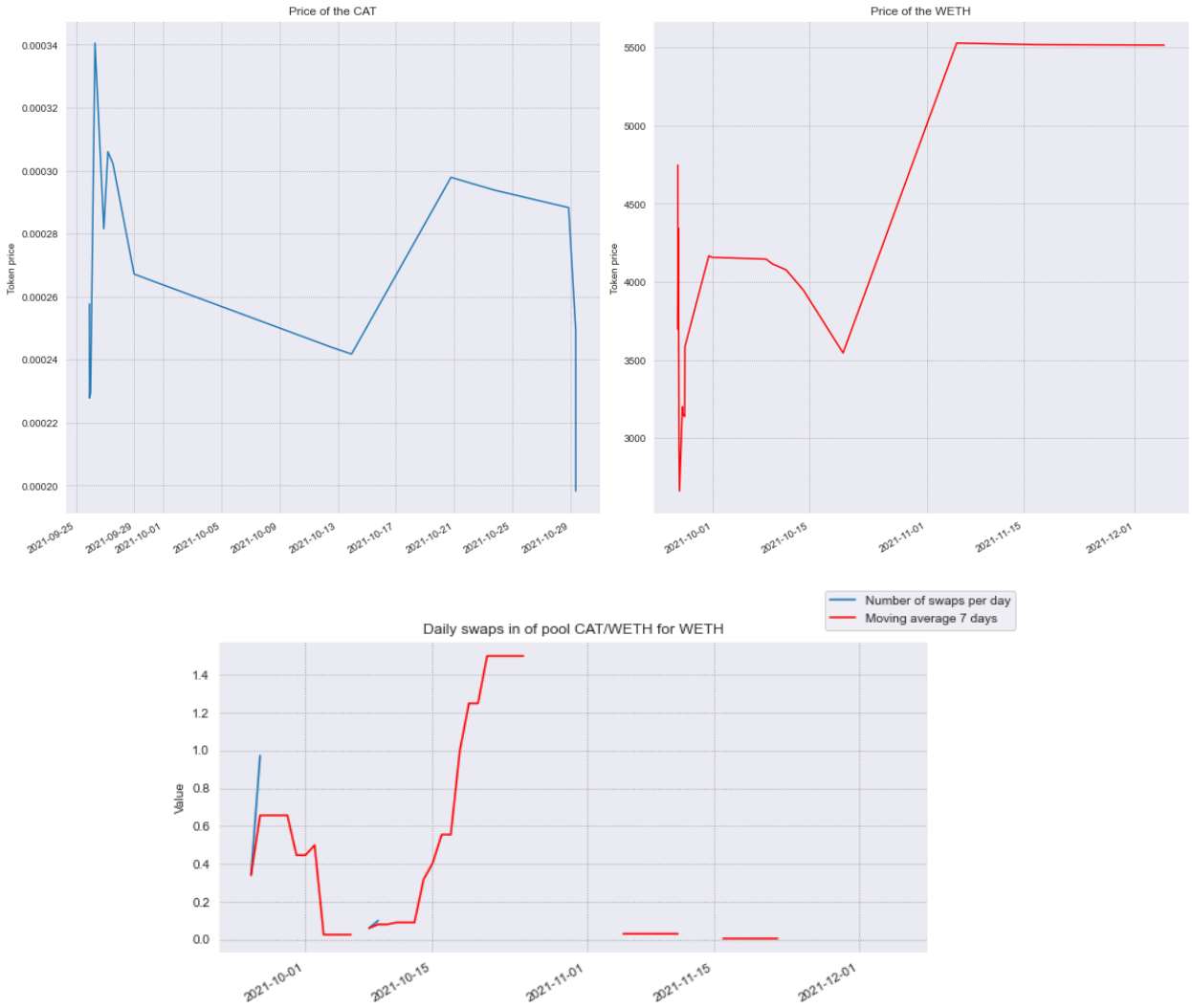
The interesting observation about fractionalized NFTs is that MEV attacks are less aggressive than in previous cases with smaller extracted profits. For example, the presented transaction history contains a MEV attack, during which the attacker extracted around 0.13 WETH token (equal to 580 USD). In one block there are transactions 37, 38, and 39. Conform values the sequence of transactions is 39, 38, and 37. This section additionally demonstrates that transaction history has some problems with ordering the transactions.

Dead pools or how fractionalized NFTs presented unexpected low activity

CAT/WETH (fractionalized NFTs)

CAT token is representing “Cool Cat Yellow Backgrounds” NFTs and there was not found any platform containing information about token price distributions. Considering DappRadar data is one of the most popular NFTs it was decided to check the CAT/WETH pool on the SushiSwap.

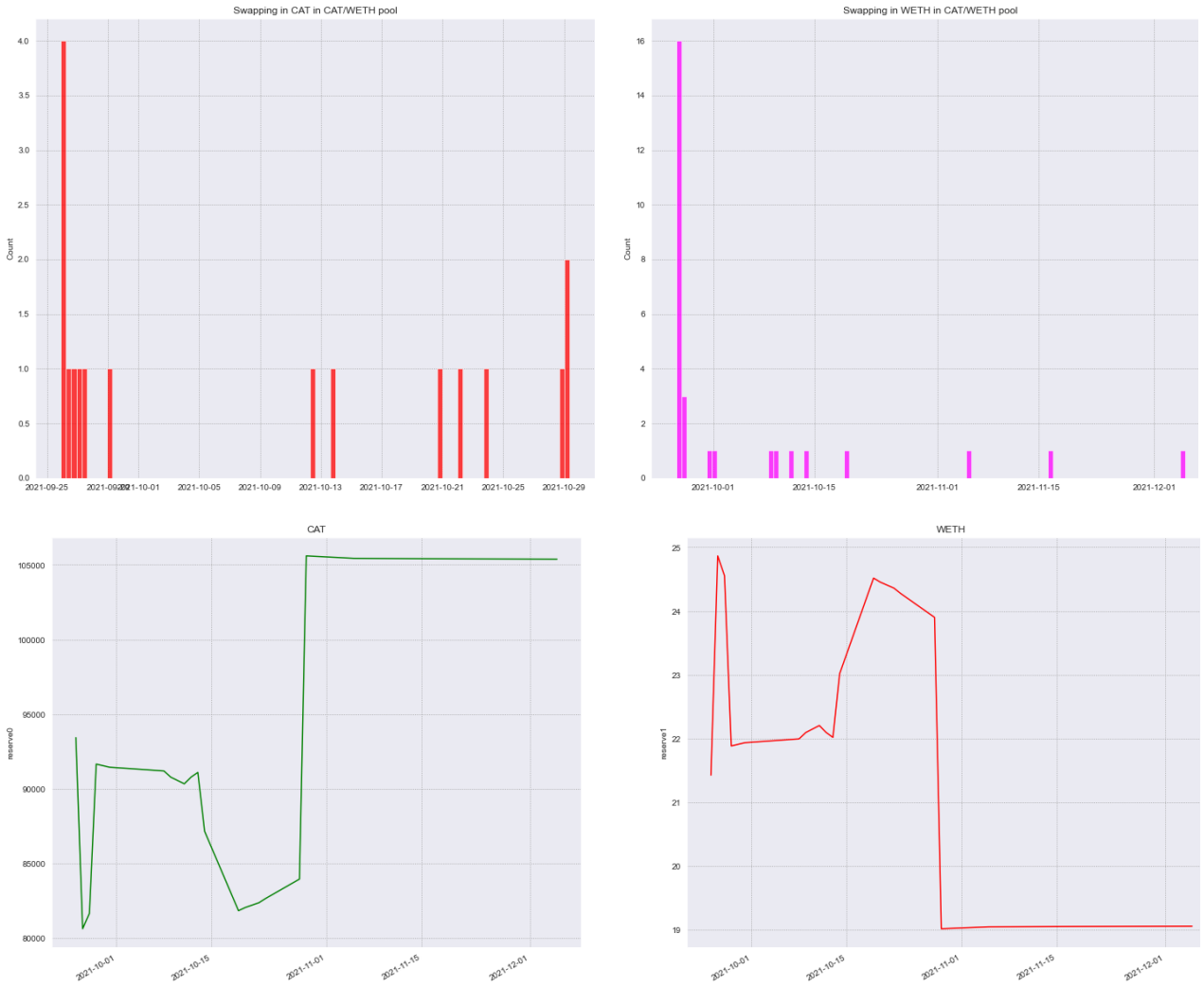
The presented information about this pool shows low activity with small capitalization of overall activity. The distributions are unstable, their behavior is hard to predict and future changes are untraceable.



Picture 178: price distributions and swap activity for WETH side of the CAT/WETH pool

Activity is too low and there is no option of performing efficient data analysis based on extracted data. Reserves of the pool are also low and changes presented there do not demonstrate positive tendency of the pool, leading to the pool activity death without mints.

Strange thing about this token is that, conform DappRadar data, this is one of the most popular fractionalized NFTs. Therefore, pool activity should be bigger and tendency must be more positive. Possibly this happened due to low trust to the presented pool by traders and these tokens are more traded on other platforms.



Picture 179: transactions count distributions and reserves distributions of the CAT/WETH pool

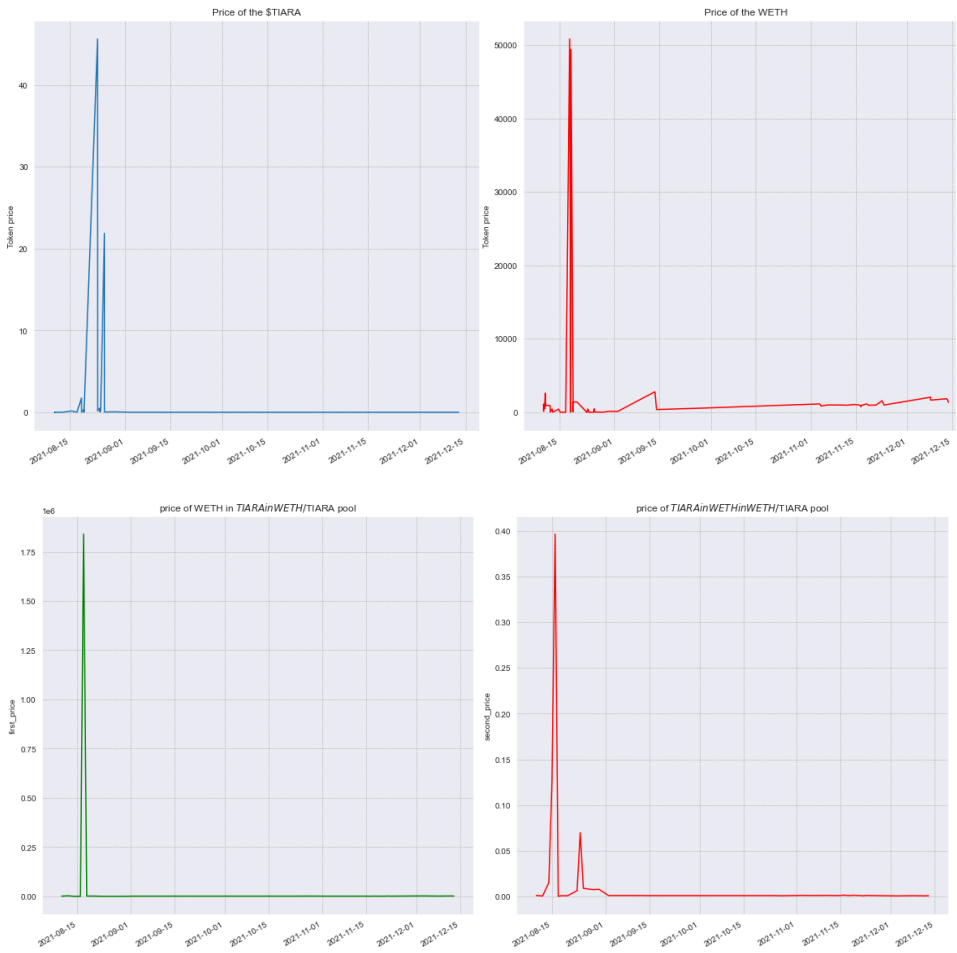
Most likely this pool will not have activity increase and pool parameters will degrade through time, reducing pool attractiveness and removing the option of possible pool revival.

TIARA/WETH (fractionalized NFTs) or inactive pool

House of Tiara is also a fractionalized NFTs. There was found a small external market price distribution.

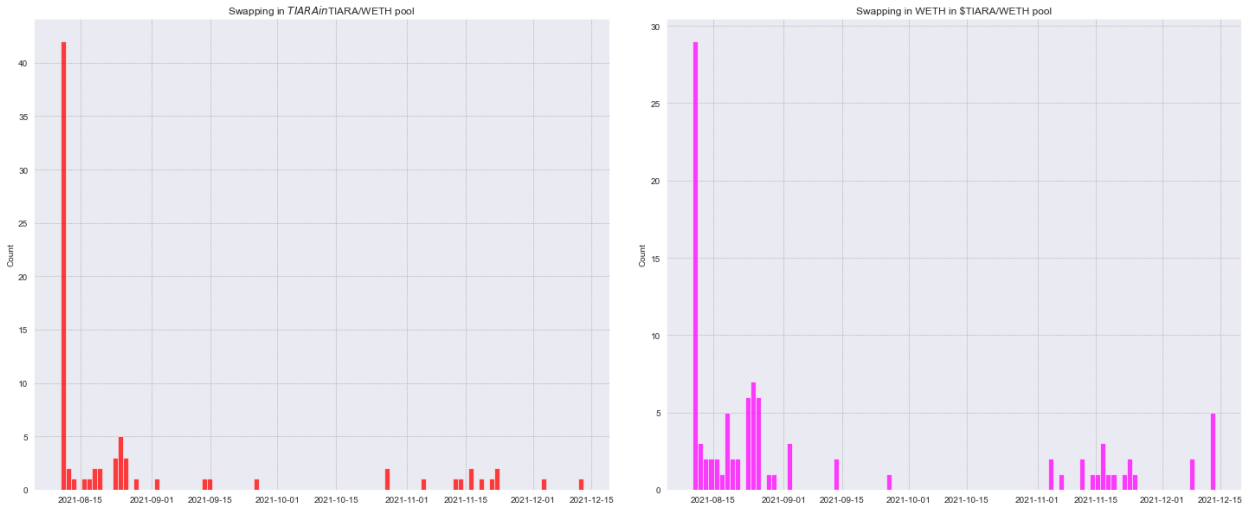
Picture 180: TIARA token price in USD distribution taken from nomics.com

Price changes of the token are unstable. The problem of the pool is that price distributions contain a small amount of information and therefore it is hard to compare local and external prices.



Picture 181: swap-based and reserve-based distributions in the TIARA/WETH pool

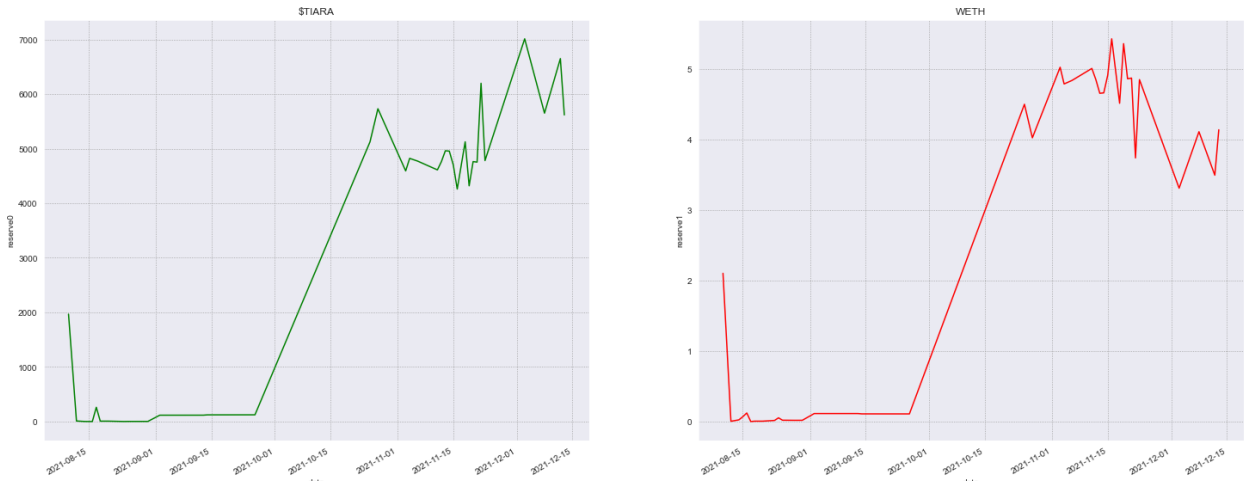
Activity of the pool is on such a low level that it is impossible to make any assumptions and to generate some conclusions about the data.



Picture 182: transaction count distributions for the TIARA/WETH pool

ACAB/WETH (fractionalized NFTs)

The presented distributions of the ACAB/WETH pool show lack of information. It was not possible to find any external market data and therefore it is impossible to perform efficient pool analysis and it looks more like a dead pool without activity and there will be no activity in the future. This can be even seen via the reserves distribution.



Picture 183: reserves distribution of the $TIARA/WETH pool

Reserves of the pool are too small, causing each transaction to have an impact over the token prices. This pool is vulnerable to MEV attacks and market manipulations, meaning that

attractiveness of this pool is low for investors and therefore there will be no activity in future with such distributions.

Simulations

To identify how the volatility mitigation mechanism impacts the overall state of the pool and the change of the price of tokens inside the pool, as well as identify under which circumstances the volatility mitigator kicks in, simulations using real transaction history have been conducted in 2 different modes: with and without the volatility mitigation mechanism.

WBTC / DAI

This is a pool with a relatively low frequency of transactions and capitalization value (among the pools with popular tokens). At the moment of the analysis the total locked liquidity inside the pool was 1 306 087$, the median of the swaps count per day across the entire history being 18, mean - 25.

Historical stats:

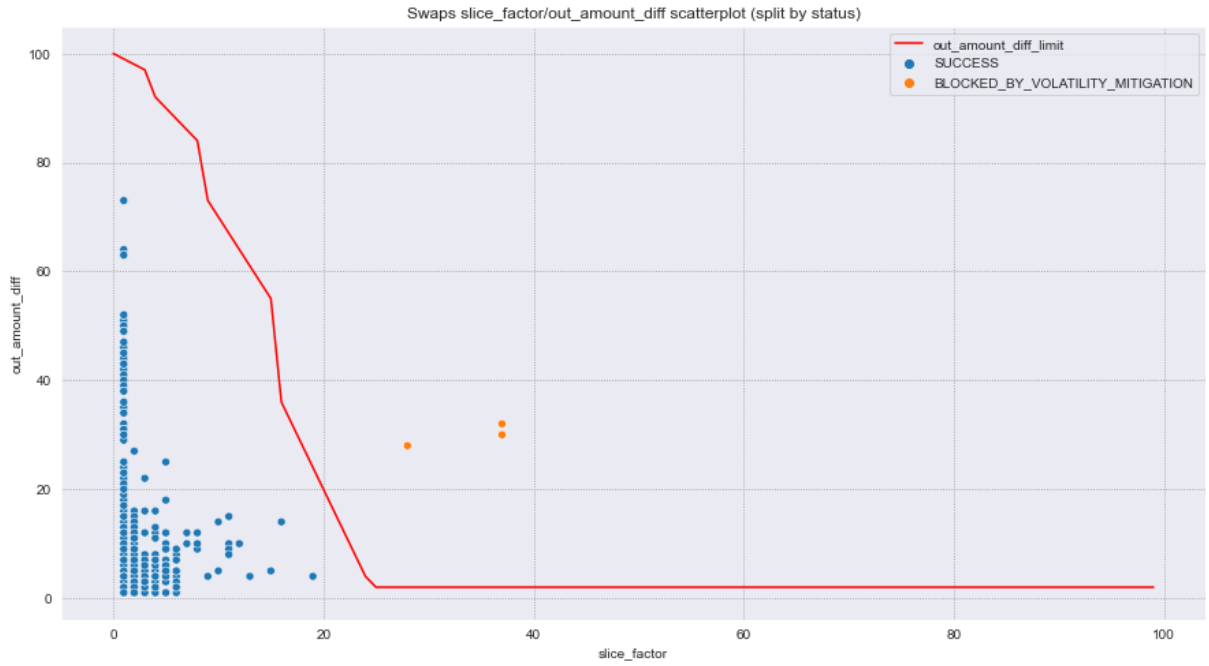
- 13 873 swaps
- 187 mints
- 138 burns
- Initial liquidity: $311
- Last day liquidity: $1.3
- Max liquidity: $16.15 mln
- Median swaps per day: 18
- Mean swaps per day: 25

A more detailed overview of the pool can be found here.

After running the historical transactions from this pool through the synthetic AMM with the volatility mitigation mechanism enabled **3** swap-transactions have been **blocked**. During about **33.9%** of the cases the volatility mitigation mechanism didn't check the transaction because of the missing priceCummulative observation inside the DSW oracle. Below, is presented a table containing the information about each blocked transaction.

token_in	token_out	token_in_amount	token_out_amount	slice_factor	oracle_amount_out	out_amount_diff	reserve_X_before	reserve_Y_before
DAI	WBTC	4000.000000	0.096852	37.0	0.134965	32.0	0.361719	10829.600689
DAI	WBTC	152135.514321	2.853247	28.0	3.795402	28.0	13.200136	546180.486138
WBTC	DAI	4.872345	143681.055827	37.0	195377.007969	30.0	13.332136	540804.943638

Picture 162: Blocked by volatility mitigator transactions

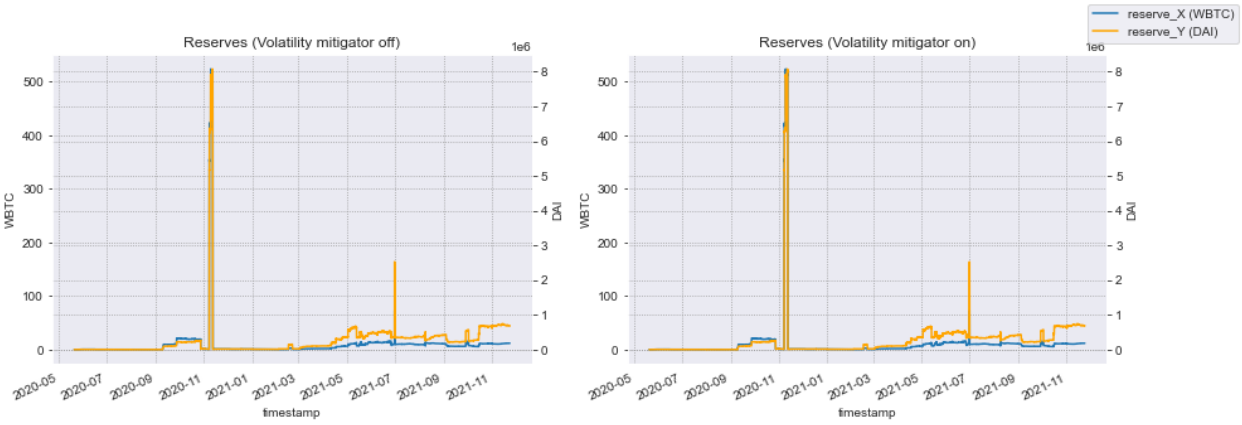


Picture 163: Swaps slice_factor/out_amount_diff scatter plot, split by status (with visualization of the out_amount_diff_limit)

Notes:

- in the plot above are not included the transactions for which TWAP couldn't be computed and which represent 33% from all of the transactions
- The out_amount_diff_limit border is not smooth, because the slice_factor_curve is computed according to the formula slice_factor * sqrt(slice_factor), where the sqrt(slice_factor) is rounded down in the original contract

The out_amount_diff limit separates the successful and blocked transactions visually very well. It can be observed that by varying the PRICE_TOLLERANCE_TRESHOLD by an amount of less than 20, no effect would be obtained. It would require to change this number by at least 20 in order to change the distribution of the successful/blocked transaction.



Picture X: reserves distributions with and without mitigation mechanism

The reserves of the pool visually vary almost identically in the 2 distinct regimes. The second spike in the reserves (near 07.2021), which is not present in pool analysis section from the historical data, is caused by a large mint and burn during a single day (in the first section the extracted reserve values were daily, therefore the spike is not visible on the plot)

Picture X: price distribution of token X (WBTC)

It can be seen from the variation of price that the volatility mitigation mechanism slightly decreases the price variation in several cases. The sudden price increase in 02.03 is caused by a single transaction whose swap_in value is bigger than the current reserves.

	token_in	token_out	token_in_amount	token_out_amount	mitigator_check_status	reserve_X_before	reserve_Y_before
4219	DAI	WBTC	10000.0	0.224279	CANT_CONSULT_ORACLE	0.440354	9537.874801

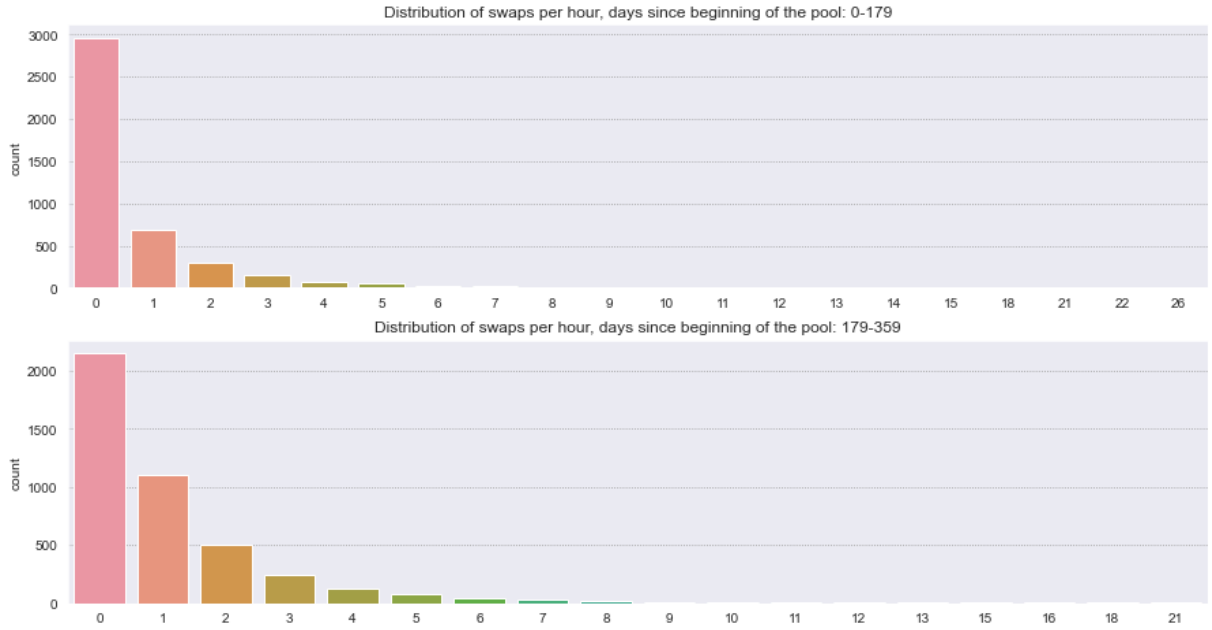
Picture X: transaction that caused price deviation

It can be seen that the volatility mitigator didn't check this transaction, as there were no swaps happening in the 1 hour window exactly 24 hours ago, even though during the entire 24 hour window_size period more than 10 swaps happened.

	token_in	token_in_amount	token_out_amount	mitigator_check_status	reserve_X_before	reserve_Y_before	transaction_timestamp	X_price
4208	DAI	23.169225	0.000725	CANT_CONSULT_ORACLE	0.360166	11365.037586	2021-02-02 21:20:12	31682.906432
4209	DAI	12.259807	0.000382	CANT_CONSULT_ORACLE	0.363637	11538.114135	2021-02-03 03:14:03	31796.775544
4210	DAI	101.080406	0.003120	CANT_CONSULT_ORACLE	0.363255	11550.324902	2021-02-03 04:26:15	32351.807538
4211	WBTC	0.000297	9.506241	CANT_CONSULT_ORACLE	0.360134	11651.000987	2021-02-03 04:36:03	32298.664654
4212	WBTC	0.001544	49.166394	CANT_CONSULT_ORACLE	0.360432	11641.456721	2021-02-03 04:39:35	32024.511635
4213	WBTC	0.000043	1.355833	CANT_CONSULT_ORACLE	0.361976	11592.093662	2021-02-03 09:50:32	32016.967973
4214	WBTC	0.000043	1.353929	CANT_CONSULT_ORACLE	0.362018	11590.732406	2021-02-03 10:55:02	32009.435793
4215	WBTC	0.000021	0.676528	CANT_CONSULT_ORACLE	0.362061	11589.373061	2021-02-03 10:58:20	32005.672464
4216	DAI	15.976918	0.000494	CHECKED	0.362082	11588.693827	2021-02-03 16:51:46	32093.364850
4217	DAI	16.363380	0.000504	CANT_CONSULT_ORACLE	0.361589	11604.606837	2021-02-03 18:13:00	32183.302391
4218	WBTC	0.079270	2074.731038	CANT_CONSULT_ORACLE	0.361085	11620.904763	2021-02-03 23:10:39	21659.537618
4219	DAI	10000.000000	0.224279	CANT_CONSULT_ORACLE	0.440354	9537.874801	2021-02-03 23:10:39	90236.450623

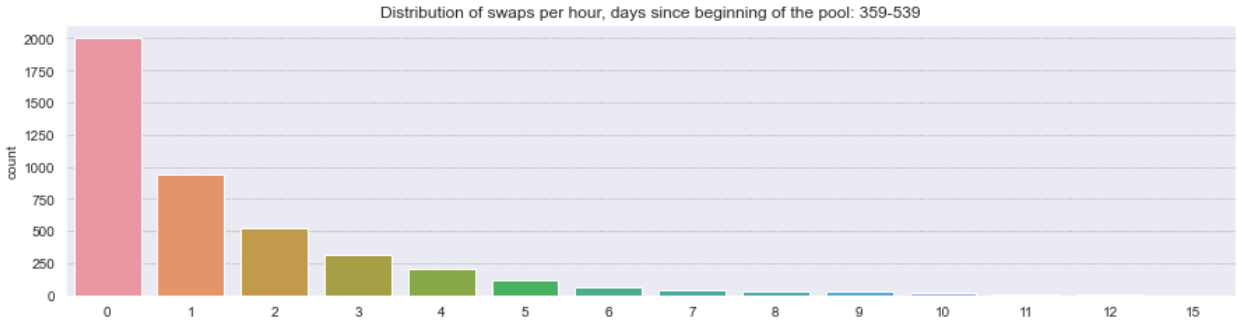
Picture 166: transaction frequency fragment around anomalous swap_in value

It was decided to analyze the distribution of swaps per hour during 3 stages of the pool (1st stage - initial period - days 0-179 since creation, 2nd stage - days 179-359 since pool creation, 3nd stage - days 359 till the end).



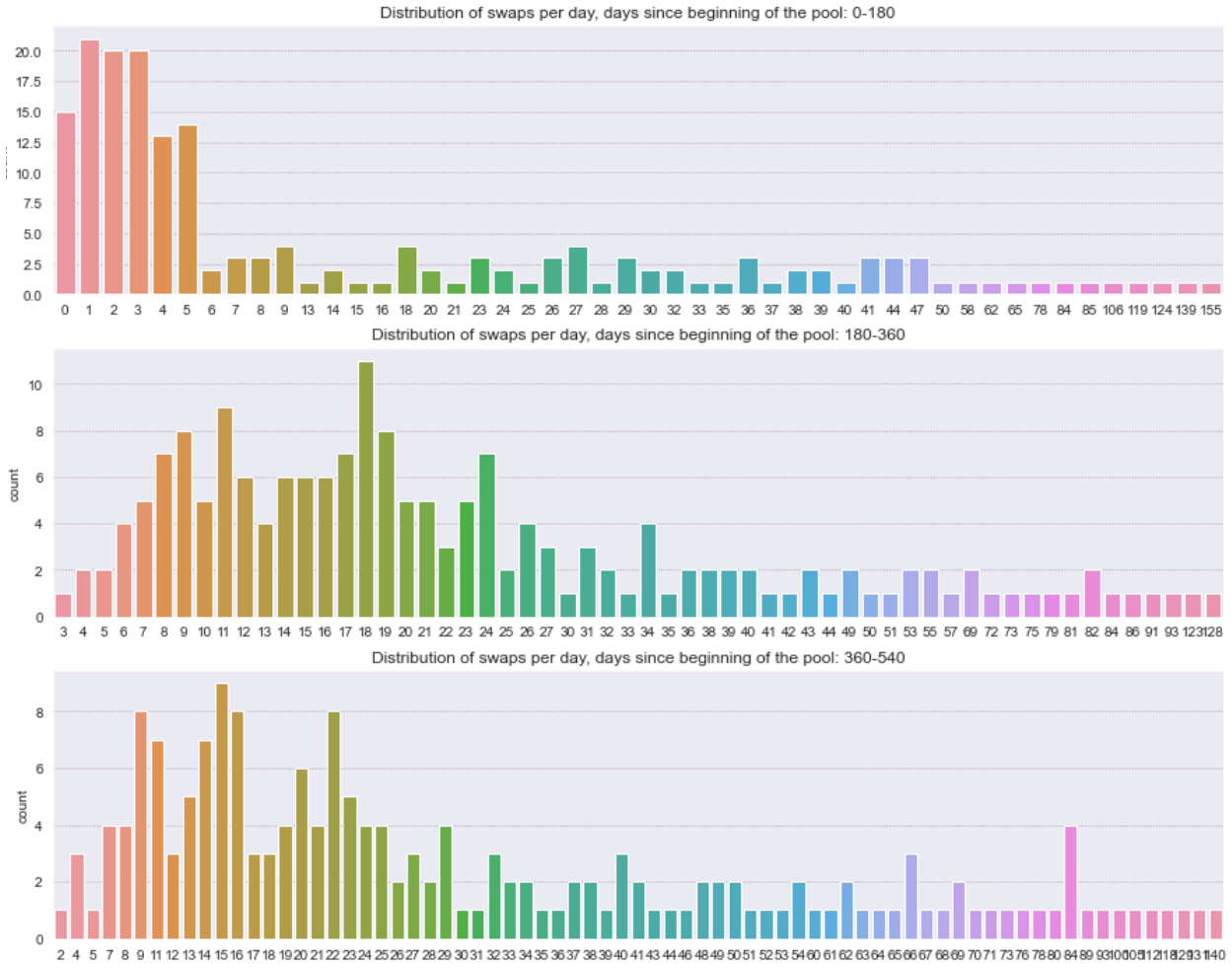
Picture X: count of swaps per hour

The count for x = 0 (no swaps per hour), shows how many missing windows for TWAP value exist. It can be seen that in the first period since creation, the highest number of missing TWAP values was registered (almost 3000).



Picture 167: swaps per hour distributions

Below, the distribution of the number of swaps per 24 hours is shown, similarly for the 3 stages in pool development.



Picture 168: swaps per day count distributions

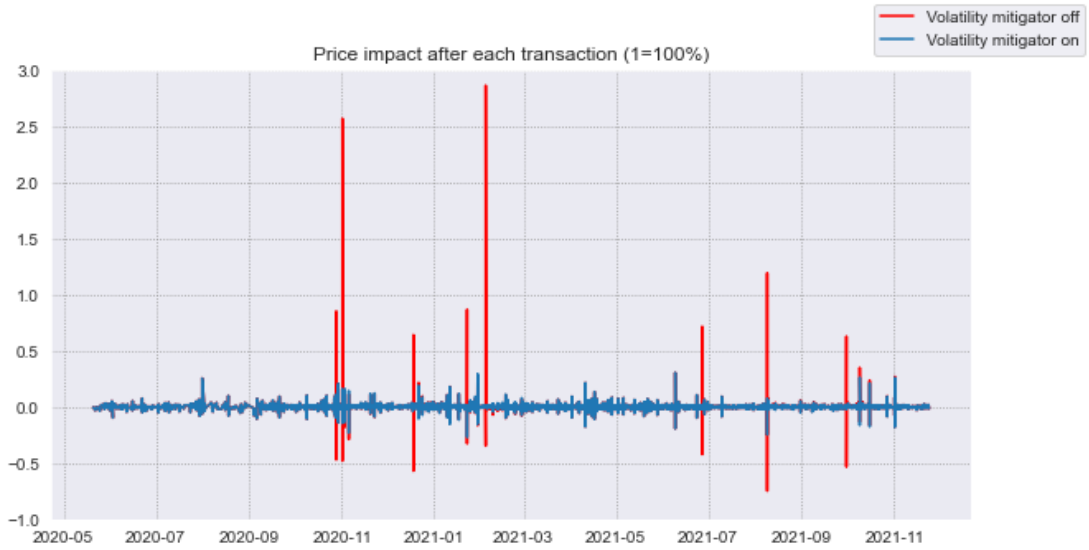
It can be seen that in the second and last stage, there were no days with no swaps happening, the least number of swaps per day being 3 and 2 accordingly.

If the volatility mitigator mechanism would consider an older recorded cumulative price for computing the TWAP value, in case the one that happened exactly 24 hours ago (in the period_size window) would be missing, it would allow to perform the volatility mitigator check for each swap in the 2nd and 3rd stage of the pool development.

A modification was decided to be introduced in the pool: in case the cumulative price in the buffer for 24 hours ago index is not available, to take the oldest value from the buffer, which is not older than 48 hours ago (this number can be tweaked later). By introducing this modification in the simulator, the following plot for variation of X price across time is obtained:

Picture 169: price distribution over time with enabled/disabled mitigation mechanism, with 48 hour fallback_window_size

It can be seen that now almost all of the instantaneous price drops and increases are avoided. The price variation over time is much more smooth.



Picture X: price deviation distribution in percents

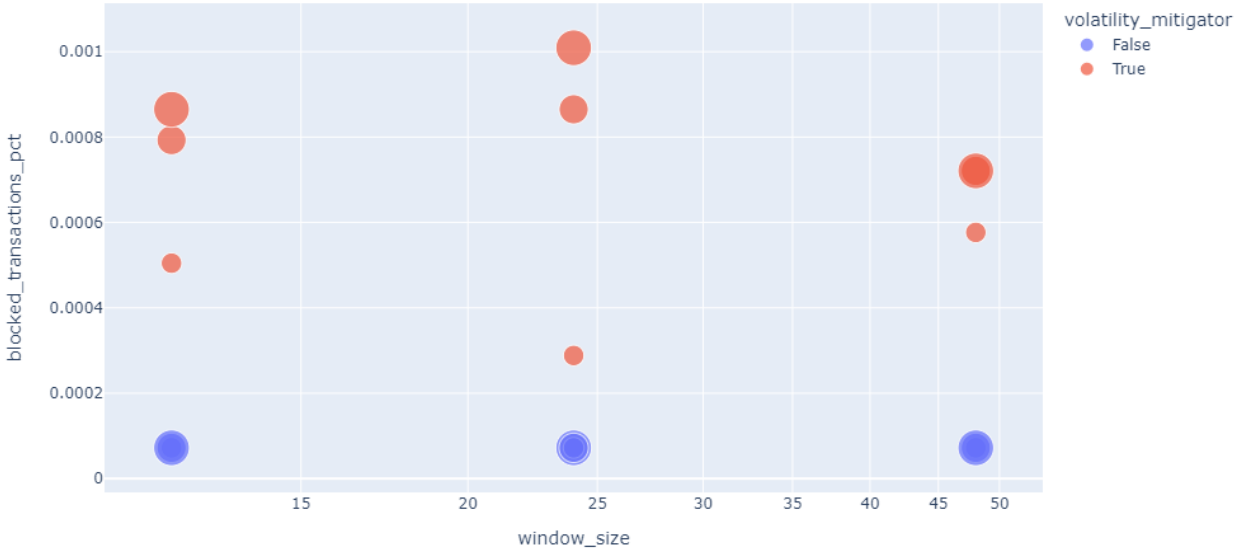
All of the swaps with a significant price impact are blocked by the volatility mitigation mechanism.

Simulations results for distinct VM related parameters

Below are analyzed the simulation results with different volatility mitigator related parameters set.

Examined parameters:

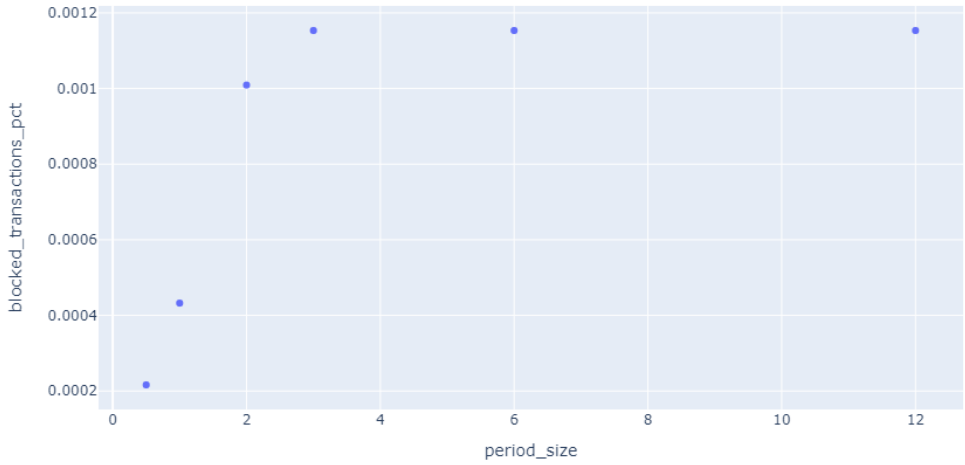
- `window_size: [12, 24, 48]`
- `period_size: [1, 3, 6]`
- `Units: hours`



Picture 170: correlation between blocked transactions, window sizes and volatility mitigation mechanisms

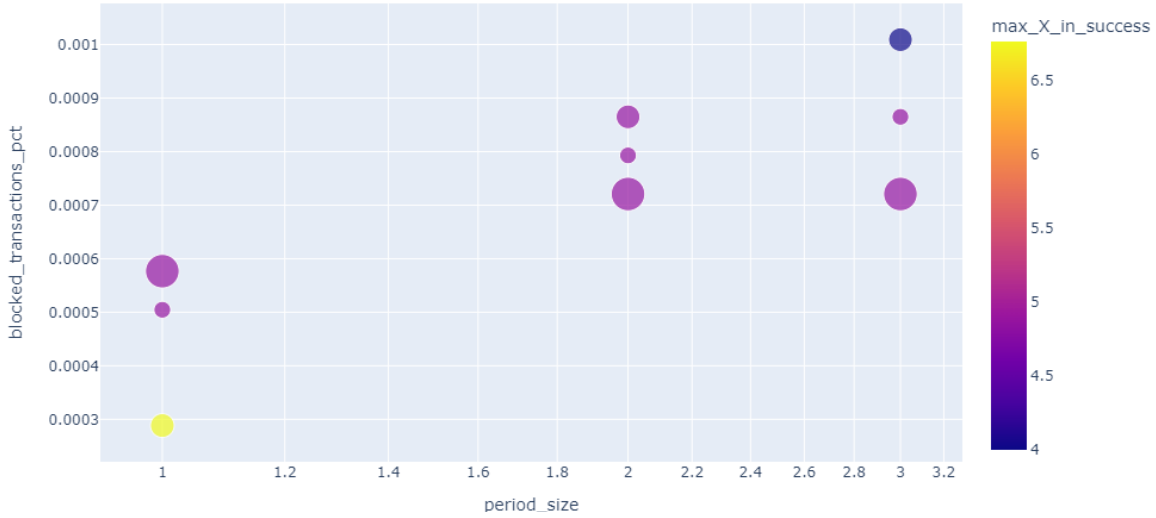
On the **x** axis is set up the window size and on the y - percentage of totally blocked transactions. Each point represents a simulation with different parameters. The size represents period_size.

It can be observed to be consistent behavior for all simulations with a fixed window_size value - the bigger the period_size - the more transactions are blocked.



Picture 171: period size correlation with blocked transactions in the WBTC/DAI pool history, `window_size` = 24h and enabled volatility mitigation

The number of blocked transactions increases as the period_size is being increased. This happens because of 2 reasons - the TWAP price is more up-to-date as the period number increases, and in law frequency pools there will be less windows of missing TWAP values, therefore the volatility mitigator check would be performed more often.

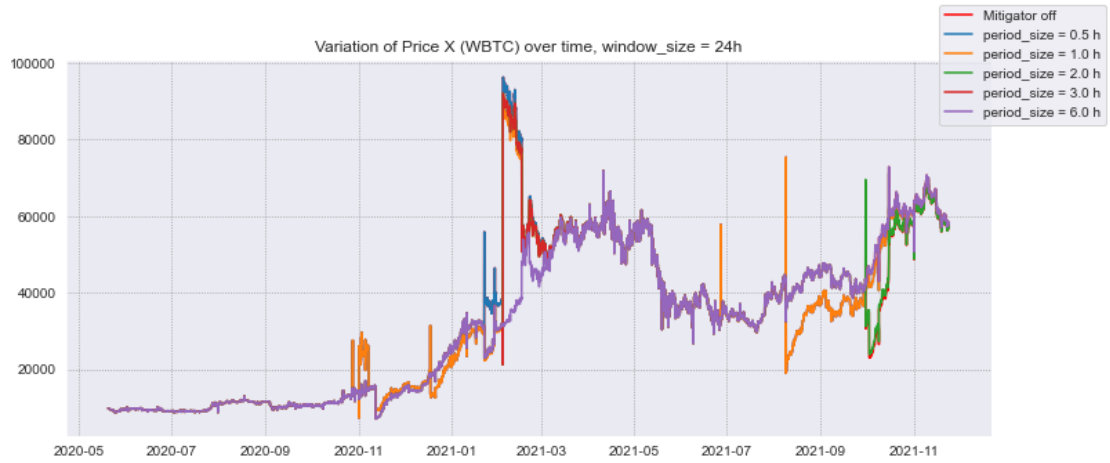


Picture 172: period size correlation with blocked transactions

In the above plot the maximal swap_in value in X token (WBTC) of a successful transaction is represented by color, and the size - window_size. The more transactions are blocked - the less is the maximal swap_in value.

Window size set to 24h

Comparison of price variations, for **different period_size** values, **window size = 24h**:



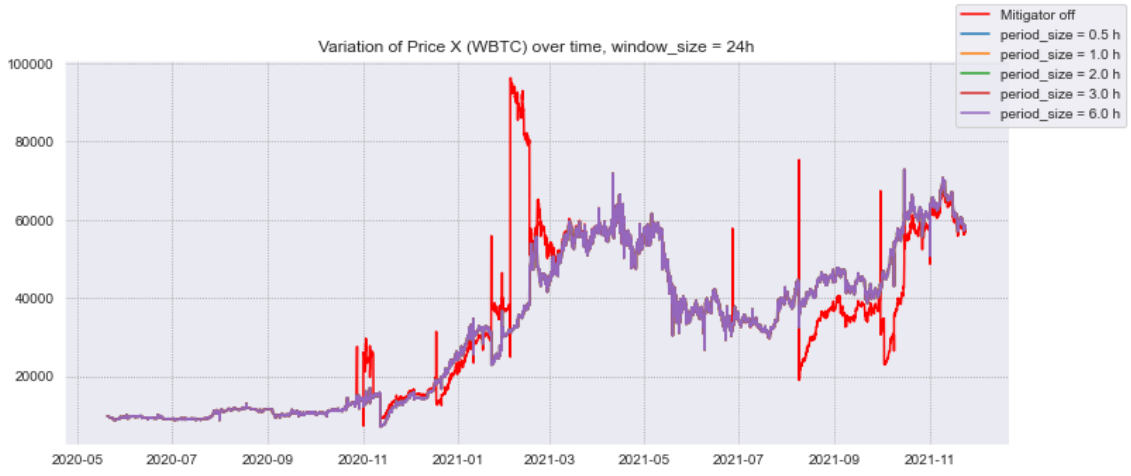
Picture 173: WBTC token price variation with different parameters

It can be seen that the price is much less volatile for bigger period_size values. With bigger period size there will be less missing TWAP windows and more blocked transactions:

period_size (h)	No TWAP available ratio	Swaps blocked by volatility mitigator
0.5	0.539	2
1.0	0.339	3
2.0	0.174	11
3.0	0.096	13
6.0	0.032	15

Picture 174: table of period sizes, TWAP ratios and amount of blocked transactions

If the volatility mitigator would use a more recent cumulative price for computing TWAP value in case the one exactly window_size hours ago would be missing, the presented below results would be obtained.



Picture 175: Variation of price for a slightly modified way of computing TWAP (in case the cumulative price for `window_size` hours is missing, but there were swaps in-between, a more recent observation is used for computing TWAP value), `window_size` = 24h.

It can be seen that the number of blocked transactions becomes the same for all distinct period_size parameters, and the number of no_twap_available windows decreases significantly, being relatively equal across simulations with different period_size parameter values.

period_size (h)	No TWAP available ratio	Swaps blocked by volatility mitigator
0.5	0.00022	15
1.0	0.00029	15
2.0	0.00029	15
3.0	0.00036	15
6.0	0.00050	15
12.0	0.00065	15

Picture 176: table of period sizes, TWAP ratio and amount of blocked transactions

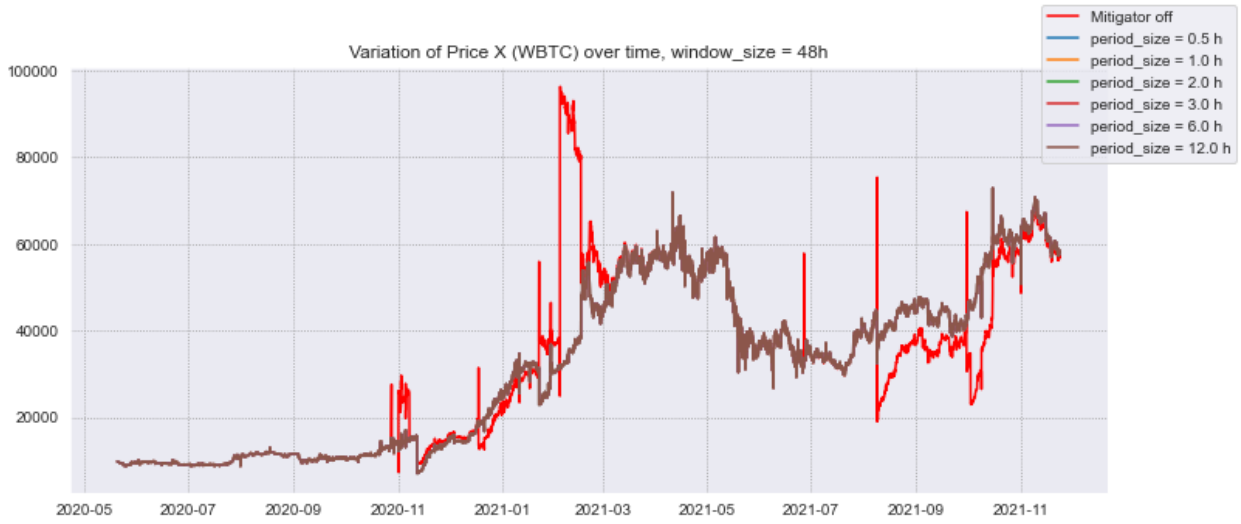
Window size set to 48h

Picture 177: Variation of price for distinct `period_size` parameters and `window_size` = 48h

period_size (h)	No TWAP available ratio	Swaps blocked by volatility mitigator
0.5	0.55655	6
1.0	0.36092	7
2.0	0.18777	9
3.0	0.11403	9
6.0	0.03049	13
12.0	0.00865	15
24.0	0.00303	15

Picture 178. Distinct stats for simulations with different `period_size` parameters and `window_size` = 48

It can be observed that for smaller period_size values, there is a larger number of blocked swap transactions



Picture 179: Variation of price for a slightly modified way of computing TWAP (in case the cumulative price for `window_size` hours is missing, but there were swaps in-between, a more recent observation is used for computing TWAP value), `window_size`=48h.

WBTC/USDC

This is a pool with a medium frequency of transactions and capitalization value (across pools with popular tokens). At the moment of the analysis the total locked liquidity inside the pool was **2 082 244$**, the median of the swaps count per day across the entire history being 71 and mean 122.

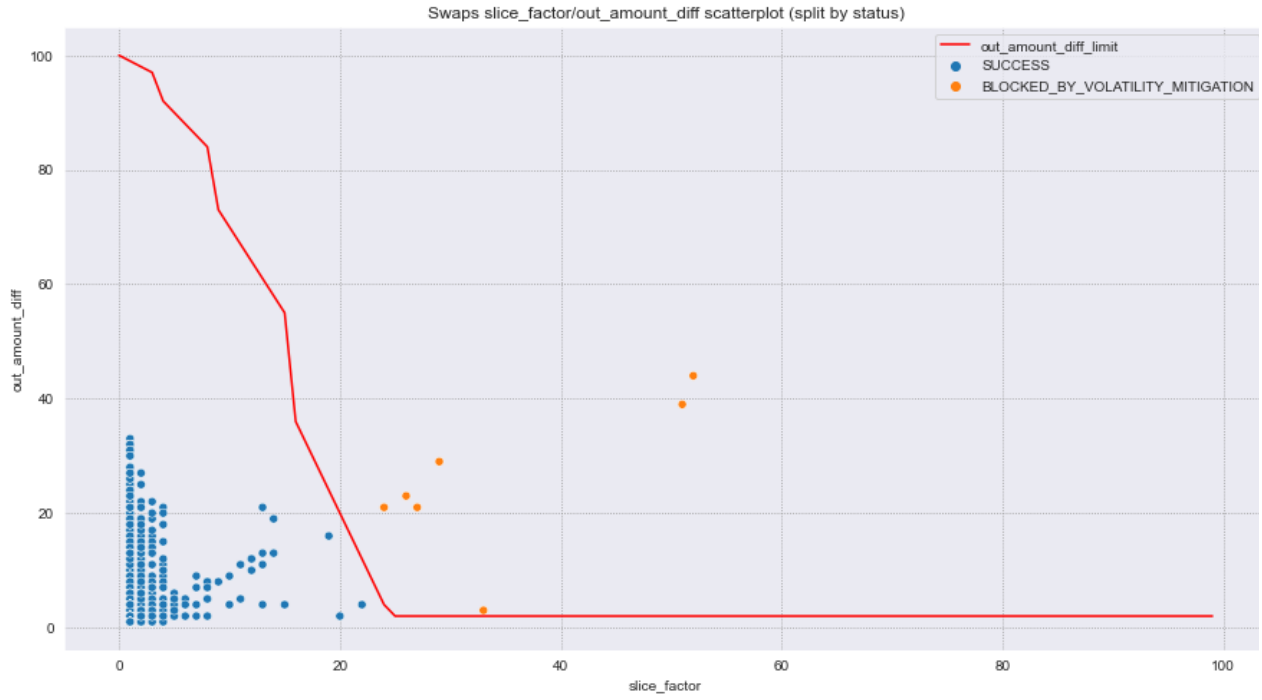
Historical stats:

- 68 197 swaps
- 632 mints
- 479 burns

A more detailed overview of the pool can be found here. The volatility mitigation mechanism blocked **only 3 out of 68 197** transactions. In about **4%** of the cases the volatility mitigation mechanism didn't check the transaction because of the missing observations in the DSW oracle. By adding the above discussed modification in the dsw oracle, this number has been reduced to **0.02%** and the total number of **blocked** transactions was **increased by 3.**

	token_in	token_out	token_in_amount	token_out_amount	slice_factor	out_amount_diff	reserve_Y_before	reserve_Y_before	transaction_timestamp
66	USDC	WBTC	31.840000	0.002410	24.0	21.0	1.368994e+02	1.368994e+02	2020-09-21 13:57:04
67	WBTC	USDC	0.003264	27.465270	26.0	23.0	1.368994e+02	1.368994e+02	2020-09-21 17:16:17
65608	WBTC	USDC	12.689636	415967.276382	29.0	29.0	1.888431e+06	1.888431e+06	2021-09-27 20:58:07
65610	USDC	WBTC	976323.861321	14.888663	51.0	39.0	1.901177e+06	1.901177e+06	2021-09-27 20:58:07
66006	USDC	WBTC	557057.298176	12.276771	33.0	3.0	1.706340e+06	1.706340e+06	2021-10-05 09:00:00
67843	WBTC	USDC	15.779159	644823.761426	52.0	44.0	1.905848e+06	1.905848e+06	2021-11-16 03:28:33
67844	USDC	WBTC	515070.490141	6.448343	27.0	21.0	1.905848e+06	1.905848e+06	2021-11-16 03:28:33

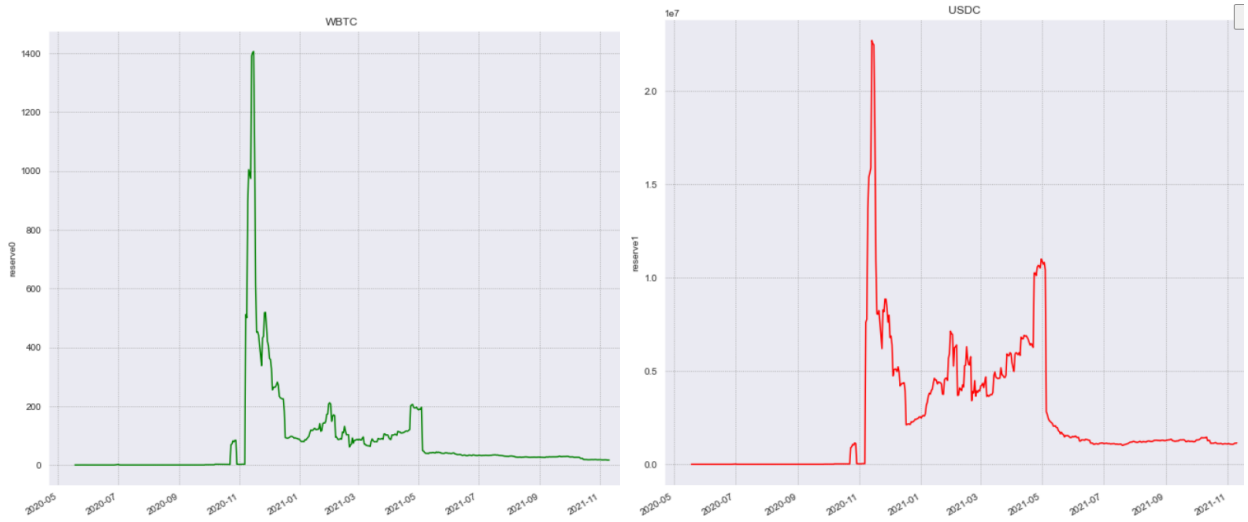
Picture X: Swaps blocked by volatility mitigator transactions, with fallback_window_size = 48h



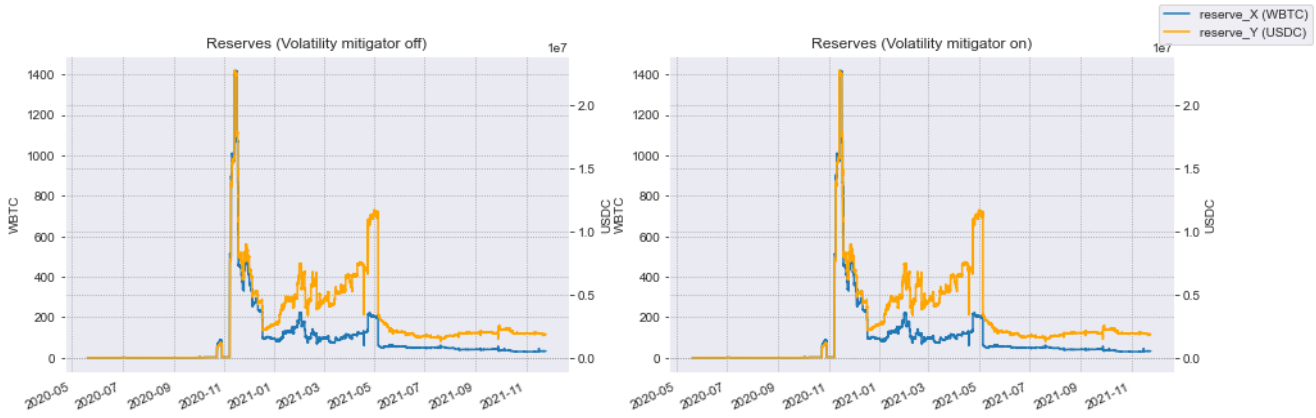
Picture X: Swaps slice_factor/out_amount_diff scatter plot, split by status (with visualization of the out_amount_diff_limit), (fallback_window_size = 48h)

Overall, the border seems to separate the successful and blocked transactions pretty well, and the slice_factor_curve formula doesn't seem to require additional adjustments. There can be observed one swap, which would have been accepted if the price_tollerance_threshold would be a little bit higher.

The distribution of the simulation-based reserves is identical to the real ones that were present in the WBTC/USDC pool.

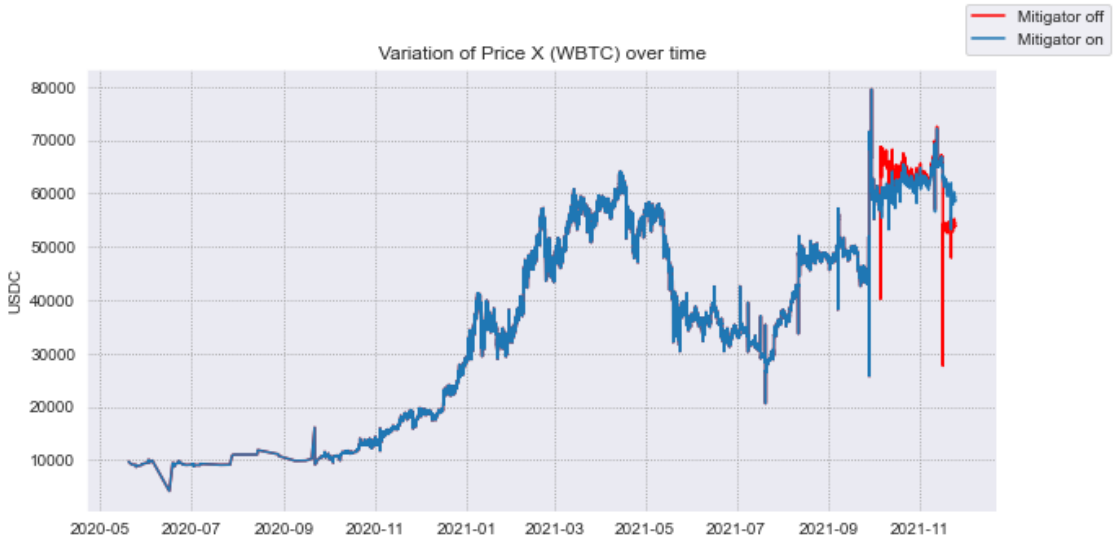


Picture 157: Historical pool reserves variation over time in the real WBTC/USDC pool

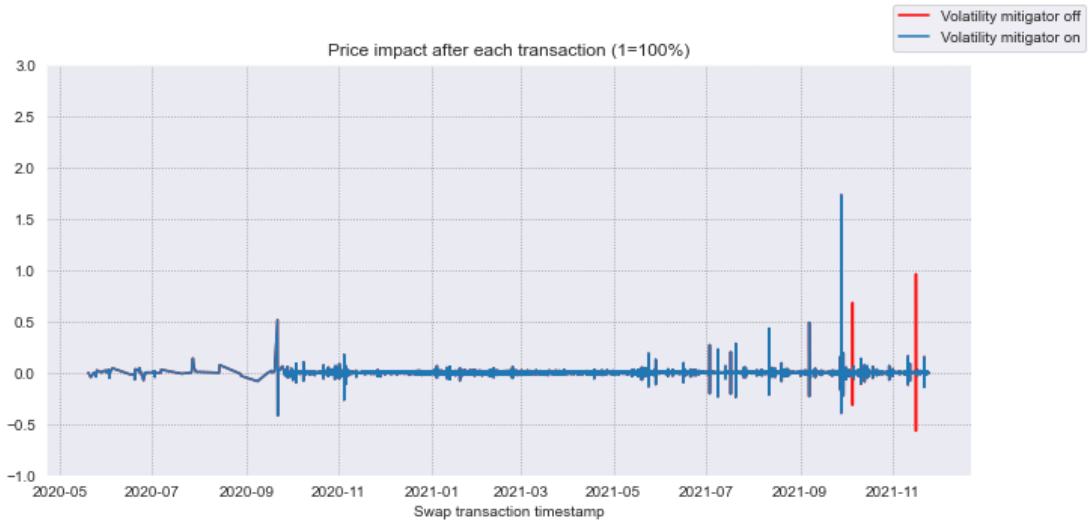


Picture 158: reserves variation over time with with enabled/disabled volatility mitigation mechanism, without fallback_window_size

The reserves of the pool visually vary almost identically in the 2 distinct regimes. In the modification with added fallback_window_size, the reserves variation is also similar.



Picture 169: price distribution over time with enabled/disabled mitigation mechanism, without fallback_window_size



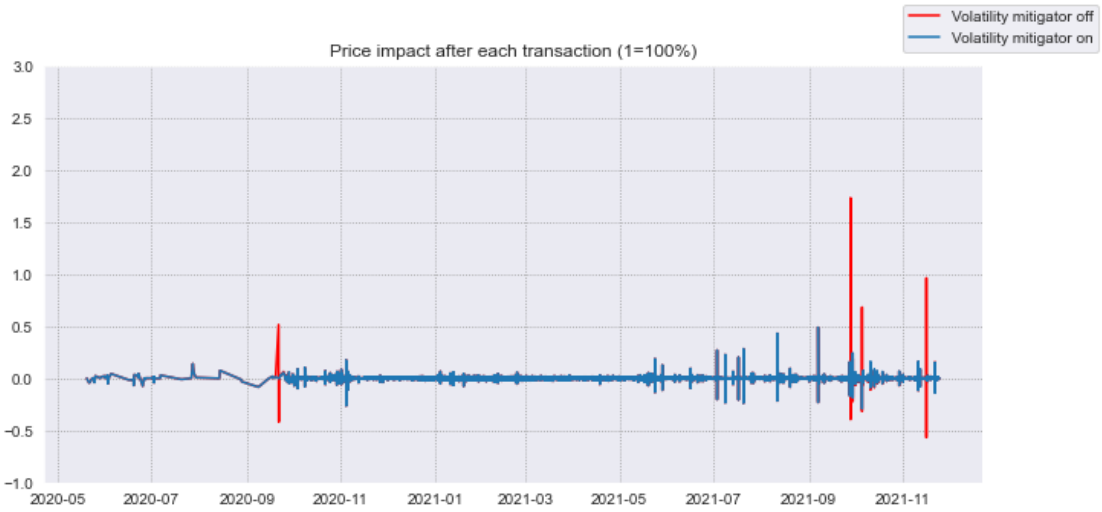
Picture 169: price impact after each transaction enabled/disabled mitigation mechanism, without fallback_window_size

It can be seen from the variation of price that the volatility mitigation mechanism slightly decreases the price variation in several cases, toward the end of the plot. It's caused by blocking 2 pairs of transactions, which are MEV-bot sandwich attacks. The swap with the highest price impact hasn't been blocked because of the missing observations inside the oracle:

	token_in	token_out	token_in_amount	token_out_amount	mitigator_check_status	reserve_Y_before	reserve_Y_before	price_impact	status
66	USDC	WBTC	31.840000	0.002410	CANT_CONSULT_ORACLE	1.368994e+02	1.368994e+02	0.515241	SUCCESS
62586	USDC	WBTC	321079.590468	7.790564	CHECKED	1.622870e+06	1.622870e+06	0.431521	SUCCESS
64256	USDC	WBTC	391863.363760	8.328070	CHECKED	1.764882e+06	1.764882e+06	0.489570	SUCCESS
65610	USDC	WBTC	976323.861321	22.356863	CANT_CONSULT_ORACLE	1.483546e+06	1.483546e+06	1.734041	SUCCESS

Picture 169: transactions with the highest price impact, without fallback_window_size = 48h

Picture 169: price distribution over time with enabled/disabled mitigation mechanism, with fallback_window_size = 48h



Picture 169: price distribution over time with enabled/disabled mitigation mechanism, with fallback_window_size = 48h

Adding the modification inside the dsw oracle with fallback_windwo_size = 48h, solves the issue with missing observations, and there remain less sudden price increases/decreases.

However, it can be observed that there still remain several swap pairs with a price impact near 50%, most of them being MEV-bot sandwich attacks.

	token_in	token_out	token_in_amount	token_out_amount	mitigator_check_status	reserve_Y_before	reserve_Y_before	price_impact	status
62586	USDC	WBTC	321079.590468	7.790564	CHECKED	1.622870e+06	1.622870e+06	0.431521	SUCCESS
64256	USDC	WBTC	391863.363760	8.328070	CHECKED	1.764882e+06	1.764882e+06	0.489570	SUCCESS

Picture 169: transactions with the highest price impact, with fallback_window_size = 48h

WETH / USDC

This is a pool with a high frequency of transactions and capitalization value. At the moment of the analysis the total locked liquidity inside the pool was 227 082 625$, the median of the swaps count per day across the entire history being 5493, mean - 5294.

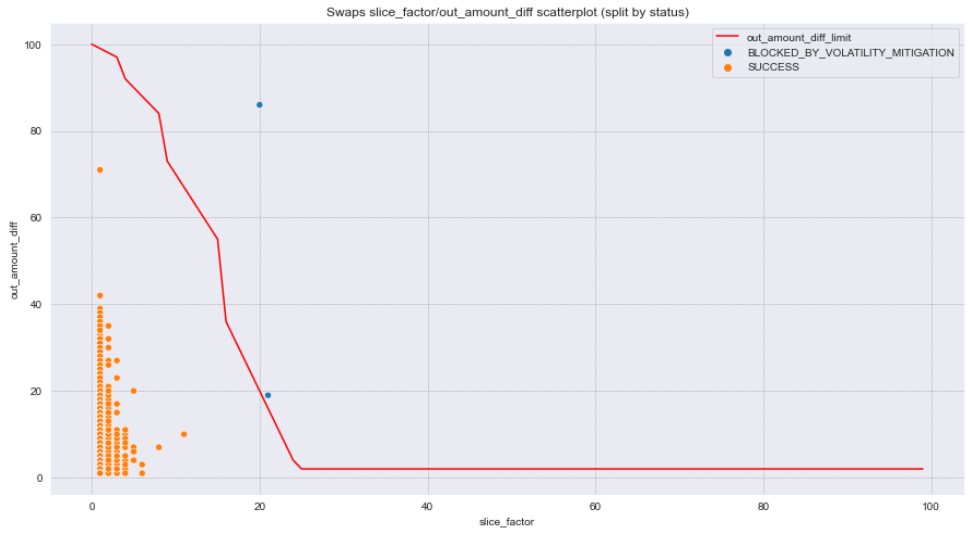
Historical stats:

- 2 895 926 swaps
- 32 940 mints
- 23 363 burns

A more detailed overview of the pool can be found here. After running the historical transactions from this pool through the synthetic AMM with the volatility mitigation mechanism enabled, only **2 out of 2 895 926** total swap-transactions have been **blocked**. For **0.008%** of the swaps, the volatility mitigation mechanism didn't check the transaction because of the missing priceCummulative observation inside the DSW oracle. All of these cases were during the initial phase since pool creation, when the reserves and the transactions frequency were low. Below, is presented a table containing the information about each blocked transaction.

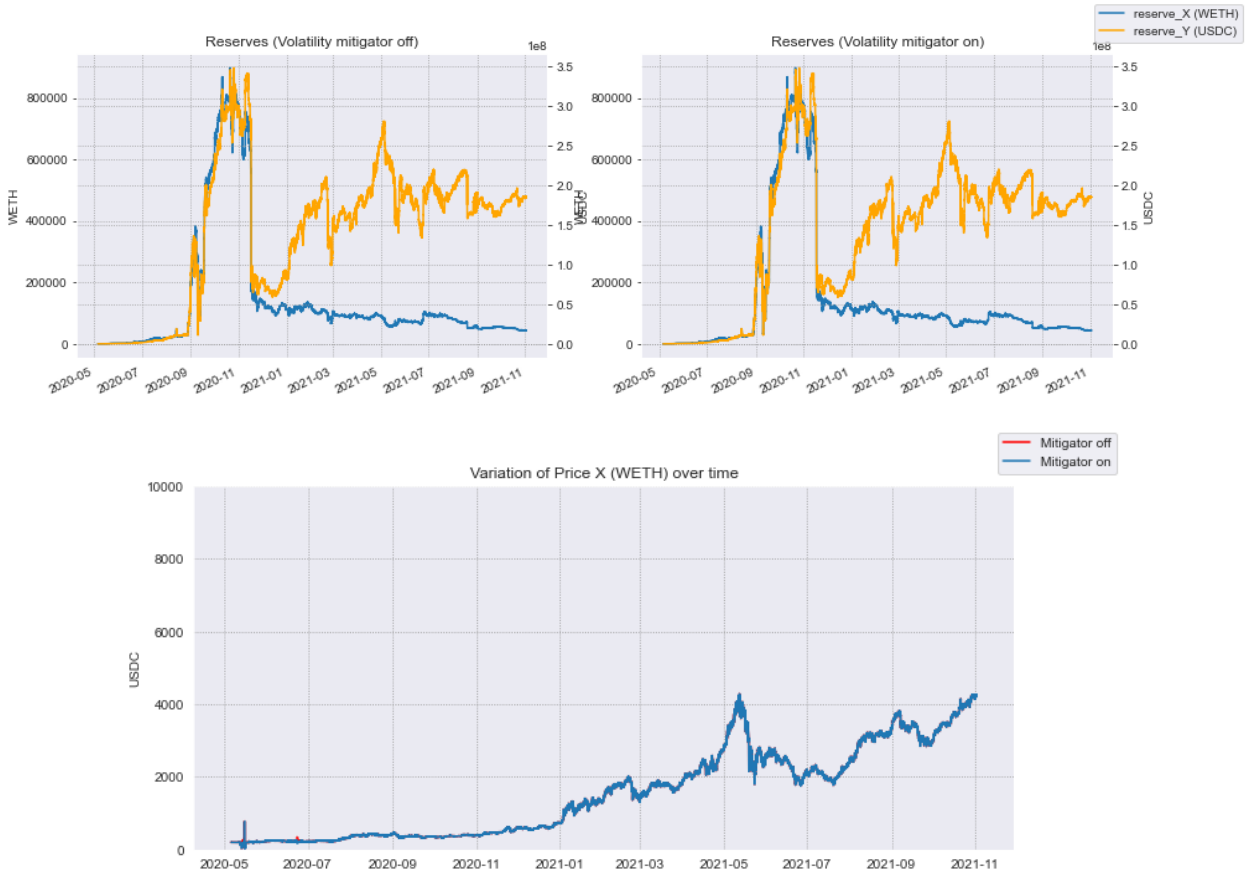
token_in	token_out	token_in_amount	token_out_amount	slice_factor	out_amount_diff	reserve_Y_before	reserve_Y_before	transaction_timestamp
USDC	WETH	3.5	0.018075	20.0	86.0	1.780154e+01	1.780154e+01	2020-05-13 22:25:22
USDC	WETH	296400.0	1024.751691	21.0	19.0	1.460402e+06	1.460402e+06	2020-06-23 02:42:56

Note that both transactions that were blocked happened during the **first 2 months since pool creation**, when the reserves were not yet so high as now.

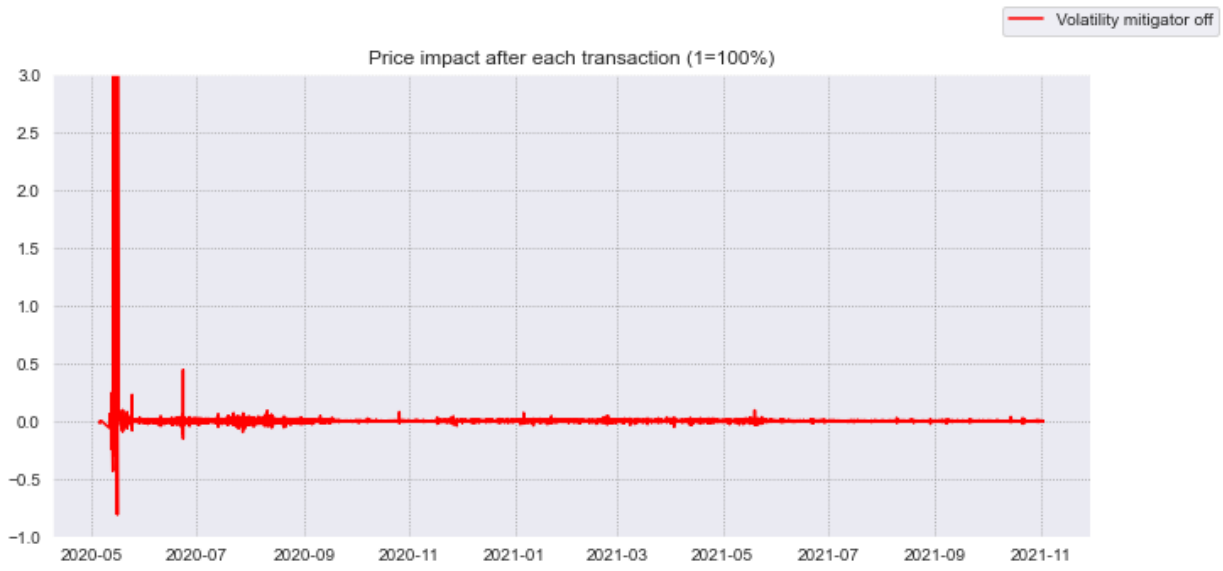


Picture 182: Distribution of difference with the price from DSW oracle, separated by status

Because of the high locked liquidity, it requires an extremely high financial power to execute a swap with a large slice_factor. It can be seen that for almost all of the swaps, the slice_factor is much smaller, compared to the previously analyzed pools.



The variation of price resembles the real exchange rate of ETH / USDC.



It can be noticed that only during the initial period there exist transactions with a significant price impact. Once the reserve inside the pool grew, no peculiar transactions that would suddenly deviate the price were registered.

Note: In the following sections, if not specified explicitly otherwise, the plots represent simulation results after applying the discussed change inside the DSW oracle

BPT / WETH (STO)

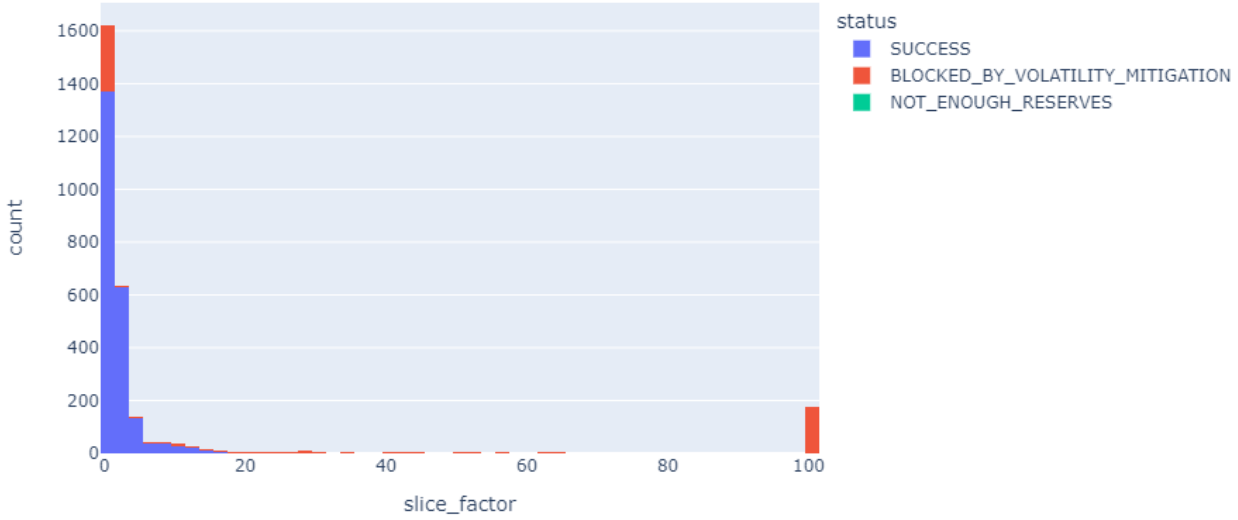
This is a pool which at the moment of analysis had only **72$** locked liquidity. The **maximum amount** of locked liquidity equal to **72 539$** was registered at 2020-06-19. After that, as a result of numerous huge consecutive transactions BPT -> ETH, the majority of Ether was withdrawn from the pool, and in the following months the activity inside the pool decreased to almost 0. The median number of swaps per day across the entire pool history is 0, mean - 6.56

Historical stats:

- 42 mints
- 18 burns

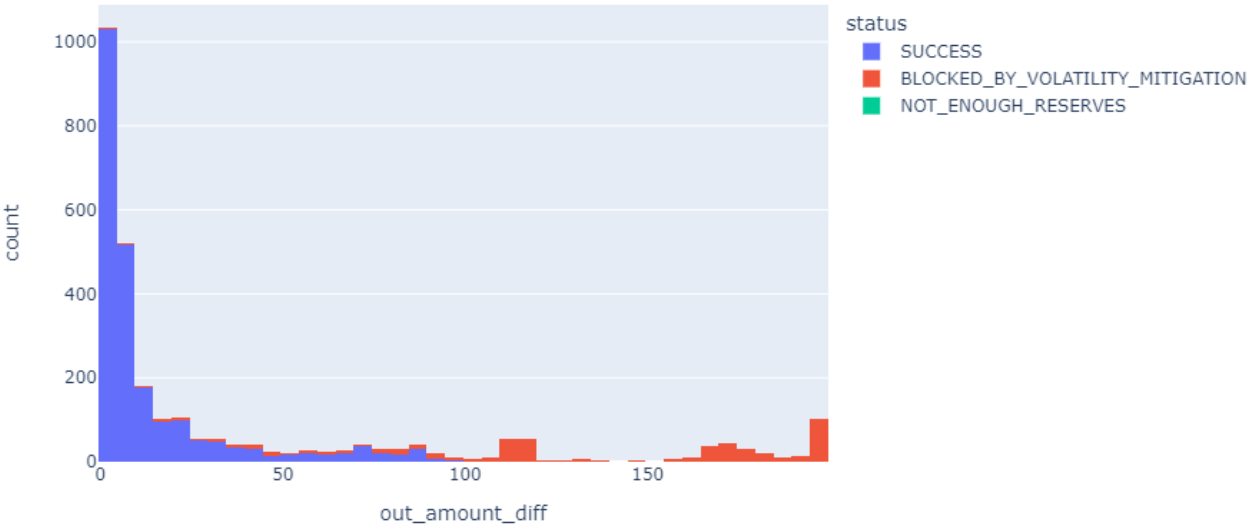
A more detailed overview of the pool can be found here. The volatility mitigation mechanism blocked **611 out of 3 155** transactions, which is much more than in the previously analyzed pools. In about **31%** of the cases the volatility mitigation mechanism didn't check the transaction because of the missing observations in the DSW Oracle. By adding the above discussed modification in the dsw oracle, this number has been reduced to **0.008%**. At the same

time, after that, 564 transactions have been blocked by the volatility mitigation mechanism and 19 transactions because of insufficient reserves to perform the swap.



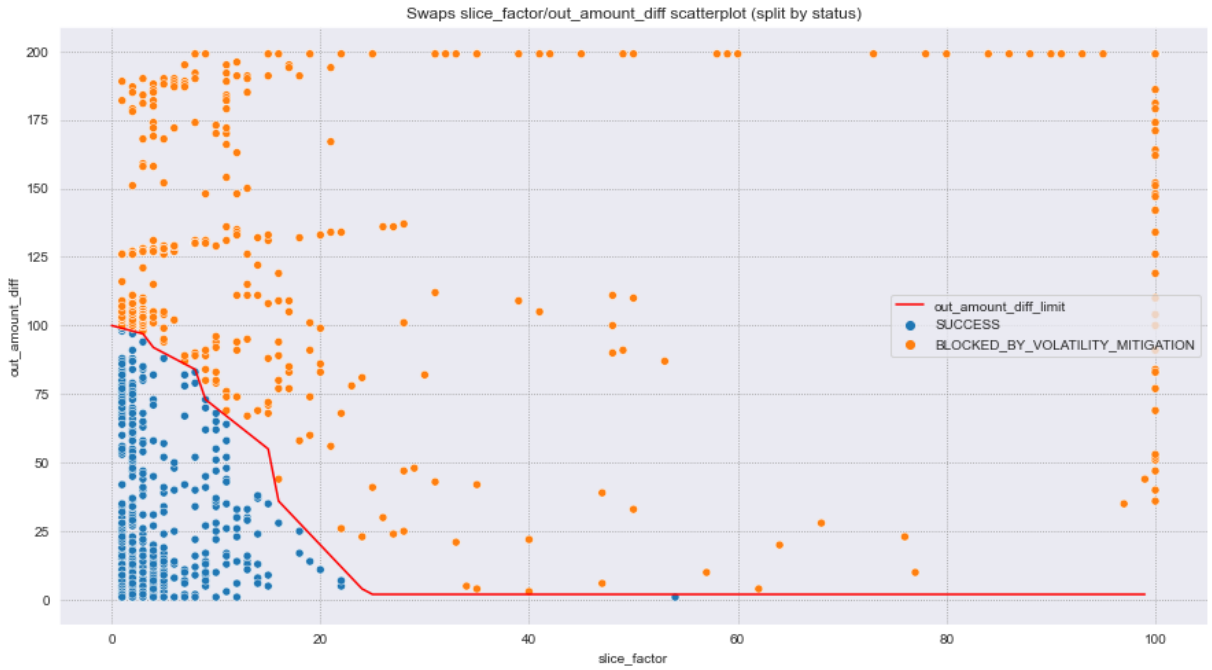
Picture X: Slice factor distribution, split by transaction status

It can be observed that there is a high number of blocked transactions, with a slice_factor near zero, which is not typical for an usual pool. The reason for this strange pattern is described below.



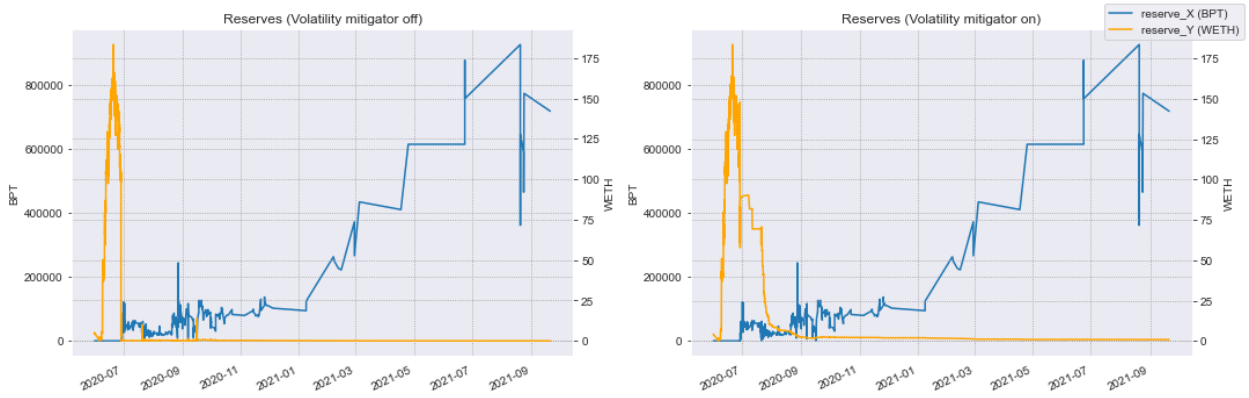
Picture X: percentage difference of amount out with oracle based amount out, histogram

The distribution of out_amount_diff indicates that there is a huge number of blocked transactions with a price difference from the oracle one by more than 100%.



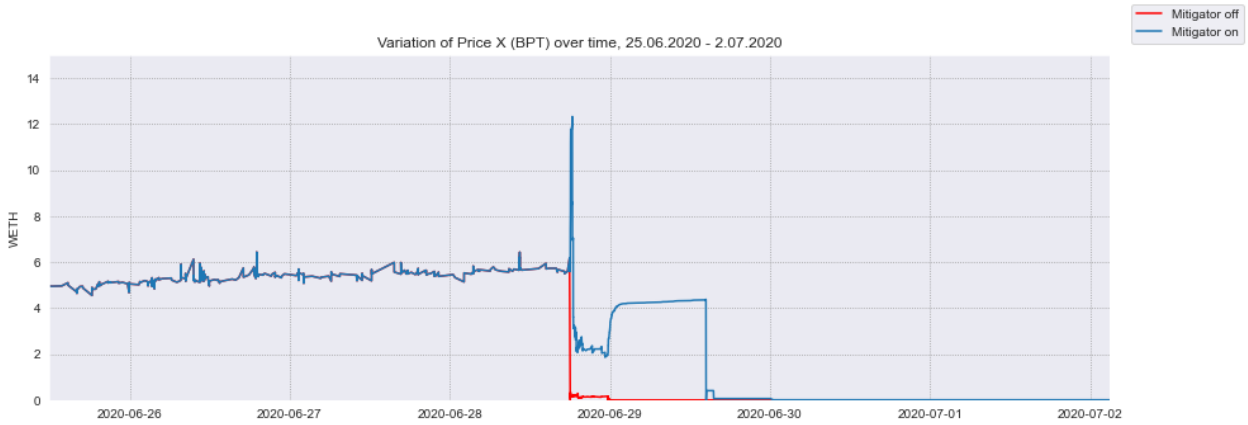
Picture X: Swaps slice_factor / out_amount_diff scatterplot (split by status)

The successful and blocked transactions are dispersed and not separated clearly by the out_amount_diff_limit, as in the previous cases.



Picture X: reserves distributions with and without mitigation

With the volatility mitigation mechanism disabled, it can be seen that all of the reserves of WETH are depleted all at once. The volatility mitigation mechanism allowed sustaining the reserves at relatively high levels for several months more, after a sudden ~50% drop.



It was decided to analyze the swaps happening near 2020.07 more thoroughly. On 28.06.2020, a series of **huge swaps BPT -> WETH were blocked** by the volatility mitigation mechanism, as a result of which the price of BPT suddenly increased (but decreased to almost 0 with volatility mitigation disabled). After the sudden price increase, some of the huge transactions were allowed to pass (as the price from oracle was lower than the current price), leading to a price decrease till about 2 ETH per BPT. The biggest price decrease from **4 ETH per BPT** till **0.06 ETH per BPT** happened as a result of several large **mints**, in which the proportion of the tokens didn't correspond to the one at the moment (because the volatility mitigation mechanism blocked a lot of transactions, the price of BPT was much higher)

These mints led to a sequence of **290 consecutively blocked transactions** during a **6 hours** period. As a result, there is a chain of 290 consecutively blocked transactions happening, which is the main reason for the large amount of swaps blocked with a small slice_factor.

mAAPL / UST (STO)

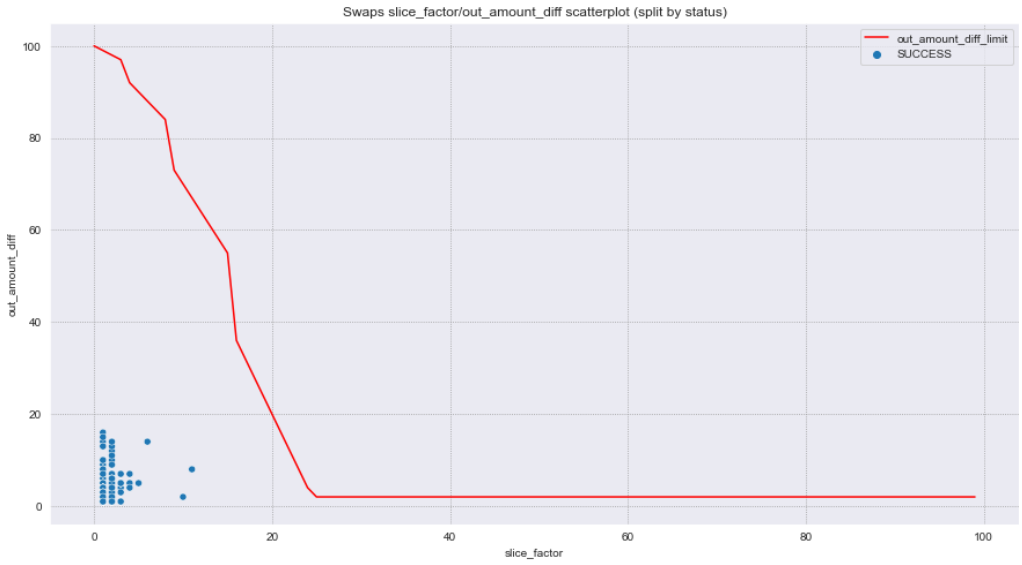
Pool mAAPL / UST has high reserve values (at the moment of analysis tokens equivalent of 7 434 365$ were locked in the pool) and low transaction frequency (the median number of transactions per day is 4, mean - 5. During the analysis of the pool, no strange behaviour was identified.

Historical stats:

- Total swaps: 2 117
- Total mints: 515
- Total burns: 273
- Initial liquidity (first day): $1.4 mln
- Min liquidity: $1.4 mln

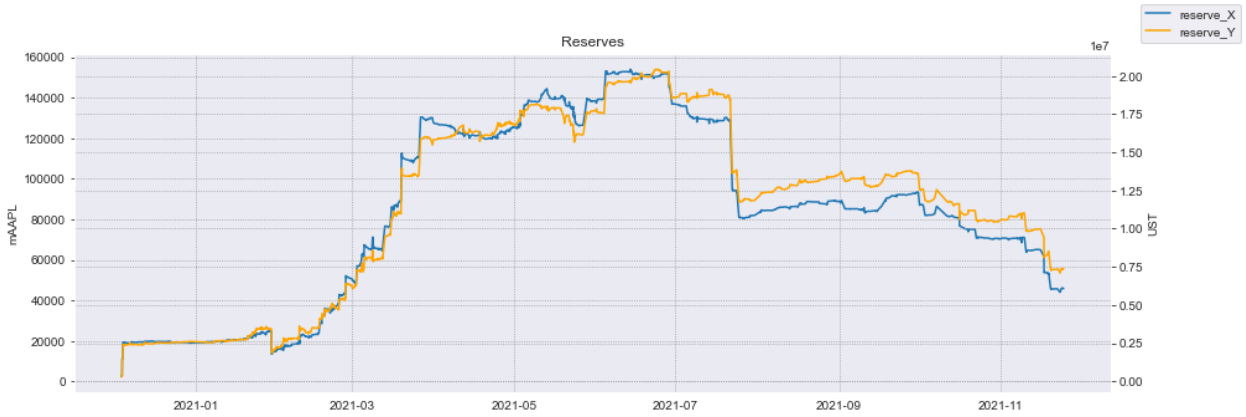
- Maximal liquidity: $20.5 mln
- Most recent liquidity: $7.43 mln
- Median swaps per day: 4
- Mean swaps per day: 5

A more detailed overview of the pool can be found here. The volatility mitigation mechanism didn't block any transaction from this pool. Before the change applied inside the DSW oracle for **77%** of the cases TWAP couldn't be computed, after that, the number has been reduced to **0.4%**.



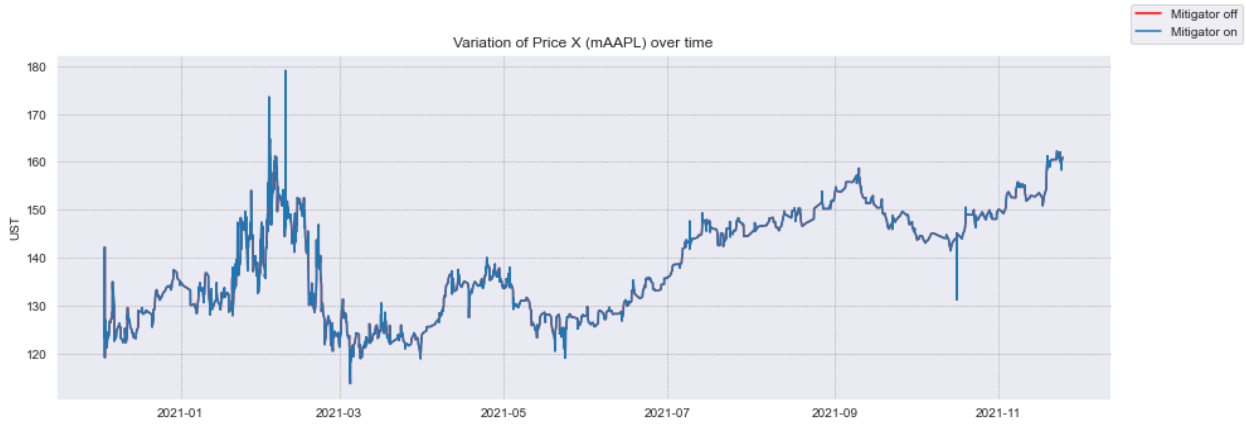
Picture X: Swaps slice_factor / out_amount_diff scatterplot (split by status)

As the reserves of the pool are high and the price of mAAPL sec token didn't experience any instant increases/drops, almost all of the swaps fell in the lower-left corner of the plot, having a small slice_factor and a small price difference from the oracle one.



Picture 158: reserves variation over time with volatility mitigation mechanism disabled/enabled

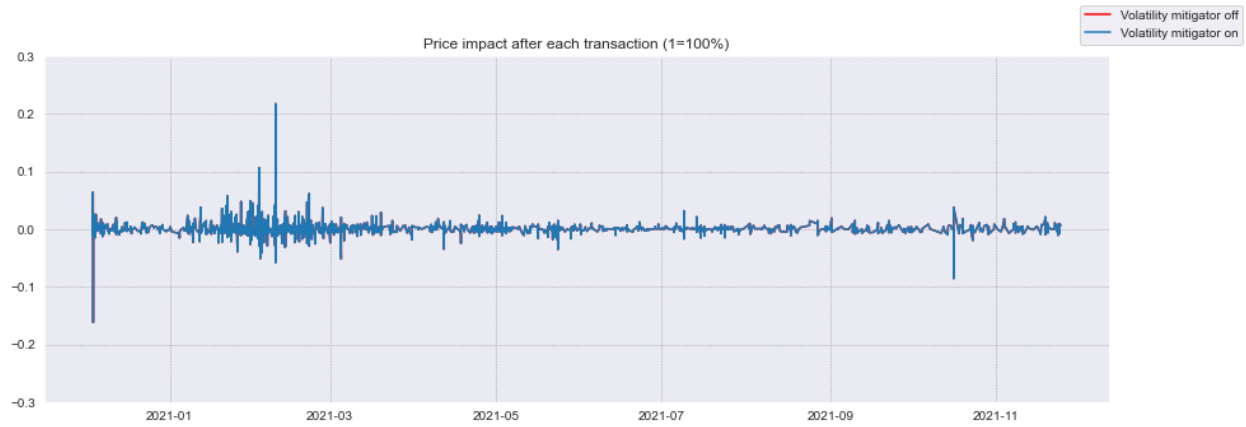
The reserves vary similarly to the real values obtained from the Uniswap subgraph and described in the pool-analysis section. As no transactions have been blocked, the plot is the same for both 2 regimes (with VM disabled/enabled).



Picture X: variation of price over time

The overall trend of the price shows a slight increase from the beginning of the year. A sudden price decrease/increase can be observed toward the end of the plot, which is caused by a large transaction mAAPL to UST. However, the following 3 transactions in the opposite direction restored the price to the initial value.

	token_in	token_in_amount	token_out_amount	out_amount_diff	slice_factor	reserve_Y_before	reserve_Y_before	transaction_timestamp	X_price
2028	mAAPL	113.991059	16235.929193	NaN	NaN	1.162036e+07	1.162036e+07	2021-10-16 08:18:42	143.666459
2029	mAAPL	3553.094634	483217.805281	5.0	5.0	1.109084e+07	1.109084e+07	2021-10-16 09:32:45	131.305929
2030	UST	200000.000000	1480.292948	6.0	2.0	1.060569e+07	1.060569e+07	2021-10-16 09:32:59	136.269587
2031	UST	150000.000000	1074.977346	2.0	2.0	1.080489e+07	1.080489e+07	2021-10-16 09:37:13	140.052552
2032	UST	199850.638625	1387.636288	NaN	NaN	1.095429e+07	1.095429e+07	2021-10-16 09:39:32	145.172997



Picture X: price impact after each transaction

The transactions with a high price impact are present predominantly during the initial period since pool creation. It's important to note, that at that stage the reserves exceeded $1 mln.

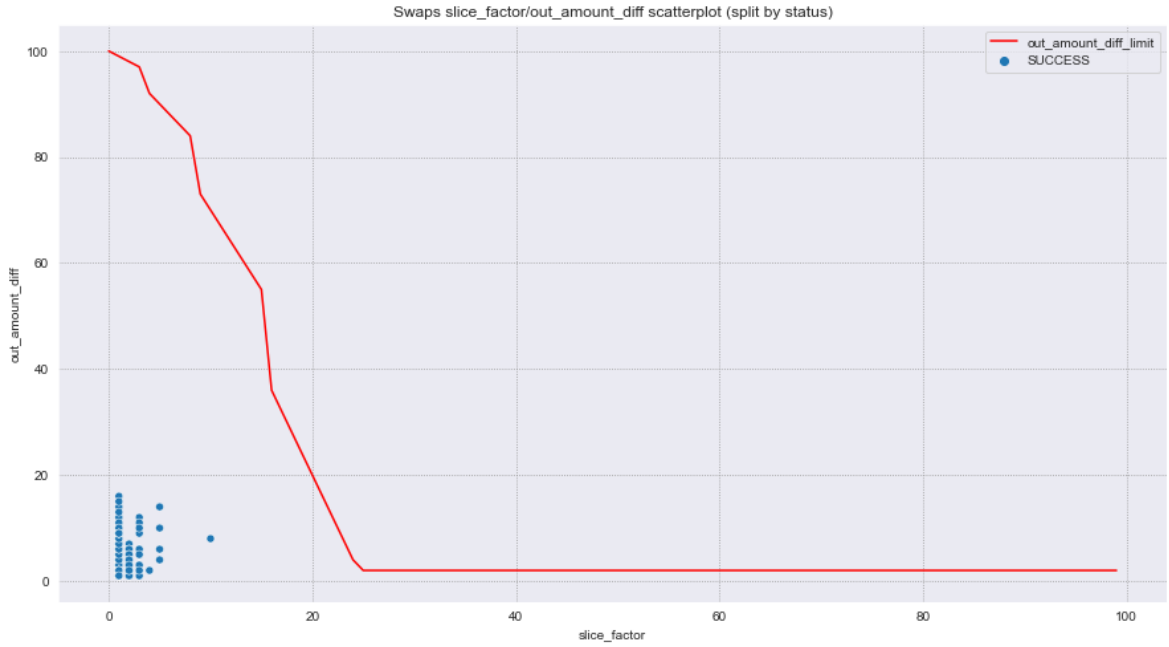
mBABA / UST (STO)

Pool mBABA / UST has high reserve values (at the moment of analysis tokens equivalent of 5 683 297$ were locked inside the pool) and low transaction frequency (the median number of transactions per day is 4, mean - 5.12. During the analysis of the pool, no strange behaviour was identified and the situation is very similar to the pool mAAPL / UST

Historical stats:

- Total swaps: 1 830
- Total mints: 302
- Total burns: 143

A more detailed overview of the pool can be found here. The volatility mitigation mechanism didn't block any transaction from this pool. Before the change applied inside the DSW oracle for **79%** of the cases TWAP couldn't be computed, after that, the number has been reduced to **0.6%**.



Picture X. Swaps slice_factor/out_amount_diff scatterplot (split by status)

Picture X. The price impact after each transaction doesn't exceed 0.25

As no transactions have been blocked, the variation of reserves and price over time with the volatility mitigation mechanism disabled/enabled is the same.

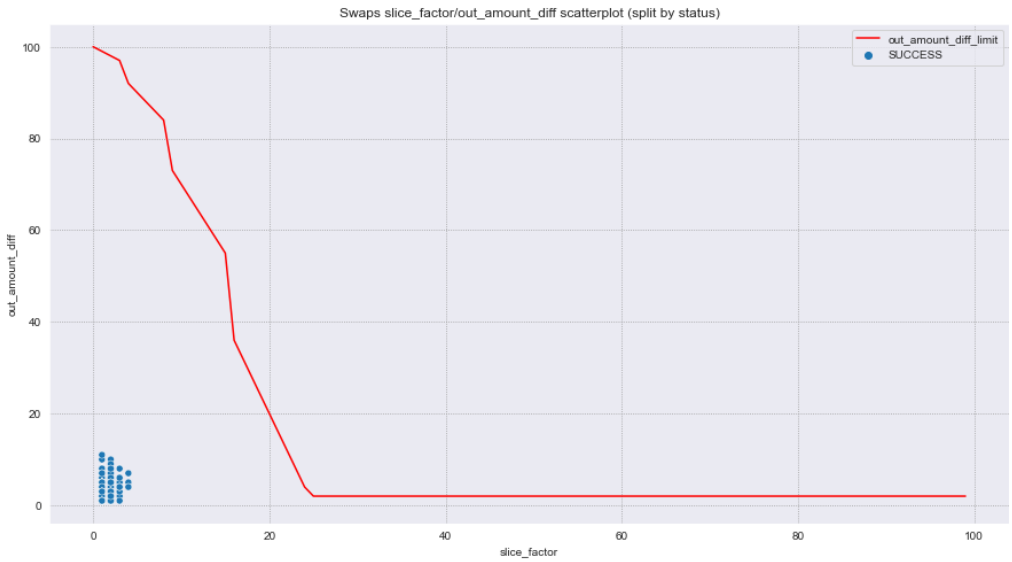
mAMZN / UST (STO)

Historical stats:

- Total swaps:1 626

- Total mints: 375
- Total burns: 214
- Initial liquidity: ~ $1.12 mln
- Maximal liquidity: ~ $39.8 mln
- Liquidity last day: ~ $14.2 mln
- Median swaps per day: 3
- Mean swaps per day: 4.55

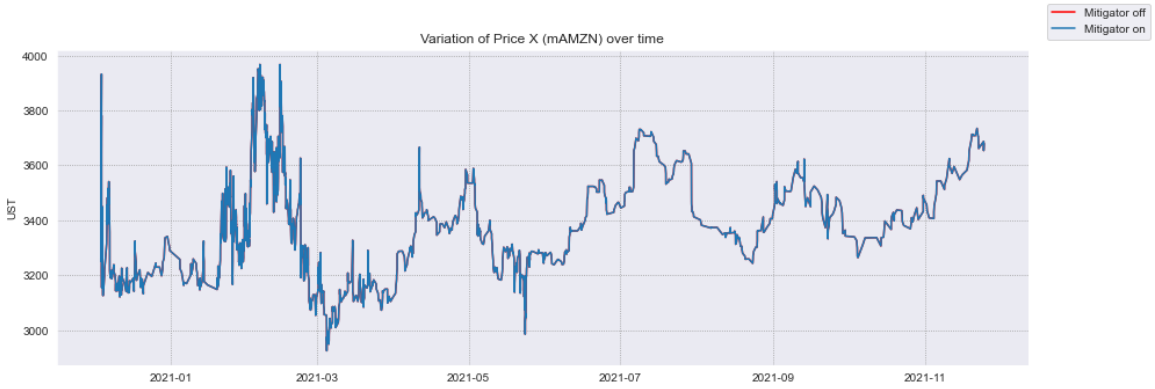
A more detailed overview of the pool can be found here. The volatility mitigation mechanism didn't block any transaction from this pool. Before the change applied inside the DSW oracle for **81%** of the cases TWAP couldn't be computed, after that, the number has been reduced to **1.1%**.



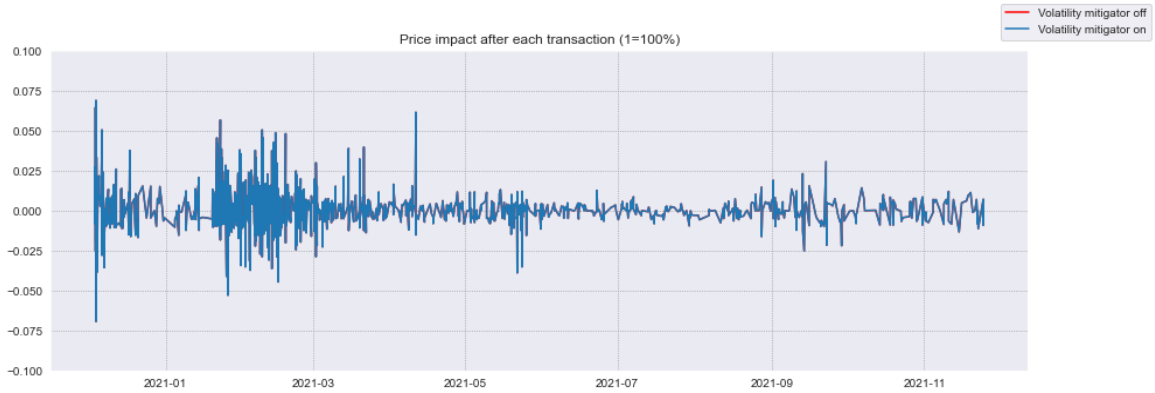
Picture X. Swaps slice_factor/out_amount_diff scatterplot (split by status)

Picture 158: reserves variation over time with volatility mitigation mechanism disabled/enabled

The reserves vary similarly to the real values obtained from the Uniswap subgraph and described in the pool-analysis section. As no transactions have been blocked, the plot is the same for both 2 regimes (with VM disabled/enabled).



Picture X: variation of price over time



Picture X: price impact after each transaction

The transactions with a high price impact are present predominantly during the initial period since pool creation. Overall, the variation of price is the same with volatility mitigation mechanism enabled / disabled (as no transactions have been blocked) and the price impact doesn't exceed 7.5% in any case.

PERL / WETH (STO)

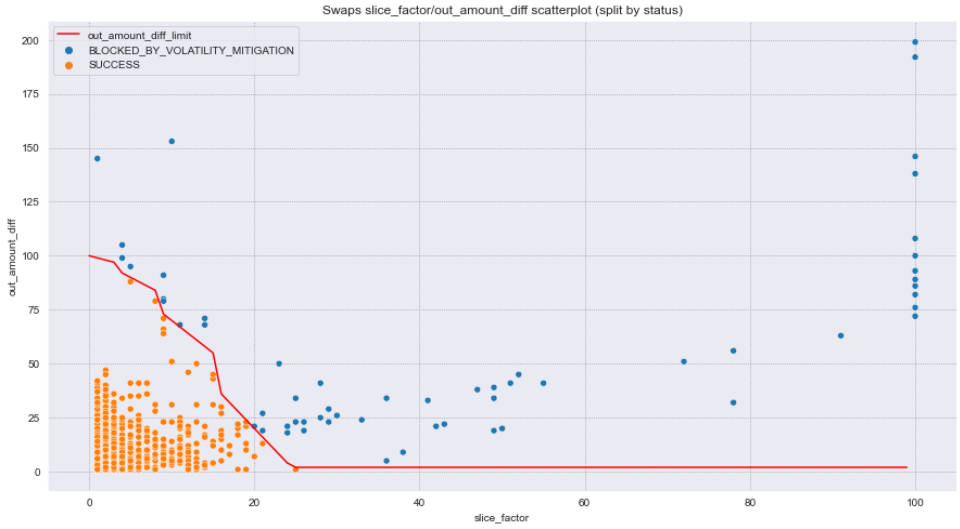
At the moment of analysis, the total locked liquidity in USD equivalent inside the pool was **697 804$**, the median number of transactions per day - 1, mean number of transactions per day being 3. The reserves of this pool were extremely low during the first first year since creation and then they increased significantly as a result of a series of large mints.

Historical stats:

- Swaps: 1534

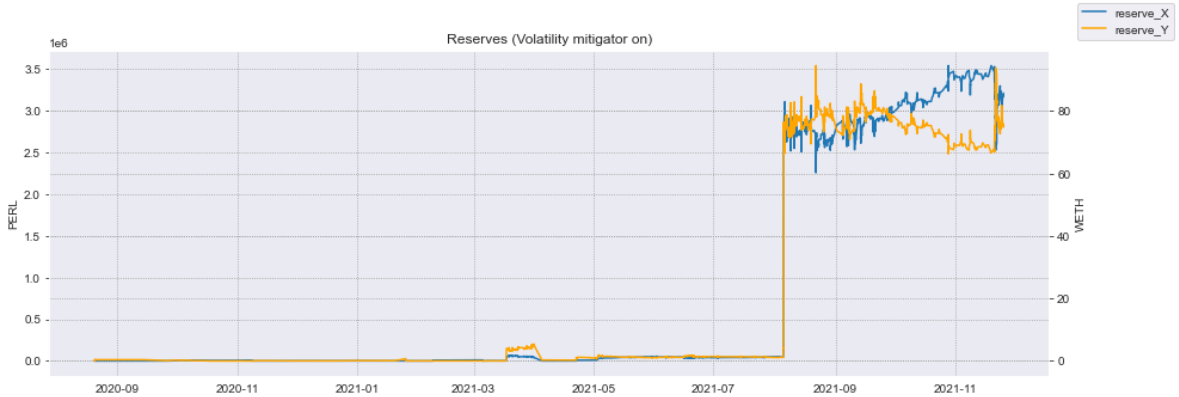
- Mints: 13
- Burns: 4
- Initial liquidity: $62
- Max liquidity: $697 804
- Most recent liquidity: $644 753

A more detailed overview of the pool can be found here. After running the simulations with the historical transactions from this pool, no transactions were blocked by the volatility mitigation mechanism and in **82%** of the cases TWAP couldn't be computed. The **modification** in the DSW oracle reduced this number to **3.9%** and led to **61 swaps blocked** by the volatility mitigation mechanism.

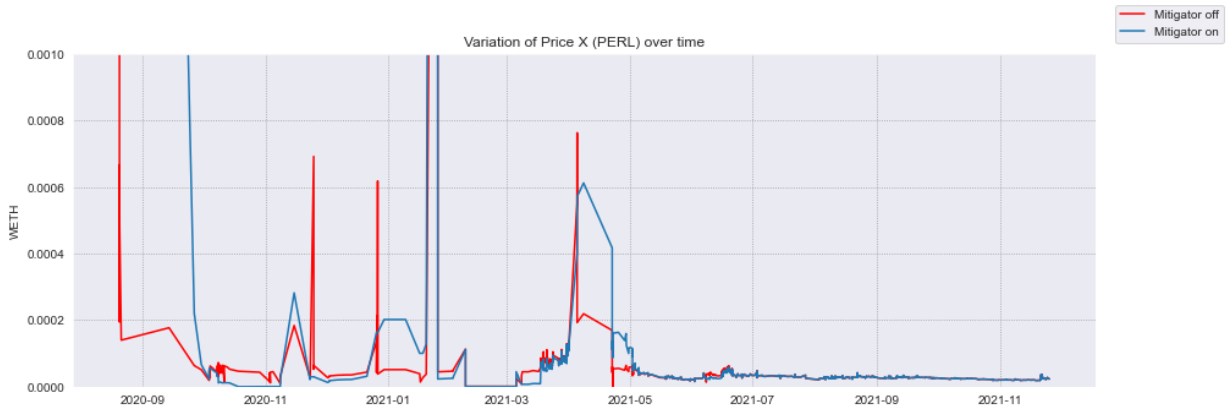


Picture X. Swaps slice_factor/out_amount_diff scatterplot (split by status)

It should be noted that all of the blocked swaps happened before the increase of the reserves.

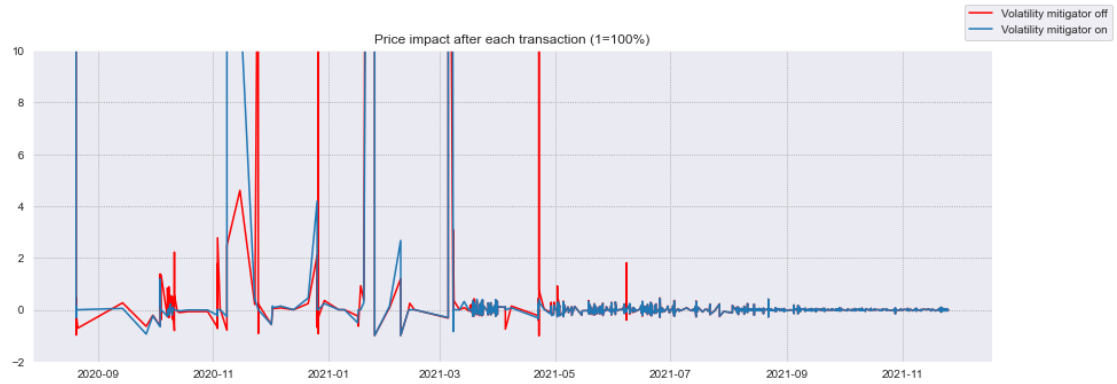


Picture X. Variation of pool reserves over time with volatility mitigation mechanism enabled



Picture X. Variation of price after each transaction with volatility mitigation mechanism disabled / enabled

In the first half of the plot there are a lot of transactions with a high price impact. Most of them were not blocked by the volatility mitigation mechanism because of the missing observations inside the oracle. As the liquidity increased, the price became much more stable and the transaction frequency also increased.



Picture X. Price impact after each transaction with volatility mitigation mechanism disabled / enabled

It can be observed that during 2021.03 and 2021.05 there was a small period with a relatively high transaction frequency, all of them having a small price impact. It corresponds to the period when the reserves were increased slightly (can be observed on the plot with reserves).. After that, a consequent drop of reserves happens.

UMA / FEI

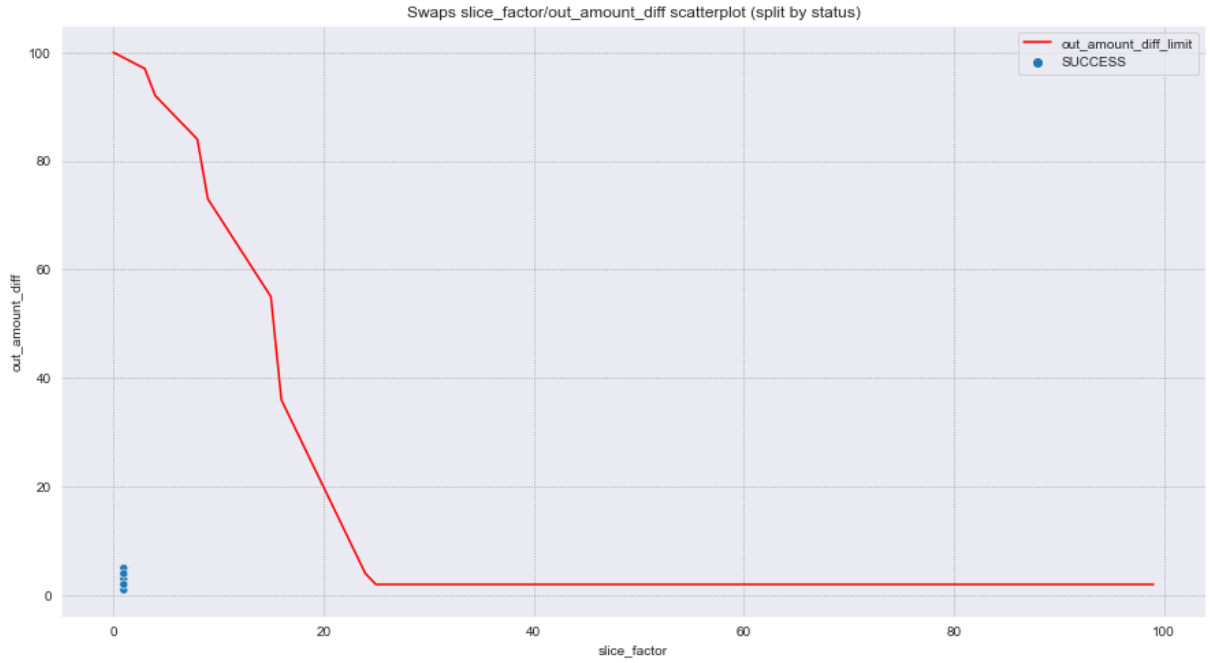
For this pool, at the moment of analysis only 2 days of history were available.

Historical stats:

- 26 swaps

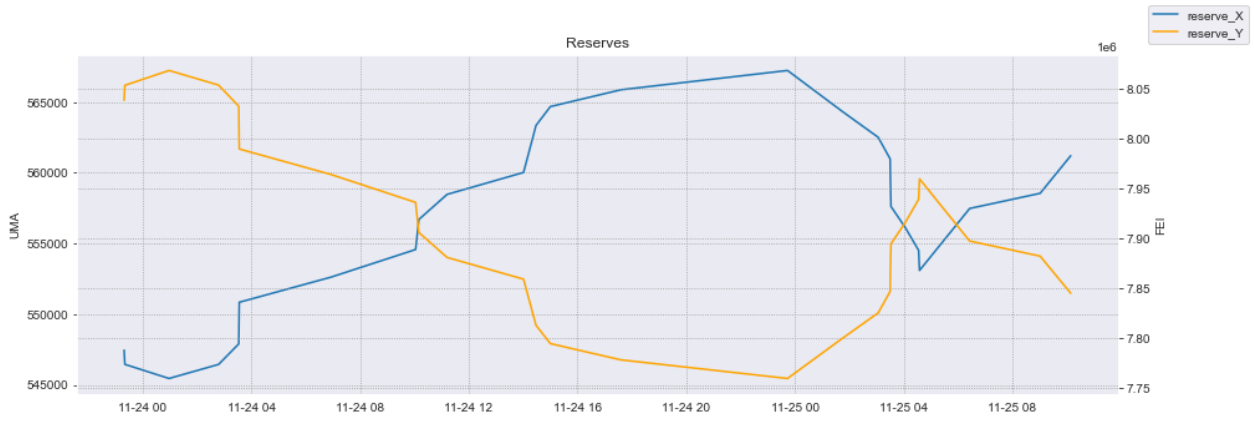
- 4 mints
- 0 burns
- Initial liquidity: $16.4 mln

No swaps were blocked by the volatility mitigation mechanism. Before the change in the DSW oracle in 84% of the cases TWAP couldn't be computed, after the change - only in 3.8%.



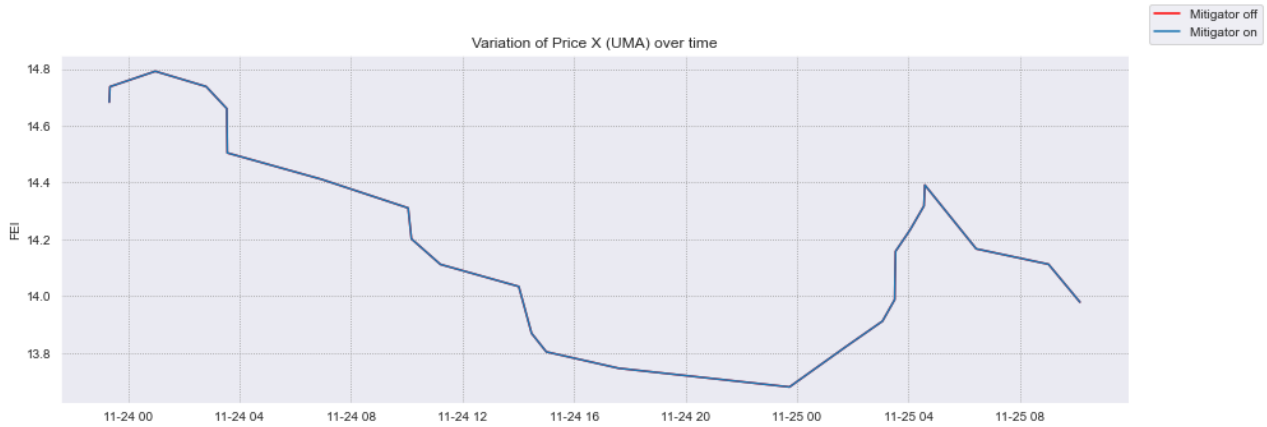
Picture X

As the amount of swapped tokens was significantly lower than the amount the pool was initialized with, all of the swaps fall in the lower-left corner of the slice_factor / out_amount_diff scatterplot.



Picture X. UMA / FEI - variation of reserves over time

The variation of reserves is caused only by swaps, as no mints after the ones at the creation of the pool were registered.



Picture X. UMA / FEI - variation of price over time

As no swaps have been blocked, the variation of reserves and price is the same with volatility mitigation mechanism disabled / enabled and it corresponds to the real historical price UMA-FEI.

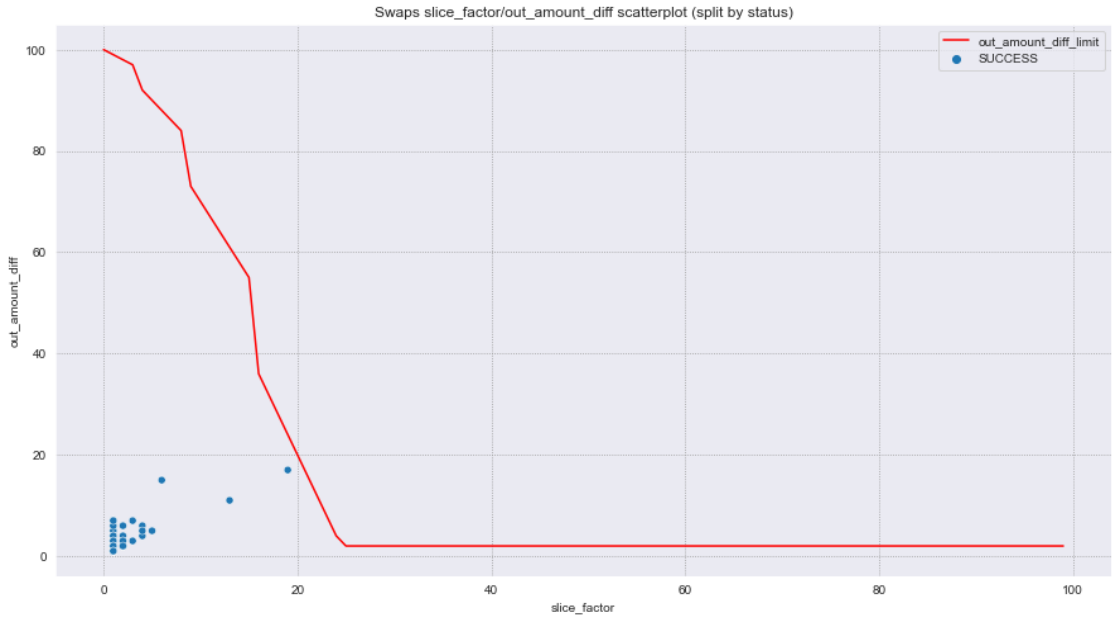
USTONKS / WETH

At the moment of analysis, the total locked liquidity in USD equivalent inside the pool was about **32 000$**, the median number of transactions per day - 1, mean number of transactions per day being 1,7.

Historical stats:

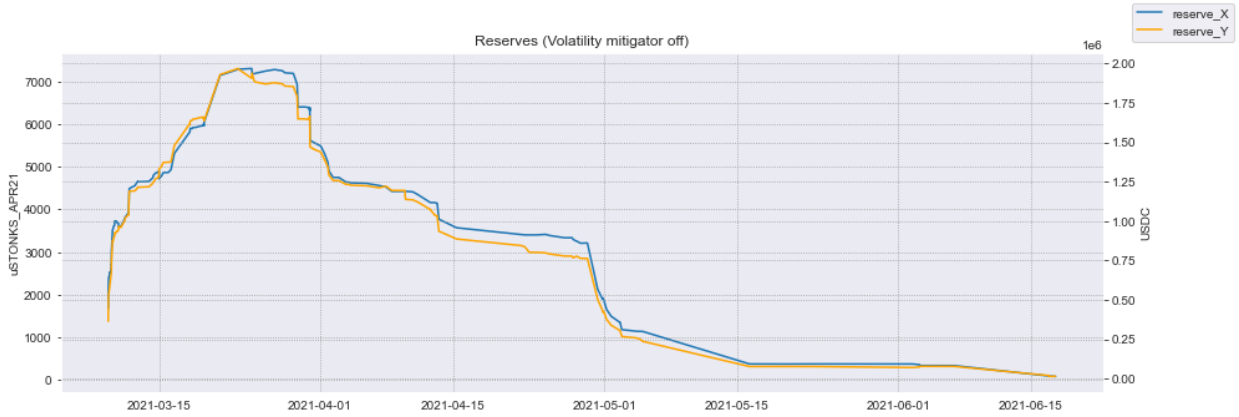
- Swaps: 175
- Mints: 169
- Burns: 134

A more detailed overview of the pool can be found here. After running the simulations with the historical transactions from this pool, no transactions were blocked by the volatility mitigation mechanism and in **94%** of the cases TWAP couldn't be computed. The **modification** in the DSW oracle reduced this number to **3.9%**.



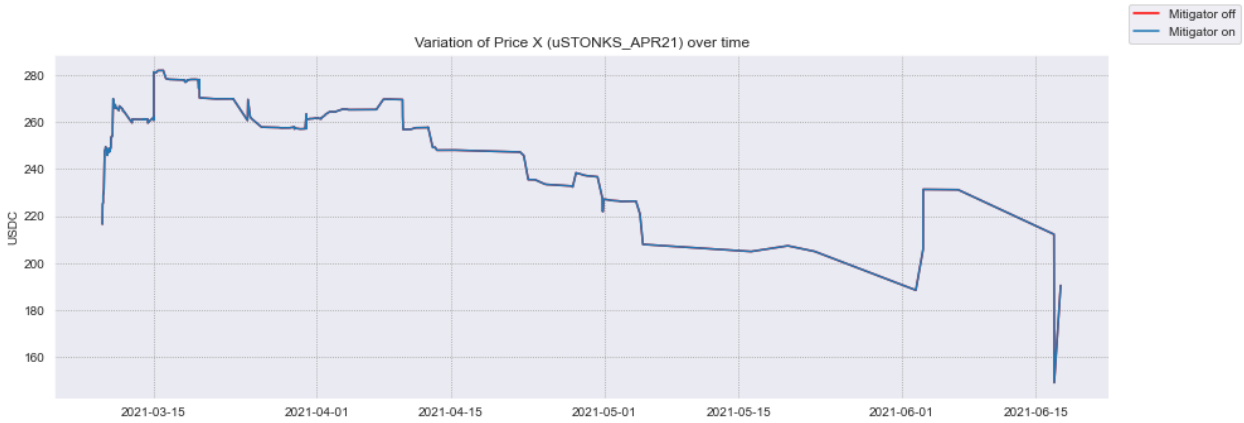
Picture X

As no swaps have been blocked, it can be seen…



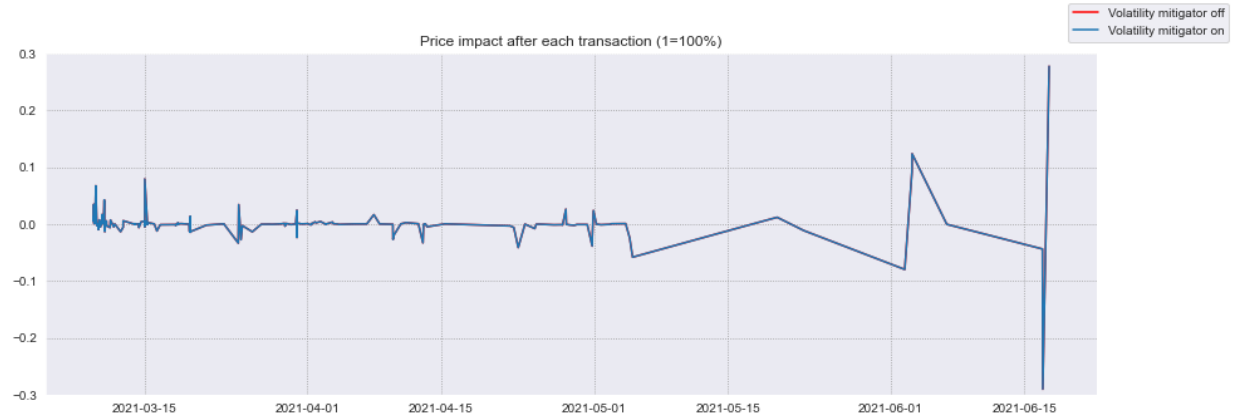
Picture X. UMA / FEI - variation of reserves over time

The variation of reserves corresponds exactly to the real data obtained from the Uniswap subgraph. The reserves decrease gradually from the end of March.



Picture X. UMA / FEI - variation of reserves over time

The variation of price also is similar to the data demonstrated in the pool analysis section.



Picture X. UMA / FEI - price impact after each transaction

The price impact of each swap becomes bigger, as the reserves decrease. As no swaps are blocked, it's the same with the volatility mitigation mechanism enabled / disabled.

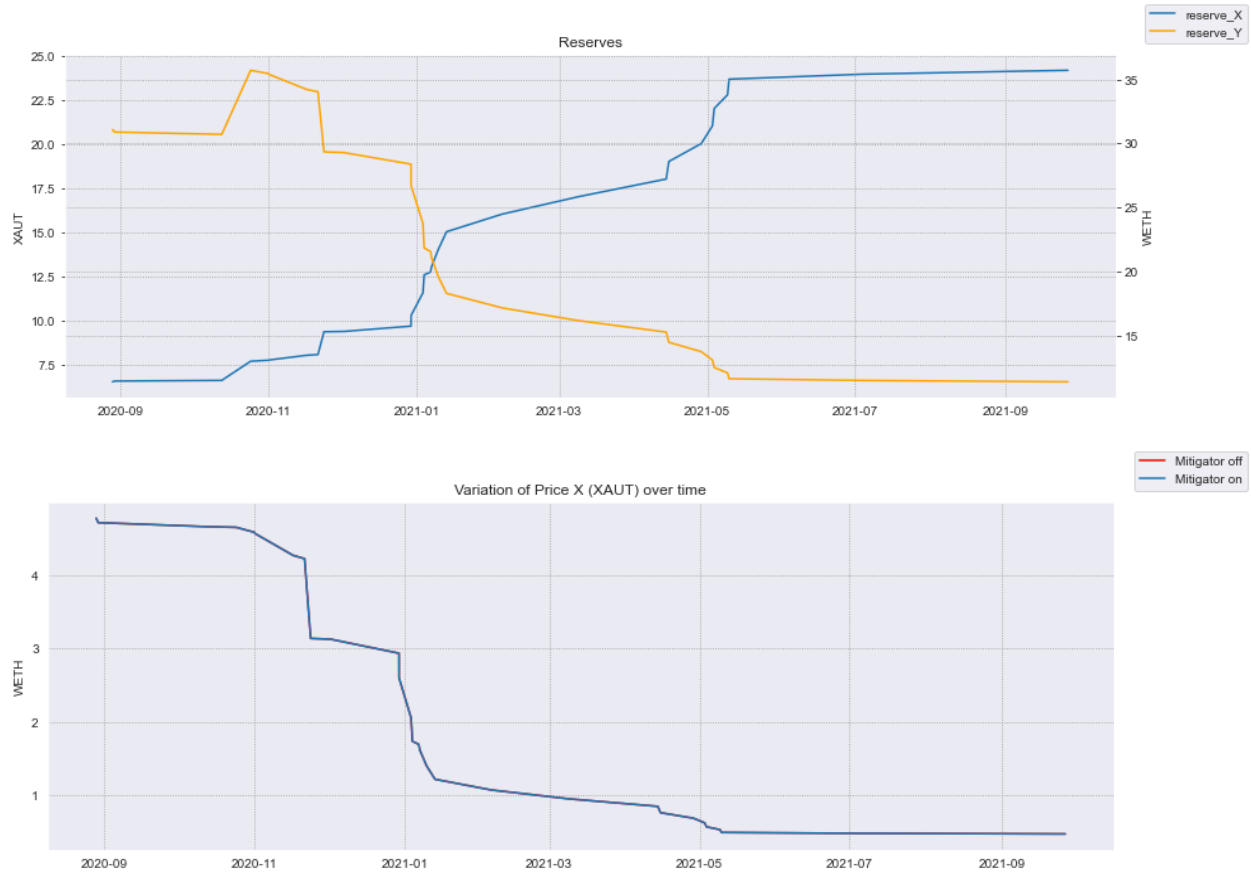
XAUt / WETH

At the moment of analysis, the total locked liquidity in USD equivalent inside the pool was about **77 654$**, the median number of transactions per day - 0, mean number of transactions per day being 0,07. All of the swaps were in the direction XAUt -> WETH.

Historical stats:

- Swaps: 31
- Mints: 5
- Burns: 0
- Reserves first day: 23 810$
- Reserves last day: 77 654$

A more detailed overview of the pool can be found here. After running the simulations with the historical transactions from this pool, no transactions were blocked by the volatility mitigation mechanism and in **100%** of the cases TWAP couldn't be computed. The **modification** in the DSW oracle reduced this number to 77**%**.



DOGE / WETH

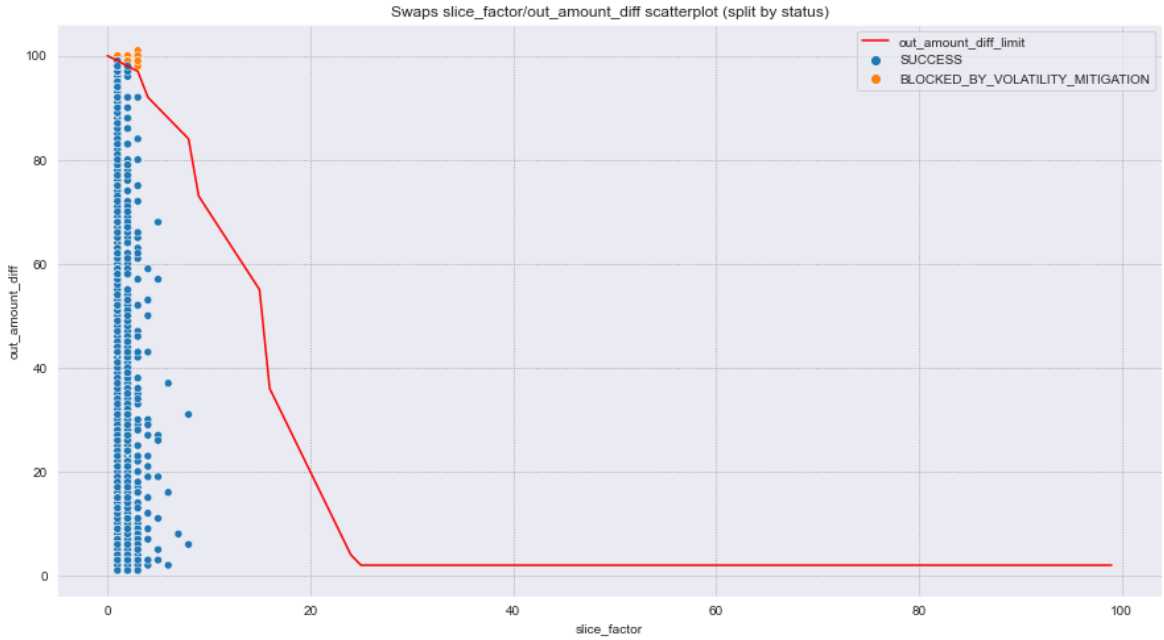
As the price of memecoins is extremely unstable, and there were several moments when DOGE price increased / decreased significantly in a matter of several hours, the analysis of the simulations on data from this pool can show how adaptive is the volatility mitigation mechanism to instant changes in price and how it can affect the state of the pool if such cases.

Historical stats:

- Swaps: 12 176
- Mints: 26
- Burns: 16
- Reserves first day: $1.14 mln

- Reserves last day: $5.14 mln
- Max reserves: $19.4 mln

A more detailed overview of the pool can be found here. After running the simulations with the historical transactions from this pool, **19** transactions were blocked by the volatility mitigation mechanism and in **26%** of the cases TWAP couldn't be computed. The **modification** in the DSW oracle reduced this number to 77**%** and led to 20 blocked transactions.

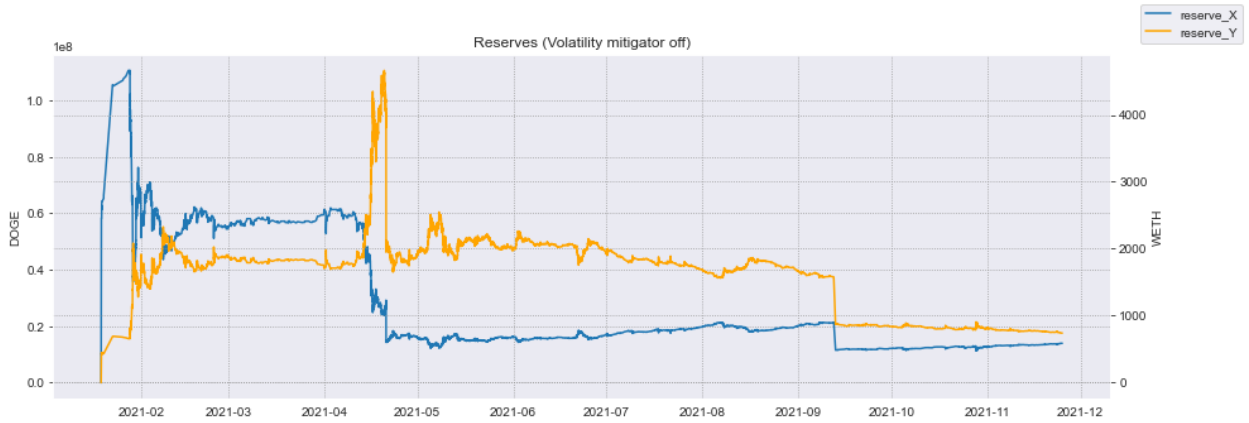


Picture X. Swaps slice_factor/out_amount_diff scatterplot (split by status)

As the reserves of the pool are quite big, all of the swaps have a small slice_factor despite their relatively big amount_in. In this case, the volatility mitigation mechanism kicks in only when the percentage price difference of the price with the one from oracle is near 100% or greater, and the change in price occurs as a result of multiple swaps.

In case the percentage difference of the price compared to the one from oracle (out_amount_diff) is greater than 100%, the swaps are being blocked no matter the slice_factor. Therearefore, in the case of a significant shift in price in a short period of time, all of the swaps in a single direction risk to be blocked.

There were several sudden price increases in the price of DOGE registered. More, on this, in the following sections.

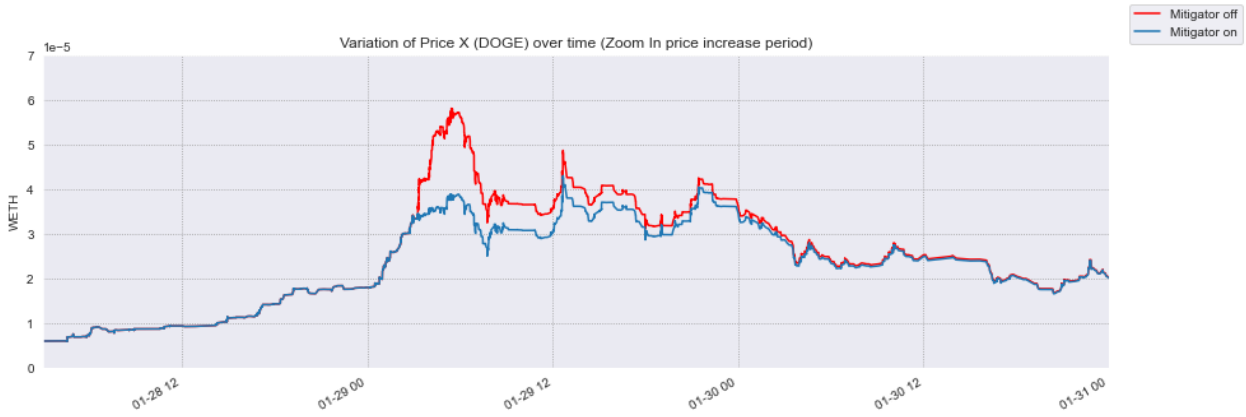


Picture X: reserves variation over time with disabled volatility mitigation mechanism

From the instantiation of the pool, the reserves are high enough. There are 3 periods with sudden reserves variation. Near 2021.02 - when the price of DOGE went up, between 2021.04 and 2021.05 (another spike in price), and in the middle of september, when the reserves of both of the tokens endured a decrease as a result of a large burn (of 701 WETH).

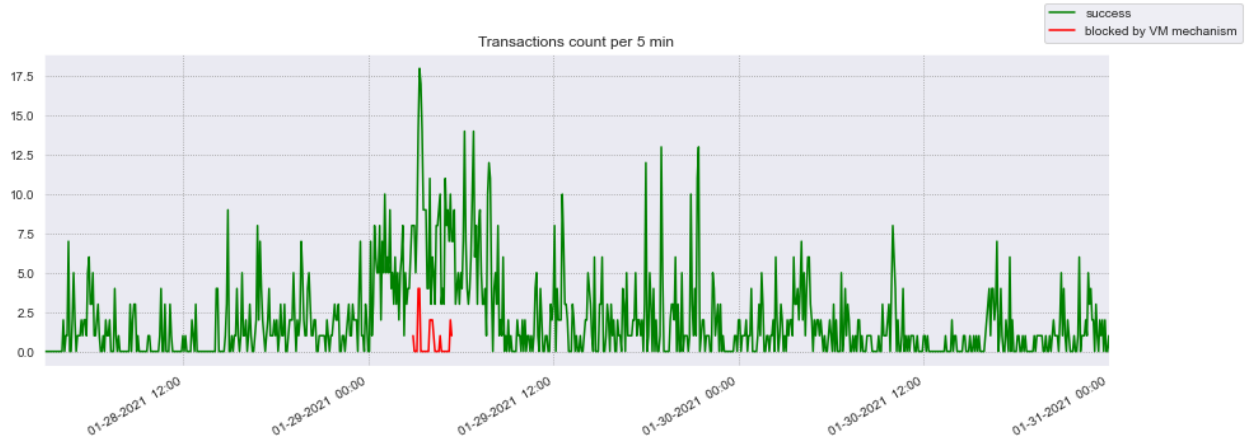
Picture X: price variation with volatility mitigation mechanism disabled / enabled

There is only one time period when the volatility mitigation mechanism kicked in and started blocking the transactions, lowering the overall price increase. It's not very visible on the above plot, so it was decided to zoom in into that period and analyze the phenomenon in more detail.



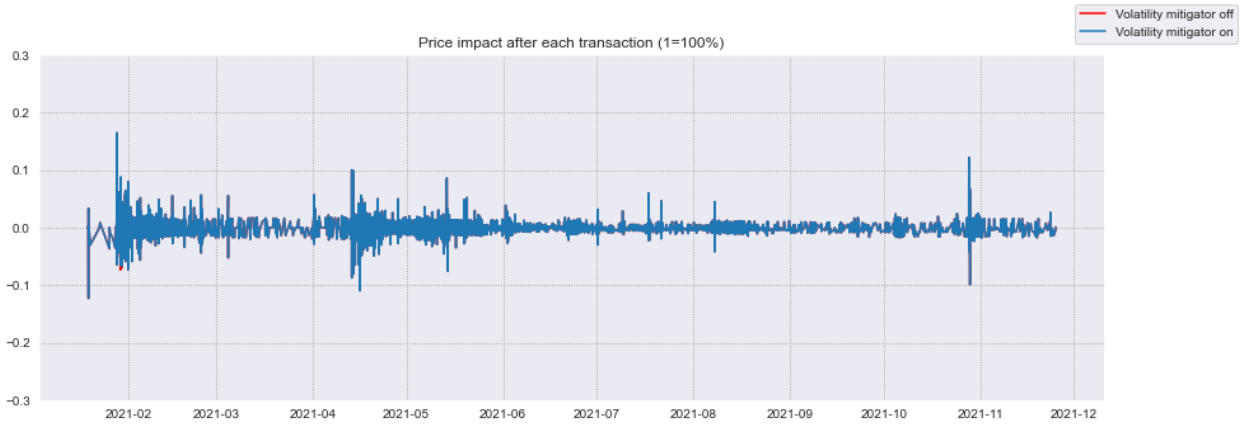
Picture X: price variation with volatility mitigation mechanism disabled / enabled, 1.28.2021 - 1.31.2021

It can be seen that without the volatility mitigation mechanism the price of DOGE increased from 0.6e-5 to about 6e-5 in about a 24 hours period. The **x10** increase was reduced to a little bit less than **x7** by the volatility mitigation mechanism. It was decided to look at the frequency of the blocked transactions to understand whether the pool was completely blocked, or only some of the transactions weren't allowed to pass.



Picture X: swaps total count per 5 min, split by status, 1.28.2021 - 1.31.2021 period

It can be seen that only 20 transactions during the period of sudden price increase were blocked, and even during that time the majority of swaps were successful. A complete blockage of the pool didn't occur. As the price started to decrease, no swaps were blocked any more. If the increase in the price would have continued a blockage of all of the transactions DOGE -> WETH would have occurred.



Picture X: price impact after each transaction

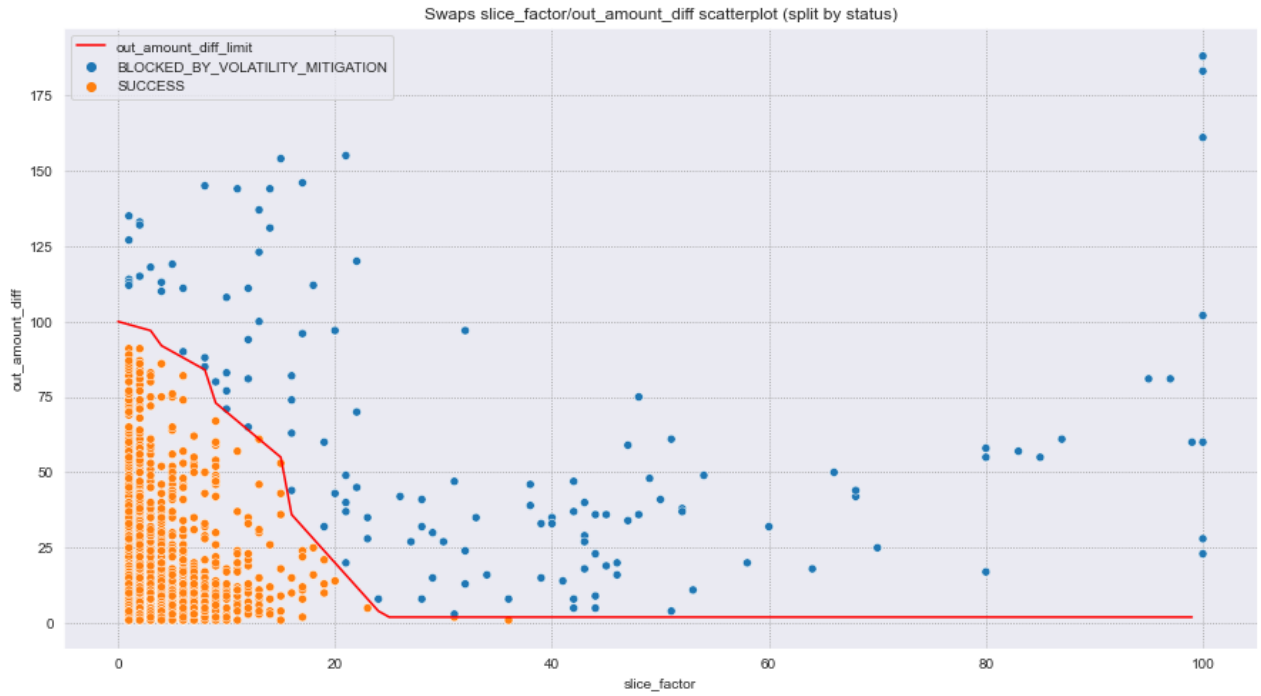
There can be observed several transactions with a price impact near or greater than 10%. Most of them seem to be MEV-bot attacks.

AXS / WETH

Historical stats:

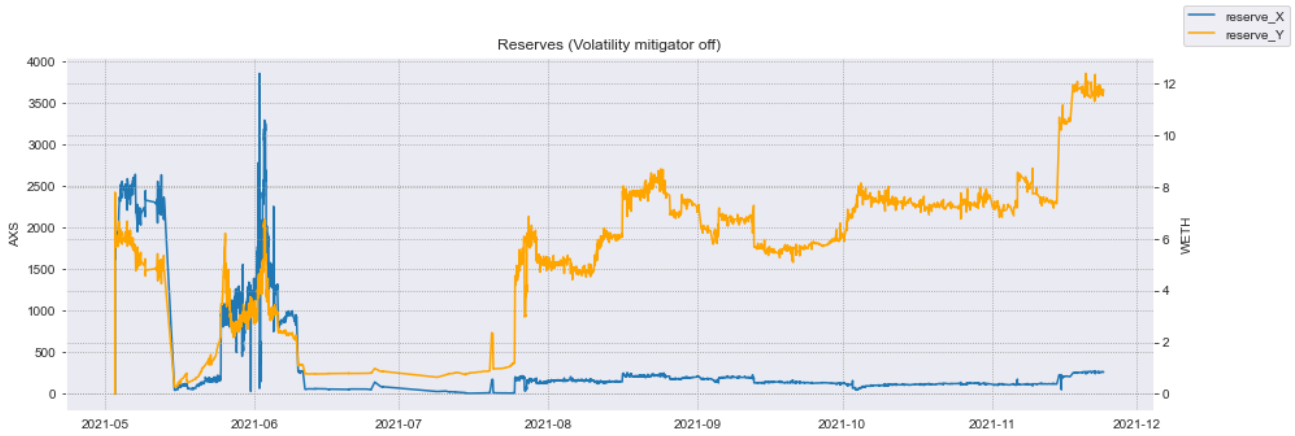
- Swaps: 4587
- Mints: 72
- Burns
- Initial liquidity (first day): $43 248
- Maximal liquidity: $66 640
- Minimal liquidity: $1.15e-13

A more detailed overview of the pool can be found here. After running the simulations with the historical transactions from this pool, 34 transactions have been blocked by the volatility mitigation mechanism and in **36%** of the cases TWAP couldn't be computed. The **modification** in the DSW oracle reduced this number to **0.1%** and led to **130 swaps blocked** by the volatility mitigation mechanism.

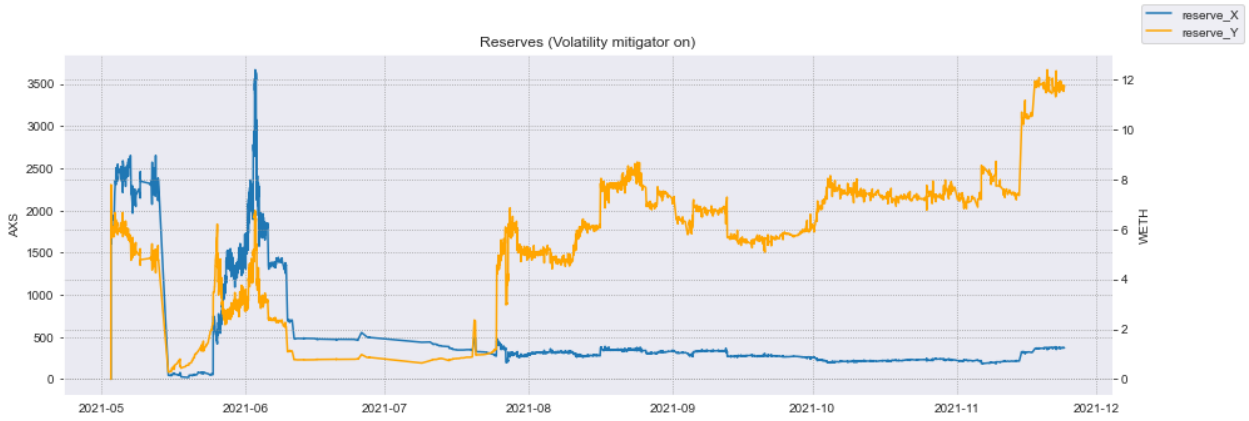


Picture 182: Swaps slice_factor / out_amount_diff scatterplot (split by status)

It can be observed that there are quite a lot of swaps lying right near the border.

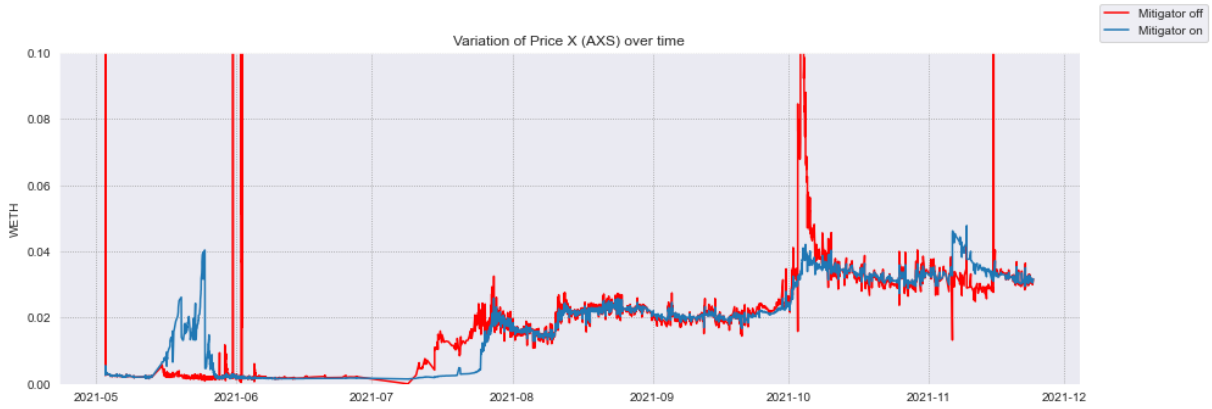


Picture 183: reserves variation over time (volatility mitigation mechanism disabled)



Picture 183: reserves variation over time (with volatility mitigation mechanism enabled)

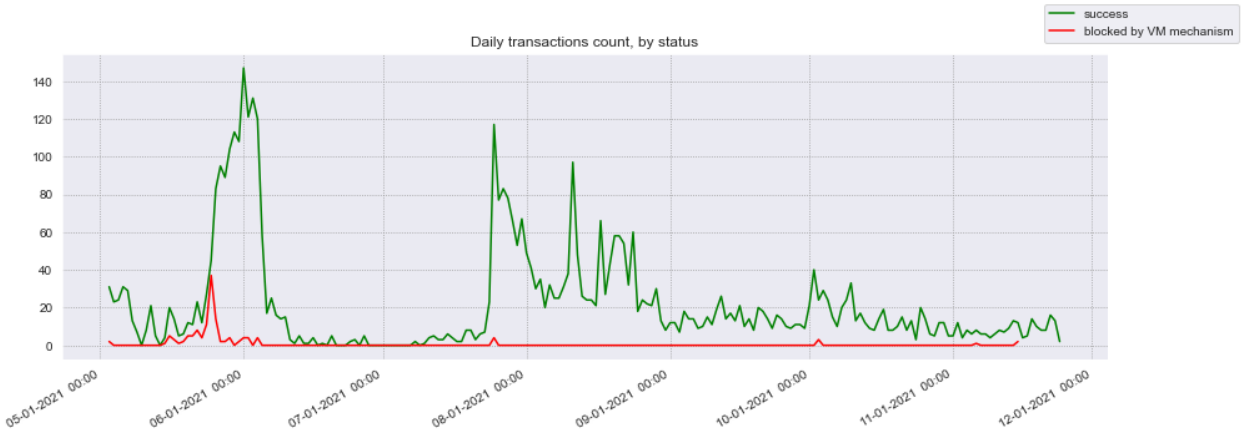
Without the volatility mitigation mechanism enabled, it can be seen that there are some sudden raises and drops in the reserves near 06.2021.



Picture 184: AXS - WETH price variation over time with volatility mitigation mechanism disabled / enabled

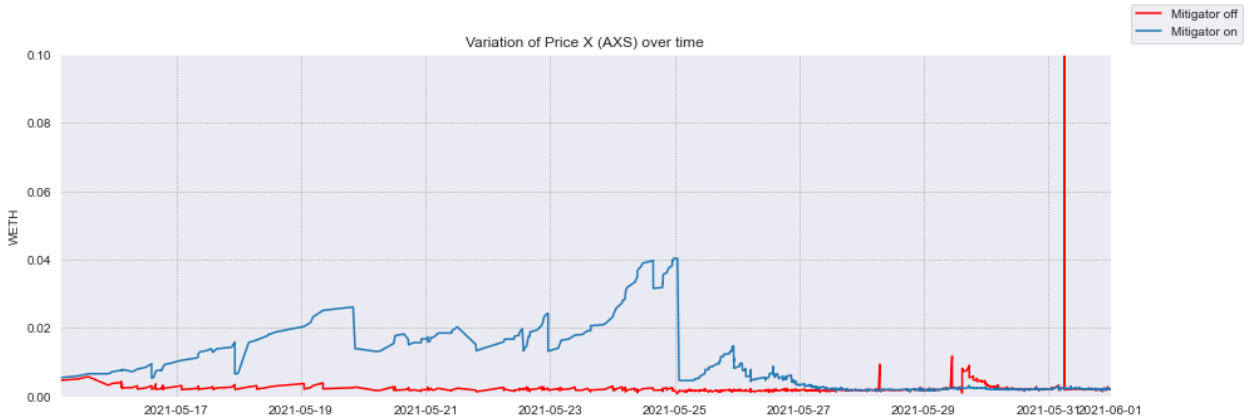
Despite the low reserves inside the pool, the volatility mitigation mechanism is able to significantly decrease the price variation.

It can be observed that during 2021.05, the price of AXS increases significantly in the mode with volatility mitigation (even though it stays almost constant in default regime). It has been decided to analyze this period in more detail.

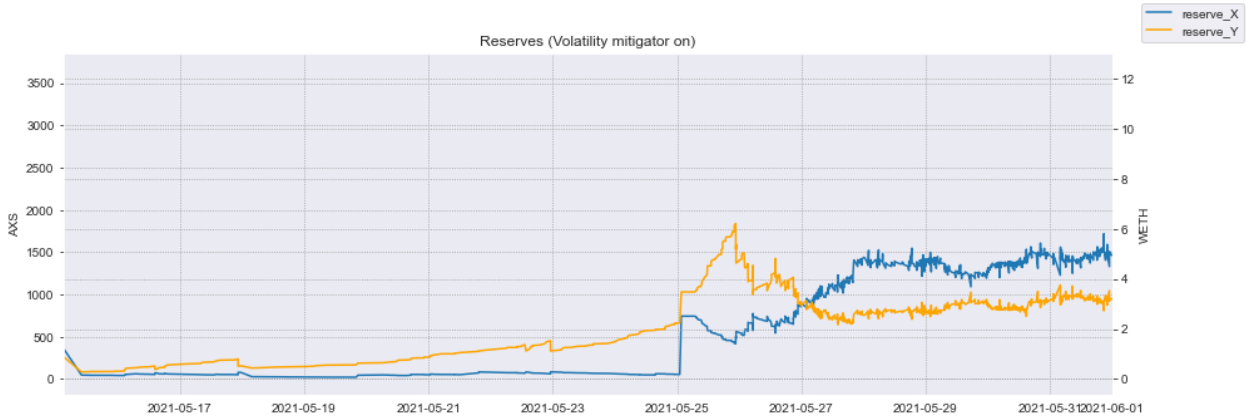


Picture 184: Daily transactions count, split by status, with enabled VM mechanism

The increase in the number of blocked daily transactions corresponds to the period with the examined price increase and subsequent drop at the end of 2021.05.

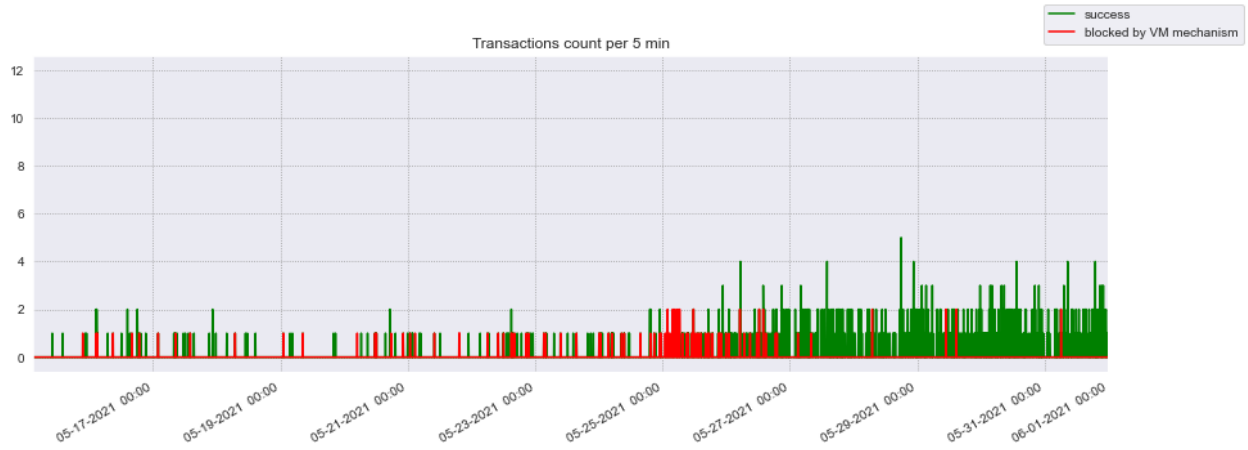


Picture 184: AXS - WETH price variation over time 17.05.2021 - 01.06.2021 period (with volatility mitigation mechanism disabled / enabled)



Picture 183: reserves variation over time 17.05.2021 - 01.06.2021 period (with volatility mitigation mechanism enabled)

The decrease in price near 06.2021, is caused by a mint, it can be observed by looking at the reserves.



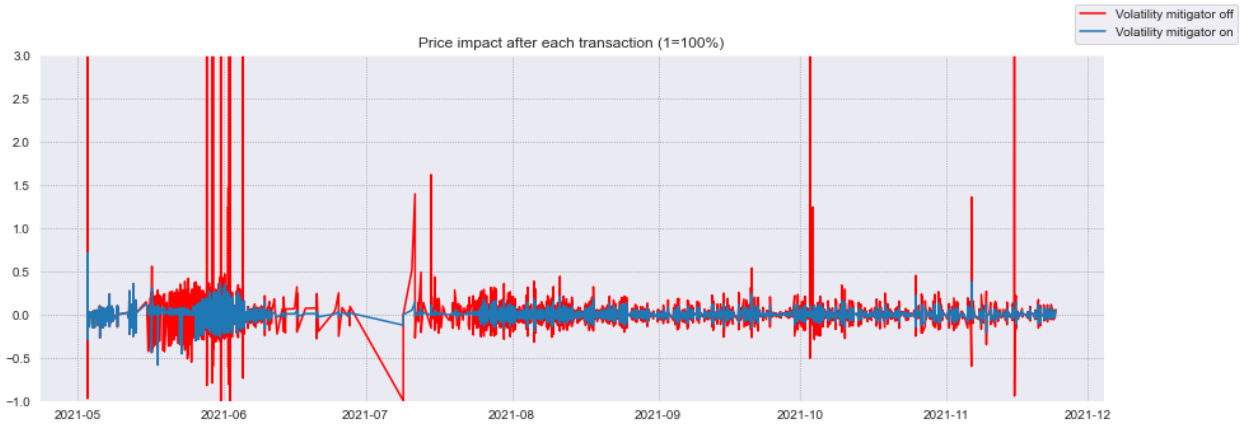
Picture 183: transactions count per 5 min, 17.05.2021 - 01.06.2021, split by status

The price increase happens due to the blockage of some large transactions AXS -> WETH (swaps which didn't cause price change in the long run without the mitigation mechanism enabled), and the sudden price decrease is a result of the mint, in which the proportion of tokens doesn't correspond to the current price (because of the previously blocked swaps).

By examining the executed swapped in that period it can be seen that in the majority of them WETH is exchanged for AXS. However, there are significantly larger in size (but much more rare) transactions in the opposite directions, arbitraging the price. Because of the small reserves, those transactions have a significant **slice_factor** and are being blocked by the volatility mitigation mechanism.

token_in	token_out	token_in_amount	status	slice_factor	oracle_amount_out	out_amount_diff	reserve_X_before	reserve_Y_before
WETH	AXS	0.020704	SUCCESS	4.0	2.388992	24.0	56.895236	0.601006
WETH	AXS	0.007204	SUCCESS	2.0	0.947033	41.0	55.018849	0.621628
WETH	AXS	0.027000	SUCCESS	5.0	3.544503	46.0	54.394786	0.628803
AXS	WETH	22.946799	BLOCKED_BY_VOLATILITY_MITIGATION	44.0	0.181298	9.0	52.176816	0.655694
WETH	AXS	0.012810	SUCCESS	2.0	1.673474	51.0	52.176816	0.655694
WETH	AXS	0.009000	SUCCESS	2.0	0.975759	36.0	51.186803	0.668453
WETH	AXS	0.004770	SUCCESS	1.0	0.590603	51.0	50.513495	0.677417
WETH	AXS	0.009000	SUCCESS	2.0	0.942792	37.0	50.163784	0.682168
WETH	AXS	0.014154	SUCCESS	2.0	1.428406	25.0	57.109053	0.711319
AXS	WETH	20.115300	BLOCKED_BY_VOLATILITY_MITIGATION	36.0	0.207846	8.0	56.005811	0.725416

The blockage of arbitrage will be examined in more detail while performing the stress testing of the volatility mitigation mechanism with the simulated transactions.



Picture 183: Price impact after each transaction, split by status

There can be observed multiple transactions with significant price impact, especially near 2021.06. Most of them are MEV bot attacks.

Example:

The attacker extracts 1126 of AXS from the pool, performing a sandwich attack on Sushiswap and then returns the tokens to the Uniswap v2 pool.

- Attacker (transaction 0 in block):

  Swap 98.999966005306335222 Ether For 1,126.031271544230690794 AXS On Uniswap V2

  Swap 1,126.031271544230690794 AXS For 2.447279468441064749 Ether On Sushiswap

- Simple user (transaction 1 in block)

  Swap 2.447279468441064749 Ether For 1,175.907785087144601029 AXS On Sushiswap

  Swap 1,175.907785087144601029 AXS For 99.085486318484602635 Ether On Uniswap V2

- Attacker (transaction 2 in block)

  Swap 98.999966005306335222 Ether For 1,126.031271544230690794 AXS On Uniswap V2

  Swap 1,126.031271544230690794 AXS For 2.447279468441064749 Ether On Sushiswap

Those transactions are blocked by the volatility mitigation mechanism. The total liquidity of the pool in that period varied between $10 000 - $30 000.

MANA / WETH

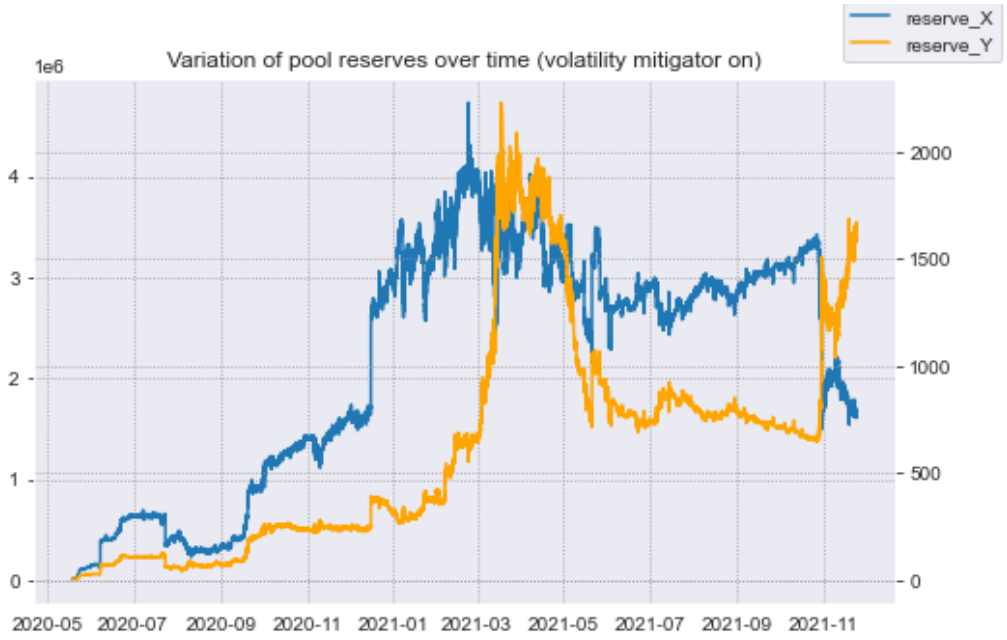
This is a medium capitalization pool with an NFT token. By running the simulations on the historical transactions from it, only 3 out of 72 981 swap-transactions were blocked.

Below, is shown the volatility mitigator check status for swap transactions:

```
CHECKED                69319
CANT_CONSULT_ORACLE     3662
```

Picture 190: amount of passed transactions and cases where TWAP was not calculated

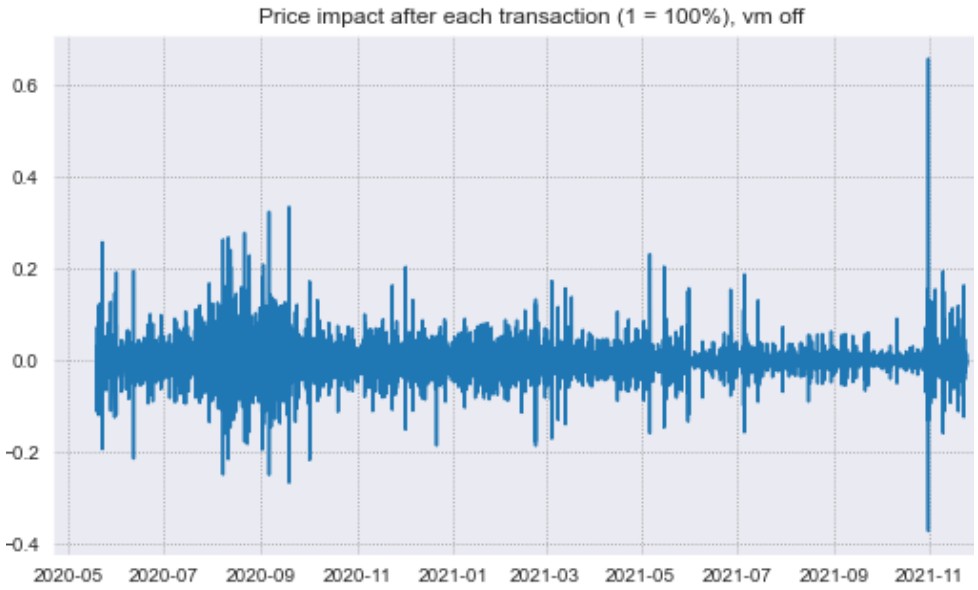
For 3662 it wasn't possible to compute the TWAP value, meaning that exactly 24 hours ago there was an hour gap with no transactions happening.



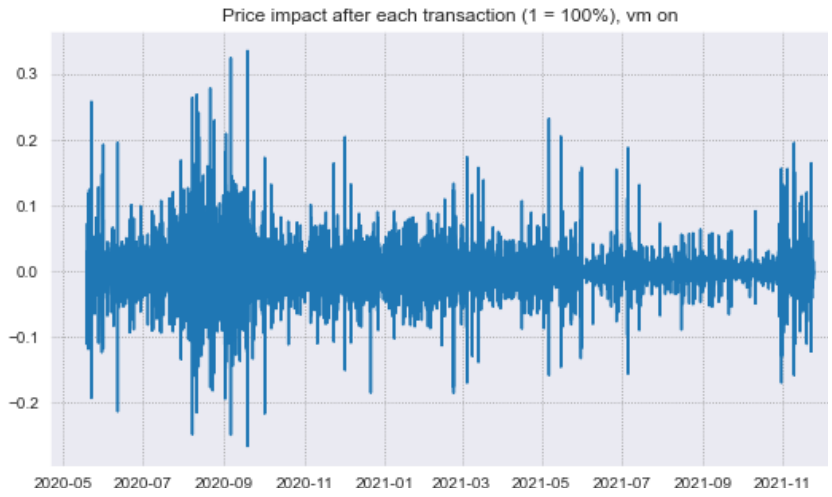
Picture 191: Variation of reserves. Pool MANA/WETH (volatility mitigator on)

Picture 192. Variation of price of X token over time for the MANA/WETH pool (volatility mitigator off/on)

The volatility mitigator blocks only one big transaction toward the end of the period. The transaction is a mev-bot sandwich attack. Besides this, the behaviour for different volatility mitigator regimes is the same.



Picture 193: price of X token change rates distribution for MANA/WETH pool, volatility mitigation off



Picture 194: price of X token change rates distribution for MANA/WETH pool, volatility mitigation on

It can be observed that the swap with the highest price impact is blocked, besides this the behaviour is consistent with volatility mitigator on/off. The remaining swaps with a high price impact will be examined afterwards to determine whether they are mev-bot sandwich attacks or not.

Simulations results for distinct VM related parameters

period_size (h)	No TWAP available ratio	Swaps blocked by volatility mitigator
0.5	0.14328	3
1.0	0.05018	3
2.0	0.01520	3
3.0	0.00614	3
6.0	0.00127	3
12.0	0.00001	2

Picture 195: `window_size`=24h, distinct `period_size` values. Stats.

Picture 196: price variation over time with `window_size`=24h, distinct `period_size` values

It can be observed that the overall behaviour is very similar for distinct values for period_size parameter.

Next steps:

- Finish running the simulations using the extracted historical transactions of fractionalized NFT
- Determine the parameters for value generator* in order to perform simulations using generated transactions:
- Determine the optimal initial reserves of the pool for distinct trading behaviours (including transaction size / frequency)
- Perform stress testing of the volatility mitigation mechanism using simulated transactions, considering all possible edge cases

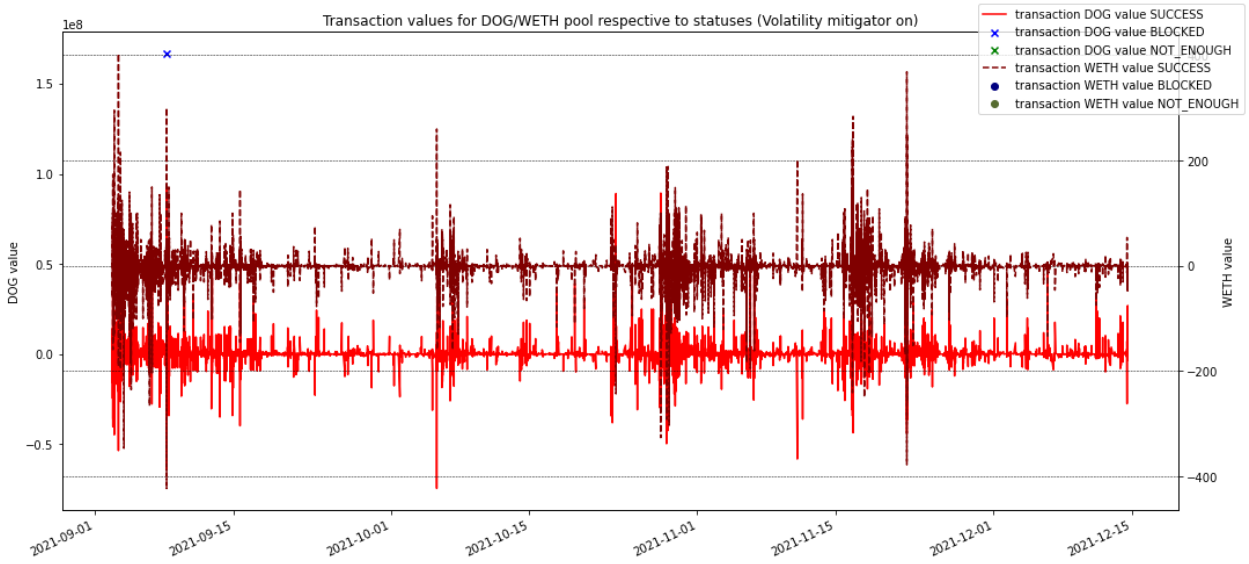
*Steps:

- Estimate the lognormal distribution parameters of the stablecoin (shape, scale) using maximum likelihood estimation method (or/and alternative methods)
- As it was observed that the average size of transactions depends on the current reserve values (for larger reserves, the probability of big transactions increases), for each pool, several sets of parameters will be estimated (each for a different range of reserves at the moment of the swap)
- Generalize the parameters in order to highlight several trading behaviours (e.g. distinct shape and scale parameters will be selected, describing appropriate small/medium/large transactions)

Example of stablecoin amount_in probability density function, of estimated lognormal distribution vs real historical data (pool WBTC-DAI, considered only swaps which occurred during reserves range 0.5mln+):

DOG / WETH (fractionalized NFT)

DOG/WETH pool has a rich transaction history with bi-directional token exchange and small value of blocked transactions (one blocked transaction). Pool contains 4 rises of the transaction values in the presented pool history time period. Simulation blocked only one transaction, meaning that other transactions had acceptable influence on the pool properties.

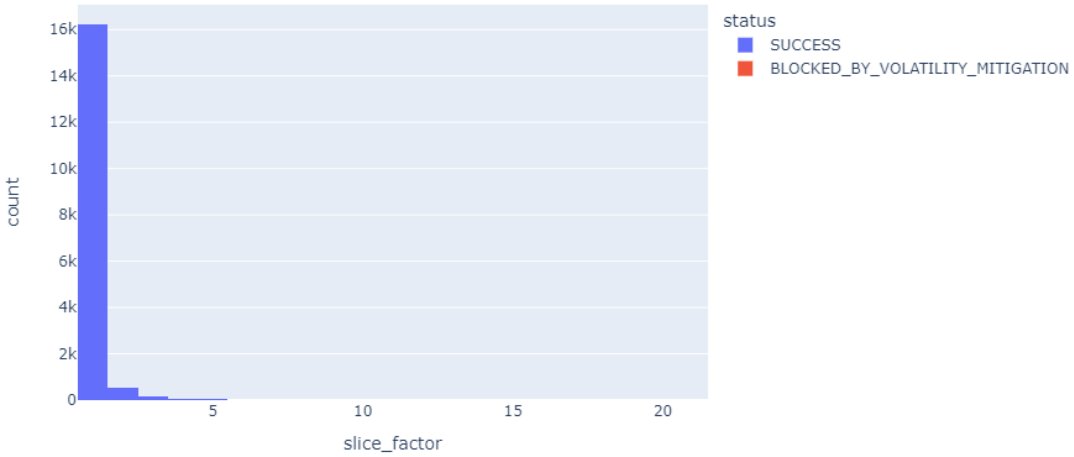


Picture X: token movement in DOG/WETH pool and blocked transactions values

Data visualization in the presented plot works by next properties:

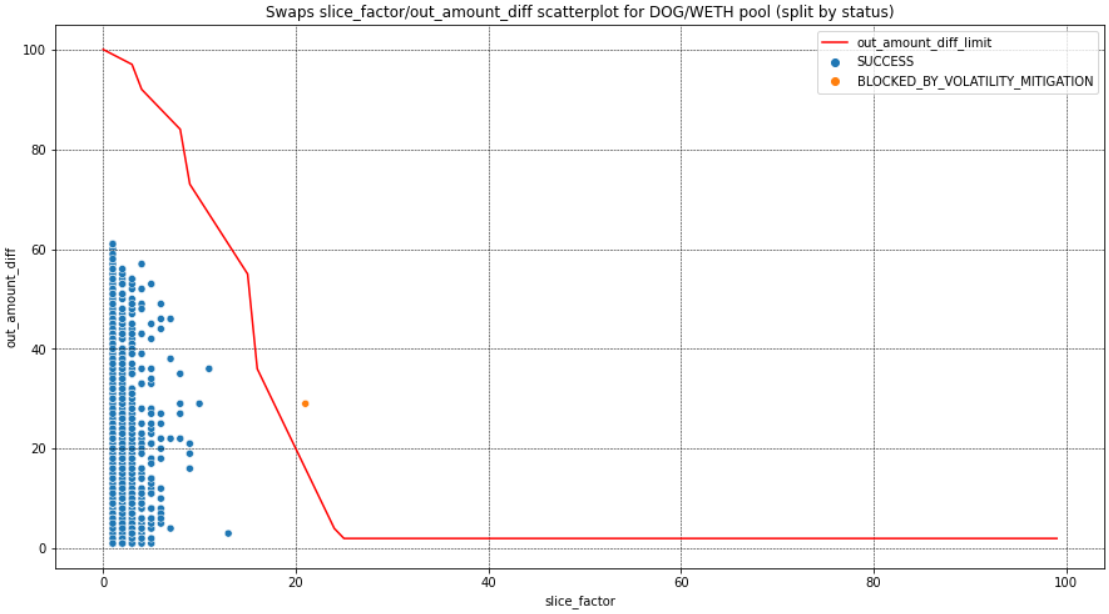
- On the left is presented DOG token axis (X token axis) with respective values meaning that bright red line corresponds with it, blue X and green X are representing blocked and higher than reserves transactions respectively;
- From the right is presented WETH token axis (Y token axis) with darker red line, darker blue and darker green dots representing successful, blocked and higher than reserves transactions via WETH token

Important point about the data is that both bright and darker red lines should cover both positive and negative values, demonstrating balanced token activity inside the pool. Otherwise pools can be considered as unbalanced with problems in traders' interest in tokens and pools.



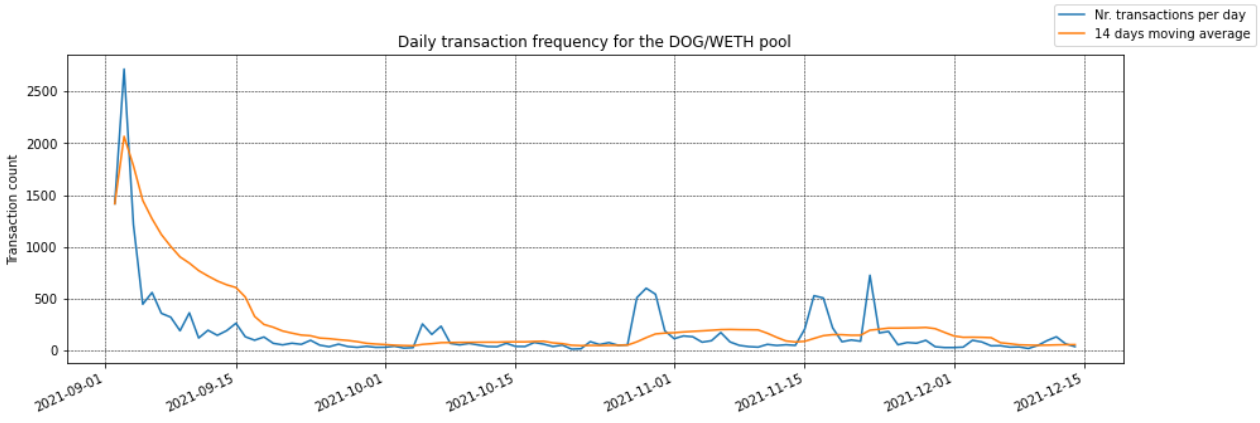
Picture X: slice factor distribution for DOG/WETH pool (split by transaction status)

The only blocked transaction has a too high slice factor. In most of the cases slice factor below 20 is acceptable and transaction is not blocked, but the presented one has value higher than 20.



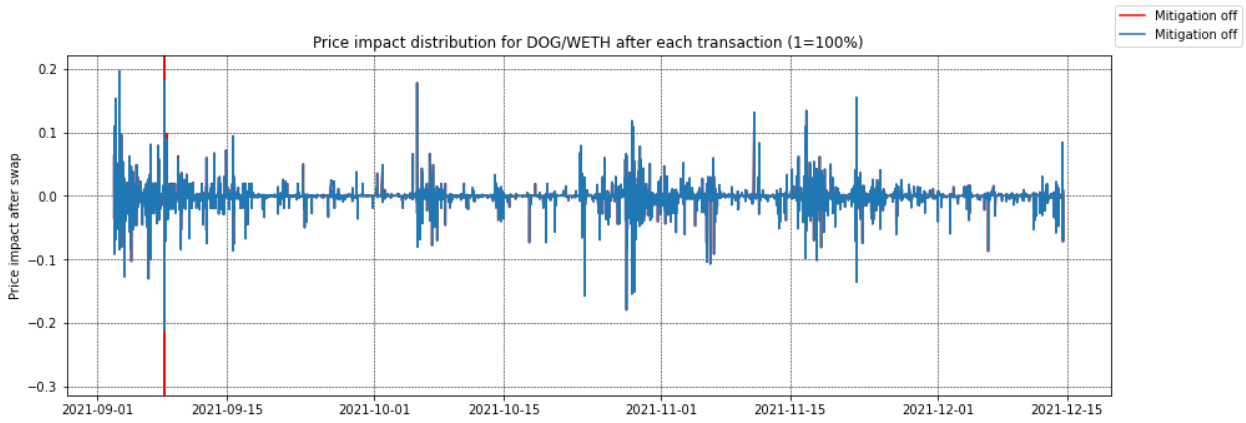
Picture X: swap slice factor and out amount difference distribution

Successful transactions have small slice factors, meaning that distribution is healthy and it is possible that pool will have a long lifecycle. There is unstable behavior of the transaction count distribution with peak in the beginning of the pool lifecycle with several rises of the activity in the beginning and in the middle of November 2021.



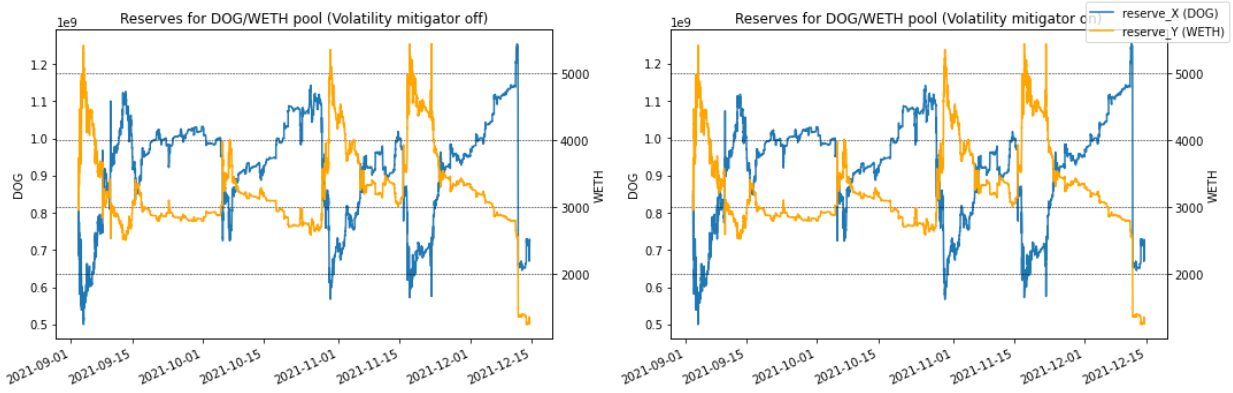
Picture X: transaction count distribution for DOG/WETH pool

Mitigation mechanism stabilizes pool token prices limiting changes by 20% deviation.



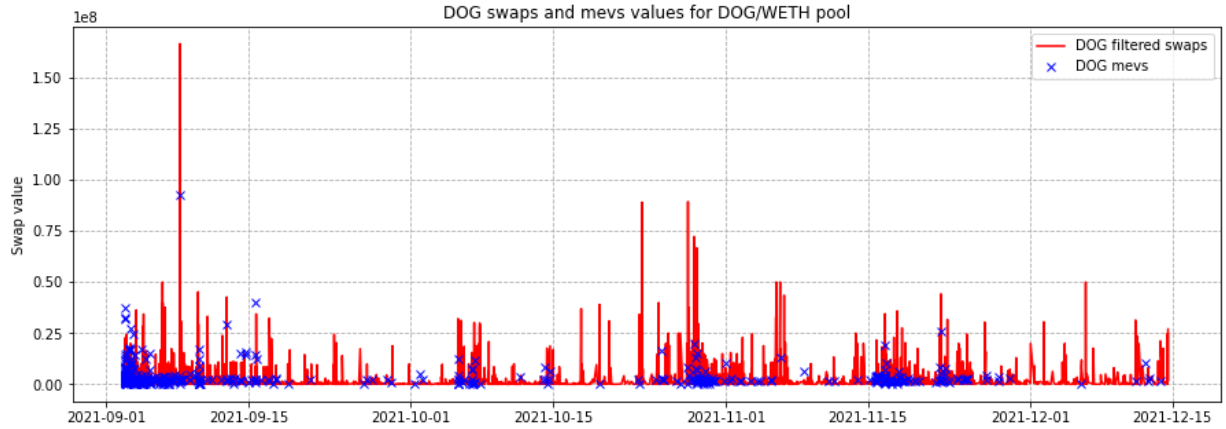
Picture X: price impact after each transaction for DOG/WETH pool

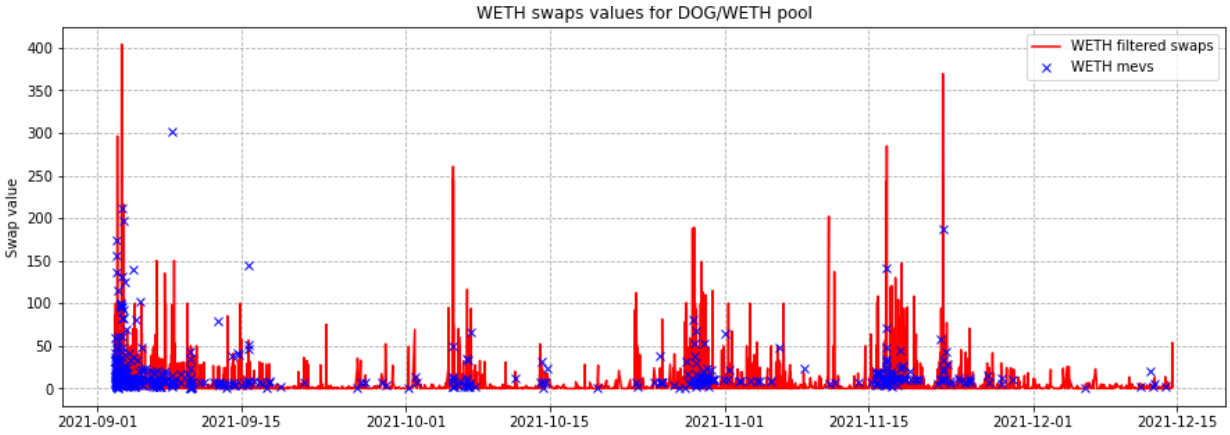
Mitigation mechanism stabilizes prices but has almost no effect on the pool reserves, meaning that the general picture is unchangeable.



Picture X: reserves with enabled/disabled volatility mitigation for DOG/WETH pool

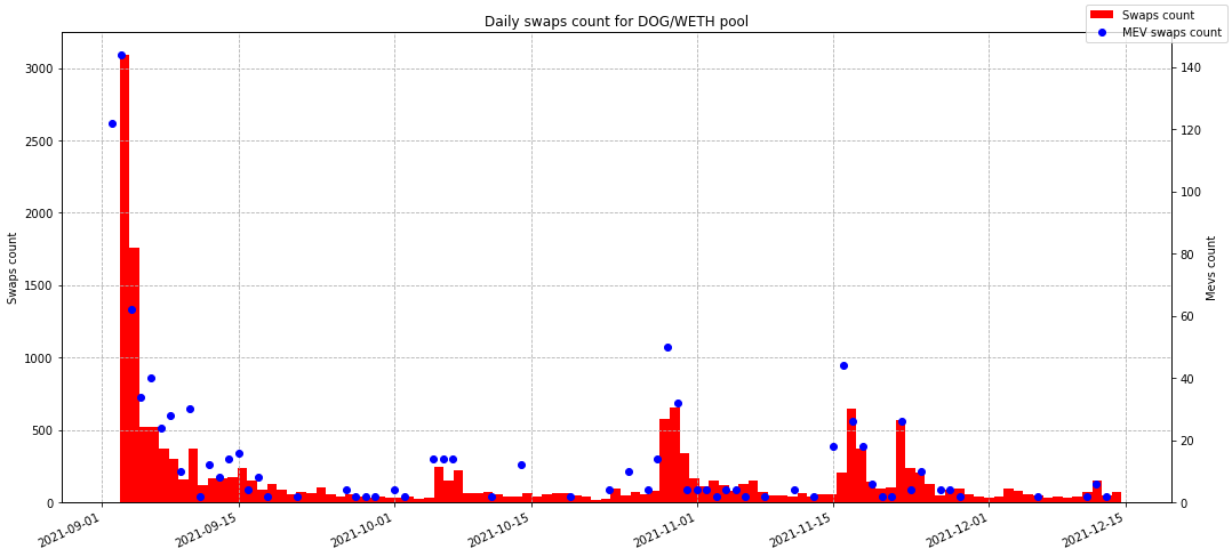
Out of 18560 transactions in the pool there are 564 MEV “sandwich” attacks. They are performed during higher activity periods and bigger transaction values.





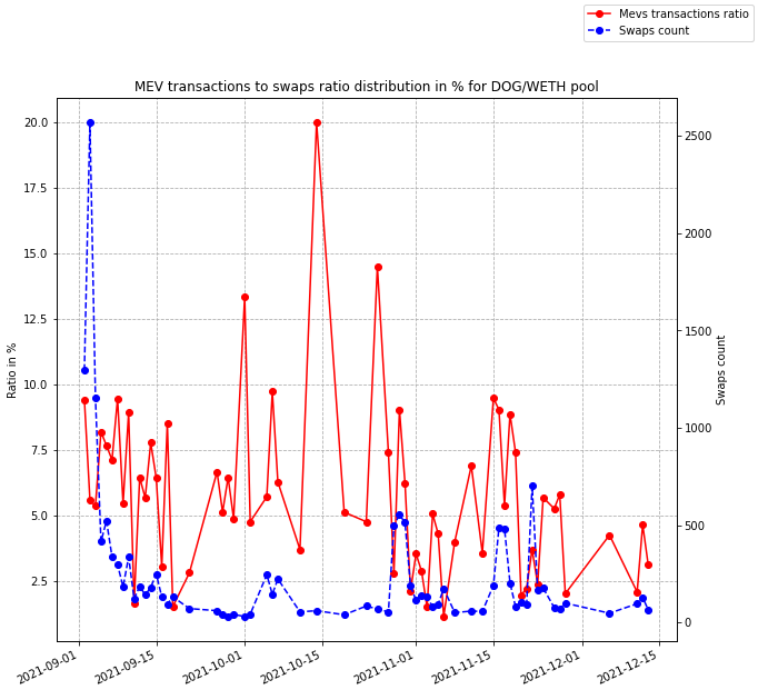
Picture X: transaction values with MEV transactions values

On the presented charts can be seen the connection of higher transaction values with MEV activity and MEV transactions values. To ensure connection between the amount of MEV attacks and transactions frequency below is presented count distributions.



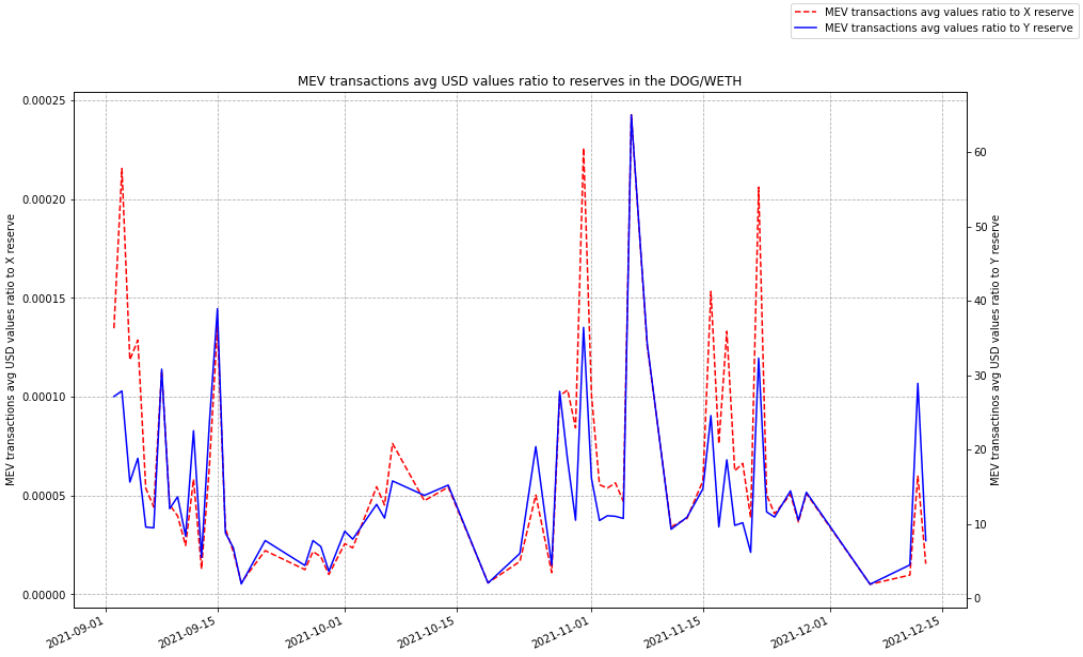
Picture X: swap transactions and MEV transactions count daily for DOG/WETH pool

There is a correlation between amount of swaps and amount of MEV attacks without direct dependency referring to the unstable and unpredictable behavior of the MEV transactions daily count to swap-transactions daily count ratio.



Picture X: MEV-transactions count to reserves ratio in the DOG/WETH pool

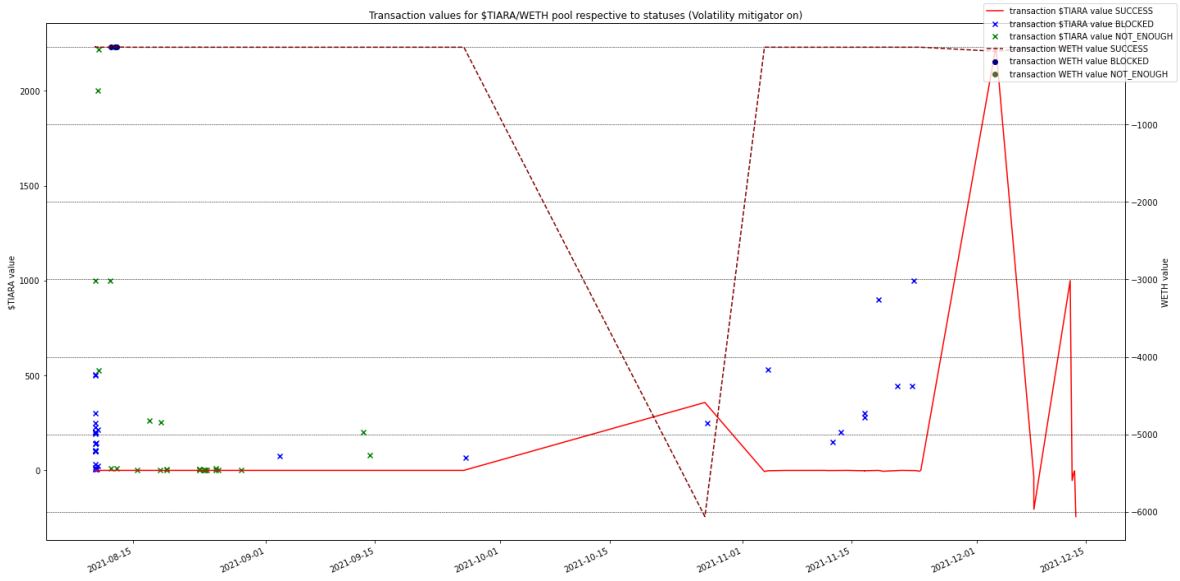
MEV transaction values are rising with bigger reserves in the pool, considering that for performing an efficient MEV attack there should be bigger transaction values to cause high enough price impact to extract profit out of the victim's transaction.



Picture X: MEV transaction avg values in USD to reserves ratio for DOG/WETH pool

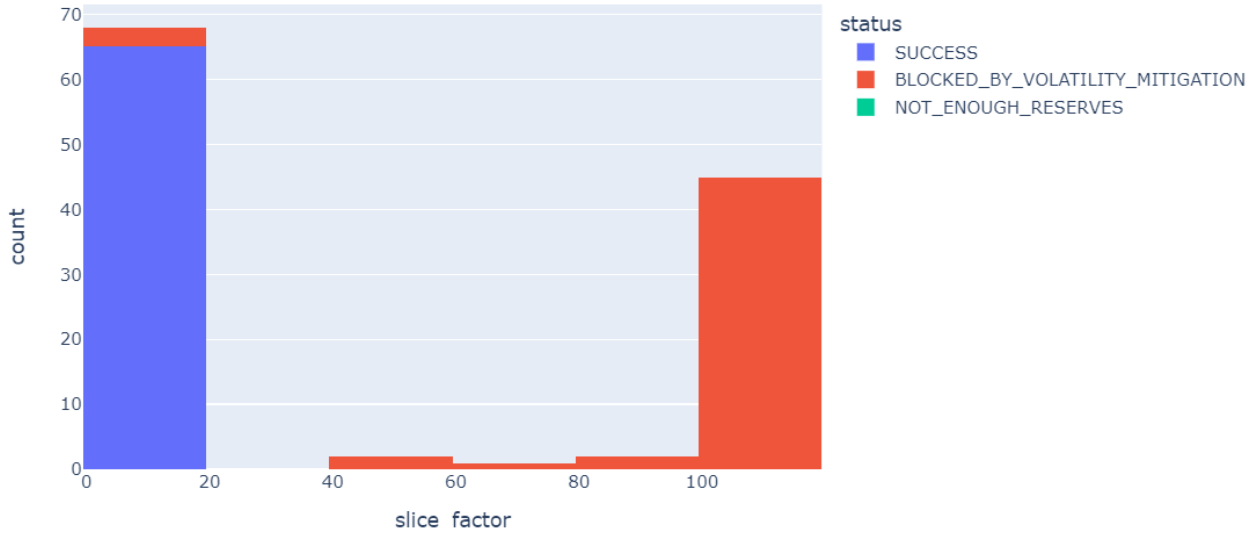
$TIARA / WETH (fractionalized NFT)

While the DOG/WETH pool contained a rich transaction history with a great overall picture, the current case is worse from all perspectives.



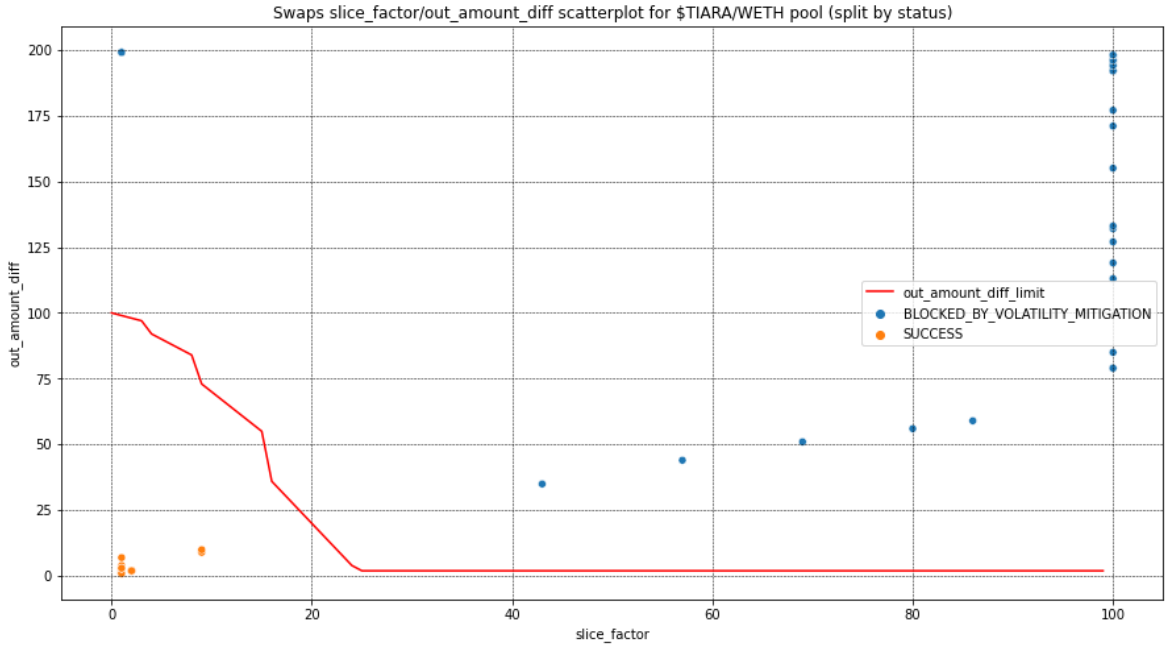
Picture X: transaction values distribution by type

The presented distribution has one-side activity demonstrating exchange of only $TIARA tokens to get WETH tokens. Traders are interested in extracting WETH token out of the pool. Blocked transactions ratio is much higher compared to the previous case: out of 180 transactions 53 were blocked by a volatility mitigation mechanism.



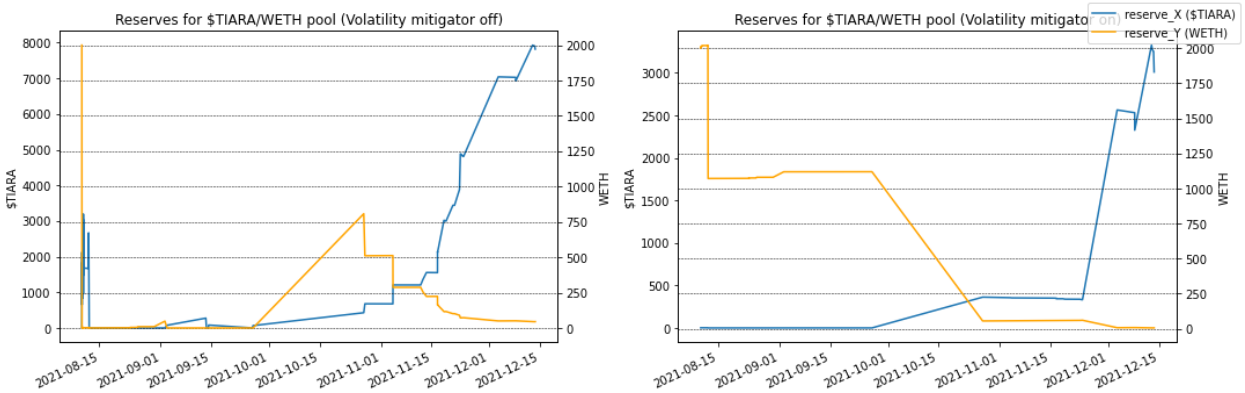
Picture X: slice factor distribution by transaction type for $TIARA/WETH pool

Compared to the previous case there are many transactions with slice factor bigger than previously mentioned 20% threshold value of slice factor, which is greatly seen on the chart below.



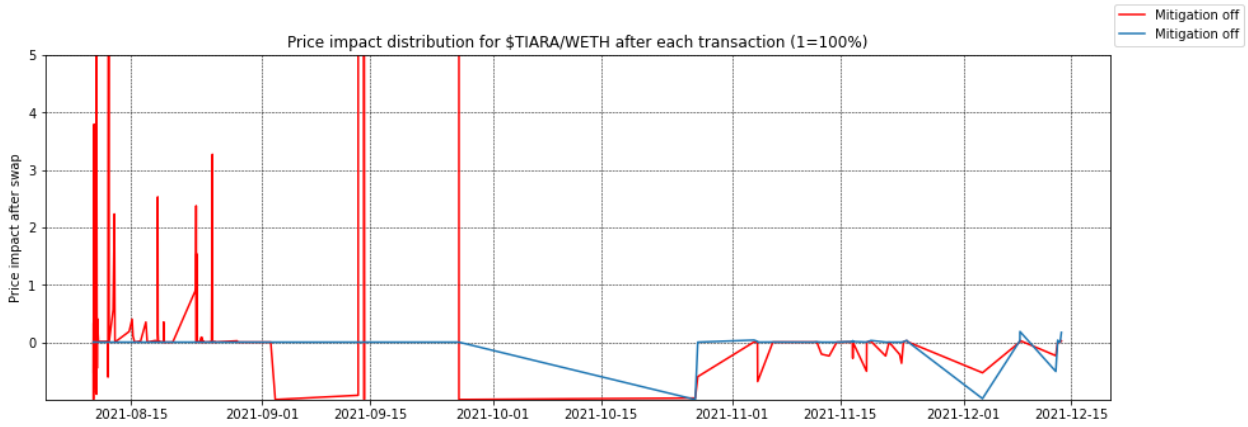
Picture X: swap slice factor and out amount difference distribution for $TIARA/WETH pool

Mitigated reserves distribution differs from non-mitigated one and it is difficult to estimate if influence was positive. Both distributions are presented below.



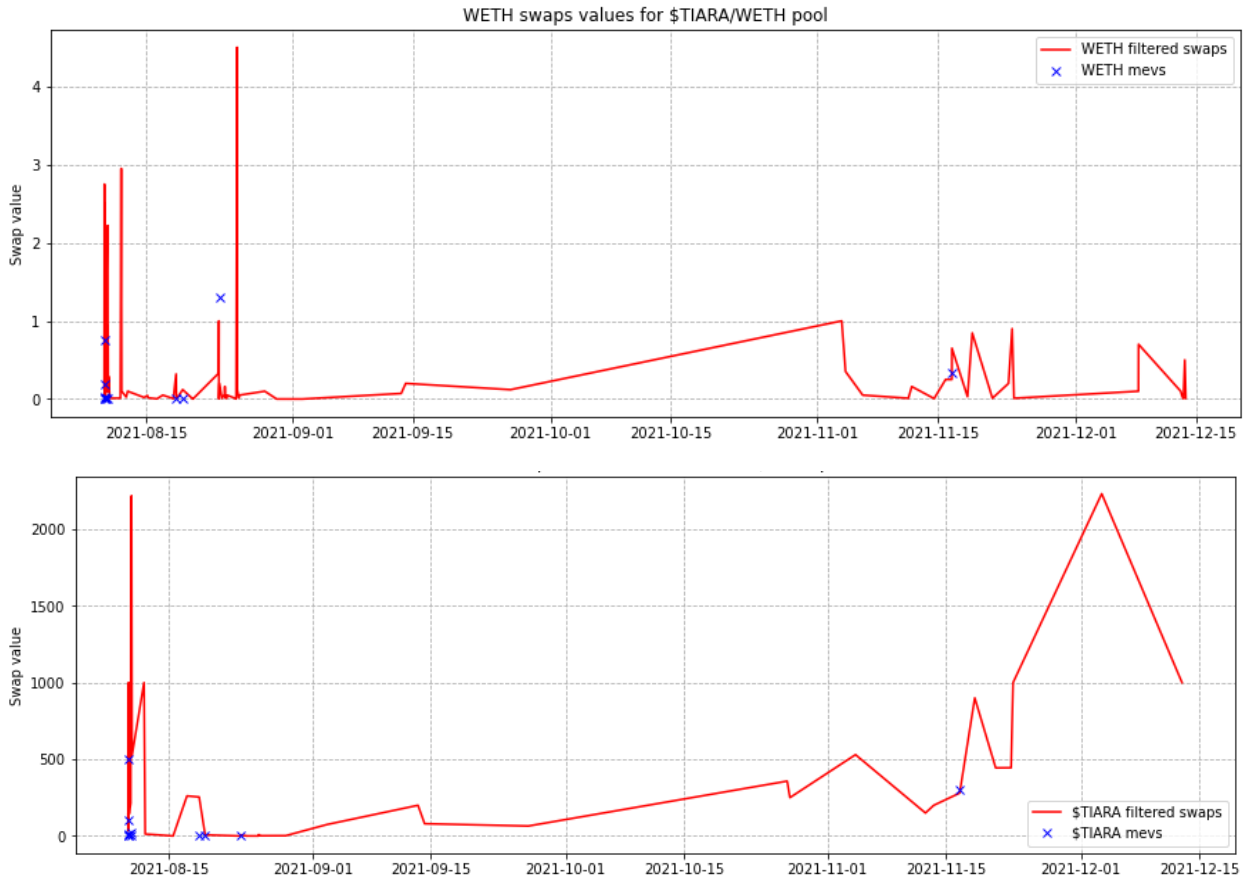
Picture X: reserves with enabled/disabled volatility mitigation

While in the previous case mitigation mechanism stabilized price distribution, in the current pool mitigation mechanism almost flatlines the distribution. Blocked transactions caused extreme price changes and therefore filtered transactions reduce price deviations.



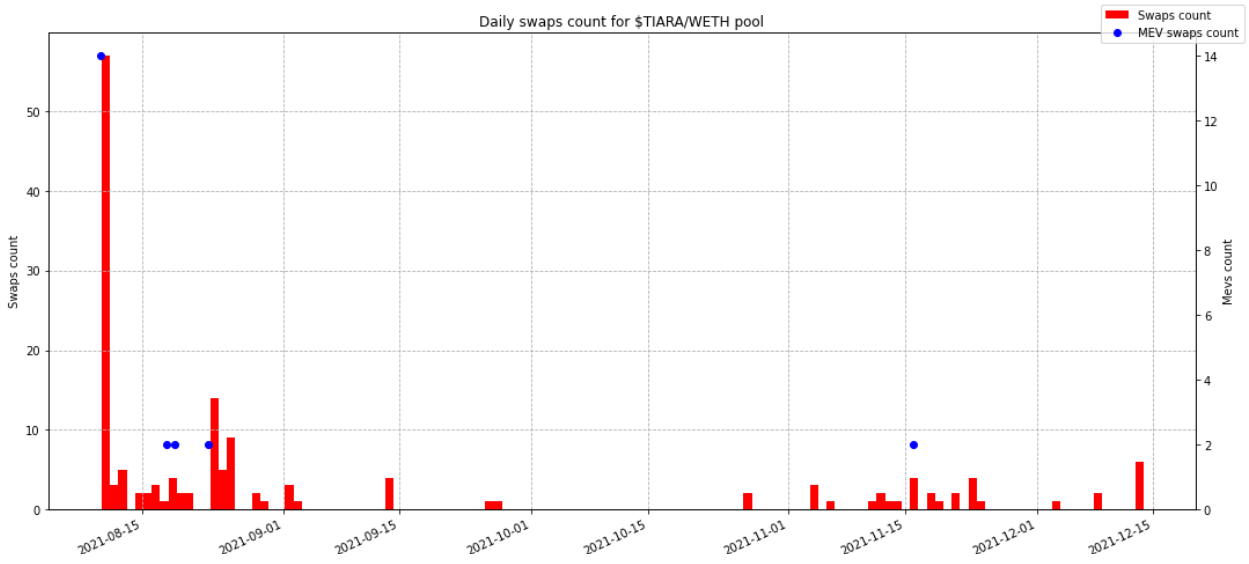
Picture X: price impact distribution for $TIARA/WETH pool

Most of the MEV transactions are located in the beginning of the pool lifecycle and they appear during rises of the swaps activity and are not much bigger than simple swaps.



Picture X: WETH and $TIARA swaps values distributions for TIARA/WETH pool

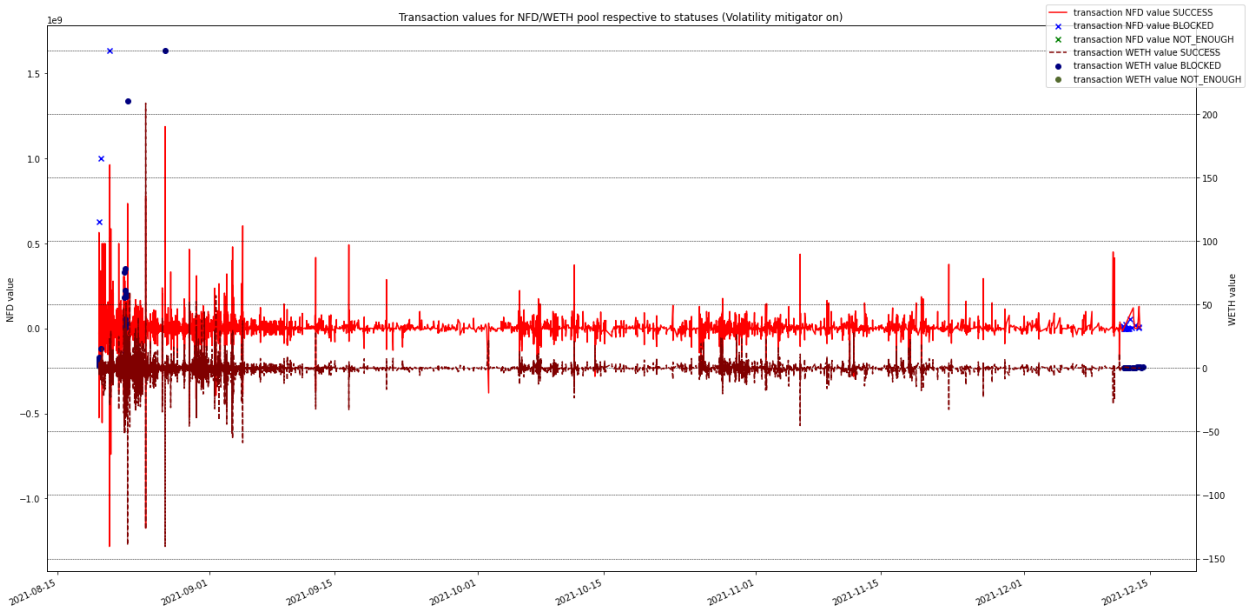
Amount of MEV attacks is higher during the rise of the swaps activity which can be seen on the distributions presented below.



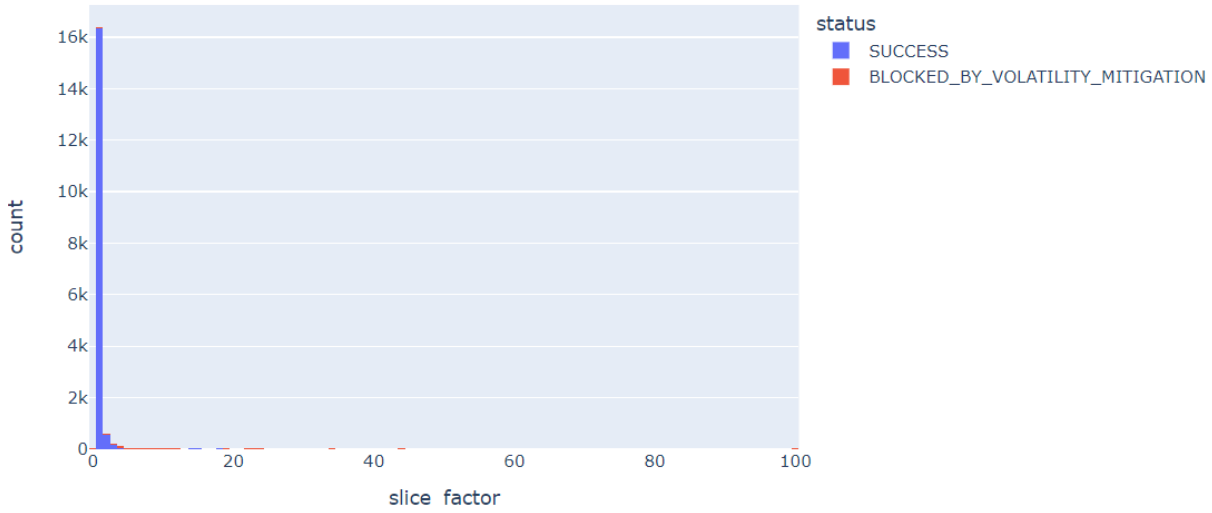
Picture X: swaps and MEV transactions count distributions

NFD / WETH (fractionalized NFT)

Pool demonstrates bi-directional token exchange with unstable behavior, where higher transaction values were registered in the beginning of the pool lifecycle. Blocked transactions are registered in the beginning and in the end of the end of the reviewed time period.

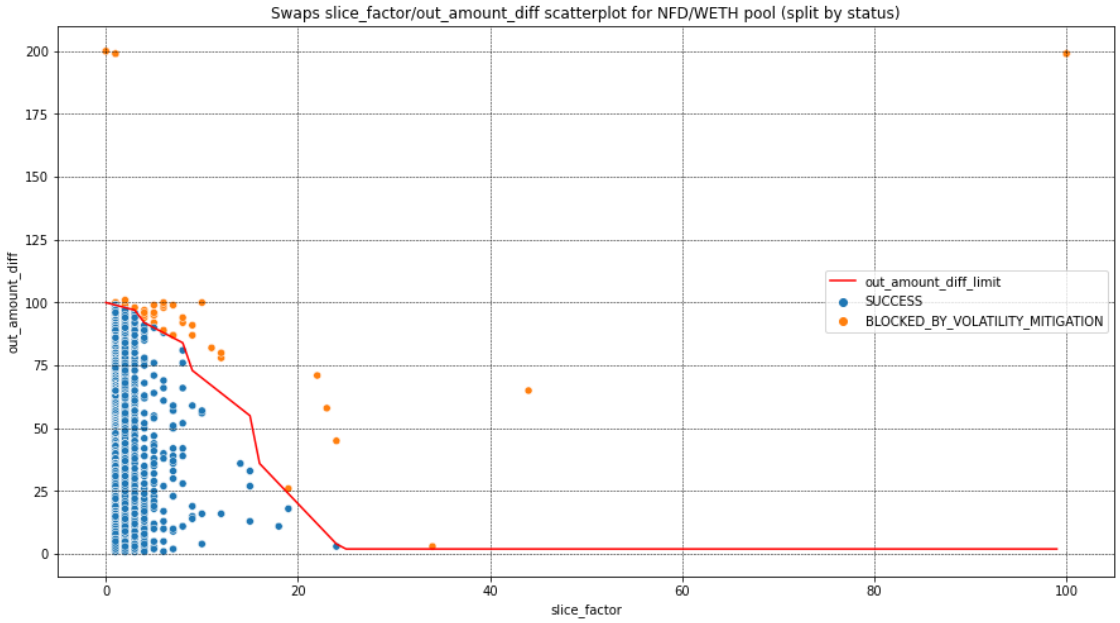


Picture X: transaction values distribution by type



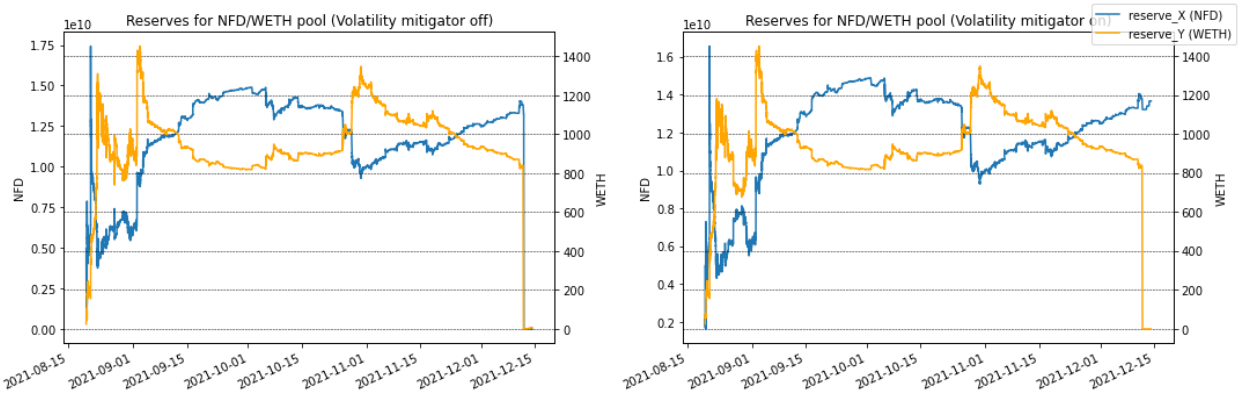
Picture X: slice factor distribution for NFD/WETH pool (split by transaction status)

Blocked transactions contain extremely high slice factor values, meaning that those transactions created instability and high deviation of tokens prices, which is similar to the pattern of the MEV "sandwich" attacks.



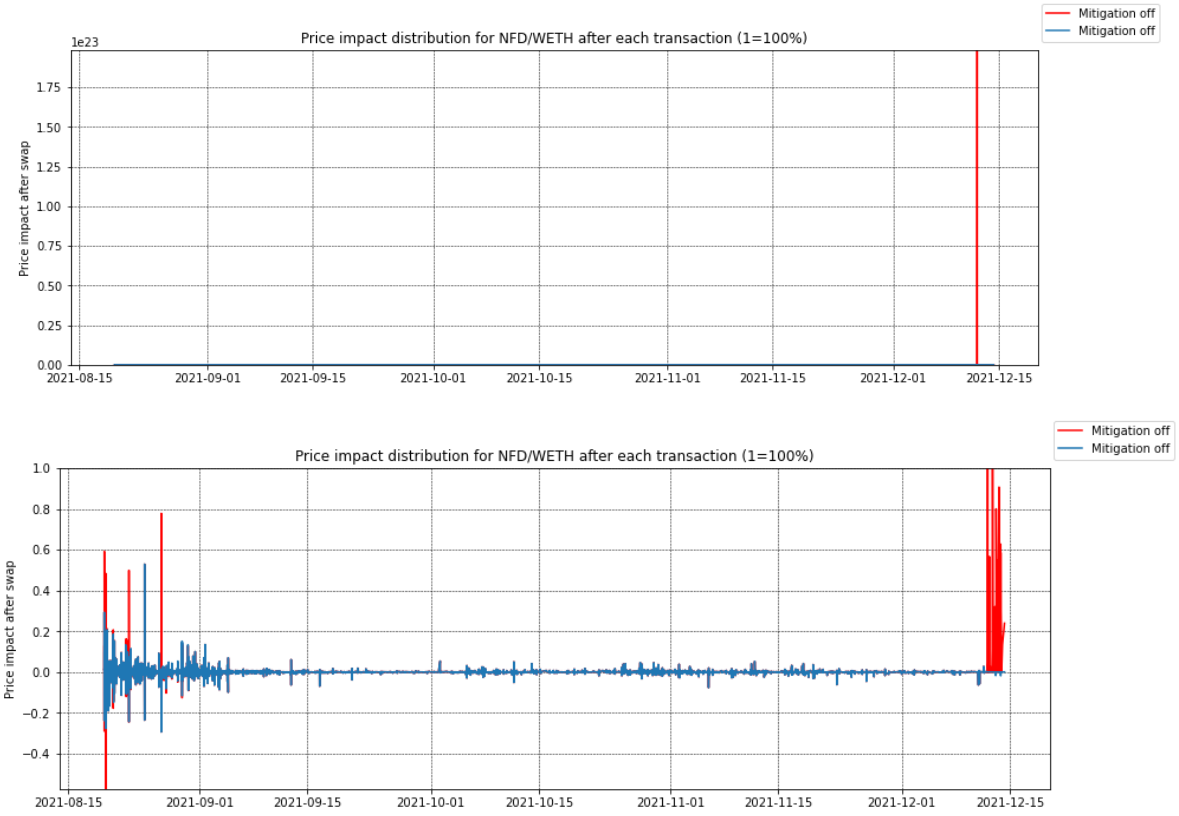
Picture X: swap slice factor and out amount difference distribution

Most of the accepted transactions are located on a slice factor smaller than 10 and out amount difference smaller than 100.



Picture X: reserves distribution with disabled/enabled mitigation mechanism

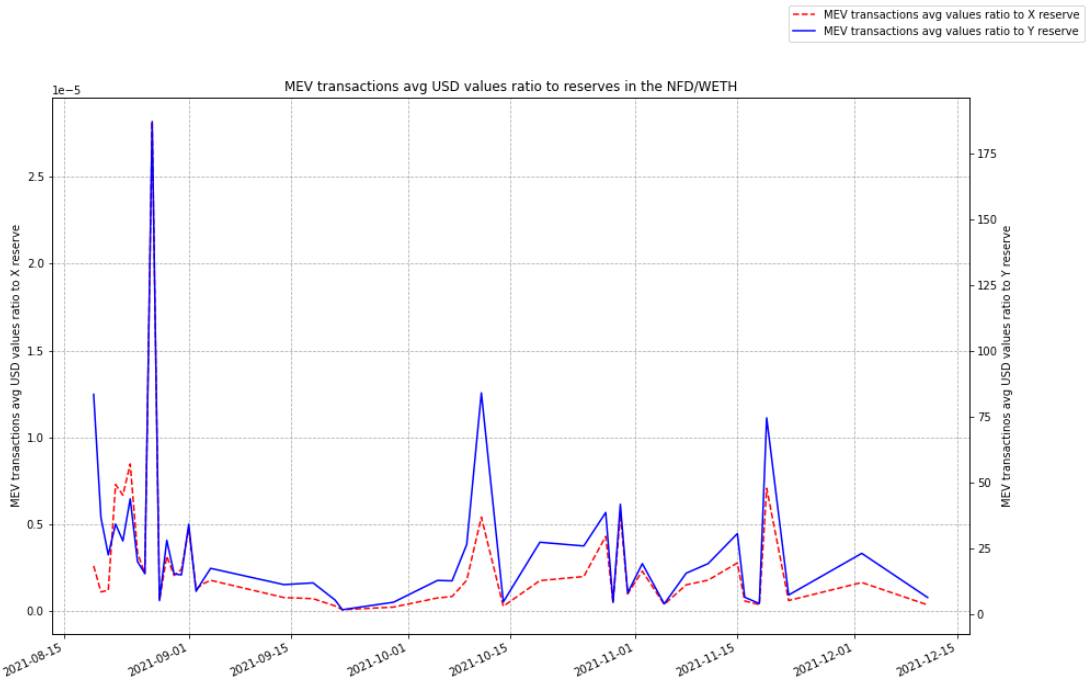
There are two observable changes on the reserves distributions: mitigation removes an extreme drop of the NFD token balance in the end of the reviewed period and decreases deviation of the tokens reserves in the beginning of the reviewed period.



Picture X: price impact after each transaction, first chart covers entire picture, second chart reduces reviewable interval to 100% deviation of tokens prices

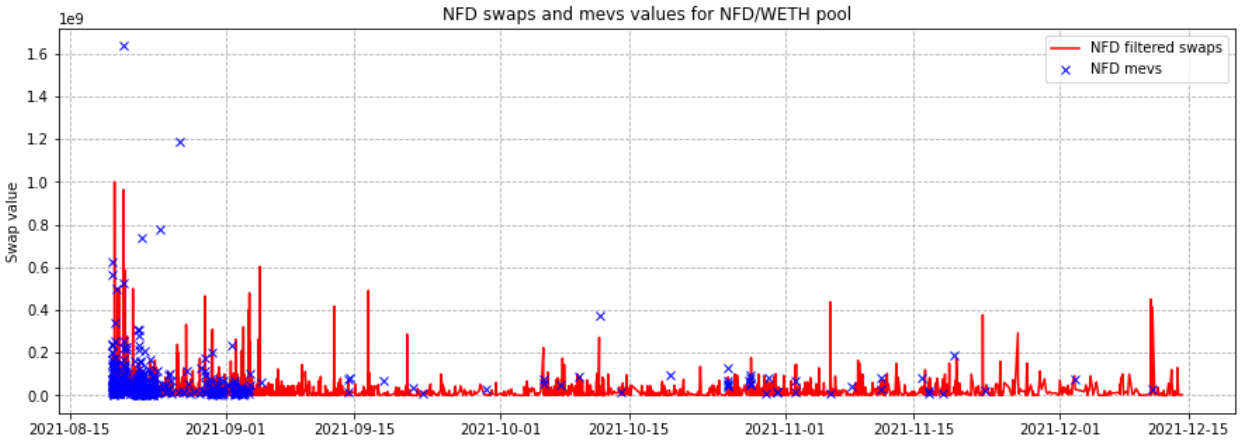
Non-mitigated price impact distribution is extremely unstable and the ending period contains catastrophically bad price impact. In this case mitigation performs price stabilization

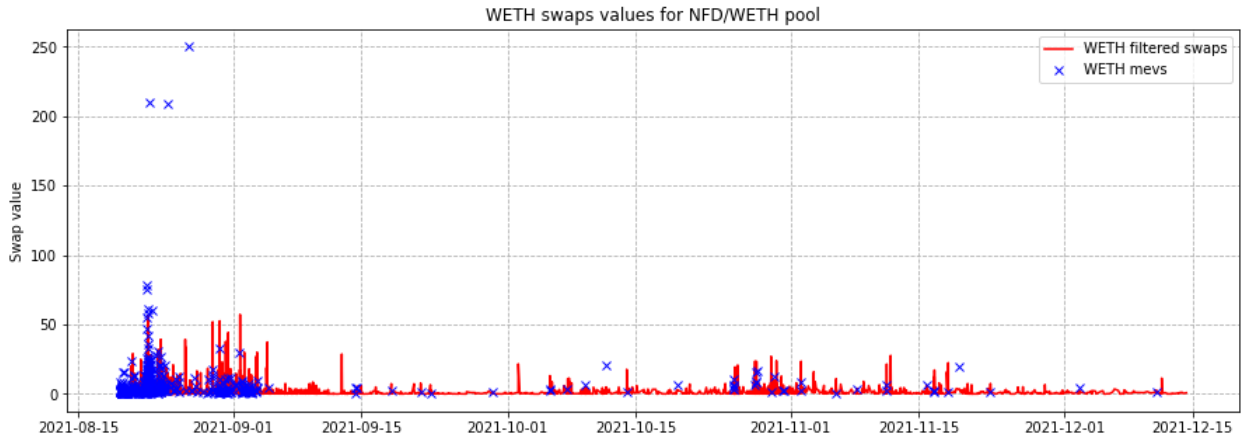
and protects the pool against destructive transactions (destructive from the perspective of lowering traders attention to the pool).



Picture X: MEV transaction USD values respective to the pool reserves

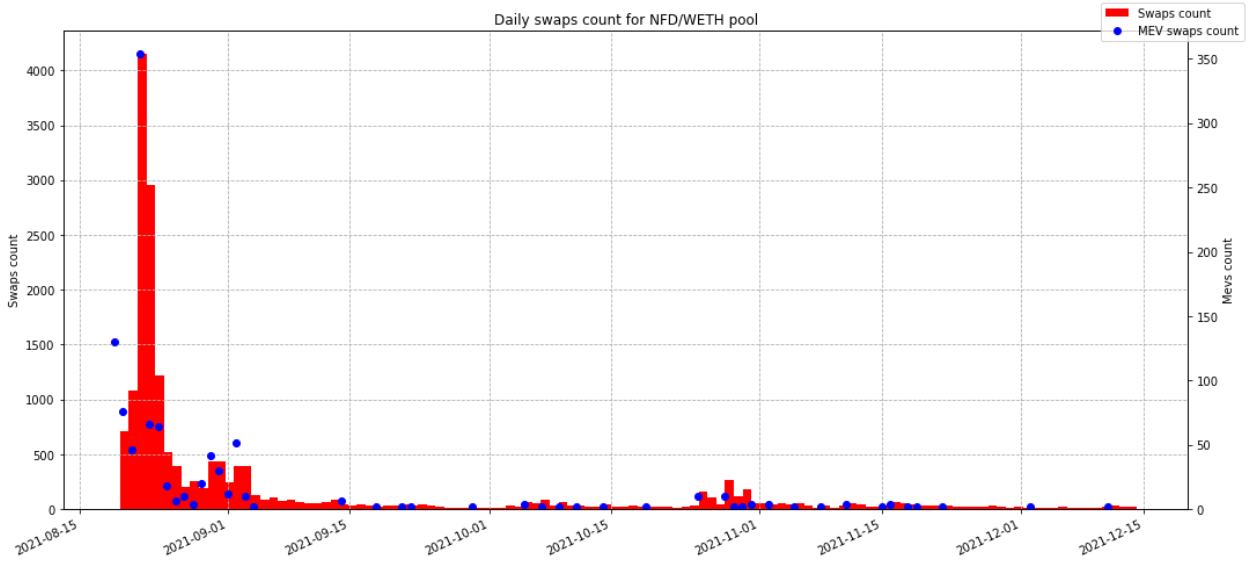
There are 513 MEV attacks performed on the pool, where transaction values correspond with pool reserves distribution. MEV transaction values look extremely high in small amounts of cases, while most of the attacks are performed in acceptable values limits, meaning that attackers perform attacks with smaller price impact and therefore smaller extracted profits. Amount of attacks performed balances the price impact limit for attacks. Attacks are performed more in the beginning of the reviewed time period when swaps activity was higher and MEVs are performed less frequently in the remaining period due to decrease of swaps activity.





Picture X: swaps and MEV transactions values distribution

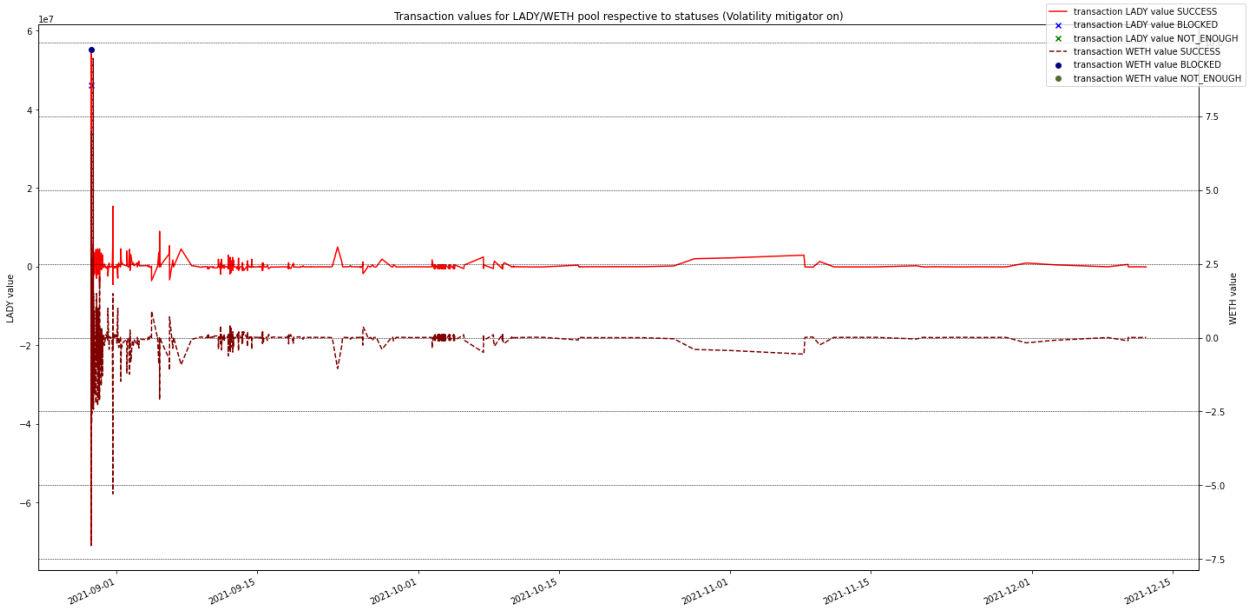
Amount of performed attacks is correlating with amount of swaps performed daily on the reviewed period but dependency between attack count and swaps count is not direct.



Picture X: swaps and MEV transactions daily count distributions

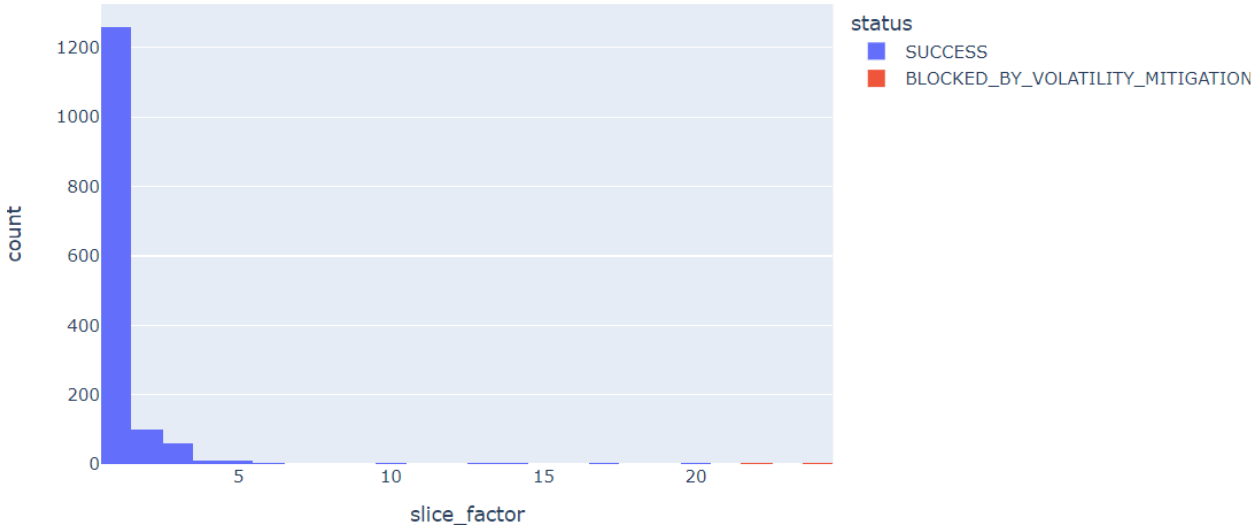
LADY / WETH (fractionalized NFT)

Current pool distribution has bi-directions tokens exchange with drop of the exchanges from the first two weeks of October 2021. There are two blocked transactions by simulation with big transaction values. Considering the reviewed time period size and transaction activity it is questionable whether the pool will become active again.



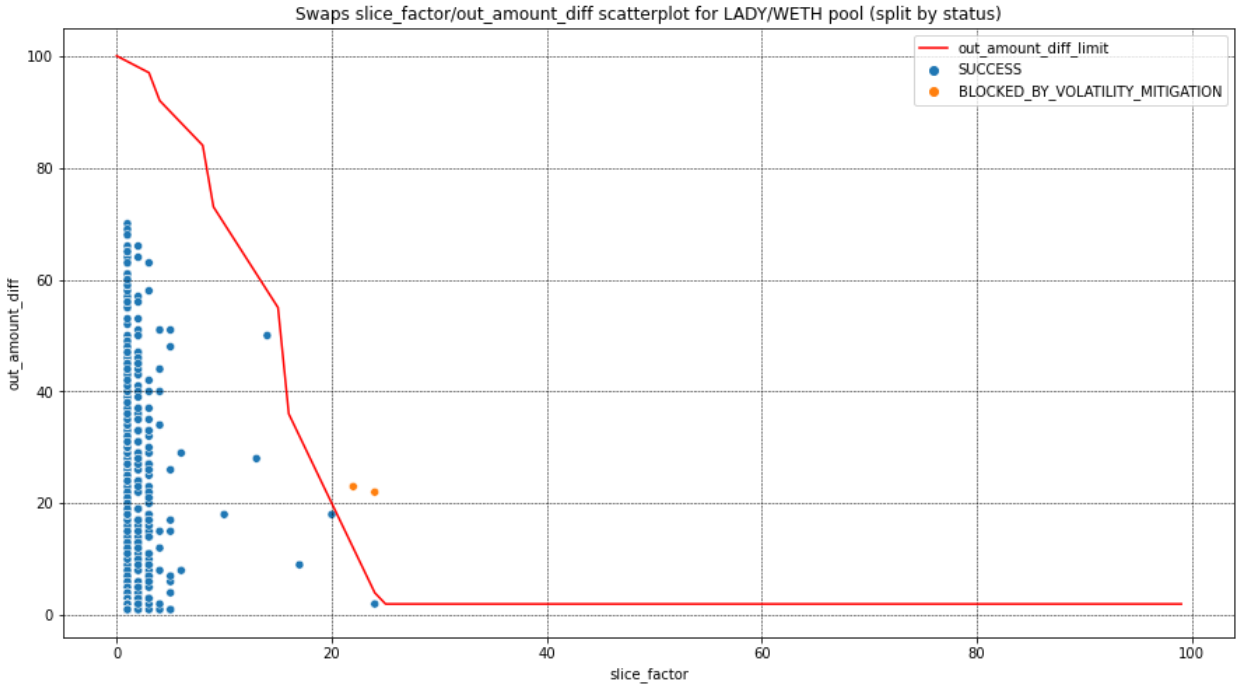
Picture X: transaction values distribution by type

Blocked transactions exceeded the limit in previous cases of the 15-20 threshold value for slice factor, while most transactions have low slice factor and small impact on tokens prices.



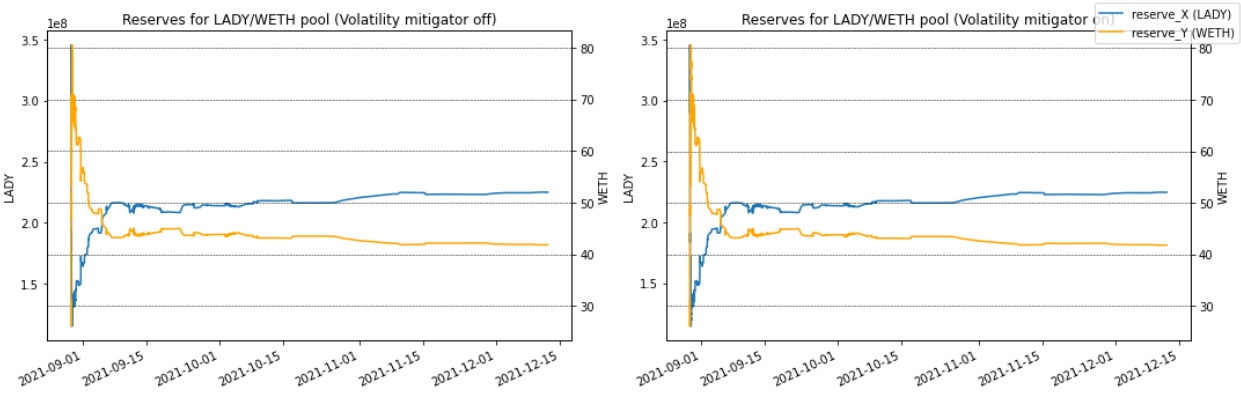
Picture X: slice factor distribution by type

Distribution of transactions by their out amount difference and slice factor demonstrates healthy pool activity and that there should be small tokens prices deviations.



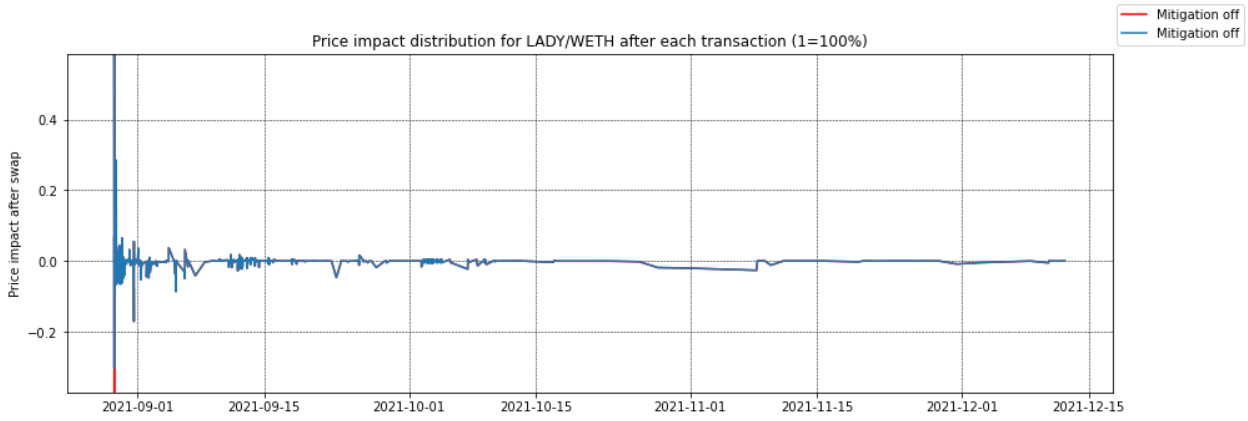
Picture X: swap slice factor and out amount difference distribution

Mitigation mechanism influence on the reserves distribution is unobservable. Reserves distributions are stable with big deviations in the beginning of the shown time period, after which distributions stabilize and activity extremely reduces.



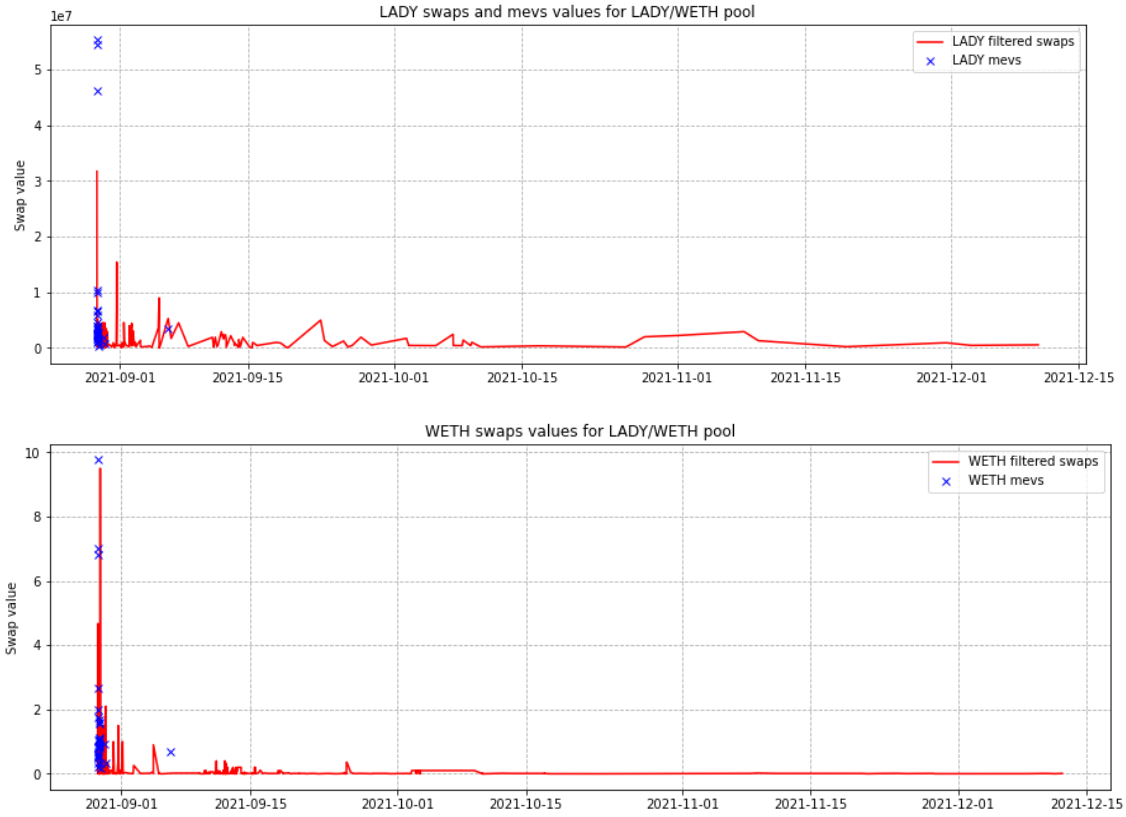
Picture X: reserves distribution with disabled/enabled mitigation mechanism

Mitigation mechanism stabilizes tokens prices, reducing extreme deviation, while the overall picture demonstrates tokens prices deviation around 15-40% of price deviation in the start of the reviewed time period and around 5% price deviation after the first week of September 2021.



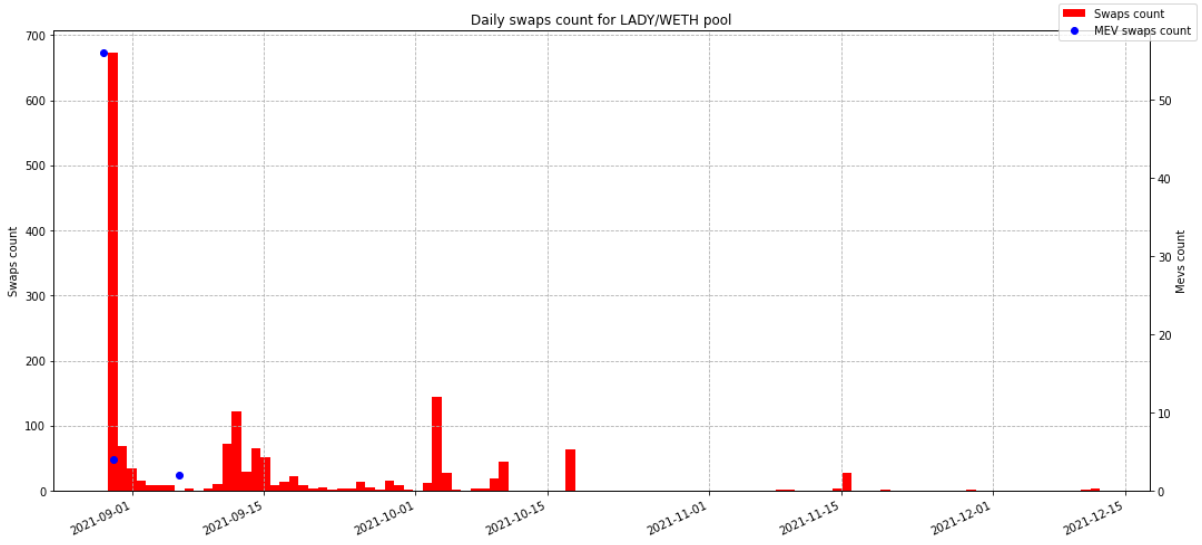
Picture X: price impact after each transaction

MEV transactions were concentrated in the beginning of the pool lifecycle while traders activity was high. Drop of traders activity caused loss of attackers interest in the pool, due to smaller possibility of extracting profit out of market manipulations. It is possible that traders' activity drop was caused by attackers' activity, reducing pool attractiveness.



Picture X: swaps and MEV transactions values distribution

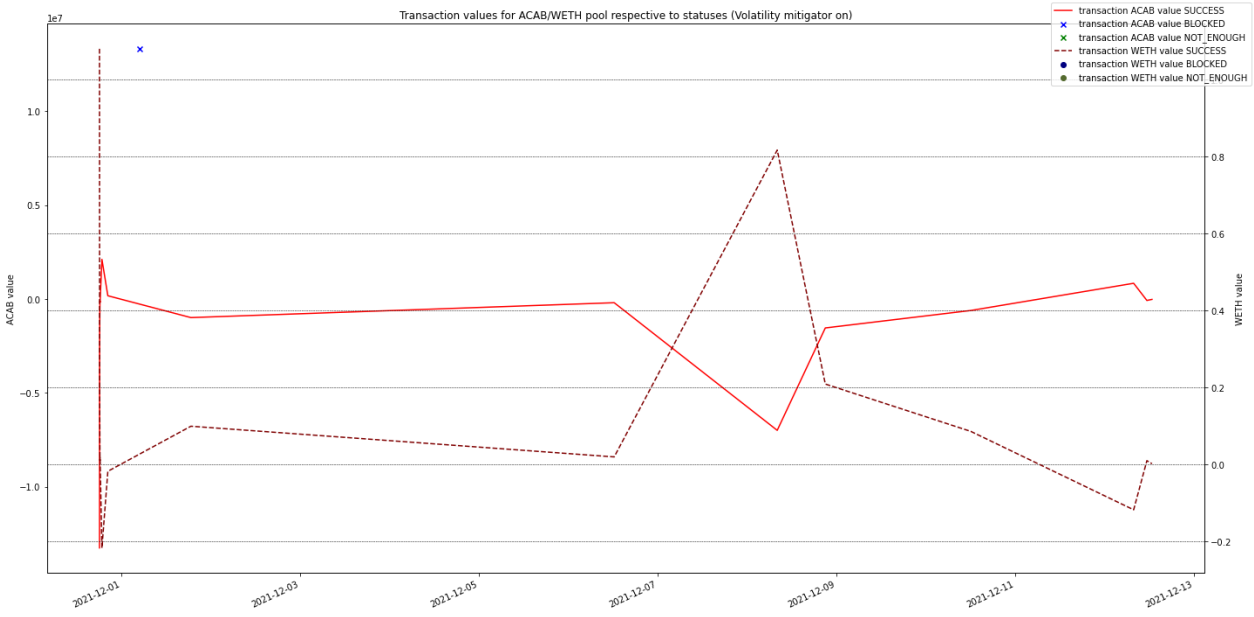
Swaps and MEV transactions count distributions demonstrate that there is a correlation between traders activity and amount of performed attacks.



Picture X: swaps and MEV transaction daily count distributions

CAT / WETH and ACAB / WETH dead pools (fractionalized NFT)

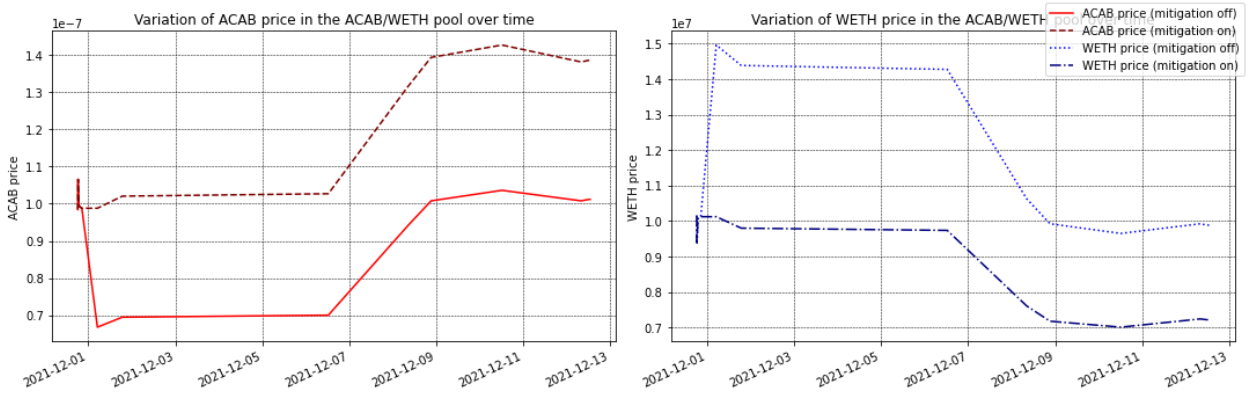
ACAB/WETH and CAT/WETH have a small transaction history without any MEV attacks present in the distribution. The reason is that those pools contain small activity meaning that for performing MEV “sandwich” it is hard to put the victim's transaction between market manipulative transactions.



Picture X: Transaction values in ACAB/WETH pool

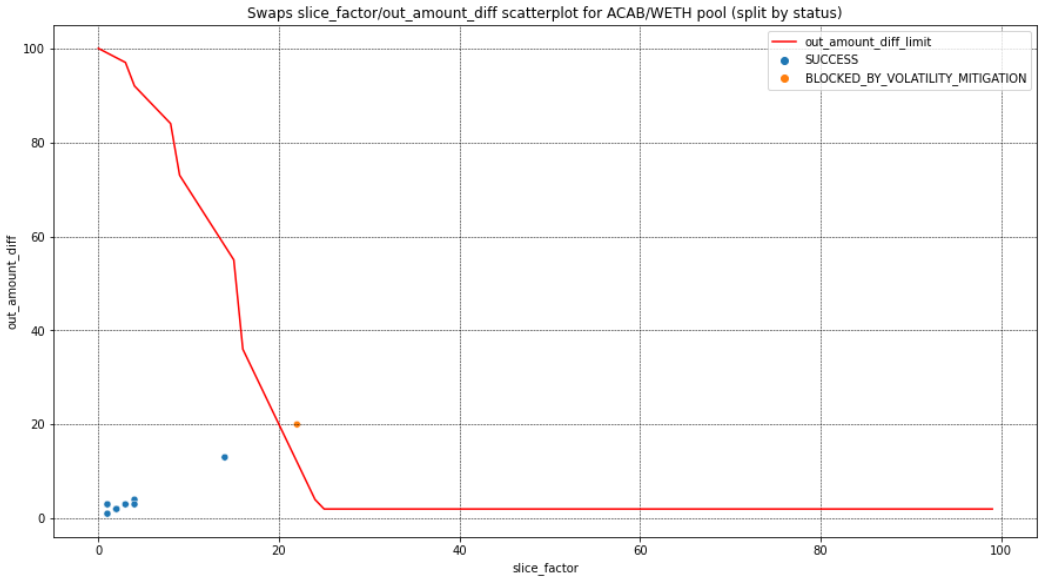
Simulation has a convex shape meaning that there is a bidirectional trading inside ACAB/WETH pool and both tokens are used by traders, but the amount of present activity is

small even considering the small time taken. Pool is able to get a better distribution in case of some changes with pool or changes in ACAB token popularity. But even in this case the mitigation mechanism was able to smooth tokens prices distributions.



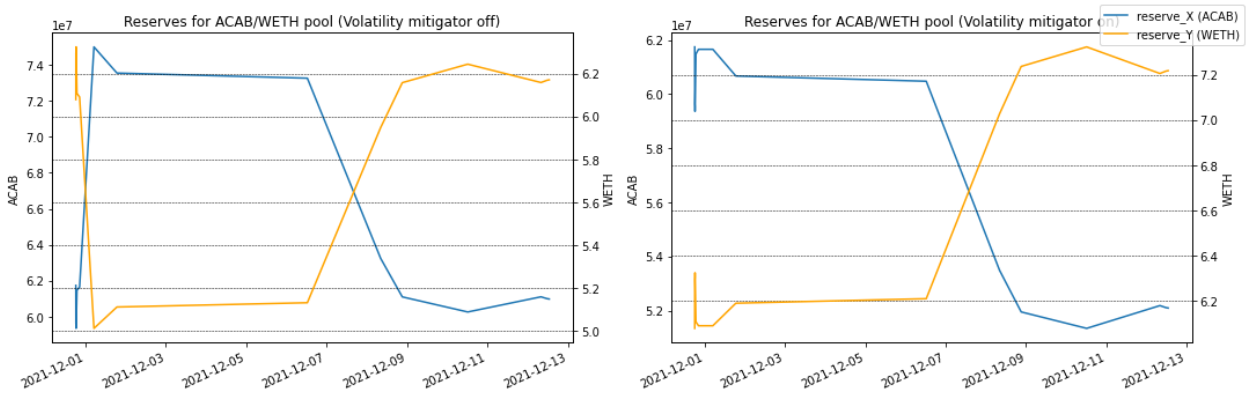
Picture X: ACAB and WETH tokens prices distributions in ACAB/WETH pool

Mitigation mechanism is able to protect the pool even in case of small present activity.



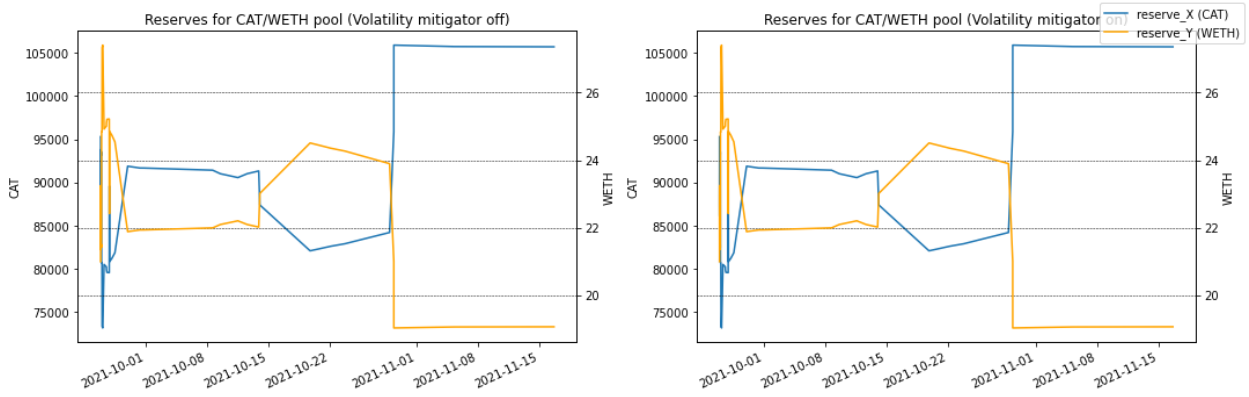
Picture X: swap slice factor and out amount difference distribution

Possible reason is that the current pool contains low reserves. With disabled mitigation WETH token reserves range is between 5-6.2 tokens and with enabled mitigation WETH token reserves range between 6.2-7.2 tokens, which transformed into USD equivalent (is suggested that WETH token price is equal to 4000 US dollars) means that pool has reserves between 20000-28000 US dollars for WETH side. All previous cases of fractionalized NFTs had big reserves available in the pool, raising the attractiveness of the pool.

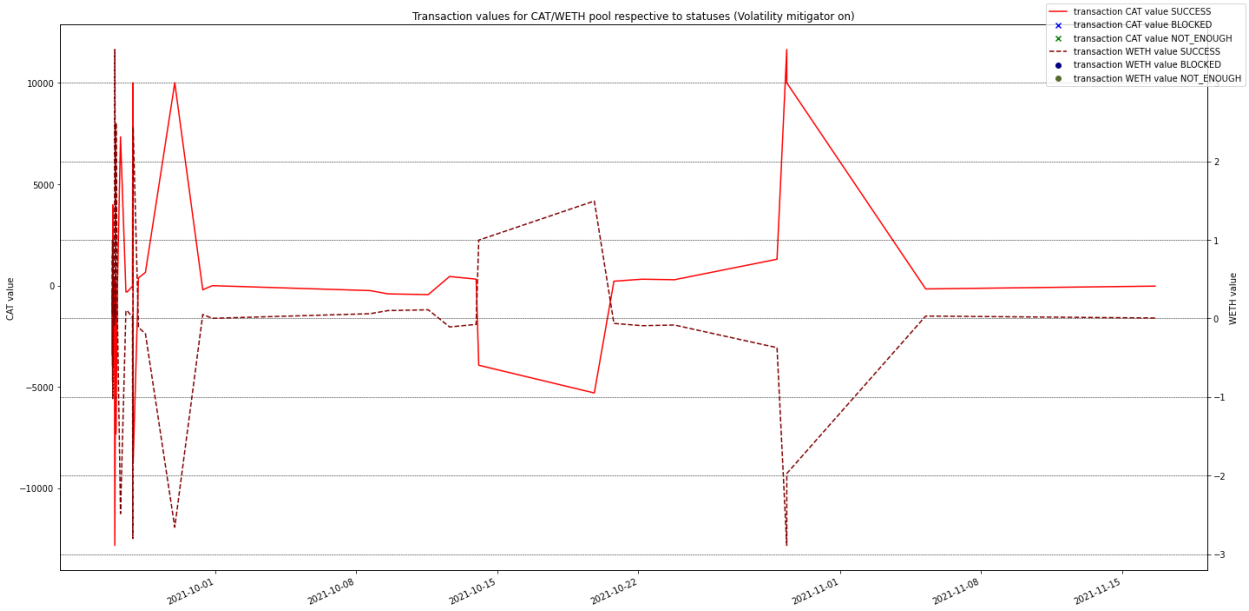


Picture X: reserves distribution with disabled/enabled mitigation mechanism

It is possible to suggest that fractionalized NFT pool popularity depends on the available reserves in the pool, but the case of LADY/WETH demonstrates that with relatively high reserves and high transaction frequency in the beginning pool has come to low activity. CAT/WETH pool also is the case of relatively high reserves (smaller than LADY/WETH ones) but activity is a little better compared to ACAB/WETH case, which is also questionable, considering that CAT/WETH transaction count and taken time period are both 3 times bigger than ACAB/WETH case.

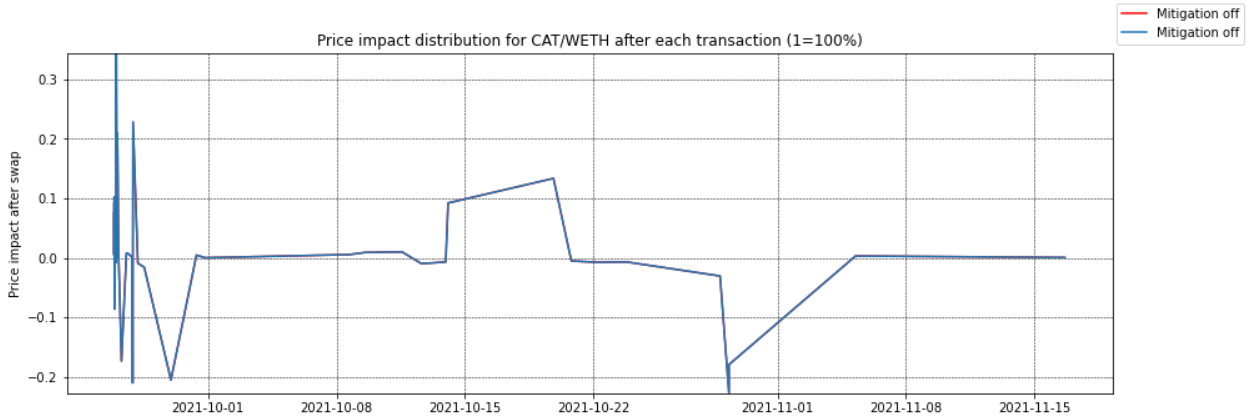


Token exchange distribution is convex, meaning bidirectional tokens exchange. Both tokens in the CAT/WETH pool are interesting for traders and the pool contains healthy behavior represented below. Mitigation mechanism has not blocked any transaction.



Picture X: Transaction values in CAT/WETH pool

Token prices change distribution is stable with high deviation only in the beginning of the reviewable time period.



Picture X: token prices impact after each transaction distribution

MEV attacks analysis

During analysis of the pools containing fractionalized NFTs it was discovered that there were many suspicious transactions looking like MEV attacks. Suspicious transactions are divided in two categories:

- Transactions with the same incoming and outgoing from the pool values present in one block while total transactions is the block count to 3 or more;

- Transactions with difference between incoming and outgoing values smaller than 5% present in one block while total transactions in the block count to 3 or more.

The principle of considering transactions suspicious is to check that they form a “MEV sandwich” - specific block sequence, when one address manipulates token prices inside of only one block to extract profit out of the victim's losses and then performs a backward transaction to the first one, moving token prices back to the original values. This principle causes extreme decrease/increase of the token prices in the pool due to price regulation structure of AMM with losses from the victim’s side due to exchange of tokens with unexpected price, causing another profitable for attacker token price change. Attacker’s profit rises with rise of the transaction value for attack. Attacker’s profit can also rise with the rise of the victim's exchange values, meaning that the victim's transaction defines how positive for the attacker the price change (detailed description of the MEV attack was demonstrated previously).

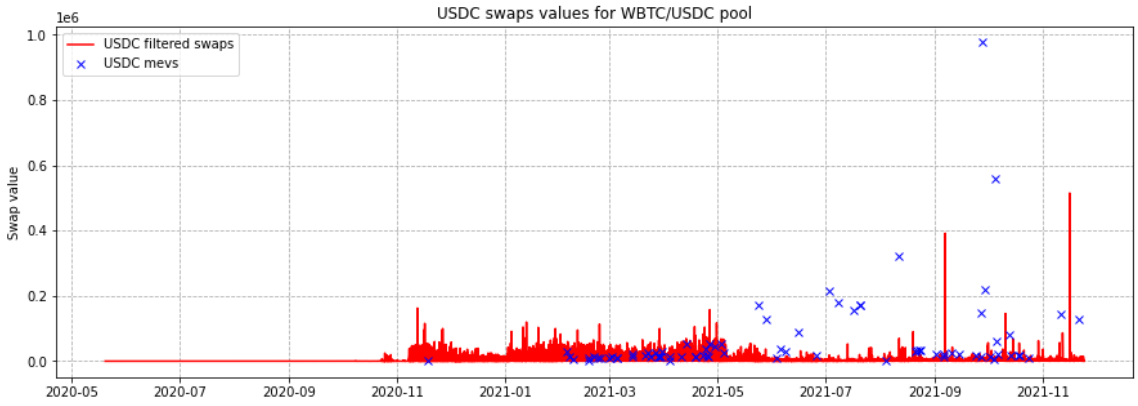
Fractionalized NFT pools had more MEVs compared to previous pool cases. Higher MEV activity caused interest in performing the same MEV analysis for previous pools to define either this is a property of the NFT-related pools, or specifics of the platform where those transactions were performed (Sushiswap platform). The analysis will be performed using simulations, considering that it provides additional information that can be useful.

WBTC/USDC simulation

Results of performing the simulation:

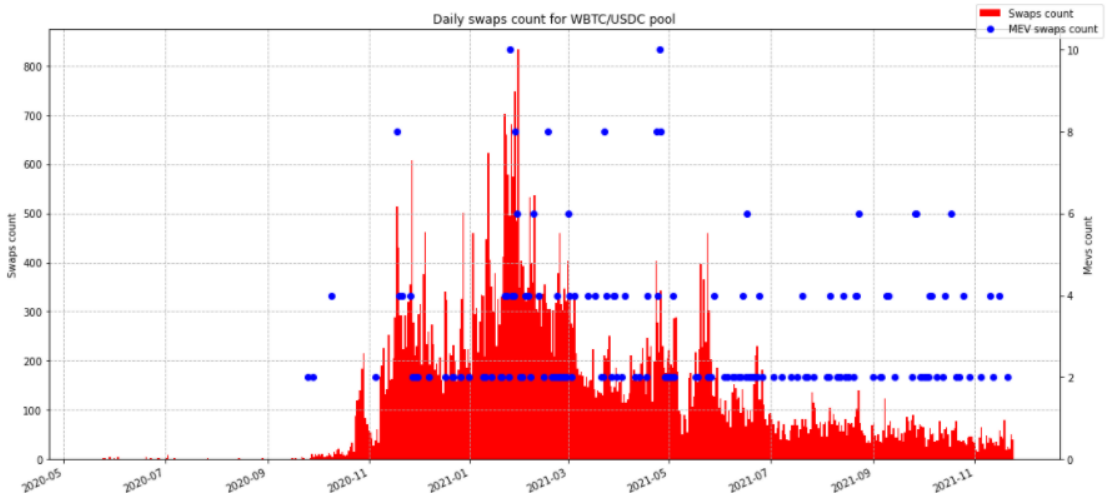
- **Transaction history size** - 68197 transactions;
- **Blocked by Volatility Mitigation** - 7;
- **Possible MEV attacks with the same values** - 77 attacks with 154 MEV-related transactions;
- **Possible MEV attacks with <5% values difference** - 230 attacks with 460 MEV-related transactions.

Distribution of the transaction values separating simple and suspicious transactions demonstrates that possible MEV attacks either have extremely high values or have values similar to the simple ones. The first category looks like a possible MEV attack, considering that transactions of this type will cause heavy price impact and therefore profit extraction out of the attackers activity. Differences between those two transaction categories are visible in the distribution below.



Picture X: transaction values distribution for WBTC/USDC pool

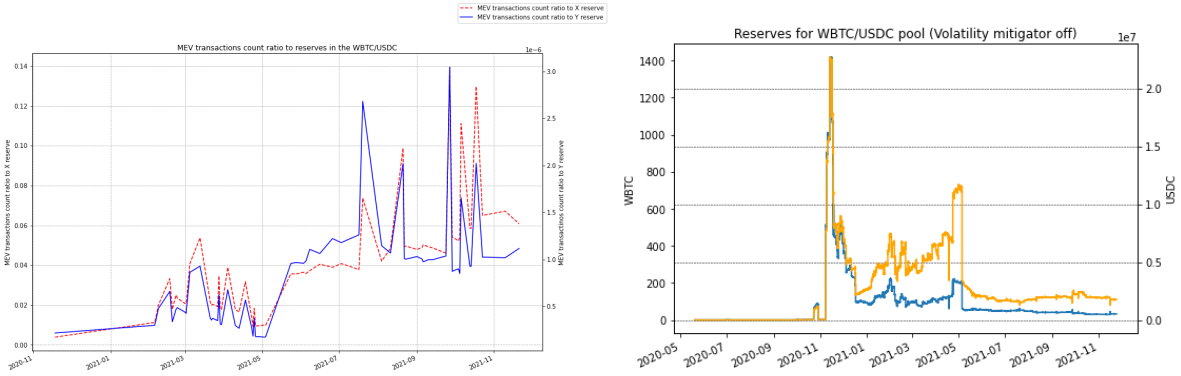
Suspicious transactions forming a “sandwich” with a difference smaller than 5% have higher frequency with much bigger count of transactions around smaller values and small value of additional cases with high values. Before November 2020 there was almost no activity present in the pool and during this low activity period there was no MEV activity present in the pool. When activity in the pool increased, MEV attacks and this caused interest in checking connection between pool activity and MEV activity.



Picture X: simple transactions and MEV transactions count distribution for WBTC/USDC pool

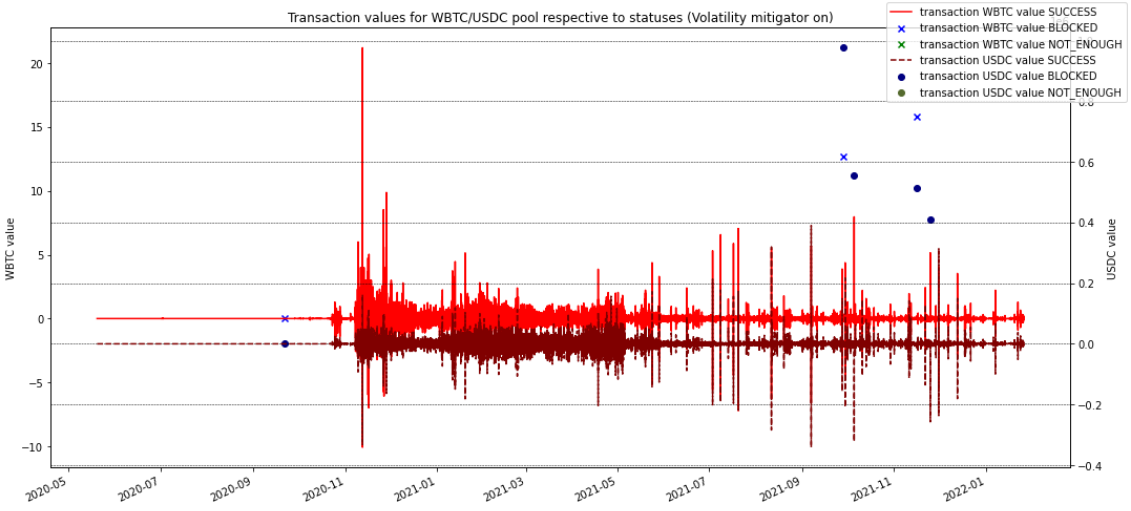
MEV activity is a little higher during high activity periods, but the amount of attacks is too low to be sure about some connection between pool activity and amount of attacks. There is a connection of MEV attacks not only with transaction activity of the pool, but also between the amount of attacks and reserves distributions of the pool. Before breaking an extremely low reserves limit of the pool there were no attacks present, while after reserves rise appeared a MEV activity. Attackers may be interested in extracting values only if there are tokens to extract. The

only way to be sure that there will be tokens to extract - there are high reserves present in the pool. The only limitation of this approach - with higher reserves values MEV attacks require higher financial power from attackers.



Picture X: MEV transactions count to reserves ratio and reserves distribution (blue - WBTC, yellow - USDC)

Volatility mitigation blocked only 3 transactions out of 77 MEV attacks. Blocked transactions had extremely high incoming values, meaning that the mitigation mechanism pays attention to price manipulative transactions (with high values). While MEV transactions have values smaller than specific threshold, which depends on current reserves, they are undetectable for mitigation mechanisms (demonstrated on the chart below).



Picture X: WBTC/USDC swaps values distribution with separation by type

Mean value of MEVs with exact values match is around 62 thousands USD, while mean value of MEVs with small value differences is around 33 thousands USD, meaning that exact matches in this case show more likely real MEV attacks. Some addresses have been seen in other

pools and at the end of this chapter it will be required to check the total amount of performed MEV attacks in reviewed pools and profit extracted by those accounts.

0x00000000008c4fb1c916e0c88fd4cc402d935e7d	52	0x7a250d5630b4cf539739df2c5dacb4c659f2488d	174
0xbfd54d7fb7059d2505069dec2222a81ead7f831a	30	0x00000000008c4fb1c916e0c88fd4cc402d935e7d	52
0xe8024625ac740573a379b290175c33eb72a7c6e5	14	0x66f04911195880984 1bbe4b81c034da2d953aa0c	46
0x000000000035b5e5ad9019092c665357240f594e	14	0xbfd54d7fb7059d2505069dec2222a81ead7f831a	36
0x00000000003b3cc22af3ae1eac0440bcee416b40	12	0x00000000b7ca7e12dcc72290d1fe47b2ef14c607	26
0x54cd18c5f9d68bee591541700a2042c6fc18e8f5	12	0x54cd18c5f9d68bee591541700a2042c6fc18e8f5	16
0x00000000032962b51589768828ad878876299e14	10	0x000000000035b5e5ad9019092c665357240f594e	14
0xd59e5b41482ee6283c22e1a6a20756da512ffa97	6	0x00000000003b3cc22af3ae1eac0440bcee416b40	14
0x1ced55180af96c2fab38069aa3e13fa81e024270	6	0xe8024625ac740573a379b290175c33eb72a7c6e5	14
0x7cf09d7a9a74f746edcb06949b9d64bcd9d1604f	4	0x46240f9d81c51e86d4bbe5938ff5a3f3b85c4654	14
0x46240f9d81c51e86d4bbe5938ff5a3f3b85c4654	2	0x0000000099cb7fc48a935bceb9f05bbae54e8987	14
0x102249e2954f88acc4e4b24395be71eafdb4c2a9	2	0x000000c52b33fa71614810224771dc8f3255b220	10
0x00000000000064c443ef440577c26525a3c34a30	2	0x00000000032962b51589768828ad878876299e14	10
0xe3c77b264c224ab4702584a0686c0ada6a83894a	2	0x000000005736775feb0c8568e7dee77222a26880	10
0xc723162117de54569861df0066761f9854dc18c5	2	0x46c4128981525aa446e02ffb2ff762f1d6a49170	8
0xce50840272d623272d6aef25e403f2265c27cfe7	2	0x1ced55180af96c2fab38069aa3e13fa81e024270	6
0x341c8dc3a41be16ce427c15a625983bdef2d2f27	2	0xd59e5b41482ee6283c22e1a6a20756da512ffa97	6
0xadc02ff103cdc8801f3fceed42ee191e1c19d920	2	0x7cf09d7a9a74f746edcb06949b9d64bcd9d1604f	4
0x46c4128981525aa446e02ffb2ff762f1d6a49170	2	0x00000000000064c443ef440577c26525a3c34a30	4
0x60f09b45dd707d0dda43f099bd87c0f49d483979	2	0xc723162117de54569861df0066761f9854dc18c5	4
0xde2f28a62ffd5d4dfda6be5855e8aa92ec370764	2	0xe16ea22554b5a99457abfbb79bdc18e3221a00a0	2
		0x102249e2954f88acc4e4b24395be71eafdb4c2a9	2
		0xadc02ff103cdc8801f3fceed42ee191e1c19d920	2
		0x4ba28ab9c05ab419a5a3ae5d3c3fe3387cceadc4	2
		0x60f09b45dd707d0dda43f099bd87c0f49d483979	2
		0xe3c77b264c224ab4702584a0686c0ada6a83894a	2
		0xce50840272d623272d6aef25e403f2265c27cfe7	2
		0x390e1d977e19fa9b7b9dc97ea5d3b1eb4347d51c	2
		0x341c8dc3a41be16ce427c15a625983bdef2d2f27	2
		0x12e98c9b9b266255bf037ccafcf87657e9a0b31b	2
		0xde2f28a62ffd5d4dfda6be5855e8aa92ec370764	2

Picture X: top suspicious addresses with count of their MEV transactions, from the left are addresses that performed MEVs with exact values match, from the right are addresses that performed MEVs with small values difference

In case of reviewing top 10 by capitalization possible MEV attacks with exact transaction values match can be seen extremely high values of transactions, meaning that attackers should either have high financial power or to have access to some financial resources with easy access.

	token_in	token_out	amount_in	amount_out	amount_usd	timestamp	sender
88	USDC	WBTC	214101.969487	5.314151	214059.231825	2021-07-03 06:13:37	0x00000000032962b51589768828ad878876299e14
128	USDC	WBTC	217495.100416	4.374650	217572.059085	2021-09-29 08:45:45	0x00000000008c4fb1c916e0c88fd4cc402d935e7d
129	WBTC	USDC	4.374650	217589.921792	217666.914012	2021-09-29 08:45:45	0x00000000008c4fb1c916e0c88fd4cc402d935e7d
89	WBTC	USDC	5.314151	218590.290717	218546.657125	2021-07-03 06:13:37	0x00000000032962b51589768828ad878876299e14
100	USDC	WBTC	321079.590468	5.483479	320886.042273	2021-08-11 08:35:26	0x00000000003b3cc22af3ae1eac0440bcee416b40
101	WBTC	USDC	5.483479	323431.903863	323236.937683	2021-08-11 08:35:26	0x00000000003b3cc22af3ae1eac0440bcee416b40
134	USDC	WBTC	557057.298176	7.966822	557352.340267	2021-10-05 09:00:00	0x00000000008c4fb1c916e0c88fd4cc402d935e7d
135	WBTC	USDC	7.966822	557619.782912	557915.122919	2021-10-05 09:00:00	0x00000000008c4fb1c916e0c88fd4cc402d935e7d
126	USDC	WBTC	976323.861321	12.689636	975595.915259	2021-09-27 20:58:07	0x00000000003b3cc22af3ae1eac0440bcee416b40
127	WBTC	USDC	12.689636	981830.211723	981098.160132	2021-09-27 20:58:07	0x00000000003b3cc22af3ae1eac0440bcee416b40

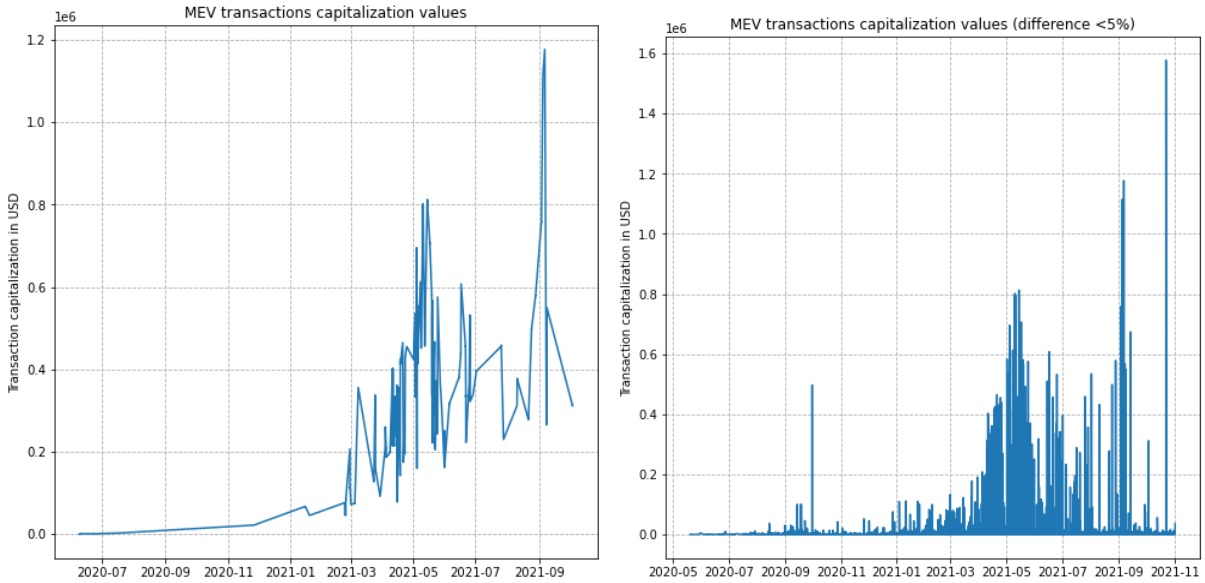
Picture X: top 10 MEV cases by capitalization with exact transaction values match

WETH/USDC simulation

Results of performing the simulation:

- **Transaction history size** - 2895926 transactions;
- **Blocked by Volatility Mitigation** - 91670 transactions;
- **Possible MEV attacks with the same values** - 136 attacks with 272 MEV-related transactions;
- **Possible MEV attacks with <5% values difference** - 8789 attacks with 17578 MEV-related transactions.

Compared to the WBTC/USDC case, the current pool contains a long transaction history with a high amount of suspicious transactions and blocks by a volatility mitigation mechanism. The first unique moment about the pool - MEV transactions values are not too big compared to other transactions values distribution in both exact and smaller than 5% difference suspicious transactions. The strange moment about distributions is that there are too many suspicious transactions with differences smaller than 5% compared to exact matches.



Picture X: comparison of possible MEVs with exact values matches and differences smaller than 5%

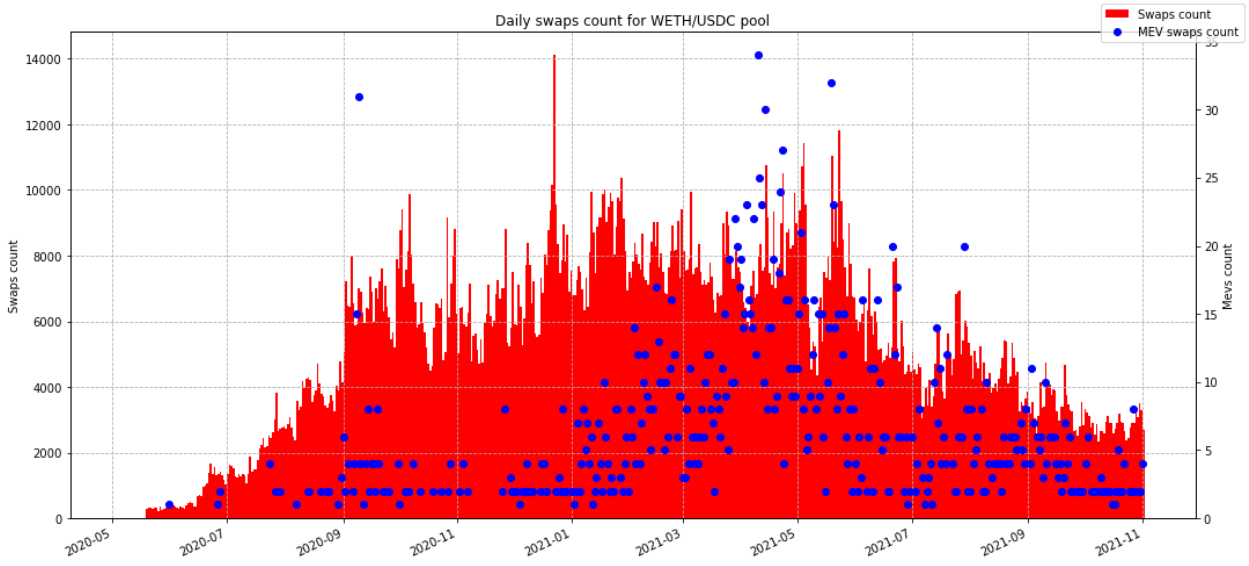
In cases of differences smaller than 5% can be seen how low are the values present in the distribution, which is not matching with the principle of price manipulations (it is required to cause heavy price impact to extract more profit out of attack). Suspicious transactions with

smaller values are less likely to be real MEV transactions. Out of all possible MEV transactions with values difference smaller than 5% there are:

- 10914 transactions with capitalization smaller than 1000 USD making them unlikely to be real MEV attacks;
- 2140 transactions with capitalization between 1000-2000 USD;
- 1013 transactions with capitalization between 2000-3000 USD;
- 508 transactions with capitalization between 3000-4000 USD;
- 612 transactions with capitalization between 4000-5000 USD;
- 2391 transactions with capitalization more than 5000 USD.

The most likely transactions to be related to MEV are ones with capitalization higher than 5000 USD, due to higher chances of causing price impact enough to get a profit out of the attack, meaning that there are around 1196 MEV attacks performed on the pool. In case of exact matches there are 32 transactions with capitalization smaller than 5000 USD, meaning that even out of 136 possible MEVs with exact values match only 120 MEVs are most likely representing real attacks on the pool.

In case of taking possible MEVs with 5% difference of values, where transaction capitalization is higher than 5000 USD, the count distribution will show dependency between amount of attacks and pool activity (conform distribution below).

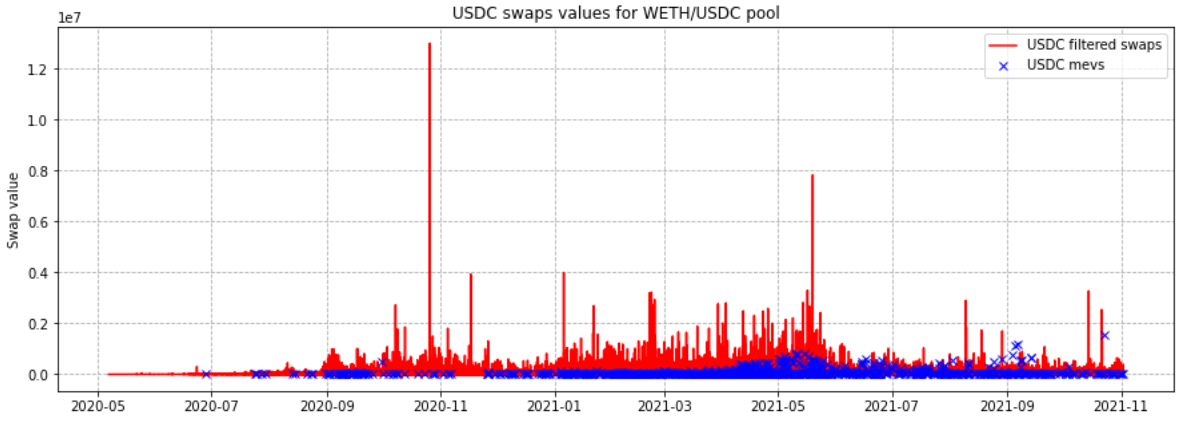


Picture X: transaction count distribution for “filtered swaps” and possible MEV transactions with capitalization higher than 5000 USD

Here it is observable that MEV transactions count rises with the rise of activity in the pool. In case of taking transactions that form a “sandwich” with difference smaller than 5% and capitalization bigger than 5000 USD distribution demonstrates that attackers are not standing out of the simple swaps distributions. This behavior lowers chances of attacks being blocked by a volatility mitigation mechanism. There is an additional interesting moment that can be observed out of the values distribution.

User is able to set a slippage to his transaction, ensuring that the difference between expected transaction values and their real values will not exceed the estimated slippage difference parameter (for example, 4% difference limit). Considering that MEV attacks values are not too “out of the distribution” of simple transactions it can be that attackers try to perform transactions on the “edge of acceptance” by slippage (if transaction will be reverted in case of difference equal to 4% or bigger, attacker can perform attack with difference of 3.9%). Considering that there are cases of small MEV attacks profits seen in transaction history it is required to review 3 moments in estimated MEV attacks:

- MEV attack profit in USD;
- Tokens extracted during attack (shows what tokens are more valuable for attacker);
- Gas spent on performing transactions.



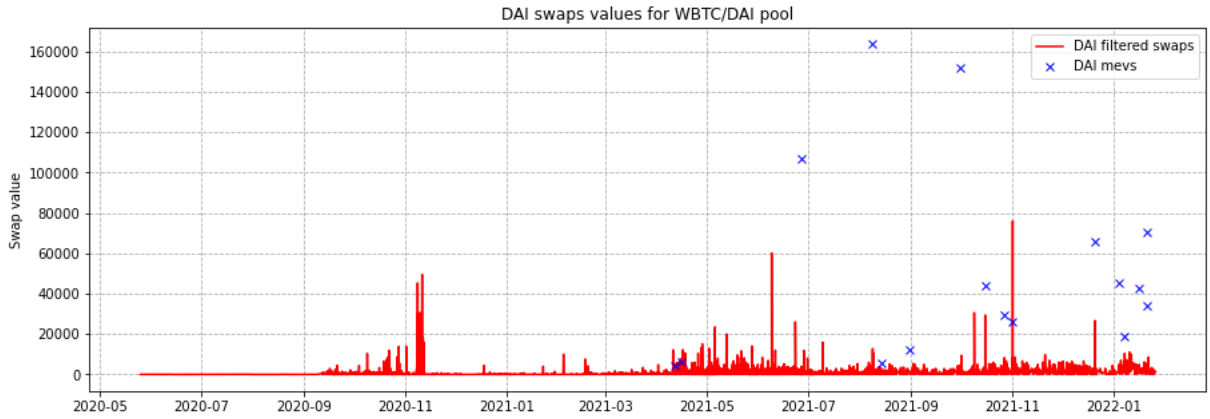
Picture X: swaps and MEV transactions values distributions in USDC for WETH/USDC pool

After review of those moments it can be estimated the amount of extracted profit by each attack and see connections of those profits with other data (connection with gas, reserves, activity and so on). This approach will also allow finding the most valuable tokens for attackers, taking into account how many transactions were performed to extract specific tokens (and how

many tokens were extracted), and allow performing analysis of the profit respective to the gas spent.

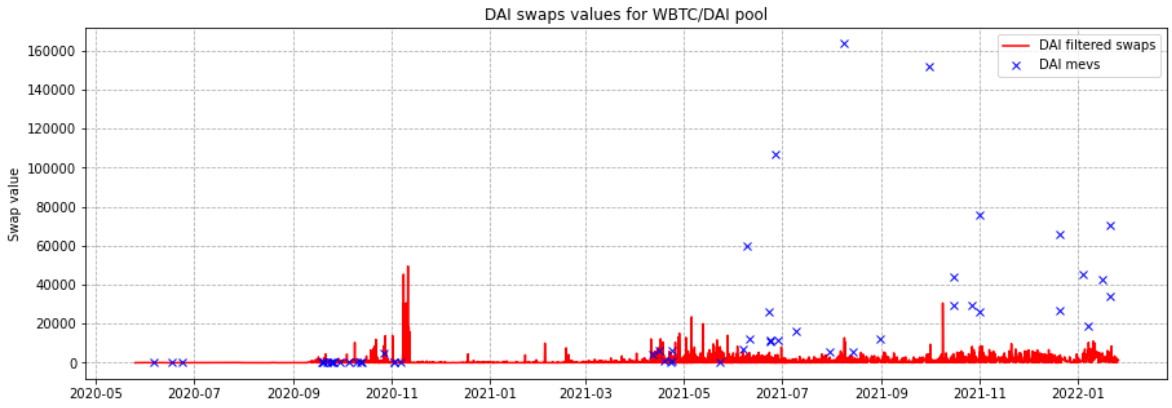
WETH/DAI simulation

Pool represents a situation of average pool with medium activity present, with medium capitalization of activity. Distribution contains 16 possible MEV transactions with exact values match and 52 possible MEV transactions with values differences smaller than 5%. Exact match MEVs are out of the standard swaps distributions, their values are too high and volatility mitigation should be able to block them.



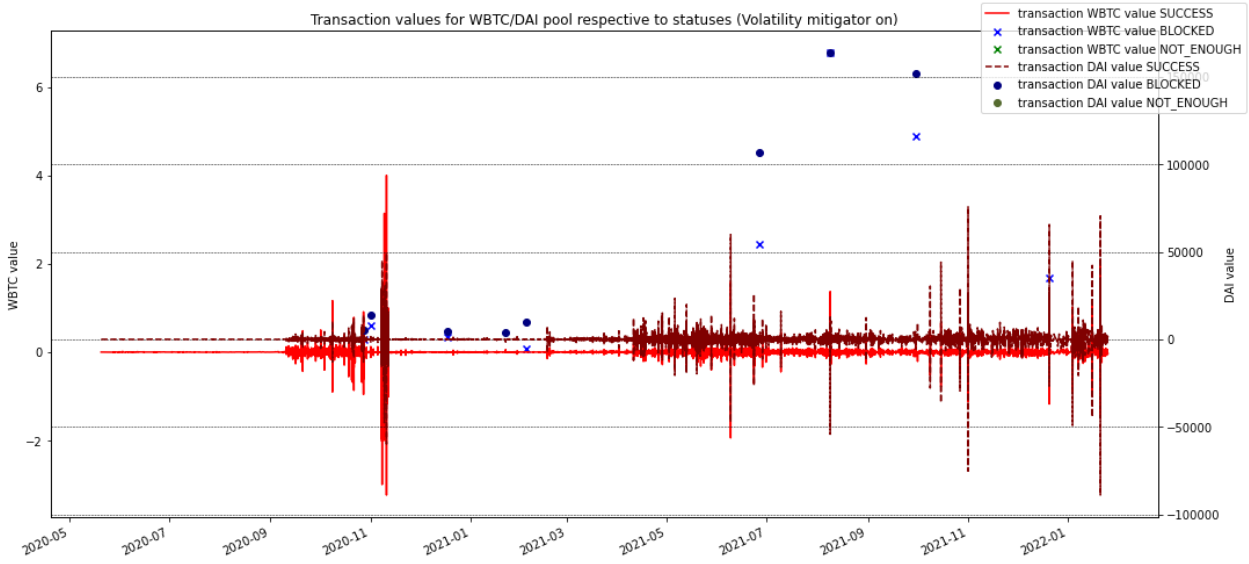
Picture X: DAI swaps values by type for WBTC/DAI pool (MEVs with exact values match)

MEVs with 5% values difference do not have the same good values distribution. Their values are not coming out of the simple swaps values range, lowering chances of them being real MEV attacks and causing impact on the pool (only in case of small reserves at transaction execution moment, and reserves drop interval matches with those low-value MEVs). MEV transactions frequency is small and therefore the pool is relatively safe for performing trades.



Picture X: DAI swaps values by type for WBTC/DAI pool (MEVs with <5% values difference)

Mitigation mechanisms block transactions with extreme value rise and some cases of small-value transactions during low-reserves periods. Another interesting moment about this pool is almost “flatlined” activity at specific time periods (from start till middle of September 2020, from middle of November 2020 till April 2021).



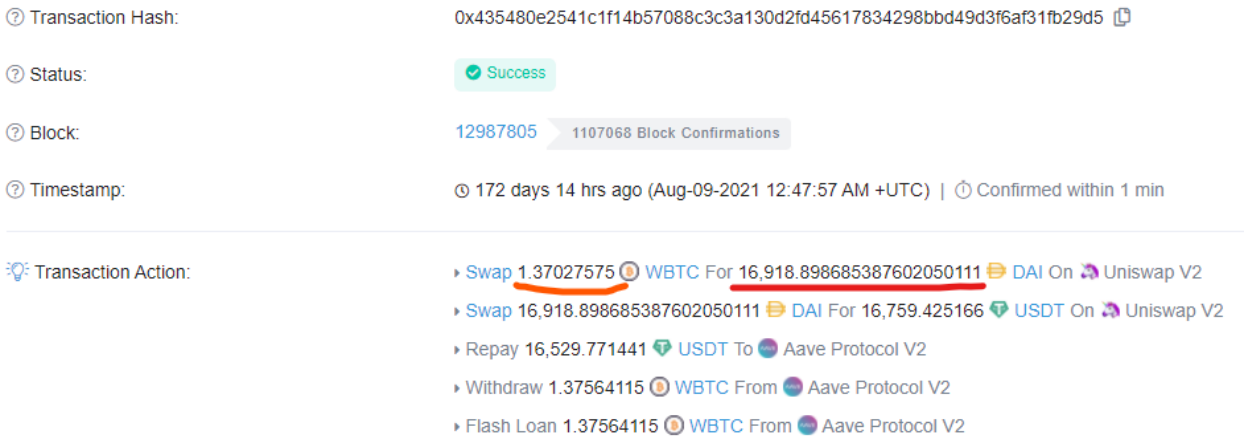
Picture X: WBTC/DAI swaps values distribution with separation by type

There are some unique cases of extremely high capitalization attacks, which can be seen on top 10 MEV transactions by capitalization, reaching 163 thousands USD of transaction capitalization. In case of the highest transaction there is no observable profit, but there was extracted 0,936114 WBTC (price of WBTC at 9 August 2021 when attack was performed was equal to 43 808,38 meaning that account extracted 41 009,637 USD profit).

token_in	token_out	amount_in	amount_out	amount_usd	timestamp	sender
DAI	WBTC	65849.408018	1.691156	65779.860645	2021-12-20 22:29:59	0x00000000008c4fb1c916e0c88fd4cc402d935e7d
WBTC	DAI	1.688847	65849.408018	65779.860645	2021-12-20 22:29:59	0x00000000008c4fb1c916e0c88fd4cc402d935e7d
DAI	WBTC	70756.285043	2.019388	70840.147088	2022-01-21 03:12:38	0x00000000008c4fb1c916e0c88fd4cc402d935e7d
WBTC	DAI	2.002565	70756.285043	70840.147088	2022-01-21 03:12:38	0x00000000008c4fb1c916e0c88fd4cc402d935e7d
DAI	WBTC	106808.338596	2.448900	107030.118475	2021-06-27 01:26:44	0x00000000032962b5158976882 8ad878876299e14
WBTC	DAI	2.448900	108073.335496	108297.742050	2021-06-27 01:26:44	0x00000000032962b5158976882 8ad878876299e14
WBTC	DAI	4.872345	152135.514321	151973.068797	2021-09-30 08:41:35	0x00000000008c4fb1c916e0c88fd4cc402d935e7d
DAI	WBTC	152135.514321	4.915263	151973.068797	2021-09-30 08:41:35	0x00000000008c4fb1c916e0c88fd4cc402d935e7d
DAI	WBTC	163521.431029	7.702063	163387.129530	2021-08-09 00:47:57	0x00000000003b3cc22af3ae1eac0440bcee416b40
WBTC	DAI	6.765949	163521.431029	163387.129530	2021-08-09 00:47:57	0x00000000003b3cc22af3ae1eac0440bcee416b40

Picture X: top 10 by capitalization MEV transactions (with exact match)

To ensure that estimation of profit received by the bot was performed correctly, search for information about this transaction sequence on Etherscan and the transaction coming right after the first transaction in MEV sequence is the victim's one (information demonstrated below).



Picture X: victim's transaction with losses caused by highest from capitalization perspective MEV attack (taken from Etherscan)

Considering real price of WBTC person should have received 60 029,56 USD (or similar amount of DAI, considering that it's a stablecoin close to USD), while received amount is only 16 918,898 DAI, meaning that person lost around 43 thousands of DAI or 43 thousands of USD. Profit extracted by the attacker is almost the same as is the loss of the victim.

0x00000000008c4fb1c916e0c88fd4cc402d935e7d	18
0xf73d5d4962e08c1d572f56e2f3e2728a77507e16	4
0x00000000003b3cc22af3ae1eac0440bcee416b40	2
0x000000000035b5e5ad9019092c665357240f594e	2
0x00000000032962b51589768828ad878876299e14	2
0x66f049111958809841bbe4b81c034da2d953aa0c	2
0x00000000726422a6fecb4759b44d47e48cf746aa	2

0x7a250d5630b4cf539739df2c5dacb4c659f2488d	46
0x00000000008c4fb1c916e0c88fd4cc402d935e7d	18
0x66f049111958809841bbe4b81c034da2d953aa0c	10
0x00000000b7ca7e12dcc72290d1fe47b2ef14c607	8
0x0000000099cb7fc48a935bceb9f05bbae54e8987	4
0xf73d5d4962e08c1d572f56e2f3e2728a77507e16	4
0x00000000003b3cc22af3ae1eac0440bcee416b40	2
0x000000000035b5e5ad9019092c665357240f594e	2
0x00000000032962b51589768828ad878876299e14	2
0x00000000726422a6fecb4759b44d47e48cf746aa	2
0xc3037b2a1a9e9268025ff6d45fe7095436446d52	2
0x499dd900f800fd0a2ed300006000a57f00fa009b	2
0x000000000027d2efc283613d0c3e24a8b430c4d8	2

Picture X: top suspicious addresses with count of their MEV transactions, from the left are addresses that performed MEVs with exact values match, from the right are addresses that performed MEVs with small values difference

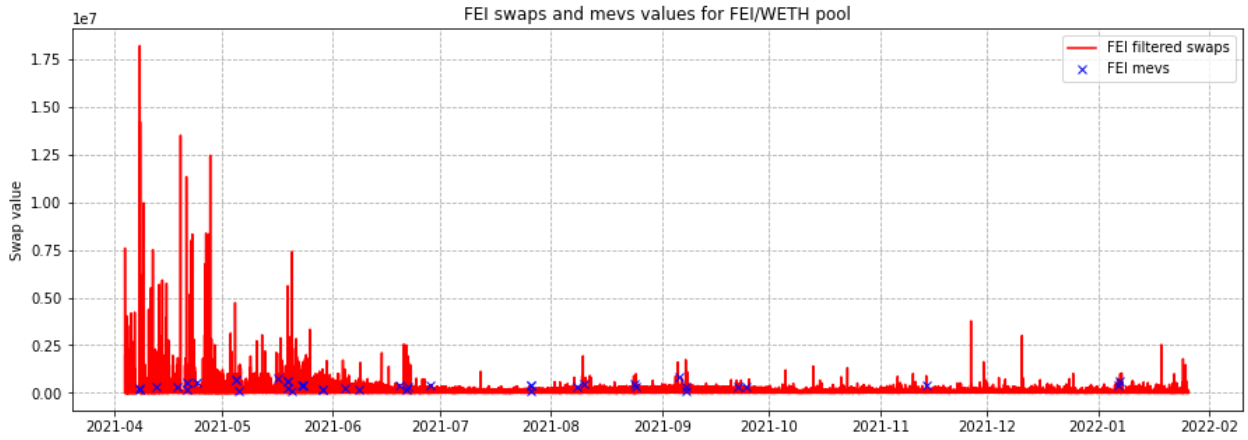
FEI/WETH simulation

Pool contains an unstable start of the lifecycle period characterized by extreme swaps values rises and drops. Starting period high swaps values range and high reserves amount should not cause a mitigation mechanism to block any MEVs with high values and it can operate only at

stabilized period with lower values range and smaller transaction frequency (still high enough to perform efficient MEV).

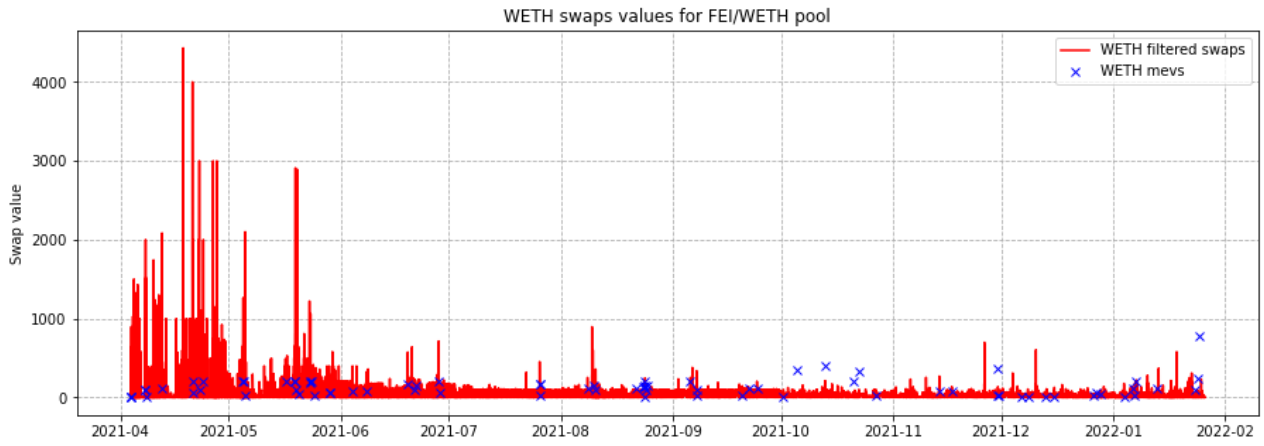
Despite relatively stable medium-level transaction history and presence of high value transactions there were registered only 41 MEV attacks with exact transaction values matches and 78 MEV attacks with transaction values differences smaller than 5%. In both cases, there is low attackers' activity registered in the pool.

Uniqueness of the possible MEVs performed on this pool is that they are not coming out of the simple swaps distribution while mean capitalization of those possible MEVs is around 356 thousands USD. Such a high value of MEVs is caused by high reserves of the pool, requiring high financial power and higher impact to be able to extract profit out of performing an attack.



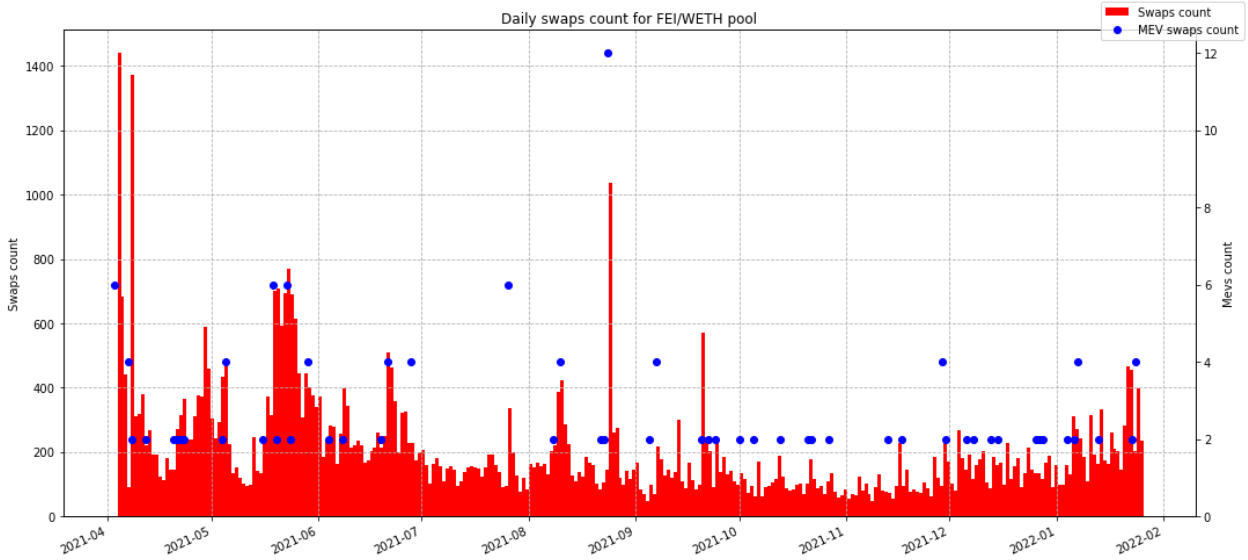
Picture X: swaps values in the FEI/WETH pool (MEVs with exact values match)

In case of taking MEVs with small values difference there are some points that are coming out of the simple swaps distribution. In this case there are some small value transactions, reducing their likelihood of being MEV attacks, while mean capitalization of all performed MEV attacks rises to 367 thousands of USD, meaning that in case of small difference MEVs are catched suspicious cases with even higher values than in the first case.



Picture X: swaps values in the FEI/WETH pool (MEVs with small values difference)

Due to the small frequency of performed attacks it is hard to establish connection between MEVs count and swaps activity in the pool. The only suggestion that can be made is that MEVs count depends on the amount of activity present in the pool, rising pool attractiveness for attackers and making it possible to catch a transaction in the middle of “sandwich”.



Picture X: transaction count distribution (MEVs with small values difference)

Interesting moment is that the mitigation mechanism has not blocked any MEV transaction but prevented some transactions with not so extreme values. The only case why this could happen is due to the influence of other transactions (by their token prices estimations).

	token_in	token_out	amount_in	amount_out	amount_usd	timestamp	sender
45164	WETH	FEI	3.464385e+02	1.182227e+06	1.195744e+06	2021-10-05 14:25:06	0x000000000035b5e5ad9019092c665357240f594e
45163	FEI	WETH	1.202610e+06	3.502651e+02	1.208952e+06	2021-10-05 14:25:06	0x000000000035b5e5ad9019092c665357240f594e
47034	WETH	FEI	3.309909e+02	1.302628e+06	1.317059e+06	2021-10-22 21:13:08	0x00000000003b3cc22af3ae1eac0440bcee416b40
47035	FEI	WETH	1.317499e+06	3.327473e+02	1.324049e+06	2021-10-22 21:13:08	0x00000000003b3cc22af3ae1eac0440bcee416b40
46046	WETH	FEI	4.092594e+02	1.400287e+06	1.414723e+06	2021-10-13 07:04:33	0x000000000035b5e5ad9019092c665357240f594e
46043	FEI	WETH	1.403605e+06	4.122923e+02	1.434223e+06	2021-10-13 07:04:33	0x000000000035b5e5ad9019092c665357240f594e
50555	WETH	FEI	3.629185e+02	1.587712e+06	1.609321e+06	2021-11-29 22:44:38	0x000000000035b5e5ad9019092c665357240f594e
50554	FEI	WETH	1.630423e+06	3.703666e+02	1.642349e+06	2021-11-29 22:44:38	0x000000000035b5e5ad9019092c665357240f594e
60998	WETH	FEI	7.760372e+02	1.735687e+06	1.839183e+06	2022-01-24 18:09:21	0x00000000003b3cc22af3ae1eac0440bcee416b40
60999	FEI	WETH	1.786125e+06	7.929845e+02	1.879347e+06	2022-01-24 18:09:21	0x00000000003b3cc22af3ae1eac0440bcee416b40

Picture X: top 10 MEV transactions by capitalization with small values differences,

The biggest MEV attack extracts profit equal to 40 thousands USD, while extracted values are around 5 thousands FEI and around 16,94 WETH (conform price of WETH for 24 January 2022 equal to 2 448,275 USD and extracted value is around 40 thousands USD). This case is interesting due to the same sender (MEV bot) as in case of WBTC/DAI pool attack and extracted profit is almost the same as in case of WBTC/DAI (around 40 thousands USD). Both cases are characterized by extremely big capitalization of transactions.

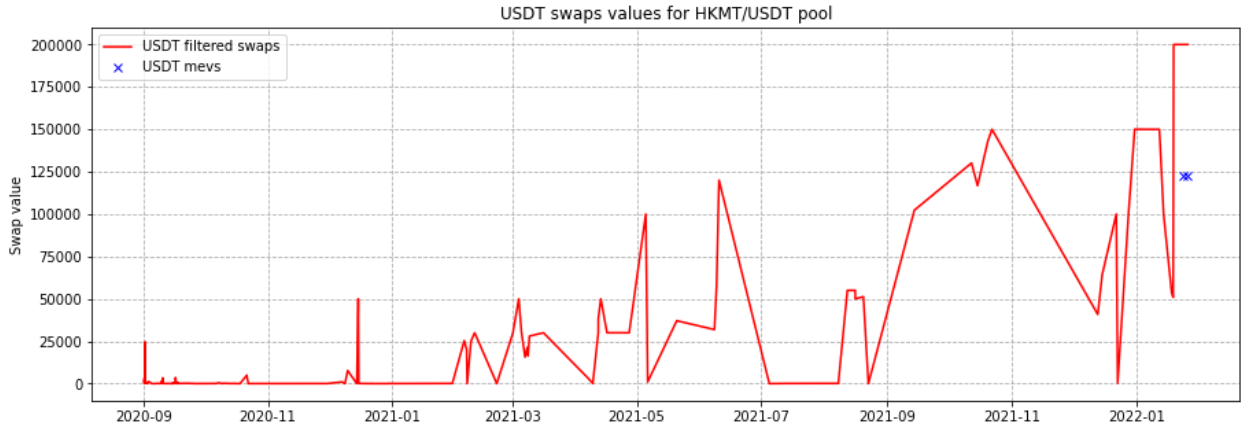
0xd78a3280085ee846196cb5fab7d510b279486d44	24
0x00000000003b3cc22af3ae1eac0440bcee416b40	16
0xa3b0e79935815730d942a444a84d4bd14a339553	12
0x00000000008c4fb1c916e0c88fd4cc402d935e7d	8
0x000000000035b5e5ad9019092c665357240f594e	6
0x66f049111958809841bbe4b81c034da2d953aa0c	4
0x7a250d5630b4cf539739df2c5dacb4c659f2488d	4
0x6ecb10b62a1eea81c24f88dcebd6fa316f12d598	2
0x00000000b7ca7e12dcc72290d1fe47b2ef14c607	2
0x83f893cc6610bfc695f8e2d4cd0e6d3033dec77e	2
0x000000005804b22091aa9830e50459a15e7c9241	2

0x000000000035b5e5ad9019092c665357240f594e	36
0x00000000003b3cc22af3ae1eac0440bcee416b40	32
0xd78a3280085ee846196cb5fab7d510b279486d44	24
0x7a250d5630b4cf539739df2c5dacb4c659f2488d	14
0xa3b0e79935815730d942a444a84d4bd14a339553	12
0x00000000008c4fb1c916e0c88fd4cc402d935e7d	8
0x00000000726422a6fecb4759b44d47e48cf746aa	4
0x55eb58655f8202ff839487886fedba2a1eb7b2d7	4
0x66f049111958809841bbe4b81c034da2d953aa0c	4
0x000000005804b22091aa9830e50459a15e7c9241	2
0x7cf09d7a9a74f746edcb06949b9d64bcd9d1604f	2
0x6ecb10b62a1eea81c24f88dcebd6fa316f12d598	2
0x9116e82841267d01b9c49f0a19617083466cc000	2
0x9271d303b57c204636c38df0ed339b18bf98f909	2
0x00000000a1f2d3063ed639d19a6a56be87e25b1a	2
0x00000000b7ca7e12dcc72290d1fe47b2ef14c607	2
0x00000000032962b51589768828ad878876299e14	2
0x83f893cc6610bfc695f8e2d4cd0e6d3033dec77e	2

Picture X: suspicious addresses and amount of performed possible MEV transactions, from the left is count of exact MEV values matches, from the right is count of small values difference MEVs

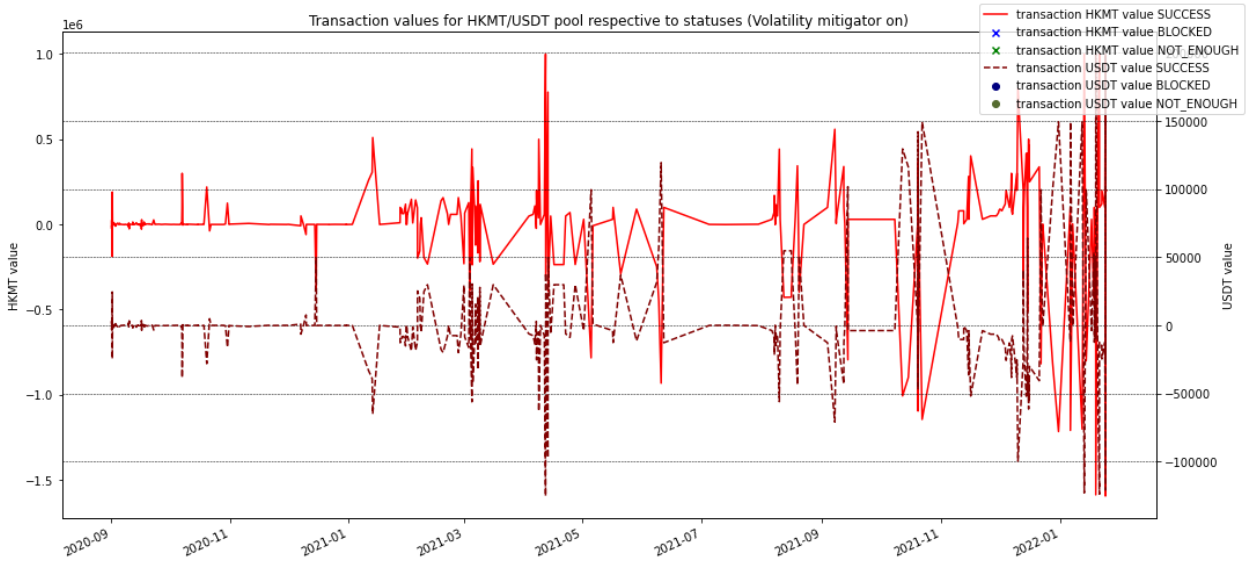
HKMT/USDT simulation

There is a small transaction history which is caused by low transaction frequency of the pool. During 4 months there were only 426 transactions containing 1 MEV with exact values match and 2 MEVs with small values difference.



Picture X: USDT swaps values for HKMT/USDT pool (MEVs with small values difference)

Out of 436 transactions can be seen 2 MEV attacks meaning that there are 432 simple swaps performed in the pool. On the presented chart can be seen drops of activity. Such a distribution lowers chances of a mitigation mechanism to stabilize pool behavior and perform efficient filters out of impactful transactions.

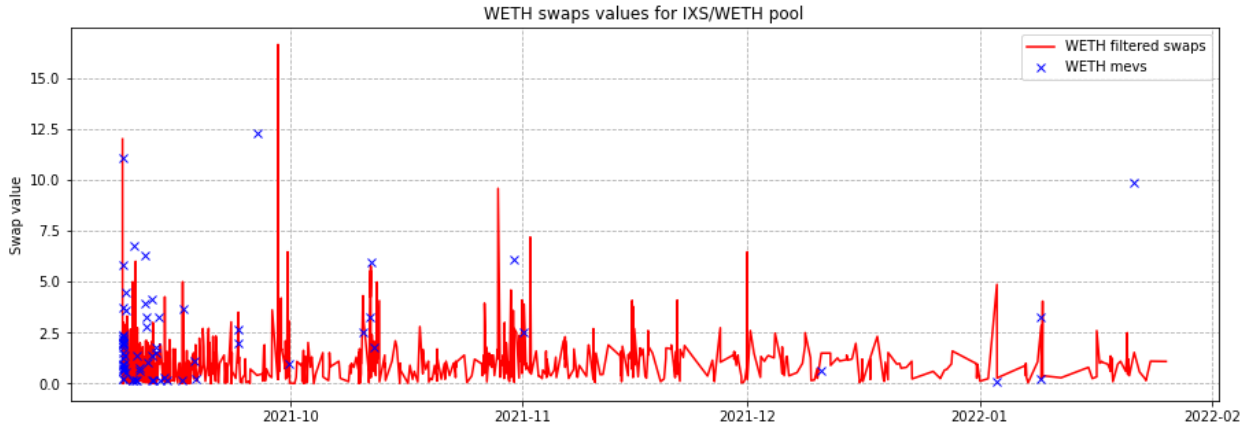


Picture X: HKMT/USDT swaps values distribution with separation by type

Conform distributions can be seen multiple activity drops, lack of mitigation activity, unbalanced token movement. Based on those moments it can be assumed that it is unlikely for the pool not only to become attractive for simple traders, attackers, but also that the pool may reach the end of its lifecycle.

IXS/WETH simulation

Current pool contains medium-level transaction frequency with medium level token movement values range. There are 70 MEV attacks with exact values match and 75 MEVs with small values difference. In case of reviewing MEVs with exact values match there are multiple cases of attacks going out of the distribution (too high values) and cases of swaps with small values considered as attacks. Even considering their low values they should be considered due to lower reserves at the start of the pool lifecycle period.



Picture X: swaps values distributions for IXS/WETH pool (MEVs with exact values match)

Mean value of MEV attacks with exact values match is around 8 thousands of USD. Separation of those attacks by their values range show next results:

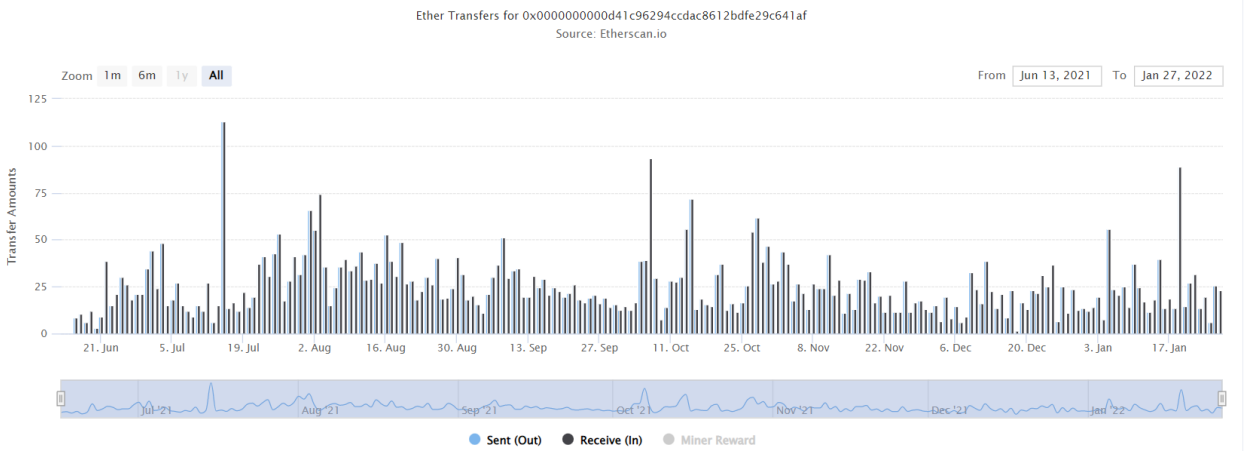
- 28 transactions with capitalization lower than 1000 USD, meaning that 14 MEVs are unlikely to be real MEV attacks;
- 2 transactions with capitalization between 1000-2000 USD, meaning that there are 1 MEV. Likelihood of being MEV attack is questionable;
- 18 transactions with capitalization between 2000-3000 USD, meaning that there are 9 MEVs with values setting transactions likelihood of being real MEVs to the medium level;

- 10 transactions with capitalization between 3000-4000 USD, meaning that there 5 MEVs with higher likelihood of being real MEVs.
- 82 transactions with capitalization above 4000 USD, meaning that there are 41 case of possible real MEV attacks

In case of taking top 10 by capitalization transactions can be seen that their values are extremely high compared to the simple swaps (their values are between 23 000-38 000 USD)

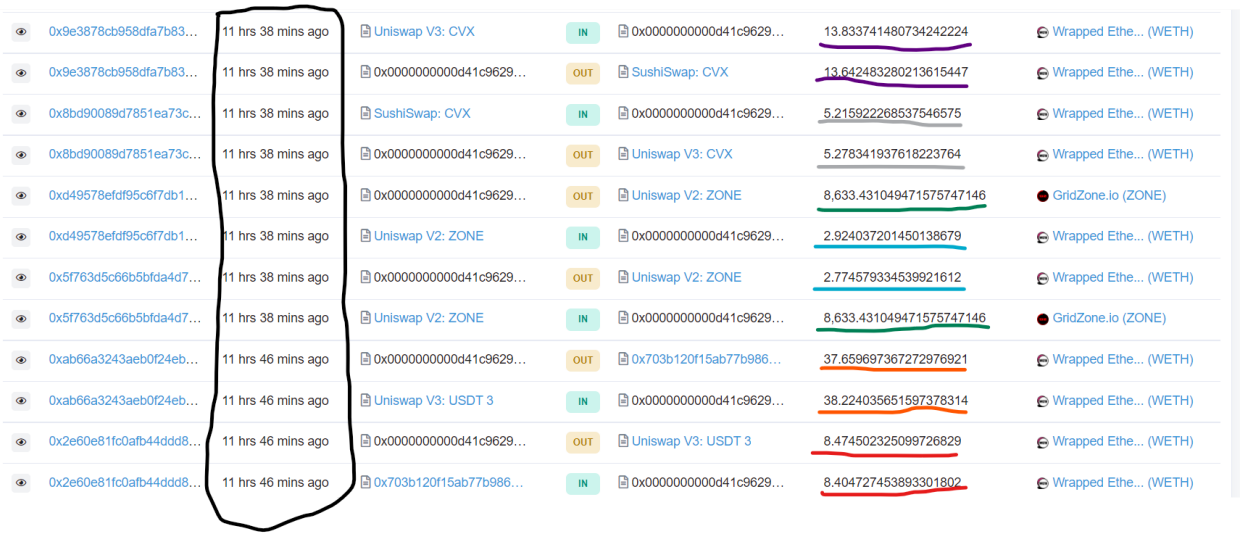
There was one interesting case worth investigating, when at the moment of 21 January 2022 a person performed MEV transactions with capitalization of each around 28 thousands USD. After checking this account on Etherscan, some interesting moments have been found:

- From first appearance of the address can be seen that by daily activity address performs transactions with equal amount of outgoing and incoming Ether;
- Daily amount of transactions performed by the address is between 200-400 transactions;
- Transactions performed by this account contain almost similar values;



Picture X: Ether transfers of possible MEV attacker (taken from Etherscan)

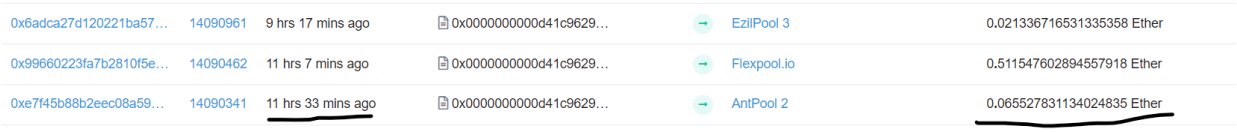
- There are multiple inner transactions happening periodically and values of those transactions look suspiciously similar to the MEV attacks pattern;



0x9e3878cb958dfa7b83…	11 hrs 38 mins ago	Uniswap V3: CVX	IN	0x0000000000d41c9629…	13.833741480734242224	Wrapped Ethe… (WETH)
0x9e3878cb958dfa7b83…	11 hrs 38 mins ago	0x0000000000d41c9629…	OUT	SushiSwap: CVX	13.64248328021361544 7	Wrapped Ethe… (WETH)
0x8bd90089d7851ea73c…	11 hrs 38 mins ago	SushiSwap: CVX	IN	0x0000000000d41c9629…	5.215922268537546575	Wrapped Ethe… (WETH)
0x8bd90089d7851ea73c…	11 hrs 38 mins ago	0x0000000000d41c9629…	OUT	Uniswap V3: CVX	5.27834193761822376 4	Wrapped Ethe… (WETH)
0xd49578efdf95c6f7db1…	11 hrs 38 mins ago	0x0000000000d41c9629…	OUT	Uniswap V2: ZONE	8,633.431049471575747146	GridZone.io (ZONE)
0xd49578efdf95c6f7db1…	11 hrs 38 mins ago	Uniswap V2: ZONE	IN	0x0000000000d41c9629…	2.924037201450138679	Wrapped Ethe… (WETH)
0x5f763d5c66b5bfda4d7…	11 hrs 38 mins ago	0x0000000000d41c9629…	OUT	Uniswap V2: ZONE	2.774579334539921612	Wrapped Ethe… (WETH)
0x5f763d5c66b5bfda4d7…	11 hrs 38 mins ago	Uniswap V2: ZONE	IN	0x0000000000d41c9629…	8,633.431049471575747146	GridZone.io (ZONE)
0xab66a3243aeb0f24eb…	11 hrs 46 mins ago	0x0000000000d41c9629…	OUT	0x703b120f15ab77b986…	37.659697367272976921	Wrapped Ethe… (WETH)
0xab66a3243aeb0f24eb…	11 hrs 46 mins ago	Uniswap V3: USDT 3	IN	0x0000000000d41c9629…	38.224035651597378314	Wrapped Ethe… (WETH)
0x2e60e81fc0afb44ddd8…	11 hrs 46 mins ago	0x0000000000d41c9629…	OUT	Uniswap V3: USDT 3	8.474502325099726829	Wrapped Ethe… (WETH)
0x2e60e81fc0afb44ddd8…	11 hrs 46 mins ago	0x703b120f15ab77b986…	IN	0x0000000000d41c9629…	8.404727453893301802	Wrapped Ethe… (WETH)

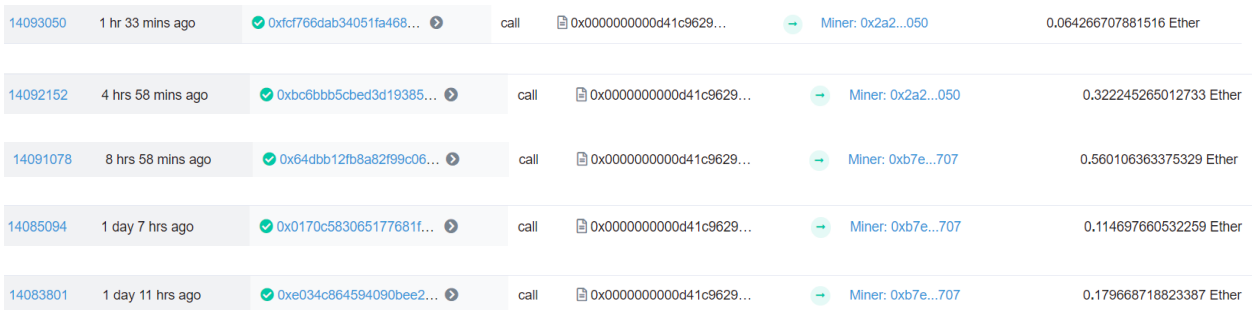
Picture X: ERC-20 transactions history fragment of possible MEV attacker (taken from Etherscan)

- There are multiple periodic interactions of this account with Miners accounts.



0x6adca27d120221ba57…	14090961	9 hrs 17 mins ago	0x0000000000d41c9629…	EzilPool 3	0.021336716531335358 Ether
0x99660223fa7b2810f5e…	14090462	11 hrs 7 mins ago	0x0000000000d41c9629…	Flexpool.io	0.511547602894557918 Ether
0xe7f45b88b2eec08a59…	14090341	11 hrs 33 mins ago	0x0000000000d41c9629…	AntPool 2	0.065527831134024835 Ether

Attacker extracted 0.471454 WETH by performing this attack and 1336.276618 USD. This is not the biggest attack by capitalization but one of the biggest from a profit perspective.



14093050	1 hr 33 mins ago	0xfcf766dab34051fa468…	call	0x0000000000d41c9629…	Miner: 0x2a2…050	0.064266707881516 Ether
14092152	4 hrs 58 mins ago	0xbc6bbb5cbed3d19385…	call	0x0000000000d41c9629…	Miner: 0x2a2…050	0.322245265012733 Ether
14091078	8 hrs 58 mins ago	0x64dbb12fb8a82f99c06…	call	0x0000000000d41c9629…	Miner: 0xb7e…707	0.560106363375329 Ether
14085094	1 day 7 hrs ago	0x0170c5830651776 81f…	call	0x0000000000d41c9629…	Miner: 0xb7e…707	0.114697660532259 Ether
14083801	1 day 11 hrs ago	0xe034c864594090bee2…	call	0x0000000000d41c9629…	Miner: 0xb7e…707	0.179668718823387 Ether

Picture X: examples of MEV attacker multiple interaction with Miners accounts

In case of taking possible MEVs with small values, the mean transaction value is around 8570 USD (from capitalization perspective). Additional cases contain big capitalization transactions that look like real MEV attacks, but profits are low. For review was taken the case of the biggest registered MEV-like attack with small difference between values (attack capitalization around 48 700 USD). Profit of this attack was equal to 283,870703 USD and extracted in the form of 0,097127 WETH.

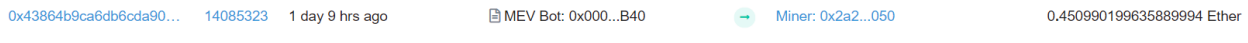
0x9fefbe601700beb5001...	27 mins ago	SushiSwap: FTM	IN	MEV Bot: 0x000...B40	28.897000525421084672	Wrapped Ethe... (WETH)
0x9fefbe601700beb5001...	27 mins ago	MEV Bot: 0x000...B40	OUT	SushiSwap: FTM	33,093.000912050916187704	Fantom Token (FTM)
0xc14bfb7a2b58e95ad0...	27 mins ago	MEV Bot: 0x000...B40	OUT	SushiSwap: FTM	28.758960207808167936	Wrapped Ethe... (WETH)
0xc14bfb7a2b58e95ad0...	27 mins ago	SushiSwap: FTM	IN	MEV Bot: 0x000...B40	33,093.001036169650759393	Fantom Token (FTM)
0xa3c095659e95973b12...	34 mins ago	SushiSwap: KAE	IN	MEV Bot: 0x000...B40	0.13291170494939136	Wrapped Ethe... (WETH)
0xa3c095659e95973b12...	34 mins ago	MEV Bot: 0x000...B40	OUT	SushiSwap: KAE	8.113424205408653052	Kanpeki (KAE)
0x0998ba7d6ade680549...	34 mins ago	MEV Bot: 0x000...B40	OUT	SushiSwap: KAE	0.113880615203373056	Wrapped Ethe... (WETH)
0x0998ba7d6ade680549...	34 mins ago	SushiSwap: KAE	IN	MEV Bot: 0x000...B40	8.113400822778105551	Kanpeki (KAE)
0x04646bd917906b3762...	36 mins ago	MEV Bot: 0x000...B40	OUT	Uniswap V3: SPELL	11.712558836633729955	Wrapped Ethe... (WETH)
0x04646bd917906b3762...	36 mins ago	SushiSwap: SPELL	IN	MEV Bot: 0x000...B40	12.017205167200927744	Wrapped Ethe... (WETH)
0x9f25834849160e7771f...	36 mins ago	Uniswap V3: SPELL	IN	MEV Bot: 0x000...B40	5.282832344415342782	Wrapped Ethe... (WETH)
0x9f25834849160e7771f...	36 mins ago	MEV Bot: 0x000...B40	OUT	SushiSwap: SPELL	5.38582183737032704	Wrapped Ethe... (WETH)
0x4bfb914ed9fd22b7f8c...	39 mins ago	MEV Bot: 0x000...B40	OUT	SushiSwap: WGK	1.722359407291623781	Wrapped Gene... (WGK)
0x4bfb914ed9fd22b7f8c...	39 mins ago	SushiSwap: WGK	IN	MEV Bot: 0x000...B40	1.406379219939753984	Wrapped Ethe... (WETH)
0x1a9abf8c4a2b2fe74bc...	39 mins ago	MEV Bot: 0x000...B40	OUT	SushiSwap: WGK	1.373433071272984576	Wrapped Ethe... (WETH)
0x1a9abf8c4a2b2fe74bc...	39 mins ago	SushiSwap: WGK	IN	MEV Bot: 0x000...B40	1.722359414875622744	Wrapped Gene... (WGK)

Picture X: ERC-20 transactions history fragment of MEV bot (taken from Etherscan)

Activity of the bot is similar to the first reviewed address: there are 4 transactions present in the block, where differences between transaction values are small and look like MEV-profit. Etherscan shows current address as a MEV bot, meaning that activity of this bot is clearly seen and considering a similar pattern with previous address, which is not labelled as a MEV-bot, it is considered that the first address also represents MEV-bot.

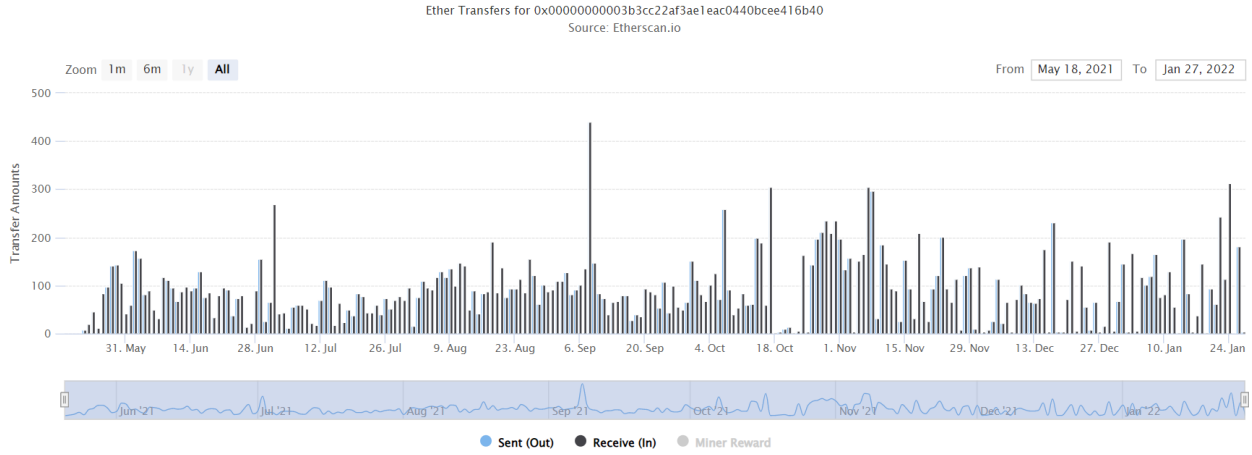
Interesting moment is that in both cases WETH was sent from a Wrapped Ether account on Uniswap (in case of first address around 6 Ether and 100 Ether for the second address) and multiple small transactions looking like profits of performing MEV-attacks. The difference between those addresses is that in the second case internal transactions are performed less frequently with higher values. Another interesting moment is that this account has transfers performed to the same Miner accounts as shown in the first case (in most of the cases Ether is sent to the Miner address ending with “707”).

0xa4c7ead1d14d774c58...	14085538	1 day 8 hrs ago	MEV Bot: 0x000...B40	Miner: 0xb7e...707	0.0287561171144156 Ether
0xd78d2c6c0ec9562ed9...	14076272	2 days 18 hrs ago	MEV Bot: 0x000...B40	Miner: 0xb7e...707	0.007059923111886436 Ether
0x5f66663482d0c6a9e0...	14075026	2 days 23 hrs ago	MEV Bot: 0x000...B40	Miner: 0xb7e...707	0.016724610516804948 Ether



Picture X: examples of MEV bot multiple interaction with Miners accounts

Activity of this address is identical by pattern to the previous case: daily transfers performed by this account are equal from incoming and outgoing Ether. Assumption is that both addresses represent MEV bots which send their profits to the specified addresses via internal transactions.



Picture X: Ether transfers of possible MEV attacker (taken from Etherscan)

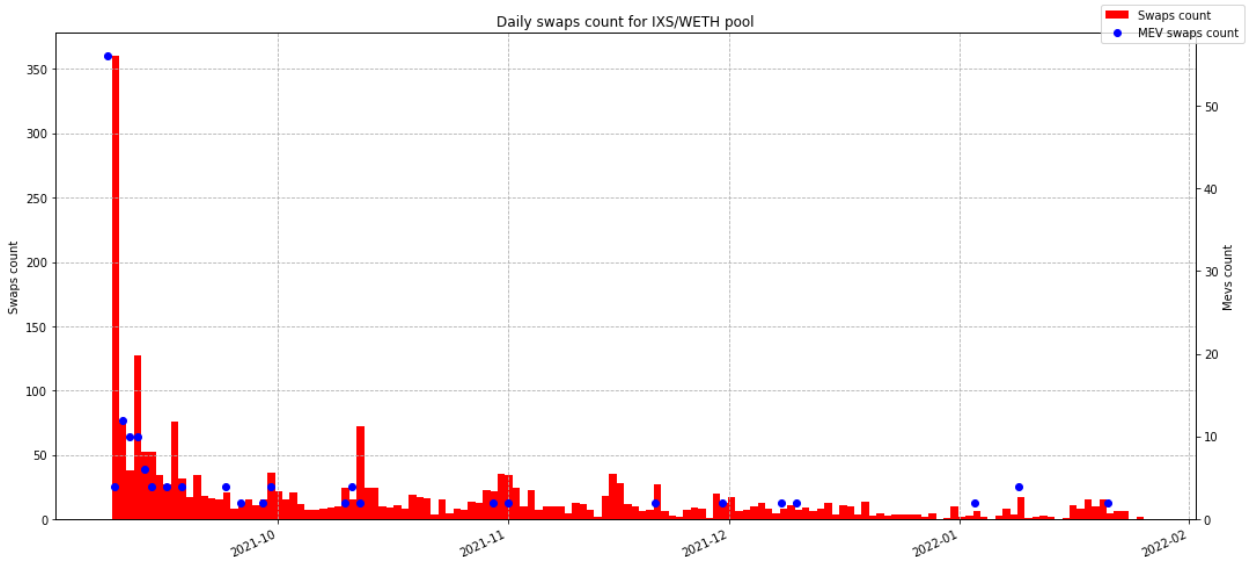
Below is the amount of MEV transactions performed by different addresses (those are transactions count, while the amount of attacks is twice smaller).

0x1d6e8bac6ea3730825bde4b005ed7b2b39a2932d	58
0xc1dfd16259c2530e57aea8a2cf106db5671616b0	26
0x000000000000294a0d3b43ec78199a84587ae012	16
0x00000000003b3cc22af3ae1eac0440bcee416b40	14
0x0000000000d41c96294ccdac8612bdfe29c641af	4
0x499dd900f800fd0a2ed300006000a57f00fa009b	4
0x000000000027d2efc283613d0c3e24a8b430c4d8	4
0x42b2c65db7f9e3b6c26bc6151ccf30cce0fb99ea	4
0xbcc7f6355bc08f6b7d3a41322ce4627118314763	4
0x6b650ca58d7b7f1525c362ee1bb380df6140c766	2
0x000000000000084e91743124a982076c59f10084	2
0x0000000061b4f7c843533200f852200dbfee086f	2

Picture X: IXS/WETH suspicious addresses and amount of performed MEV transactions (to get attacks number divide by 2)

In case of taking suspicious transactions with small value differences that look like MEVs there is a present correlation between amount of daily swaps and amount of performed attacks. This is caused by the requirement of placing transactions in the middle of “sandwich” to

extract profit. IXS/WETH pool contains medium level pool activity and correlation between count distributions are too similar.

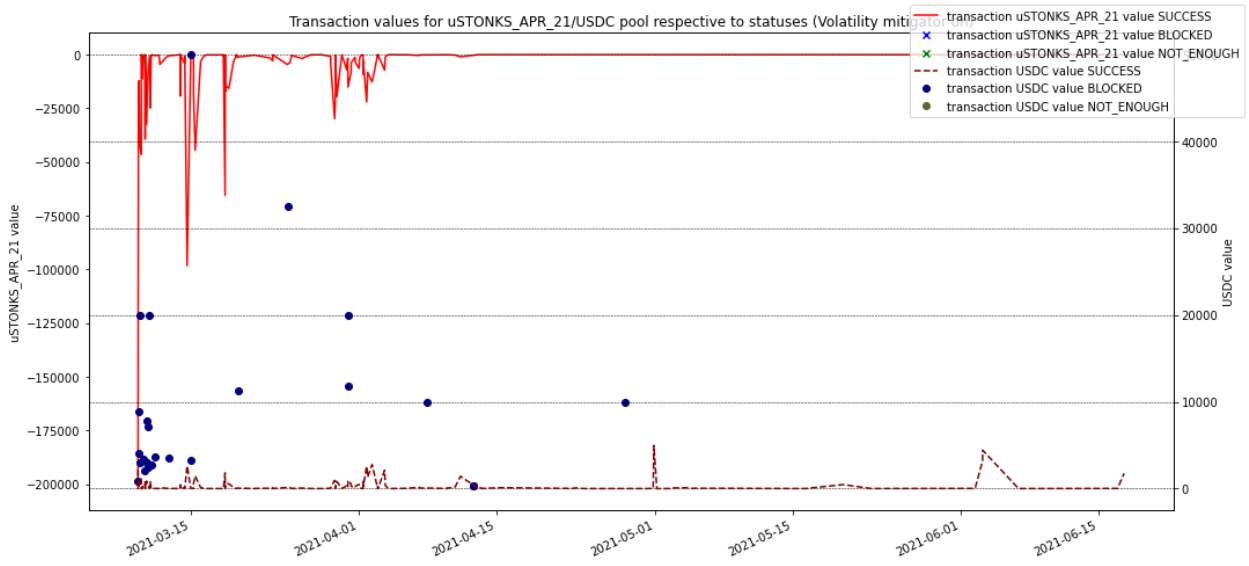


Picture X: count distributions of transactions by type (MEVs with small values difference)

XAUt/WETH, UMA/FEI and ustonks_apr_21/USDC simulations

Those first two pools will not be described here. Those pools do not contain any performed MEV attacks and therefore it is not possible to analyze MEV behavior. Those pools also will be ignored from the perspective of extracting profits out of MEV attacks.

Case of ustonks_apr_21/USDC pool contains only one performed MEV attack with small extracted profit (around 20 USD) and movement of tokens in the pool is not healthy due to one-sided movement of the tokens. Volatility mitigation blocks many transactions and distribution of price deviation, reserves changes, movement of the tokens smoothes and therefore behavior becomes more attractive for traders. Mitigation could have kept the pool alive for a longer period of time.

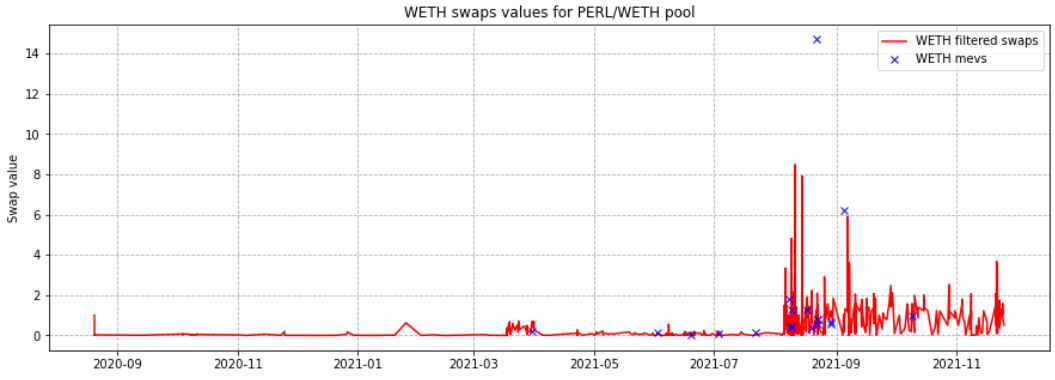


Picture X: swaps values distribution by type and by token

PERL/WETH simulation

This is a medium activity pool with medium level of values. Uniqueness of this case is that swaps activity in the pool is extremely small until August 2021, after which there is an extreme rise of swaps activity and rise of MEVs activity. This case was reviewed: there was a rise of reserves in the pool, which caused a rise of activity in the pool.

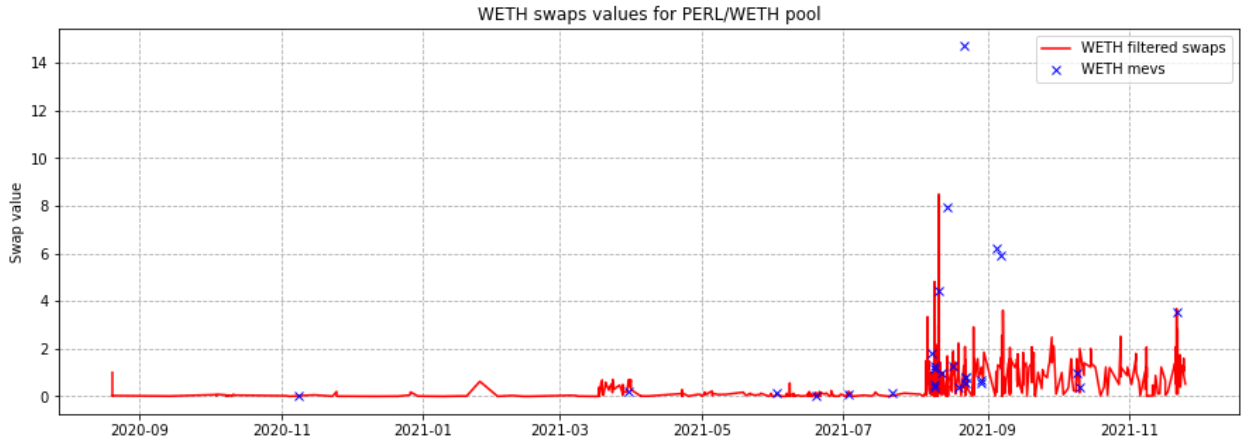
There were registered 19 MEVs with exact values matc, mean value of which is equal to 5 542,864020 USD, and 27 cases of MEVs with small values difference, mean value of which is equal to 7138,728061 USD. It is more likely that in the second case more real MEVs were caught.



Picture X: swaps values distributions by type (MEVs with exact values match)

MEVs with exact values match are not too coming out of the distribution, meaning that there are only some specific values of high-capitalization attacks. In case of taking non-exact

values matching MEVs there are more values out of the simple swaps distribution, causing their higher chances of catching real MEV attacks.



Picture X: swaps values distributions by type (MEVs with non-exact values match)

Profit extracted by the biggest capitalization MEV attack is equal to around 182 USD and profit is extracted via WETH token. Interesting moment is that here the same suspicious addresses as in previous cases.

	token_in	token_out	amount_in	amount_out	amount_usd	timestamp	sender
1427	WETH	PERL	3.561488	135030.161692	15543.012414	2021-11-21 16:01:04	0x55eb58655f8202ff839487886fedba2a1eb7b2d7
1428	PERL	WETH	139938.180486	3.772293	16463.005060	2021-11-21 16:01:04	0x55eb58655f8202ff839487886fedba2a1eb7b2d7
960	WETH	PERL	5.907399	236045.035008	23228.470565	2021-09-06 18:36:54	0x0000000000d41c96294ccdac8612bdfe29c641af
959	PERL	WETH	236234.171164	6.021829	23678.420292	2021-09-06 18:36:54	0x0000000000d41c96294ccdac8612bdfe29c641af
949	WETH	PERL	6.235537	228329.780408	24160.705959	2021-09-04 18:03:45	0x00000000003b3cc22af3ae1eac0440bcee416b40
948	PERL	WETH	228329.780408	6.361379	24648.304231	2021-09-04 18:03:45	0x00000000003b3cc22af3ae1eac0440bcee416b40
765	WETH	PERL	7.920742	323830.945439	25593.103680	2021-08-14 14:10:57	0x0000000000d41c96294ccdac8612bdfe29c641af
767	PERL	WETH	326236.808329	8.086365	26128.257320	2021-08-14 14:10:57	0x0000000000d41c96294ccdac8612bdfe29c641af
843	WETH	PERL	14.704514	407498.584031	47760.532767	2021-08-22 01:53:37	0x000000005736775feb0c8568e7dee77222a26880
845	PERL	WETH	407498.584031	14.729857	47842.849664	2021-08-22 01:53:37	0x000000005736775feb0c8568e7dee77222a26880

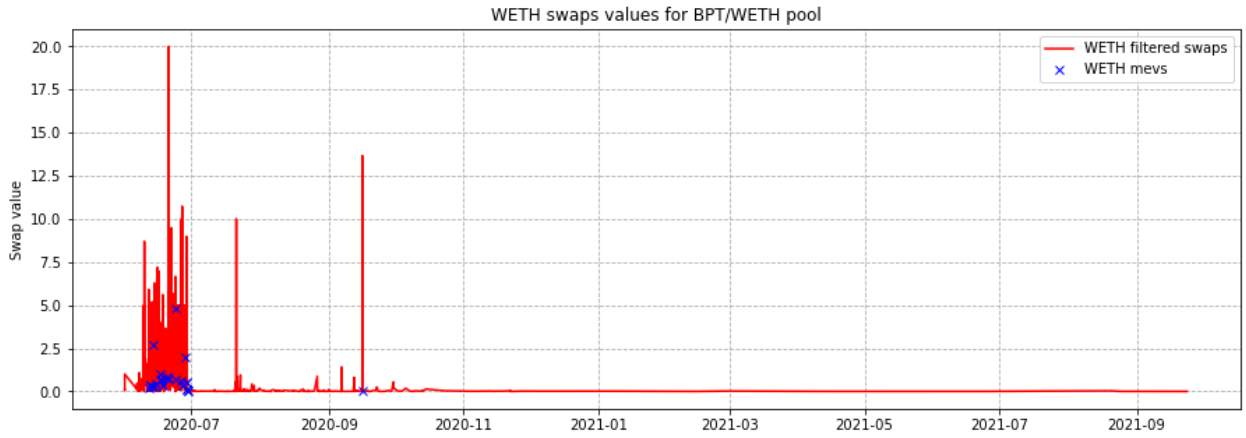
Picture X: top 10 MEV transactions by capitalization for PERL/WETH pool

BPT/WETH simulation

The first half of the current document reviewed the case of this pool, which became a victim of heavy attack with massive token extraction out of the pool and therefore traders lost their interest in this pool. Considering how negative the impact of the attack is, it is required to review it closely.

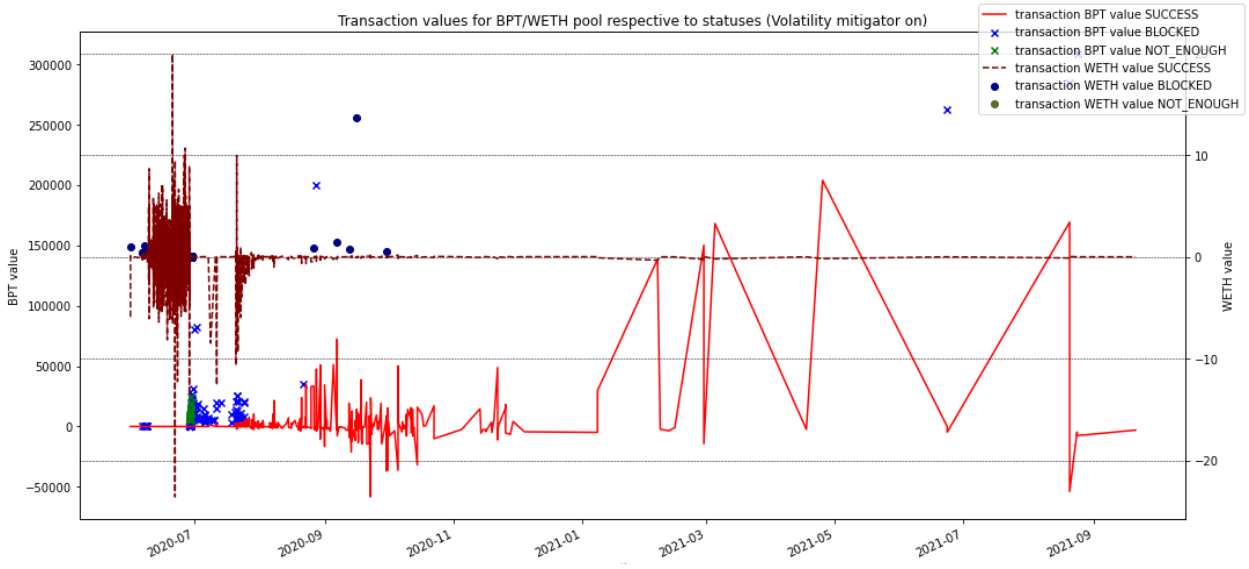
There are 21 MEVs performed with exact values match or 27 MEVs with small values difference for 3156 swaps totally performed in the pool. By reviewing the swaps values distributions for each of the tokens for both MEV cases can be seen that MEV attack values are not coming out of the simple swaps distributions, but overall distributions in the beginning is extremely unstable and contains too high for the current pool values (there are many cases of transactions with more than 5 WETH while original pool contained in the best moment around 175 WETH).

Considering the small number of MEV attacks and small transaction history it is not possible to collect useful information out of the count distribution.



Picture X: swaps values distribution by type (MEVs with small values difference)

Enabling Volatility mitigation mechanism does not only stabilize the price distribution and make pool reserves keep alive for a longer period of time, but also could save the pool.



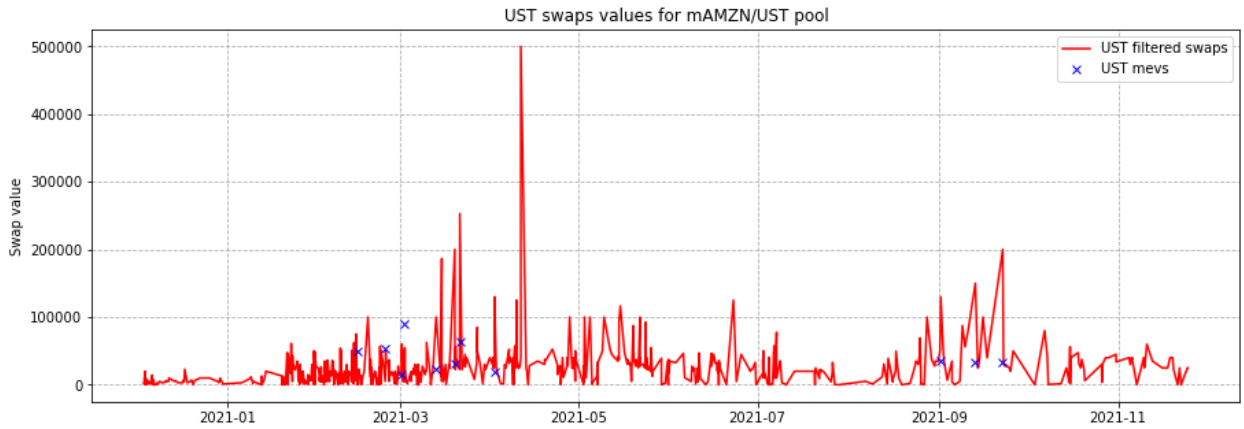
Picture X: swaps values with separation by type for each token

mAMZN/UST simulation

Current pool represents an interesting case of mirrored shares in pair with stablecoin (USD stablecoin present on the Terra blockchain). There are many interesting observations in this pool that will require deeper analysis:

- UST represents a stablecoin that represents USD coin in Terra blockchain, which conform information from coinmarketcap.com had no extreme price drops to around 0.50 USD values, while transactions present in the pool have capitalization two times smaller than the value of UST present in each transaction;
- Attacks are happening with low frequency and medium-level profit extraction (conform difference of capitalization of attacker's transactions can be seen that profit varies between 100 USD till 1100 USD).

Plot of the swap values distribution by transaction type shows that MEV transaction values are not coming out of the simple swaps distribution, meaning that mitigation mechanism may not be able to catch MEV attack cases. In the case of reviewing Volatility mitigation results it can be seen that the mechanism has not blocked any transaction through its entire history. Therefore, attacks are "hidden" in the noise of traders' activity. Another interesting moment is that profit extraction is performed via stablecoins (UST one).

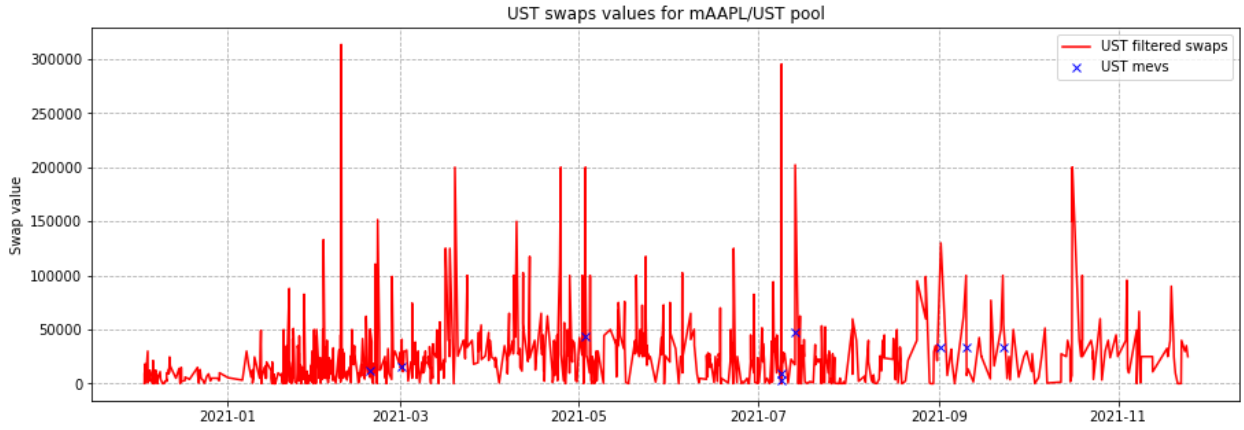


Picture X: swap values of transactions by their type (MEVs with exact values match)

Distributions of the traders' activity look promising and their behavior is healthy from multiple points of view: price deviation looks stable and has no extreme changes, activity is almost stable in terms of transaction frequency, reserves are changing gradually and all transactions have small slice factor with small differences of out values. Such distributions show promising results and the current pool may have a long lifecycle in the future.

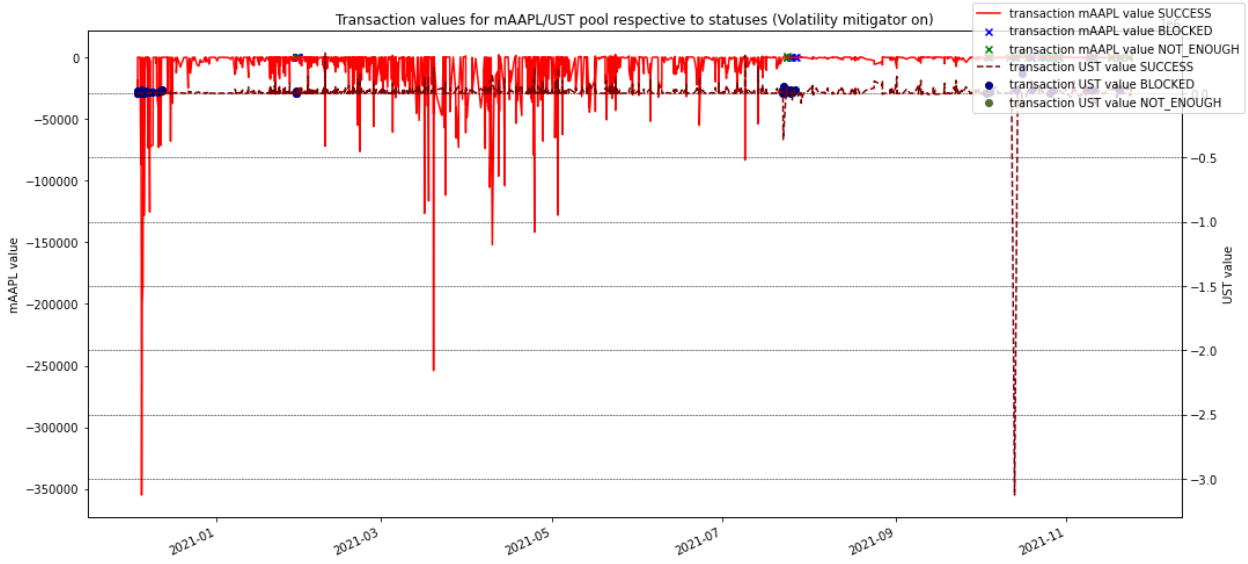
mAAPL/UST simulation

Values of MEV attack transactions are not coming out of the simple swaps distribution, meaning that it would not be possible to block them via mitigation mechanism, but values of the distribution have high deviation, which considering reserves makes them cause extreme price changes. Mitigation mechanism is able to stabilize price distributions, smooth distributions of the reserves in the pool. But there were MEV attacks blocked by the mechanism, meaning that it is a good application for pool activity stabilization, but not for attack prevention in the current pool.



Picture X: swaps values distributions by type (MEVs with exact values match)

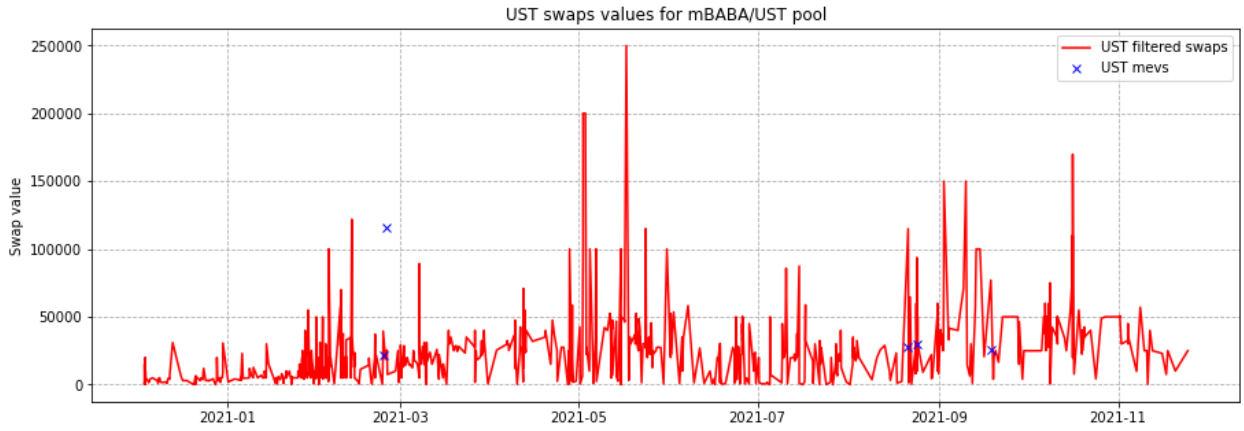
Activity in the pool is unhealthy considering the strange pattern of extracting profits only by token price manipulations without need of a third side and “inner shape” of the values distribution with multiple blocks of transactions.



Picture X: token movement in transactions by category and by token

mBABA/UST simulation

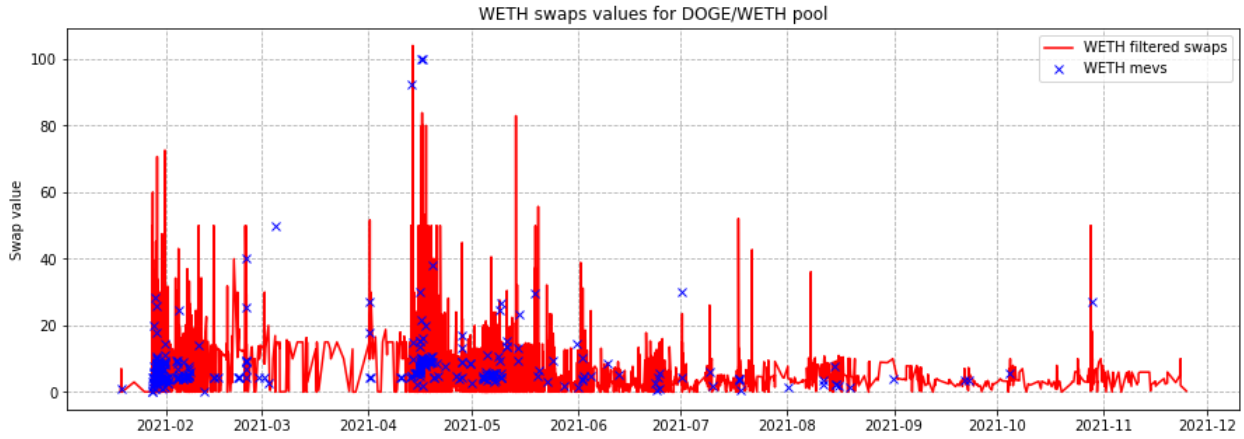
Current pool case is almost identical to the case of mAAPL/UST. From other perspectives distributions are healthy, their properties are clear, and the mitigation mechanism does not see any out of the distribution activity. The only problem is that some unique transactions reach a level of several hundreds of thousands UST, which may cause disturbance in the token prices.



Picture X: swaps values distribution by category

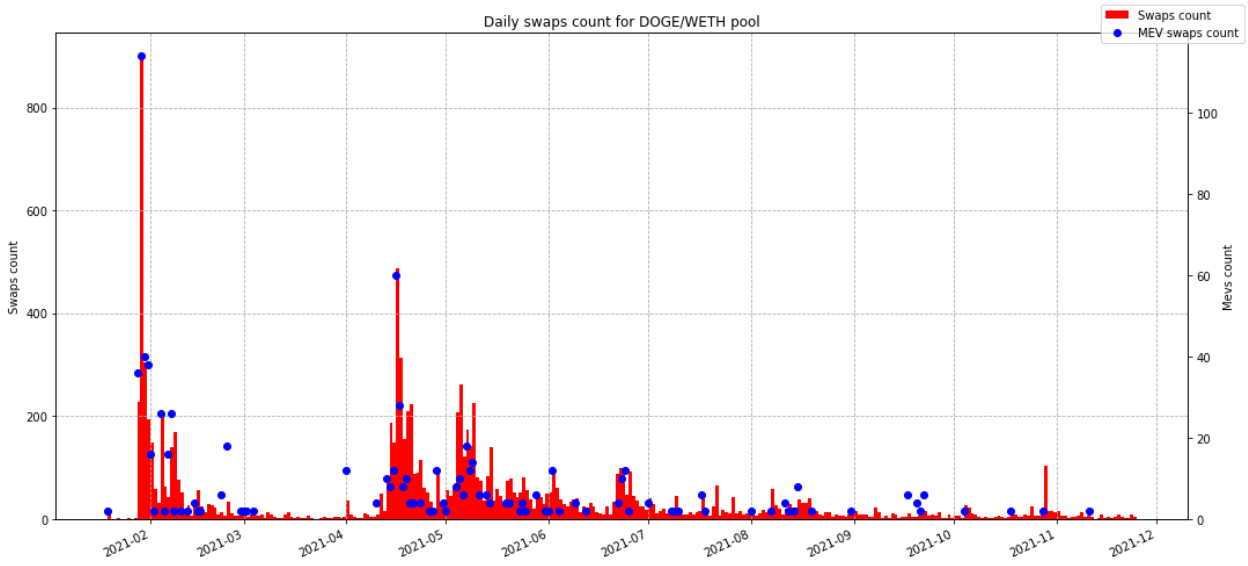
DOGE/WETH simulation

Pool contains medium size transaction history with 331 cases of MEVs where values have exact match and 388 MEVs where values have small value differences. The biggest MEV profit extracted conform capitalization of transactions is equal to 9119.93 USD. MEV transaction values are noisy and they represent both cases of transactions not coming out of the distribution and cases when values are too high compared to the distribution of other swaps. Distribution is unstable with high deviation of values.



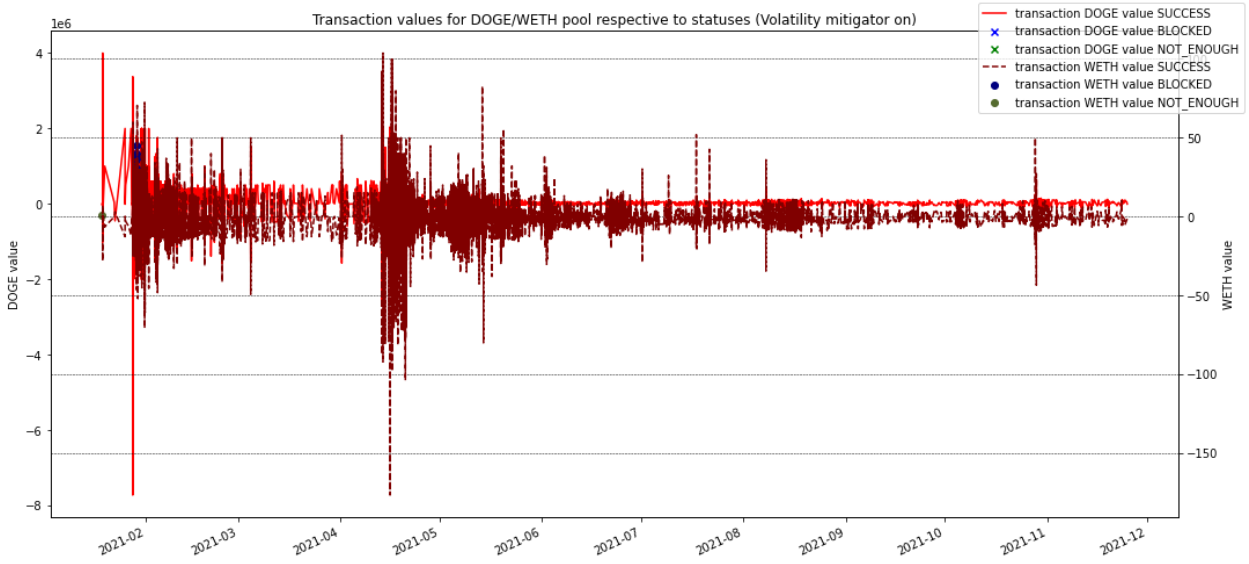
Picture X: swaps values distribution by category (MEVs with exact values match)

Current case contains a medium size transaction history with high frequency of the attacks, meaning that it is possible to show count distributions to check how the amount of attacks correlates with the amount of simple transactions, creating a direct dependency.



Picture X: count distribution of transactions and MEV transactions

There are 20 transactions blocked by the volatility mitigation mechanism and most of the blocks are happening in the beginning of transaction history. Token movement in the distribution looks healthy with small price deviation. Mitigation has blocked only 3 attacks.



Picture X: token movement in transactions by category and by token

The biggest extracted profit is equal to the 9 119.93 USD conform capitalization of each transaction. In case of taking activity of the account that extracted profit out of the chosen MEV attack can be seen that there is the same principle of activity as in case of all previously reviewed MEV bots, meaning that it is likely to be another MEV bot. Bot takes the same 4-transactions sequence for chosen moment of time.

0x08402572f2ed55394...	230 days 17 hrs ago	Uniswap V2: LEASH	IN	0x59903993ae67bf48f...	6.106599970199031037	Wrapped Ethe... (WE
0x08402572f2ed55394...	230 days 17 hrs ago	0x59903993ae67bf48f...	OUT	Uniswap V2: LEASH	5.926542580478727065	DOGE KILLER (LEAS
0x6baafe06409e9f2e8c...	230 days 17 hrs ago	Uniswap V2: LEASH	IN	0x59903993ae67bf48f...	5.926542580478727065	DOGE KILLER (LEAS
0x6baafe06409e9f2e8c...	230 days 17 hrs ago	0x59903993ae67bf48f...	OUT	Uniswap V2: LEASH	6.010628164854594006	Wrapped Ethe... (WE

Picture X: example of transaction history for account that extracted highest profit out of the MEV attack conform capitalizations

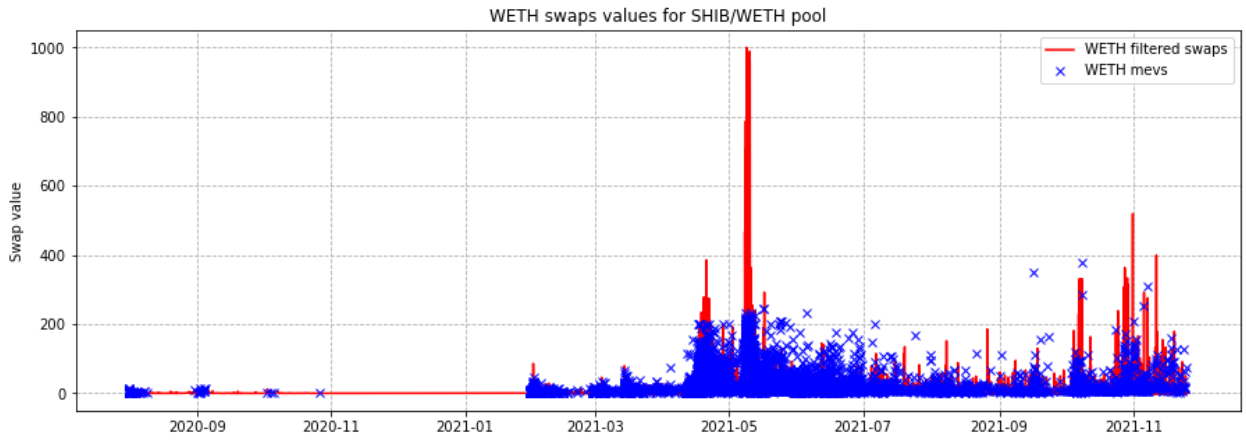
Interesting pattern of this case is that the bot extracts profit by taking out of the pools popular WETH token. Internal transactions have an interesting pattern of performing interaction with UUPool (most likely, bot is exchanging tokens). Currently, conform information from Etherscan there is no activity from this address, meaning that bot was disabled.

0xc24a1a8278b605477...	12661578	227 days 12 hrs ago	0x59903993ae67bf48f...	→	UUPool	0.053043349688709112 Ether
0xc24a1a8278b605477...	12661578	227 days 12 hrs ago	Wrapped Ether	→	0x59903993ae67bf48f...	0.053043349688709112 Ether
0xfe70820834258b0e9...	12659349	227 days 20 hrs ago	0x59903993ae67bf48f...	→	UUPool	0.049965687747354624 Ether
0xfe70820834258b0e9...	12659349	227 days 20 hrs ago	Wrapped Ether	→	0x59903993ae67bf48f...	0.049965687747354624 Ether

Picture X: internal transactions for account that extracted highest profit conform transaction capitalizations

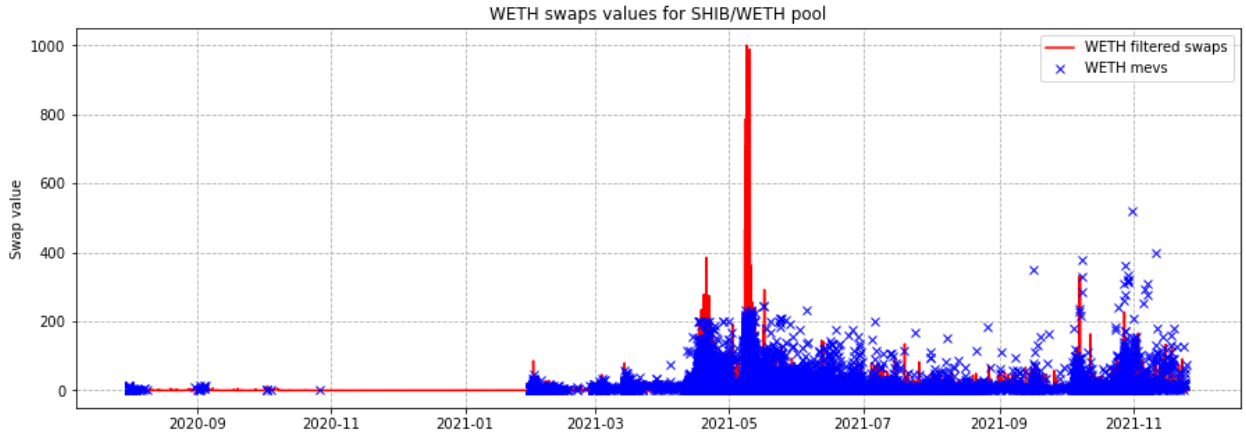
SHIB/WETH simulation

Pool has one of the biggest reviewed transaction histories and one of the largest list of MEV attacks. Out of 1 219 045 transactions there are 8 206 MEV attacks with exact transaction values match and 12 902 MEV attacks with small transaction values difference. Most of the attacks are happening after the rise of the activity in the pool (which happened during February 2021). In case of taking exact values match MEV attacks can be seen how noisy is the distribution and how many MEVs are registered. Most attacks were performed with values not coming out of the distribution of simple swaps and therefore it is required to see their capitalization and profits closer.

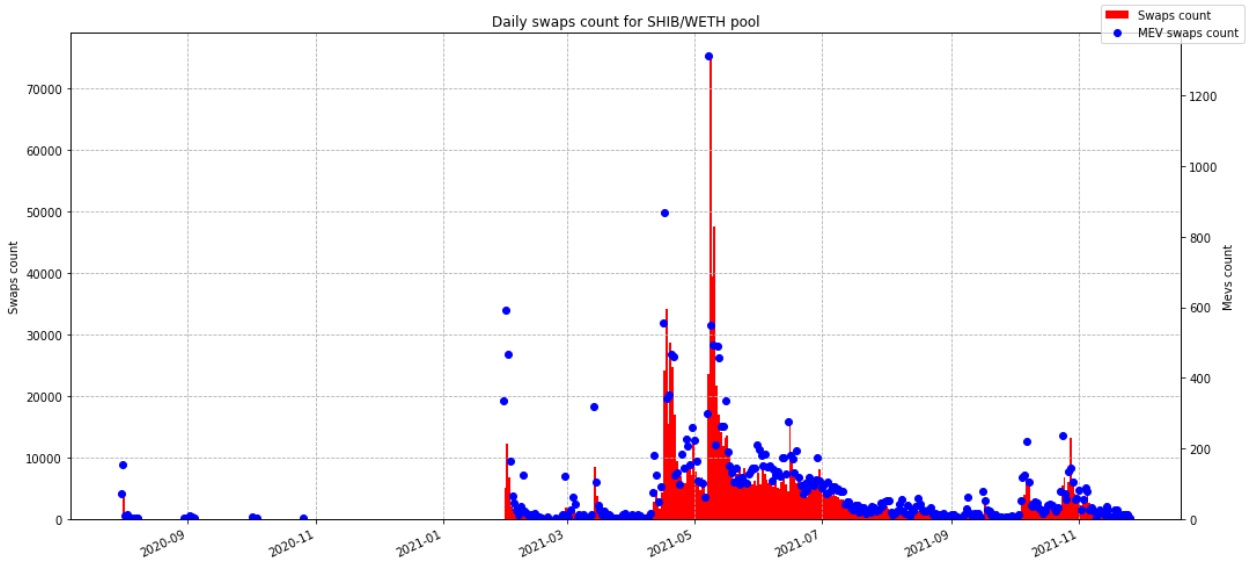


Picture X: swaps values distributions by category (MEVs with exact values match)

MEVs with small transaction value differences add new cases of transactions out of the distribution with relatively big values, meaning that those transactions are likely to be real attacks.

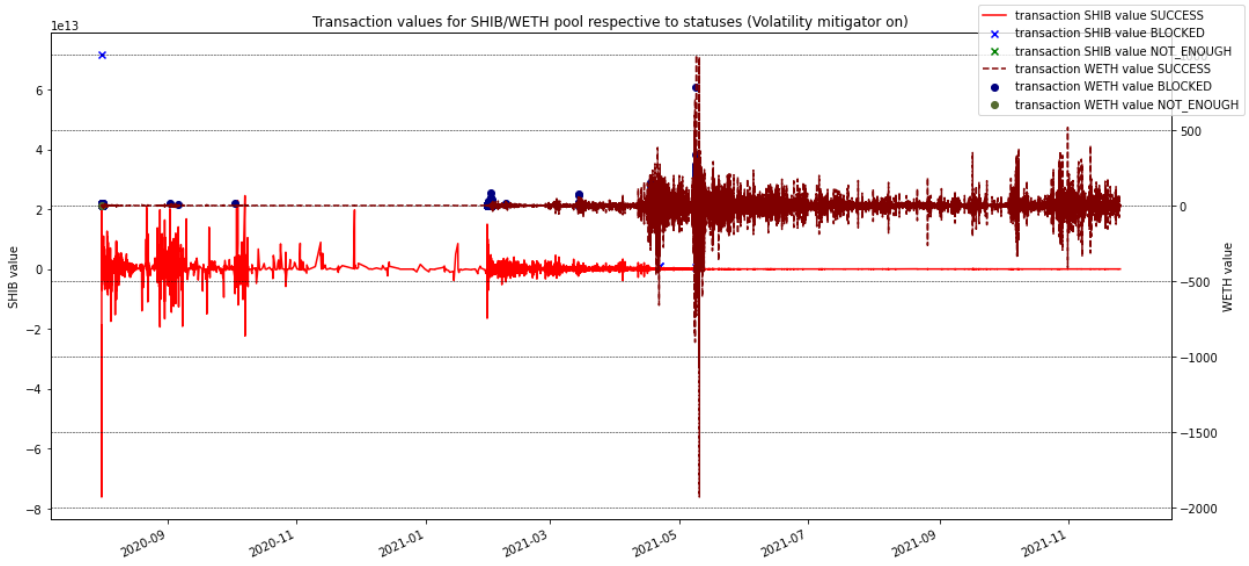


There is a correlation between MEVs and swaps count distributions with almost perfect shape similarity. Another interesting moment is that the MEV frequency is extremely high, raising the question of possible higher interest in meme-tokens pools compared to the STO-token pools.



Picture X: transaction count with separation by type (MEVs with small value differences)

Mitigation mechanism was able to prevent 436 exact value attacks and 473 small value difference attacks, meaning that mitigation mechanism is able to influence on the attacks with extreme values, out of the distribution of other swaps.



Picture X: token movement in the pool by transaction type and status

The biggest profit extracted from the MEV attack is 98 538.79 USD. Capitalization of attack is high (around 600 thousands USD) and it is required to dive deeper in this case. In case of taking MEV attacker account transactions using Etherscan can be seen that it performs similarly with MEV bot behavior. Internal transactions are performed for profit extraction to other pools and can be seen that this account is connected with miners accounts.

0x74c7a7a319f94cefe4...	163 days 5 hrs ago	0x83f893cc6610bfc695...	OUT	Uniswap V2: KYL 6	9,949.97086285255360881	Kylin Networ... (KYL)
0x74c7a7a319f94cefe4...	163 days 5 hrs ago	Uniswap V2: KYL 6	IN	0x83f893cc6610bfc695...	1.056249994887581725	Wrapped Ethe... (WETH)
0xafb79c13bb70f6b586...	163 days 5 hrs ago	0x83f893cc6610bfc695...	OUT	Uniswap V2: KYL 6	1.049377510353465756	Wrapped Ethe... (WETH)
0xafb79c13bb70f6b586...	163 days 5 hrs ago	Uniswap V2: KYL 6	IN	0x83f893cc6610bfc695...	9,949.97086285255360881	Kylin Networ... (KYL)

Picture X: example of transactions performed by the account with highest profit from capitalization perspective

Internal transactions also contain the same addresses, as ones raised in previous cases (for example, the miner account ending with 707). In most cases, the profit is small. Bot finished his activity around August 2021.

0xca32f36056b46a992...	13074518	163 days 2 hrs ago	0x83f893cc6610bfc695...	Miner: 0x01C...8cf	0.007685879579231476 Ether
0x6fcfc43bd6cc3389d0...	13073976	163 days 4 hrs ago	0x83f893cc6610bfc695...	BeePool	0.015674499055436362 Ether
0xd49f536743351f977f...	13073802	163 days 5 hrs ago	0x83f893cc6610bfc695...	ETH.SoloPool.org	0.001325959786119543 Ether
0x74c7a7a319f94cefe4...	13073697	163 days 5 hrs ago	0x83f893cc6610bfc695...	ETH.SoloPool.org	0.002939419505563925 Ether
0xe5e81f622b6639686...	13072796	163 days 9 hrs ago	0x83f893cc6610bfc695...	BeePool	0.030056006072001956 Ether
0xc920130eb7f627742...	13072763	163 days 9 hrs ago	0x83f893cc6610bfc695...	BeePool	0.00298943235624114 Ether
0xadf4db56d40fa902c1...	13072641	163 days 9 hrs ago	0x83f893cc6610bfc695...	AntPool 2	0.030165661459499674 Ether
0x67d209fc4931a1dab...	13072389	163 days 10 hrs ago	0x83f893cc6610bfc695...	BTC.com Pool	0.016122140793704723 Ether
0xd147bdc1c716dd615...	13072372	163 days 10 hrs ago	0x83f893cc6610bfc695...	MiningPoolHub	0.28246827542792876 Ether
0xb35505b0f594b4217...	13072327	163 days 10 hrs ago	0x83f893cc6610bfc695...	Miner: 0xb7e...707	0.00715934760276036 Ether

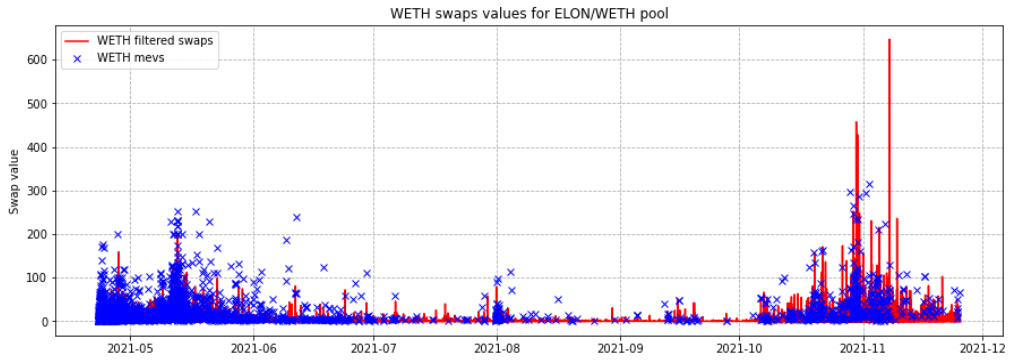
Picture X: example of internal transactions performed by MEV bot account with highlighted cases of sending tokens to the miners' accounts

This attacker performed 407 attacks on the SHIB/WETH pool, demonstrating the requirement of constructing a table of MEV profits and attacks to highlight most active accounts performing attacks.

ELON/WETH simulation

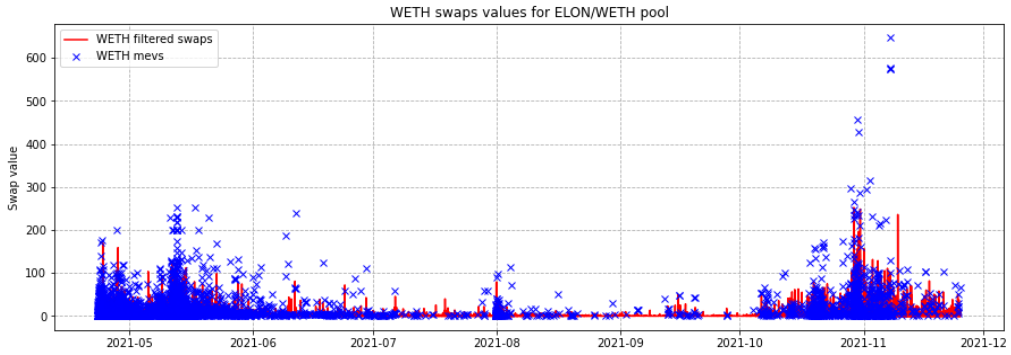
Out of 307 302 transactions there are 3705 MEV attacks with exact values match and 4920 MEV attacks with small values difference. Such properties require deeper analysis of the current pool to check MEV behavior and dive into some unique cases.

Compared to the previous cases, MEV attacks are present at the entire range of registered values in the pool with multiple cases of values out of the simple transactions distributions. Volatility mitigation mechanism is able to block transactions with extremely high values (more likely that they will cause extreme price changes which will attract attention of the mitigation mechanism.



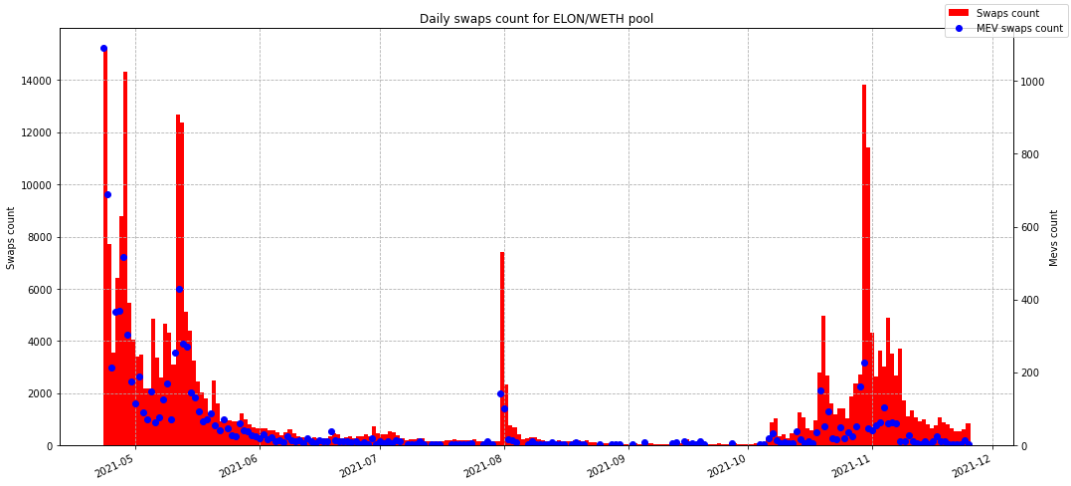
Picture X: swaps values by their type (MEVs with exact values match)

In the case of considering MEVs with small value differences there are more transactions with extreme values, greatly reducing the range of simple transactions.



Picture X: swaps values by their type (MEVs with small values difference)

Transaction count distribution demonstrates in both cases dependency of attacks from the amount of simple swaps. Can be observed that small difference MEVs correlate better with the shape of the simple swaps.



Picture X: transaction count distributions by type

Highest extracted profit from performing MEV attack was 133 622,62 USD, making it one of the biggest registered profits. Transactions in attack have extreme capitalization of around 1.2 millions USD. In the case of taking the address of the attacker on Etherscan can be seen that this attacker has extremely high profits.

0xd8a8aa0b0a923347...	14113173	1 day 2 hrs ago	0x1d6e8bac6ea373082...	→	F2Pool Old	0.000470547769390022 Ether
0x42d5aafda9e42ed43...	14110315	1 day 13 hrs ago	0x1d6e8bac6ea373082...	→	Ethermine	0.444791377037393505 Ether
0xc6334e295a48b28d8...	14108574	1 day 20 hrs ago	0x1d6e8bac6ea373082...	→	0xc280ac0b1b91d1d9c...	0.0096876421 Ether
0xc6334e295a48b28d8...	14108574	1 day 20 hrs ago	0x1d6e8bac6ea373082...	→	0x74b892425a206eb2...	2.571459375506106173 Ether
0xc6334e295a48b28d8...	14108574	1 day 20 hrs ago	0x1d6e8bac6ea373082...	→	0x30b8235f492265a73...	9.248065403383692169 Ether
0xc6334e295a48b28d8...	14108574	1 day 20 hrs ago	0x1d6e8bac6ea373082...	→	0x4f69c5b694d5a14a0...	1.465202169405574751 Ether
0xc6334e295a48b28d8...	14108574	1 day 20 hrs ago	Wrapped Ether	→	0x1d6e8bac6ea373082...	13.294414590395373093 Ether
0x0c229980ab28bea97...	14098506	3 days 9 hrs ago	0x1d6e8bac6ea373082...	→	0xc280ac0b1b91d1d9c...	0.0114079781 Ether
0x0c229980ab28bea97...	14098506	3 days 9 hrs ago	0x1d6e8bac6ea373082...	→	0x74b892425a206eb2...	24.66230257579458382 Ether
0x0c229980ab28bea97...	14098506	3 days 9 hrs ago	0x1d6e8bac6ea373082...	→	0x30b8235f492265a73...	30.870407704250872595 Ether
0x0c229980ab28bea97...	14098506	3 days 9 hrs ago	0x1d6e8bac6ea373082...	→	0x4f69c5b694d5a14a0...	12.852300798594221947 Ether
0x0c229980ab28bea97...	14098506	3 days 9 hrs ago	Wrapped Ether	→	0x1d6e8bac6ea373082...	68.396419056739678362 Ether

Picture X: example of internal transactions performed by suspicious account (highlighted high transaction values)

Each second, third or fourth day there are high values transmitted WETH tokens. It also interacts with miners.

31 days 11 hrs ago	0x5437b2fe9ca1f47450...	call	0x1d6e8bac6ea373082...	→	0xc280ac0b1b91d1d9c...	0.0081823481 Ether
	0x5437b2fe9ca1f47450...	call	0x1d6e8bac6ea373082...	→	0x74b892425a206eb2...	18.260251353705933 Ether
	0x5437b2fe9ca1f47450...	call	0x1d6e8bac6ea373082...	→	0x4f69c5b694d5a14a0...	6.115339360104342 Ether
	0x5437b2fe9ca1f47450...	call	Wrapped Ether	→	0x1d6e8bac6ea373082...	24.383773061910276 Ether
31 days 11 hrs ago	0xc8dc2998fad497e9c...	call	0x1d6e8bac6ea373082...	→	Flexpool.io	0.261976988891264 Ether
31 days 19 hrs ago	0x81b9f35c2f9e993db2...	call	0x1d6e8bac6ea373082...	→	Miner: 0xcd4...f9c	0.020655325492588 Ether

Picture X: internal transactions performed by suspicious account (highlighted miner's account and high transaction values)

In case of reviewing ERC-20 transactions it can be seen that the account repeats activity of the MEV bots with the same 4 transaction sequences with extraction of profits via getting WETH tokens. The principle is in getting some tokens from some AMM platform and then to perform exchange tokens is such a way to extract profit in another token and then return taken from the platform tokens back, keeping extracted ones by market manipulations.

0x96ba21415b57e732...	1 hr 25 mins ago	Uniswap V2: SATA	IN	0x1d6e8bac6ea373082...	0.707142583708841738	Wrapped Ethe... (WETH)
0x96ba21415b57e732...	1 hr 25 mins ago	0x1d6e8bac6ea373082...	OUT	Uniswap V2: SATA	3,598.758350650864566504	Signata (SATA)
0x37dd8875614ece0bf...	1 hr 25 mins ago	0x1d6e8bac6ea373082...	OUT	Uniswap V2: SATA	0.684055685731207569	Wrapped Ethe... (WETH)
0x37dd8875614ece0bf...	1 hr 25 mins ago	Uniswap V2: SATA	IN	0x1d6e8bac6ea373082...	3,598.758350650864566504	Signata (SATA)
0x470d51dfe9432cbafa...	1 hr 35 mins ago	Uniswap V2: LOOKS 3	IN	0x1d6e8bac6ea373082...	118.703477002245339384	Wrapped Ethe... (WETH)
0x470d51dfe9432cbafa...	1 hr 35 mins ago	0x1d6e8bac6ea373082...	OUT	Uniswap V2: LOOKS 3	61,018.801218488822069856	LooksRare To... (LOOKS)
0x3f9c1b8caf4371fd19...	1 hr 35 mins ago	0x1d6e8bac6ea373082...	OUT	Uniswap V2: LOOKS 3	115.627320478617878657	Wrapped Ethe... (WETH)
0x3f9c1b8caf4371fd19...	1 hr 35 mins ago	Uniswap V2: LOOKS 3	IN	0x1d6e8bac6ea373082...	61,018.801218488822069856	LooksRare To... (LOOKS)

Picture X: transaction history of the pool with highlighted cases of how profit is extracted

Current case may be the most performant MEV bot with extremely high profits. It is required to pay higher attention to this case and it would be great to construct a table of profits and attacks performed by each MEV-related account.

AXS/WETH simulation

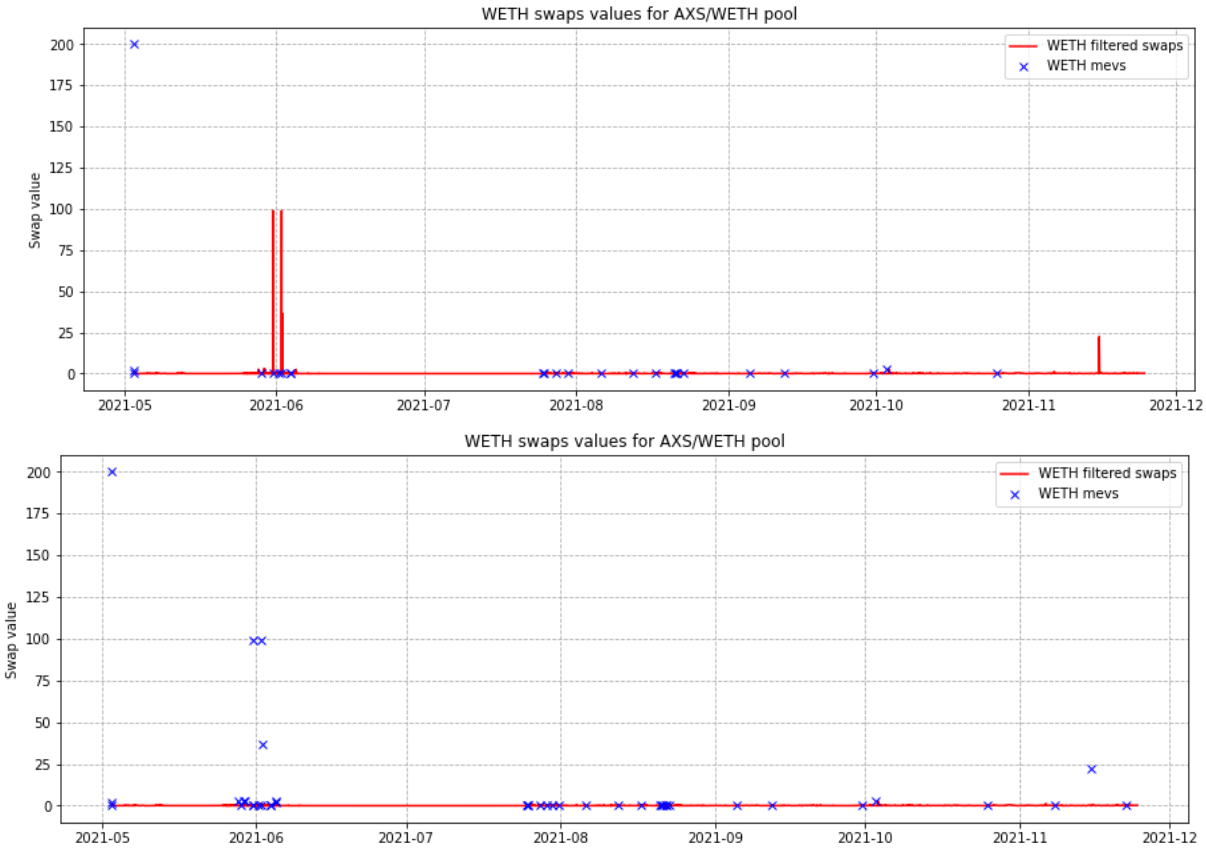
Out of 4 588 transactions there are 25 MEVs with exact values and 42 MEVs with small transaction values difference. In case of taking only capitalization of transactions it is possible to estimate by error extremely high profit via transaction capitalizations.

token_in	token_out	amount_in	amount_out	amount_usd	timestamp	sender	to
AXS	WETH	1453.949686	200.157590	312150.092977	2021-05-03 01:42:48	0xd78a3280085ee846196cb5fab7d510b279486d44	0xf6da21e95d74767009accb145b96897ac3630bad
WETH	AXS	200.000000	1453.949686	602630.784000	2021-05-03 01:42:48	0xd78a3280085ee846196cb5fab7d510b279486d44	0xf6da21e95d74767009accb145b96897ac3630bad

Picture X: example of error in transaction capitalizations

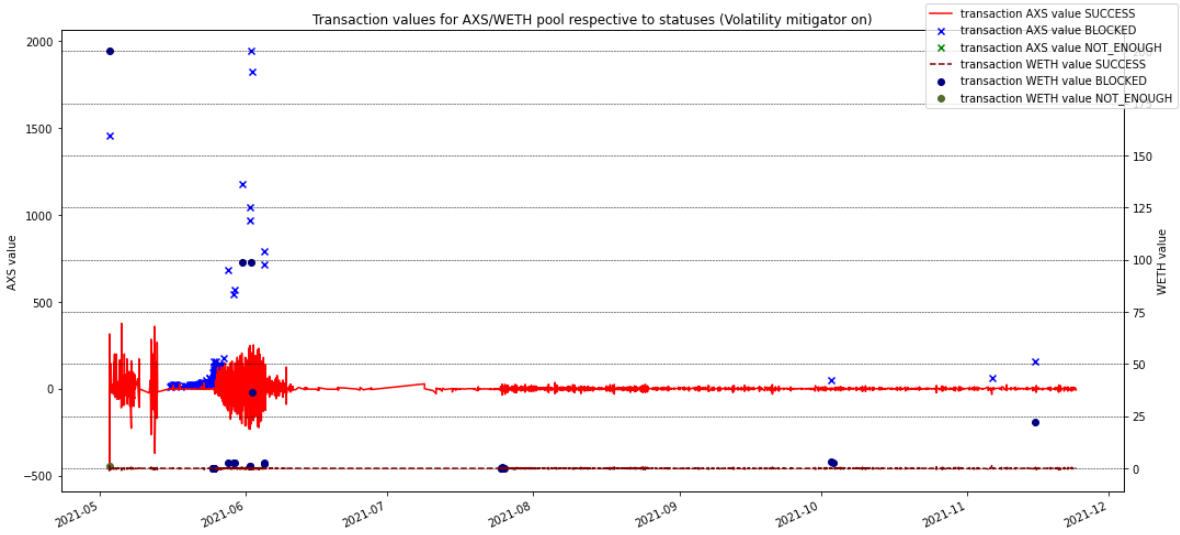
While the second transaction in the presented sequence contains capitalization close to the real one (200 WETH conform price at 3 May 2021 of 3 282,26 USD are equal to 656 452 USD) while the first one contains capitalization is two times smaller. For this reason it is required to check extracted during attack tokens with their recalculation into USD. Still, in the presented case the attacker extracted 0.157590 WETH (or 517,25 USD).

MEV attacks with exact values matches mostly are not coming out of the distribution of simple swaps, reducing chances of being blocked by the Volatility mitigation mechanism. In case of taking MEVs with small values differences there are many values out of the simple transactions distribution.



Picture X: swaps values distributions by transaction type (first one represents MEVs with exact values match, second one represents MEVs with small values differences)

Token movement distributions demonstrate healthy distributions with multiple blocks performed by Volatility mitigation. There were 5 MEVs with exact value matches and 23 MEVs with small value differences blocked by Volatility mitigation.

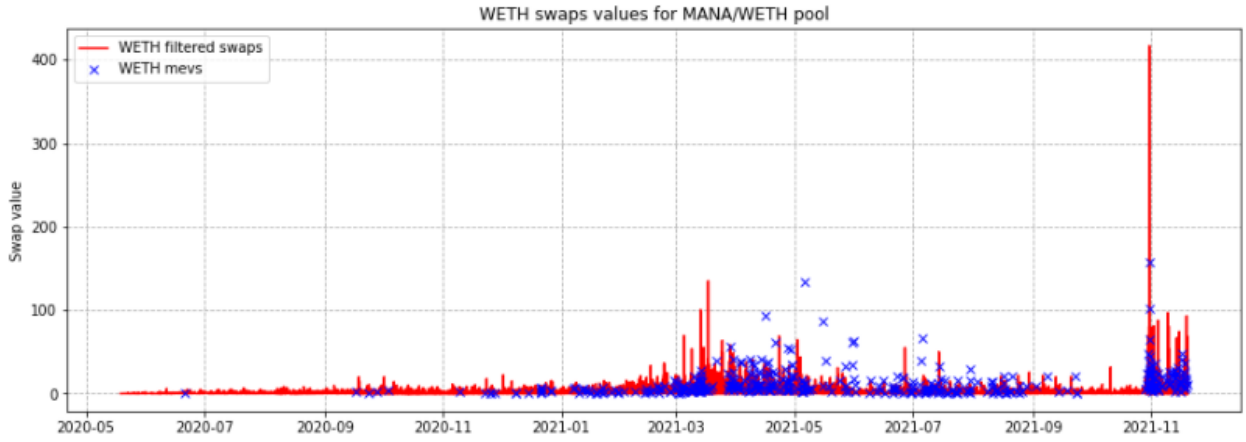


Picture X: token movement by transaction statuses in the AXS/WETH pool

All blocked transactions are out of the simple swaps distribution and reserves in case of mitigated pool have more stable distribution with different reserves relation.

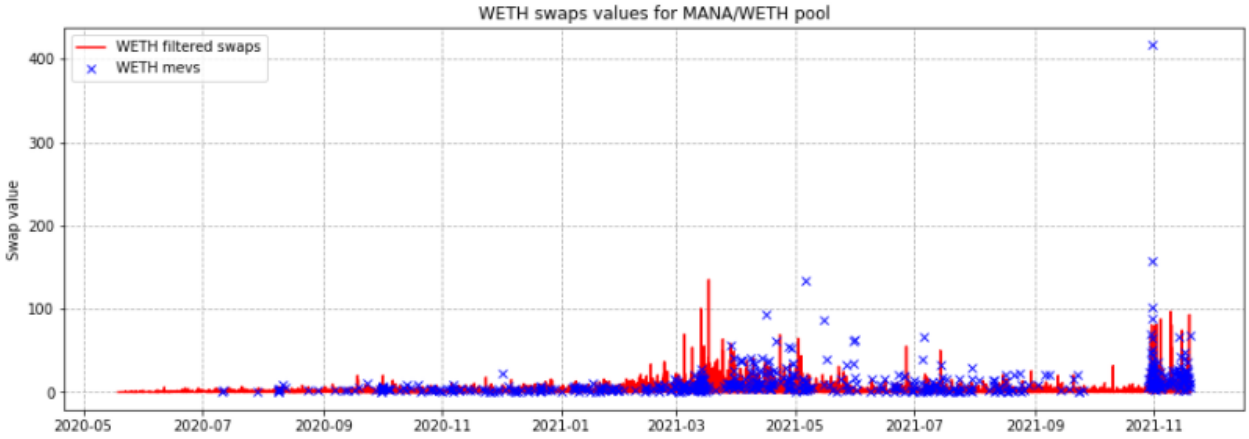
MANA/WETH simulation

Out of 72 thousands transactions there are 412 MEVs with exact value matches and 571 MEVs with small transaction value differences. The biggest extracted profit by transaction capitalization is 18 413,42 USD or 4.291188 WETH. This attack was performed by the same address as in the case of the most profitable MEV attack in case of the ELON/WETH pool. This moment ensures the requirement of constructing a general table of all addresses involved in performing MEV attacks.



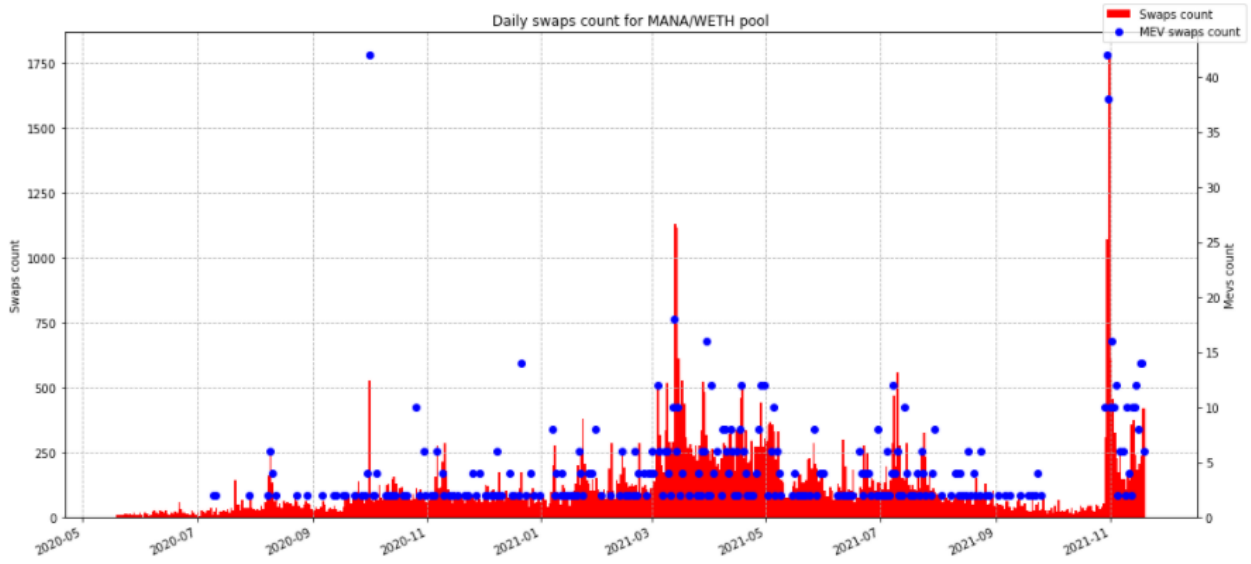
Picture X: swaps values by transaction category (MEVs with exact value matches)

In case of taking MEVs with small values difference there are more transactions with extremely high values that are out of the simple swaps distribution.



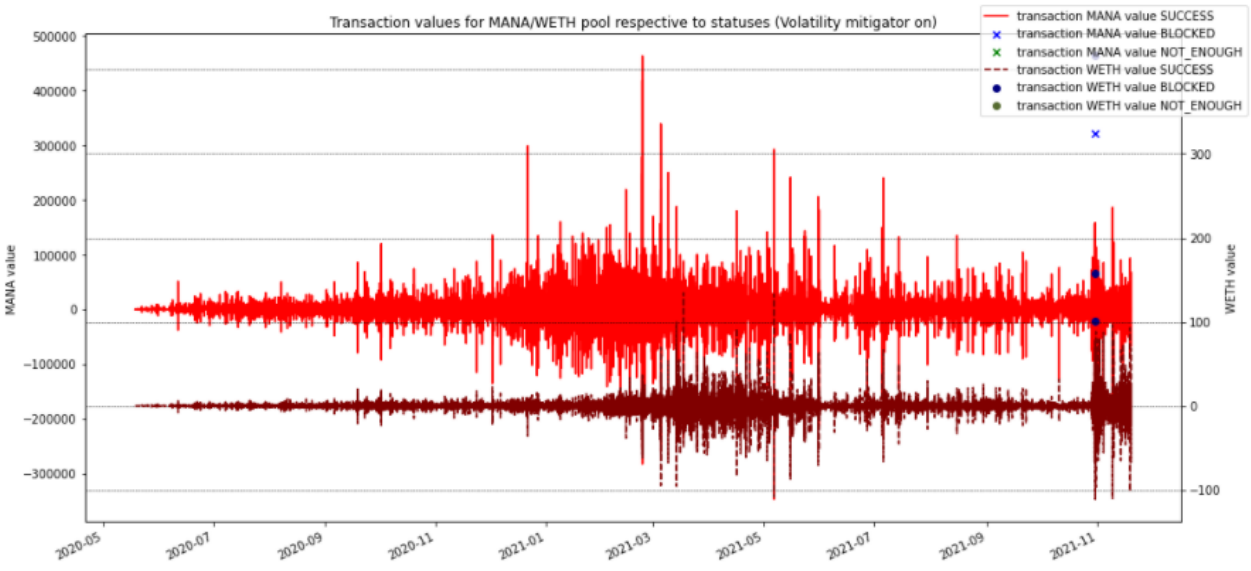
Picture X: swaps values by transaction category (MEVs with small transaction value differences)

In case of reviewing transaction count distributions it can be seen that there is a correlation between MEV attacks and traders' activity. MEV activity is medium.



Picture X: transaction count distributions by transaction category (MEVs with small transaction value differences)

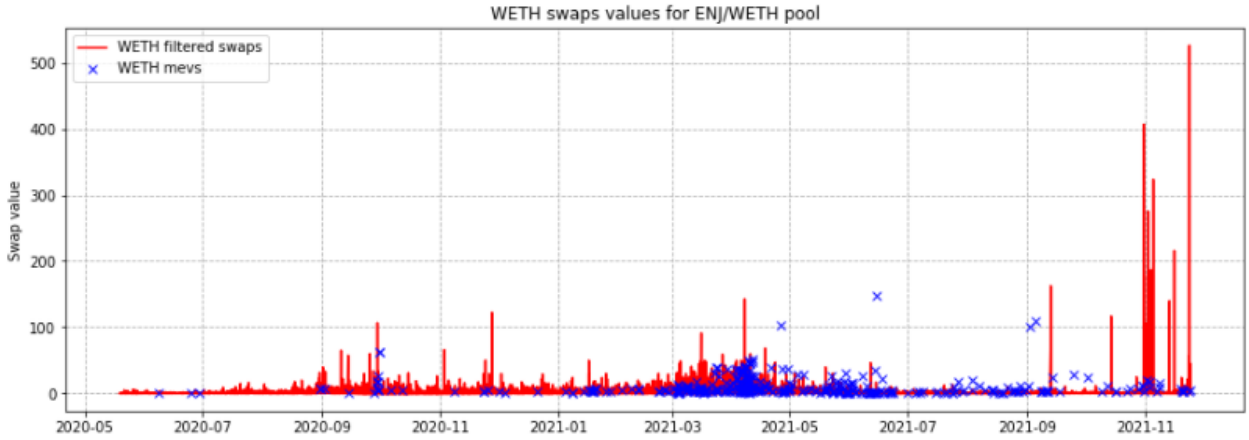
Token movement in the pool shows healthy pool activity and that there almost are no blocked transactions. Only 4 transactions have been blocked, two of which are MEVs with exact value matches and all 4 of which are MEVs with small value differences.



Picture X: token movement of the MANA/WETH pool by category

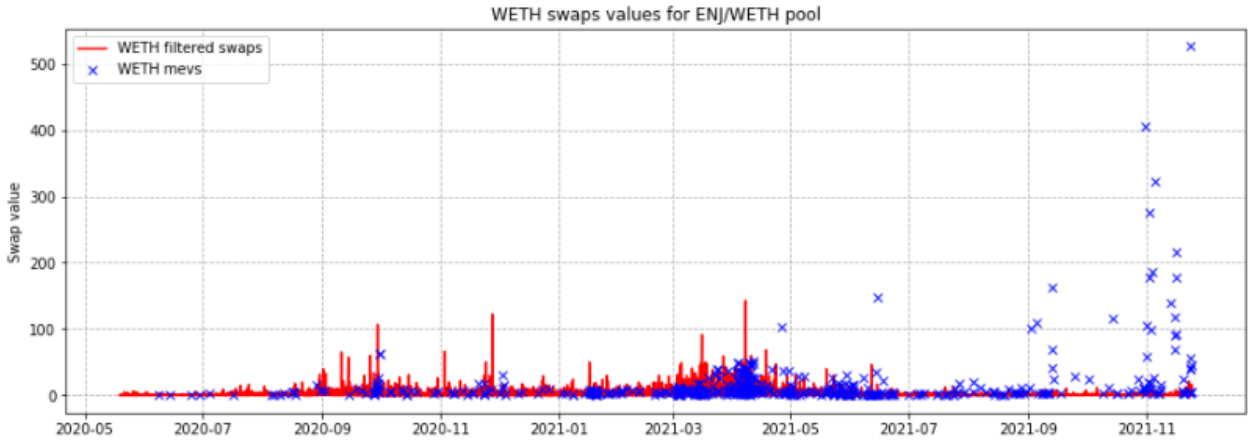
ENJ/WETH simulation

Out of 74 876 transactions there are 396 MEVs with exact value matches and 532 MEVs with small value differences. The biggest extracted profit is 4 299,35 USD, when the attacker extracted 1,144244 WETH.



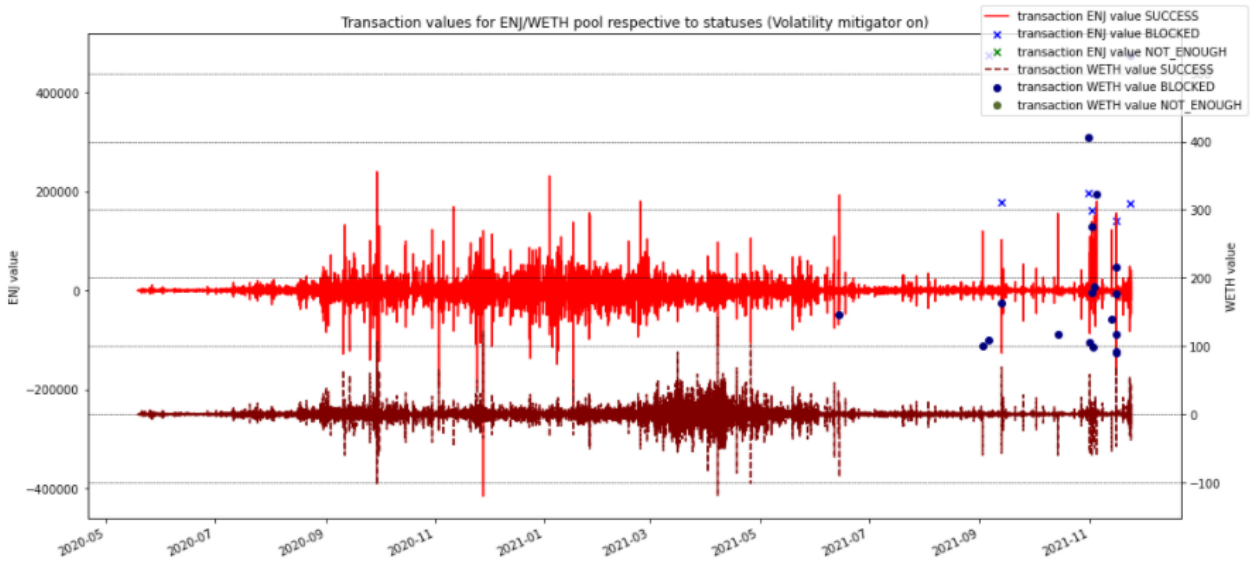
Picture X: swaps values by category (MEVs with exact value matches)

MEVs form a noisy distribution with a small count of high-value MEVs, while most of them are represented by values in a range of simple swaps. Volatility mitigation mechanisms most likely will block transactions with high values.



Picture X: swaps values by category (MEVs with small transaction value differences)

MEVs with small transaction value differences add new cases of extremely high transaction values out of the simple swaps distribution. Amount of transactions is small compared to the swaps activity, meaning that transaction count distribution will not show real correlation between attacks and traders' activity. There are 25 transactions blocked that can be seen on token movement in the pool.

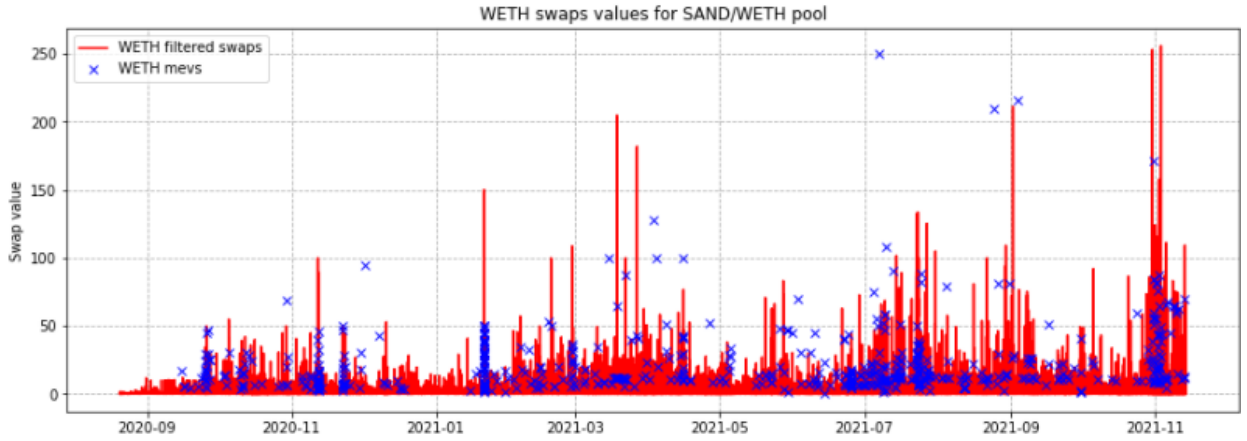


Picture X: transaction movement by category and status

Volatility mitigation mechanism blocked 4 MEVs with exact value matches, while in case of MEVs with small value differences there were 25 attacks blocked.

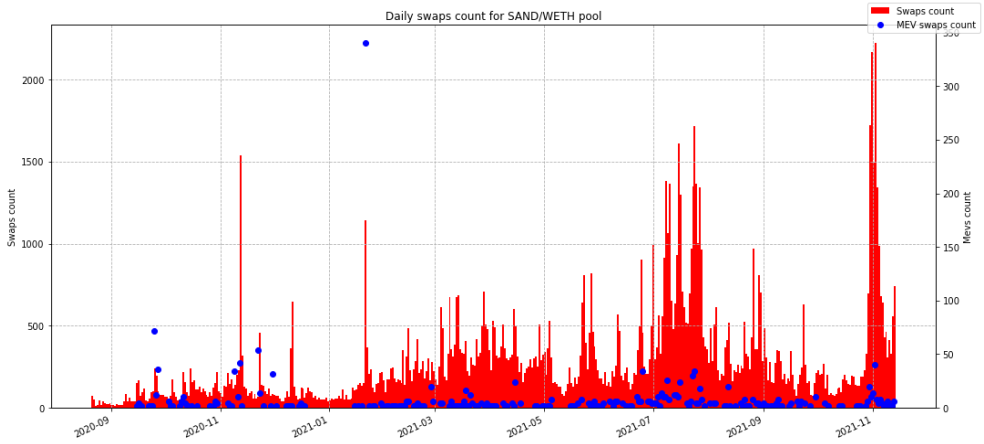
SAND/WETH simulation

Out of 129 994 transactions there are 647 MEV attacks with exact transaction value matches and 703 MEV attacks with small value differences. The biggest extracted profit is 17 749,21 USD or 4,14856 USD, by the same address that performed extremely profitable attacks on ELON/WETH and MANA/WETH.



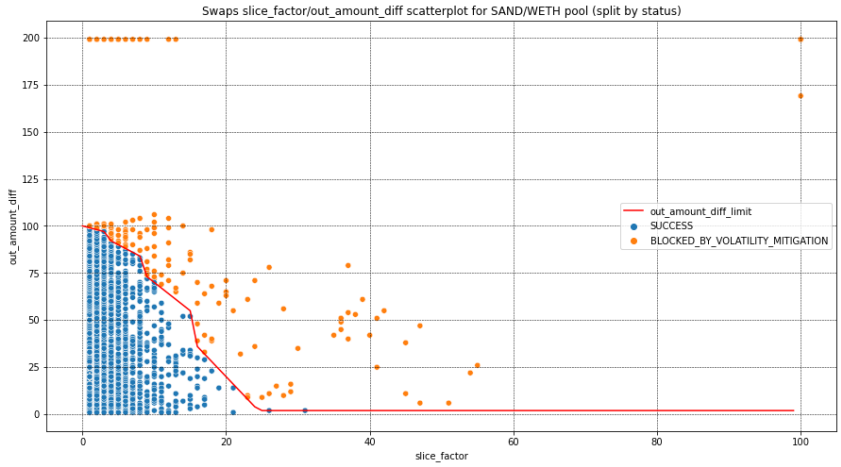
Picture X: swap values distribution

Count distribution demonstrates correlation between swaps and performed MEV attacks. In the case of reviewing possible MEVs with small values differences can be seen that correlation is better. Exact MEVs are performed relatively frequently.



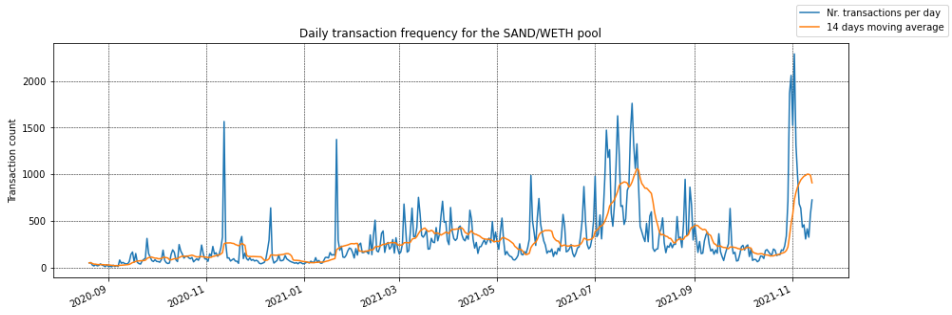
Picture X: count distribution for SAND/WETH pool

In the case of applying a volatility mitigation mechanism, it can be seen that half of transactions are blocked. In the case of reviewing the slice factor for passed/blocked transactions can be seen that blocked transactions are with a big difference of out values or higher slice factor.



Picture X: blocked and passed transactions relative to slice factor and out values differences

Swaps are performed more frequently in the second half of the reviewed time interval and both halves of distribution demonstrate medium-level transaction count.



Picture X: daily transaction count for SAND/WETH pool

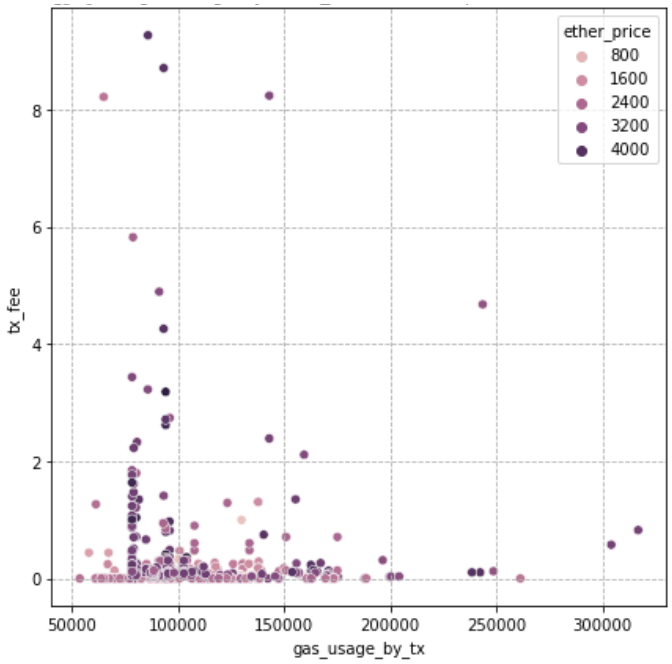
MEV profits analysis

During analysis of the MEV attacks with small values differences it was decided to perform detailed analysis of the MEV attacks with exact values matches due to discovered inaccuracies in the algorithm work and analysis of small values differences MEVs will be performed in the separate subchapter using fixed algorithm.

MEV transactions with exact values matches

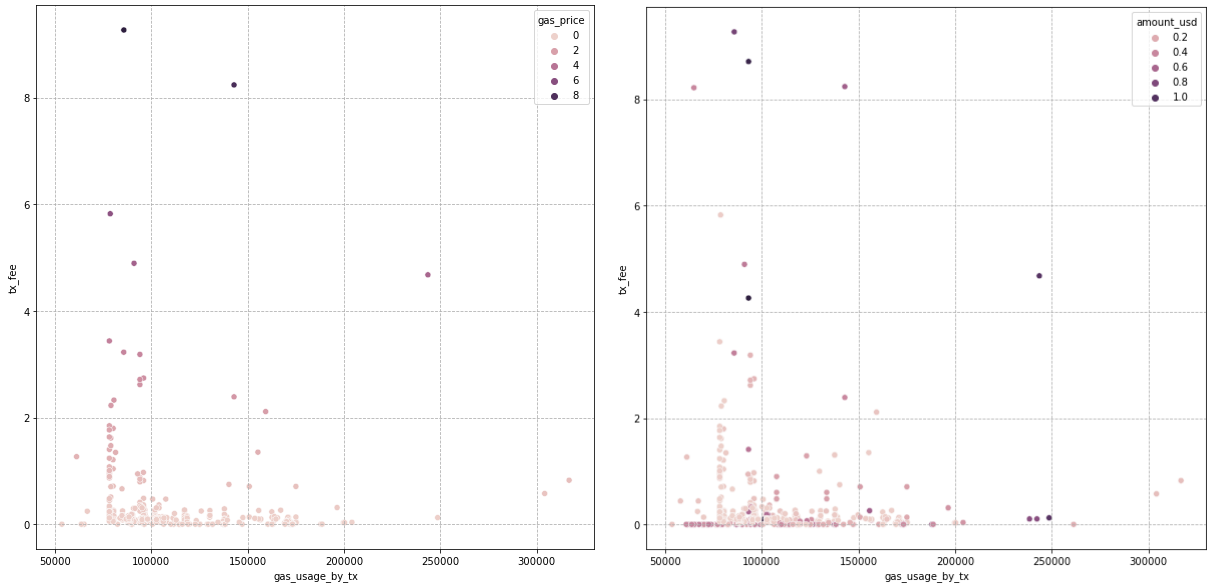
Classic pools (WBTC/USDC, WETH/USDC, WBTC/DAI, FEI/WETH, HKMT/USDT, IXS/WETH)

Most of the MEV attacks are performed with smaller gas usage and smaller transaction fees. There is no connection with Ether price, meaning that attackers perform their activity always, without any interruptions for Ether price drops.



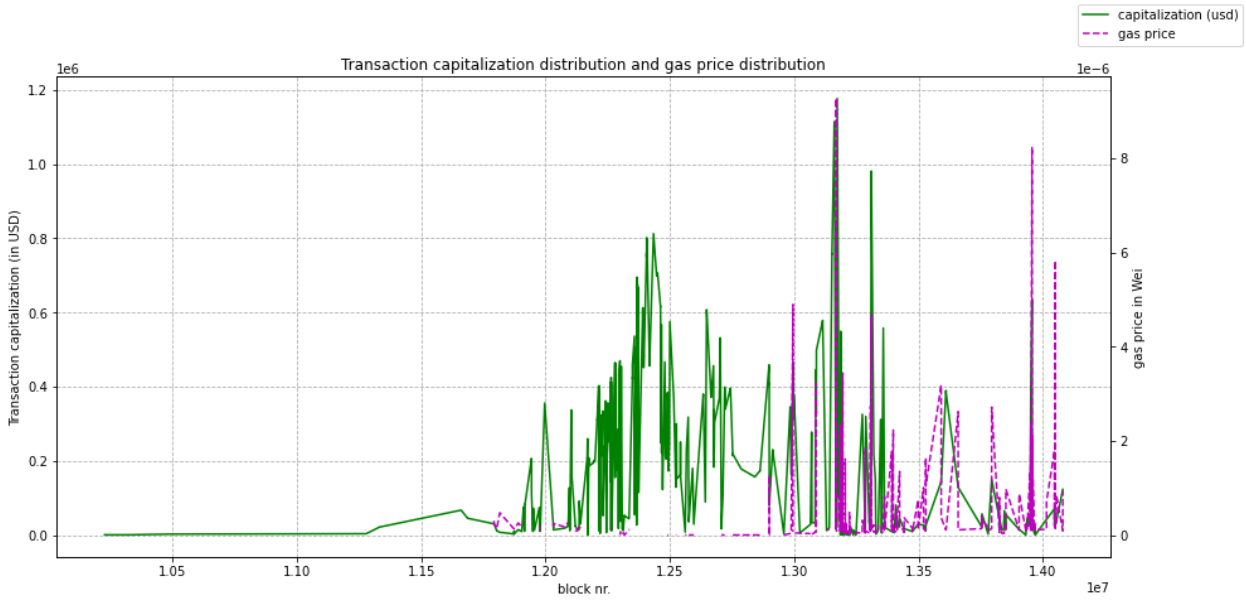
Picture X: distribution of MEV attacks by their transaction fees, used gas and Ether price

Attackers try to perform their activity during smaller gas price periods, causing smaller transaction fees paid for used gas. This leads to the assumption that attackers minimize their losses in performed attacks with minimization of gas payments. There are only unique cases of outliers that are ready to perform their transactions even with bigger gas usages and payments. Outliers perform high-capitalization transactions making them able to pay higher fees for performing their transactions.



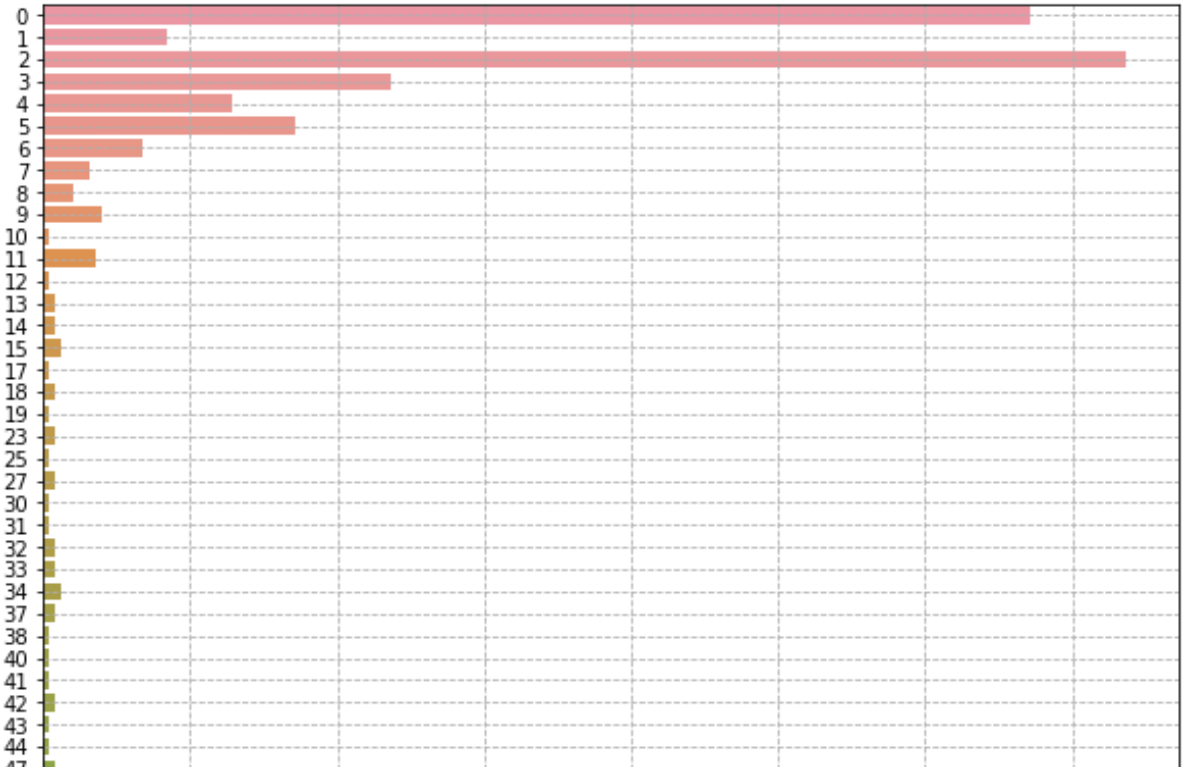
Picture X: scatter plots of MEV transactions by their gas usage and fees: from the left considering gas price; from the right considering USD-capitalization

Distributions demonstrate decrease of attackers activity during periods with rises in gas price. The only case when attackers are able to perform their activity is when there is an option of getting high profit out of the attack, where high transaction fees will not have a great impact on received profits.



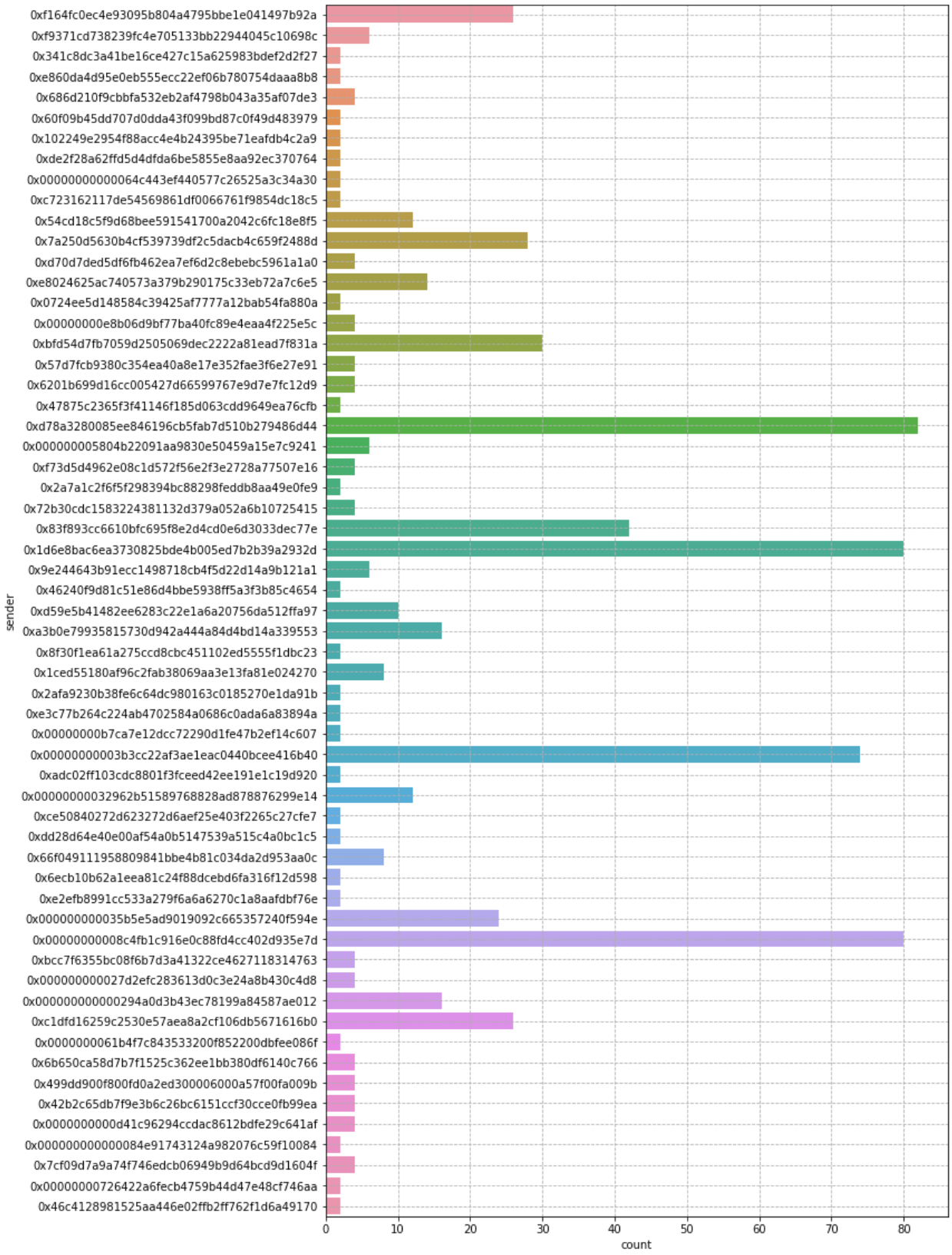
Picture X: MEV transactions capitalization and gas price distributions

In most of the cases attacks are performed using first positions in the block to ensure that transactions will be performed with expected prices, profits and to lower the possibility of transactions decline due to pool changes that may be caused during block execution.



Picture X: fragment of the MEV transactions count by their position in the block (count with values in range 0-200 records)

There are addresses with higher MEV transactions count compared to other addresses. Still, there is one important moment worth mentioning: Uniswap records transactions by the actual addresses involved in the transaction, but in some cases transactions are performed by the internal Uniswap services and instead of the original attackers addresses there will be addresses of those services recorded. It will be required to perform additional data extraction and filter to find real addresses involved in specified transactions. Still, there were many real MEV bots catched using this approach and the next charts covers some of the most active MEV bots on the market.

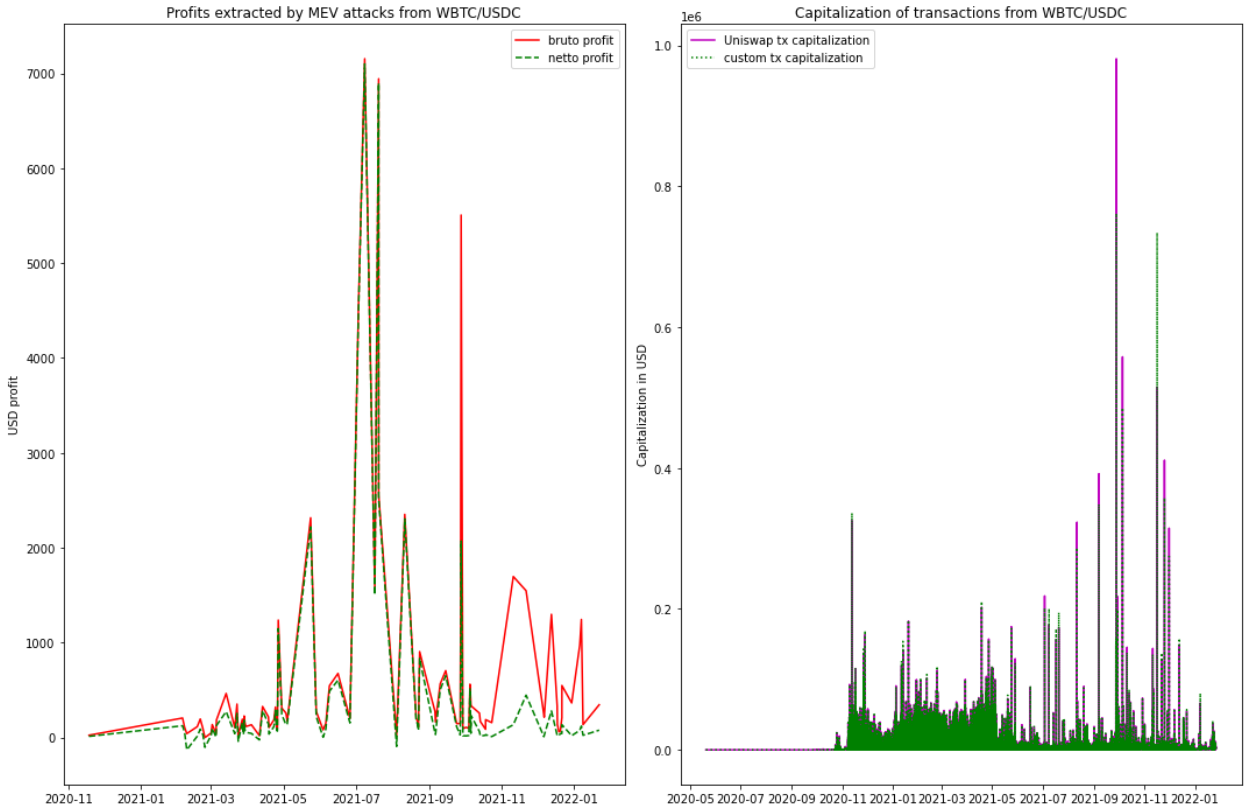


Picture X: MEV transactions count distribution by sender for classic pools.

WBTC/USDC

There is a rise of the MEV activity starting from March 2021, demonstrating a rise of interest in the WBTC/USDC pool activity on the Uniswap. As it was previously mentioned, this rise is caused by the rise of trades activity in the pool. There are only some unique cases of great difference between brutto and netto profits, but the overall picture demonstrates minimal losses in the profitability of attacks.

Attackers paid 17748,32 USD for gas usage and the sum of received brutto profit is 57938,65 USD, meaning that sum of netto profit is 40190,32. Out of 182 MEV transactions there are 11 cases of losses instead of getting profits, meaning that attackers in most of the cases are successful in performing their activity.



Picture X: brutto and netto profits extracted from WBTC/USDC from the left and WBTC/USDC transactions capitalization from the right

There is an observable connection between attacks profits distributions and capitalization of transactions performed in the pool. MEV transactions cover around 0,260618% out of all transactions, showing a small amount of attacks present in the pool. Brutto profits extracted from MEV attacks relative to Uniswap-estimated capitalization coefficient is around 0.00013676 (or

0.013676%) and netto profits extracted from MEV attacks relative to Uniswap-estimated capitalization coefficient is around 0.00011581 (or 0.011581%). MEV attacks capitalization (conform Uniswap estimations) coefficient to capitalization of all trades is 0.02668193 (or 2.668193%).

Profits extracted out of the pool are extremely small and frequency of the transactions is extremely small, while capitalization of performed attacks relative to total activity capitalization is bigger than expected. MEV attacks have a high impact on pool capitalization and in the current case demonstrate big gas payments.

WETH/USDC

Considering that analysis of MEVs will be performed with comparison of similar coefficients and percentages it was decided to set all important coefficients in the beginning of pool subchapter in a form of a list:

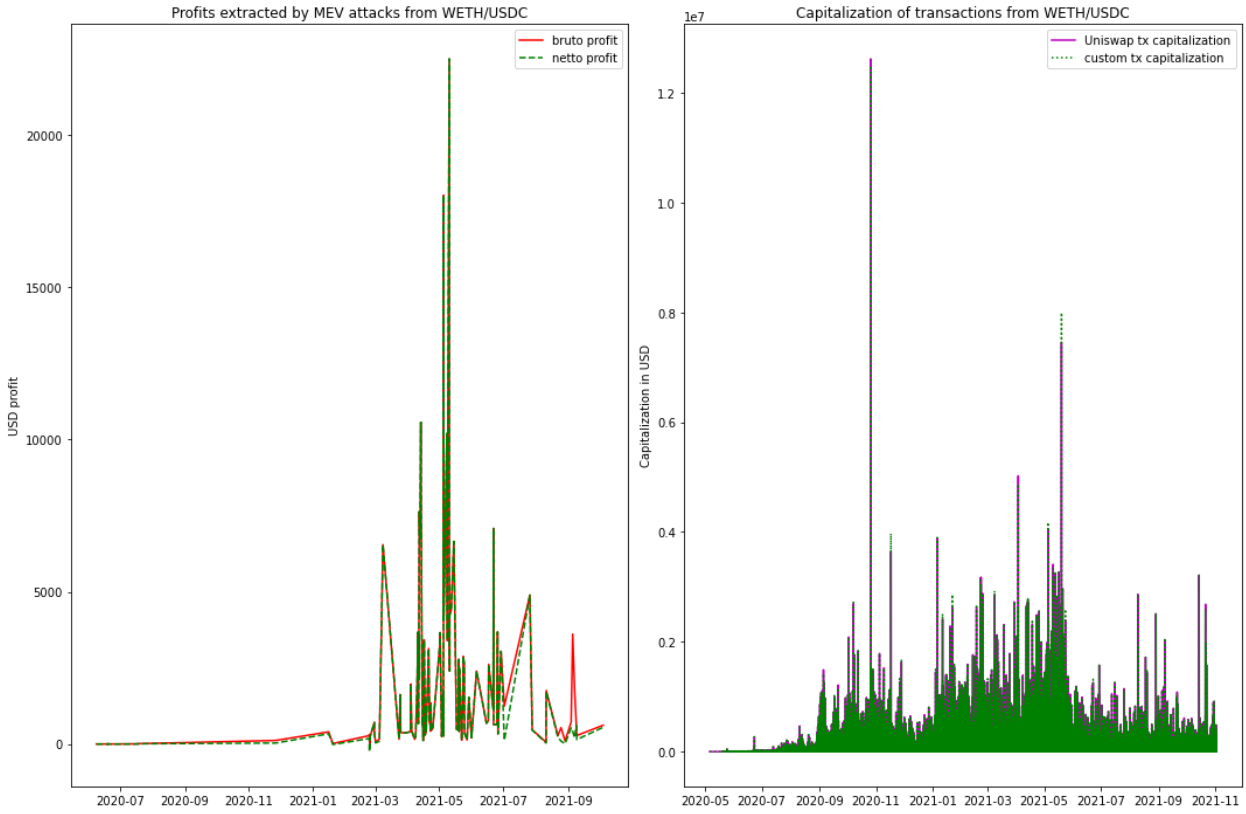
- Total brutto profit = 258 537,27 $;
- Total netto profit = 249 088,42 $;
- Total gas spendings = 9 448,85 $;
- Not profitable transactions count = 7;
- Coefficient of MEV transactions count to total transactions count = 0.00009392505 (or 0.009392505%);
- Brutto profit to total pool capitalization coefficient = 0.0000079554 (or 0.00079554%);
- Netto profit to total pool capitalization coefficient = 0.00000781003 (or 0.000781003%);
- MEV attacks capitalization to total pool capitalization coefficient = 0.000093925 (or 0.0093925%).

Current pool contains extremely big capitalization, demonstrating high traders interest in Ether-based pools in combination with stablecoins. Therefore, capitalization of MEV attacks has low impact on overall capitalization of the pool activity. Compared to the previous case, attackers paid smaller fees, got more profit out of the pool (profits are 5-6 times bigger, while attacks count is around 50% bigger and gas spendings are twice smaller). MEVs in that pool were more successful and with better performance.

Amount of transactions performed is high and attackers demonstrate low interest in the current pool from the perspective of how many attacks were performed and relatively low activity considering the amount of extracted profits.

Distributions demonstrate dependency of MEV attacks from pool activity. Before the rise of activity and after the drop in activity MEV distributions dropped. Interesting observation can be made via checking the difference in netto and brutto profits distributions - there is a rise of gas spendings closer to the end of observable period and therefore attackers lowered their activity.

Till this moment the only explanation that can be made to explain such a low distribution of MEV activities is that attackers are more interested in performing attacks over the pools with bigger tokens prices deviations.



Picture X: MEV profits distributions and trades capitalization distributions from WETH/USDC

WBTC/DAI

This pool contains medium-level activity and there is next statistics:

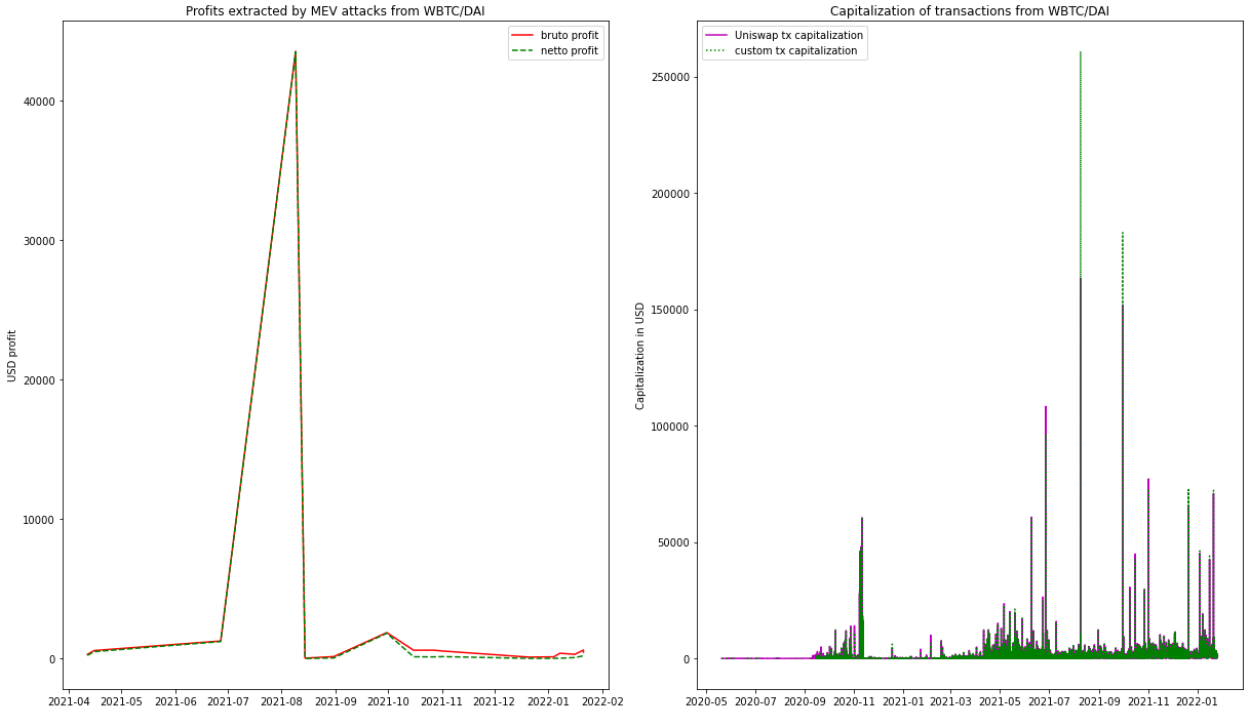
- Total brutto profit = 51 516,83 $;
- Total netto profit = 48 440,17 $;
- Total gas spendings = 3 076,66 $;

- Not profitable transactions count = 0;
- Coefficient of MEV transactions count to total transactions count = 0.0021936 (or 0.21936%);
- Brutto profit to total pool capitalization coefficient = 0.0031854 (or 0.31854%);
- Netto profit to total pool capitalization coefficient = 0.0030903(or 0.30903%);
- MEV attacks capitalization to total pool capitalization coefficient = 0.102598 (or 10.2598%).

There is a much smaller activity of the pool compared to both previous cases, while the amount of extracted profit is almost identical to the case of WBTC/USDC pool. This case is unique taking into account that one attack covers more than 80% out of entire profit extracted from the pool, meaning that there is one unique MEV attack with extreme impact on pool statistics. The biggest attacks for each pool will be reviewed separately in a specific subchapter and therefore in the current one will be only their mentionings.

Gas spendings are small and profitability of attacks are better than in the case of WBTC/USDC and capitalization of attacks is extremely impactful on the pool. Almost 10% out of total pool activity capitalization is represented by MEV attacks, which considering their small count demonstrates that each presented attack is performed with high capitalization values, which can happen in two cases: pool contains high reserves or there is a chance of getting high profits due to victim's activity. In the first chapter it can be seen that WBTC/DAI pool has only one day of extremely raised reserves, while in general distribution is relatively small.

Small amount of present MEV attacks in the pool reduces chances of performing efficient visual analysis. Still, there is a connection between the amount of MEV attacks and activity in the pool. Both WBTC/DAI and WBTC/USDC pools have similar price distributions and the only remaining assumption is that attacks are oriented towards attacking high capitalization transactions, detected in the current pool.



Picture X: profits and capitalizations distributions from WBTC/DAI

FEI/WETH

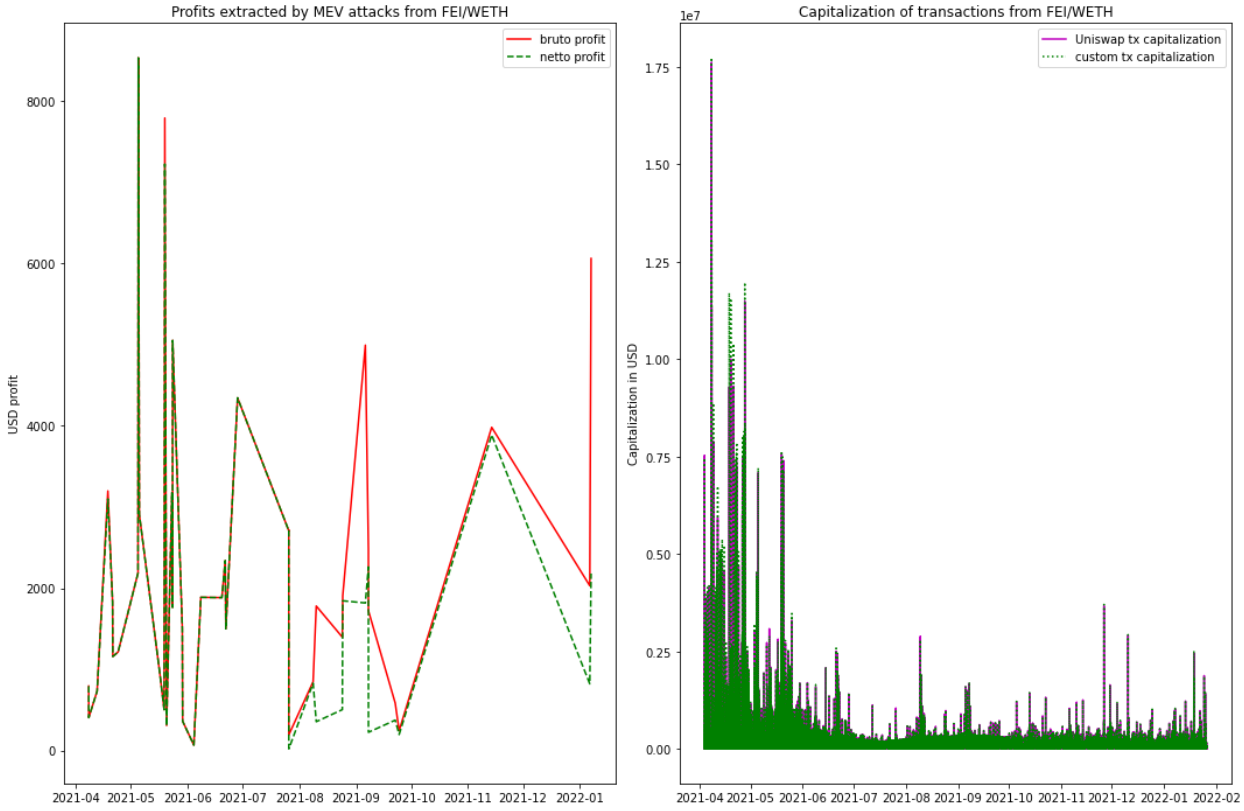
Current pool statistics:

- Total brutto profit = 91 539,22 $;
- Total netto profit = 77 956,64 $;
- Total gas spendings = 13 582,58 $;
- Not profitable transactions count = 0;
- Coefficient of MEV transactions count to total transactions count = 0.00133618 (or 0.133618%);
- Brutto profit to total pool capitalization coefficient = 0.00001147 (or 0.001147%);
- Netto profit to total pool capitalization coefficient = 0.00001062 (or 0.001062%);
- MEV attacks capitalization to total pool capitalization coefficient = 0.0036671 (or 0.36671%).

Interesting moment about this pool is that high activity starts from the beginning of the pool lifecycle attracting attention of attackers from the start. This situation demonstrates that lower activity in pools before the start of 2021 was a global problem for all pools present on Uniswap. Still, the amount of attacks is extremely low compared to the amount of simple transactions and extremely high capitalization of the pool activity. There is a smoother

distribution of profits extracted from attacks, meaning that attackers had similar profits extracted by performing their attacks and the most profitable attack is not out of the attacks distribution (the same can be seen on distribution of extracted profits below). The highest profits were extracted during rises of pool activity capitalizations.

MEV transactions are happening with low frequency and have a small impact on the pool capitalization. Interesting moment is that gas spendings are on medium level and extracted profits are not so high as in some previous cases.



Picture X: profits and capitalization distributions from FEI/WETH

HKMT/USDT

Pool contains a small amount of transactions, only one MEV attack and therefore analysis of this pool will not be an efficient approach, considering that there is almost nothing to analyze. There is only one attack with 257,91 $ brutto profit, out of which attacker paid 238.24 $ gas fees and netto profit is only 19,67 $. Small activity in the pool, small profit extracted out of the MEV attack, smaller than in previous cases capitalization of the pool activity cause almost no interest in performing attacks over current pool.

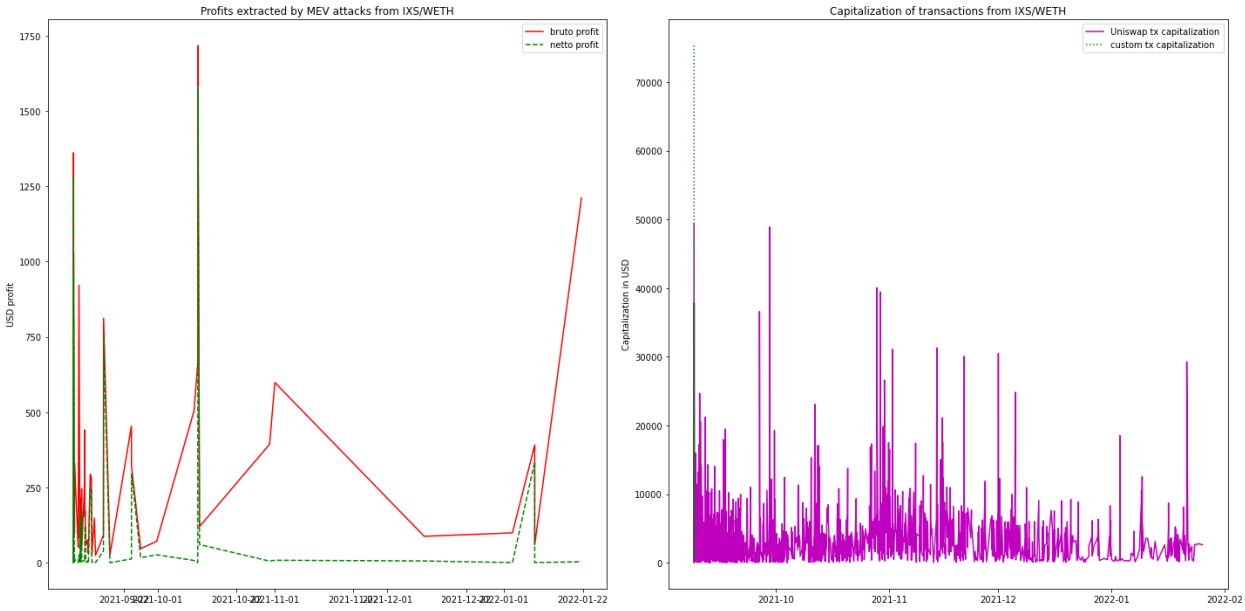
IXS/WETH

Current pool statistics:

- Total brutto profit = 21 001,27 $;
- Total netto profit = 8 225,07 $;
- Total gas spendings = 12 776,21 $;
- Not profitable transactions count = 0;
- Coefficient of MEV transactions count to total transactions count = 0.056589 (or 5.6589%);
- Brutto profit to total pool capitalization coefficient = 0.00220808 (or 0.220808%);
- Netto profit to total pool capitalization coefficient = 0.00153643 (or 0.153643%);
- MEV attacks capitalization to total pool capitalization coefficient = 0.115871 (or 11.5871%).

Due to the small time interval of analysis transactions count in the pool shows medium-level transaction frequency and medium-level capitalization of the pool activity. Comparing the count of MEV transactions relative to simple transactions can be seen that frequency of attacks is much higher compared to previous cases, but amount of extracted profits is not bigger than in previous cases and gas spendings are extremely high compared to previous cases. This demonstrates the rise of the gas fees closer to the second half of 2021 and therefore gas spendings for transactions became higher. Therefore, the profitability of MEV attacks is now lower and it is more difficult to make profitable attacks.

Highly profitable attacks were performed in the beginning of pool lifecycle, when higher traders activity was registered. After high activity periods there is registered decrease of MEV attacks and their profitability greatly decreased due to critical rise of gas spendings. Current pool contains two important aspects: MEV transactions are happening with higher frequency compared to previous cases and MEV transaction capitalization takes a big part out of total pool capitalization.



Picture X: profits and capitalization distributions from IXS/WETH

Overall situation of the MEV attacks in the classic pools

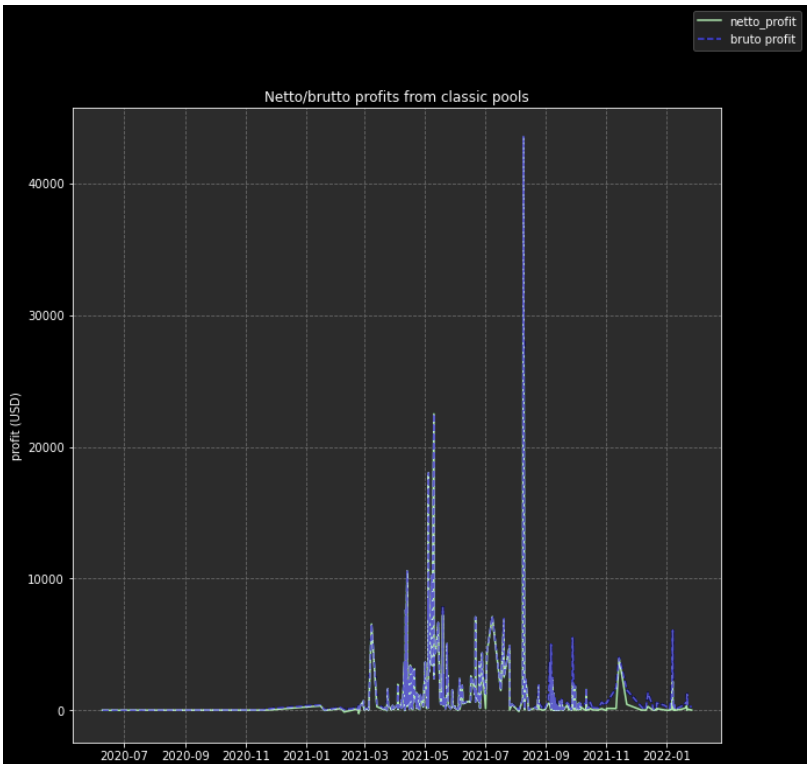
Overall distribution of the MEV attacks demonstrates low frequency of attacks and compared to further shown attacks does not provide big profits to the attacker. It is possible due to high interest of the traders and stabilization of the token price by traders interacting with this pool. Classic tokens are not so attractive to the MEV attackers. Overall distribution of profits out of all reviewed classic tokens pools is shown below.

MEV attackers started their activity from the beginning of 2021 and can be observed to drop in their activity around the end of 2021. This can be caused by the rise of the gas fees in the second half of 2021, which greatly reduced profits extracted by the attackers (also will be observable in further cases). Statistics of the MEV attacks on classic pools are next:

- Brutto profit extracted out of classic pools = 480 791,15$;
- Gas spendings for performing MEV attacks on classic pools = 56 870,85$;
- Netto profit extracted out of classic pools = 423 920,30$.

The only pool that does not perform as classic pools is an IXS/WETH pool, where attack frequency and their profits differ from other presented classic pools. This is caused by two factors: IXS/WETH history represents different time periods compared with other pools with new gas fees/costs and different pool types (other pools in the classic category contain a pair of extremely popular tokens with stablecoin).

Capitalization of all MEV attacks conform Uniswap capitalization estimations is 129619086,44$ out of total classic pools swaps capitalization is 40936487555,76$, meaning that coefficient of MEV attacks capitalization is 0,0000221004 (or 0,00221004%).



Picture X: netto/brutto profits distributions from classic pools

Based on show results and further analysis that will be demonstrated classic pools are not suffering so much from MEV attacks. Considering that there are only 710 MEV attacks out of 3044620 classic pools transactions, MEV transactions are extremely small. Still, capitalization of all attacks is too high considering the amount of attacks performed, demonstrating that attackers are able to perform big attacks on pools (even considering high reserves).

STO pools (HKMt/USDT, UMA/FEI, PERL/WETH, BPT/WETH, uSTONKS_APR_21/USDC, mAMZN/UST, mBABA/UST, mAAPL/UST)

Pools HKMt/USDT, UMA/FEI and uSTONKS_APR_21/USDC pools have no MEV transactions caused by small activity present in the pools (even considering taken time intervals) and they are not representing precious tokens that would be attractive for attackers. Remaining pools will be analyzed in detail.

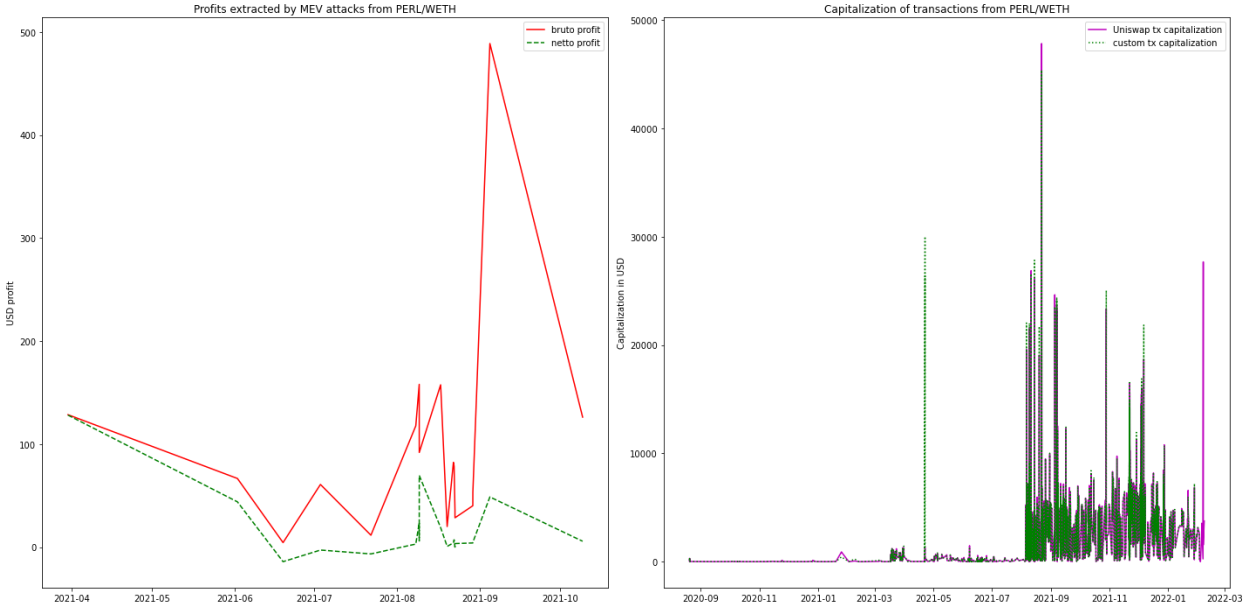
PERL/WETH

Current pool statistics:

- Total brutto profit = 1 882,72 $;
- Total netto profit = 347,78 $;
- Total gas spendings = 1 534,93 $;
- Not profitable transactions count = 2;
- Coefficient of MEV transactions count to total transactions count = 0.0199161 (or 1.99161%);
- Brutto profit to total pool capitalization coefficient = 0.000197383 (or 0.0197383%);
- Netto profit to total pool capitalization coefficient = 0.00153643 (or 0.153643%);
- MEV attacks capitalization to total pool capitalization coefficient = 0.037441 (or 3.7441%).

Out of 1908 transactions there are only 38 MEV transactions (2% of all transactions are MEV-related). Profitability of the attacks is small. While brutto profits demonstrate relatively efficient MEV attacks, gas spendings for performing attacks reduce profitability to extremely small values and therefore it is not efficient to perform attacks on this pool.

Attacks count and profitability rises during higher activity periods, but considering high gas spendings attackers extract small profits and therefore their activity is low. Distribution of brutto and netto profits demonstrates low efficiency of performing attacks on this pool.



Picture X: profits and capitalization distributions from PERL/WETH

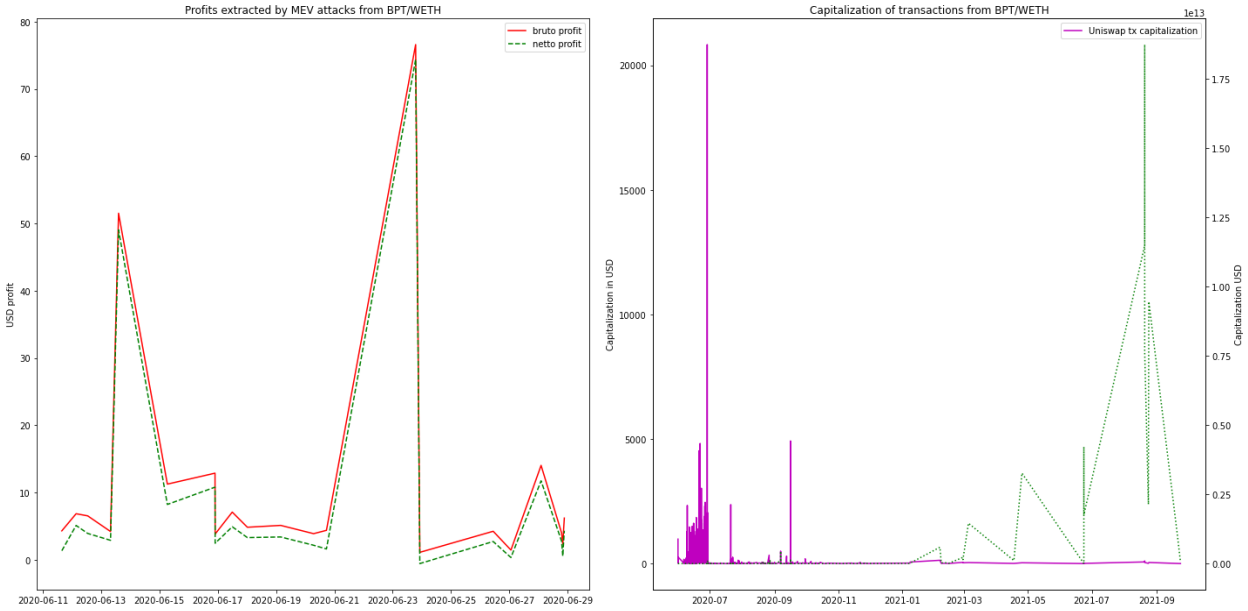
BPT/WETH

Current pool statistics:

- Total brutto profit = 236,40 $;
- Total netto profit = 195,17 $;
- Total gas spendings = 41,23 $;
- Not profitable transactions count = 0;
- Coefficient of MEV transactions count to total transactions count = 0.0133079 (or 1.33079%);
- Brutto profit to total pool capitalization coefficient = 0.000344555 (or 0.0344555%);
- Netto profit to total pool capitalization coefficient = 0.000314509 (or 0.0314509%);
- MEV attacks capitalization to total pool capitalization coefficient = 0.0133413 (or 1.33413%).

Out of 3156 transactions in the pool there are only 42 MEV-related transactions. Considering that 1,3% of all transactions in the pool are represented by MEV-related ones, which means smaller MEV attacks frequency compared to the previous case. Even with smaller attacks frequency their profitability is extremely small, demonstrating one the lowest profits distributions out of all reviewed pools.

Such a low profitability may be caused by the extremely small lifecycle of the pool. Another moment is that even such a small lifecycle was characterized by relatively small capitalization of the pool activity. Capitalization of MEV activity is almost similar to the previous case.



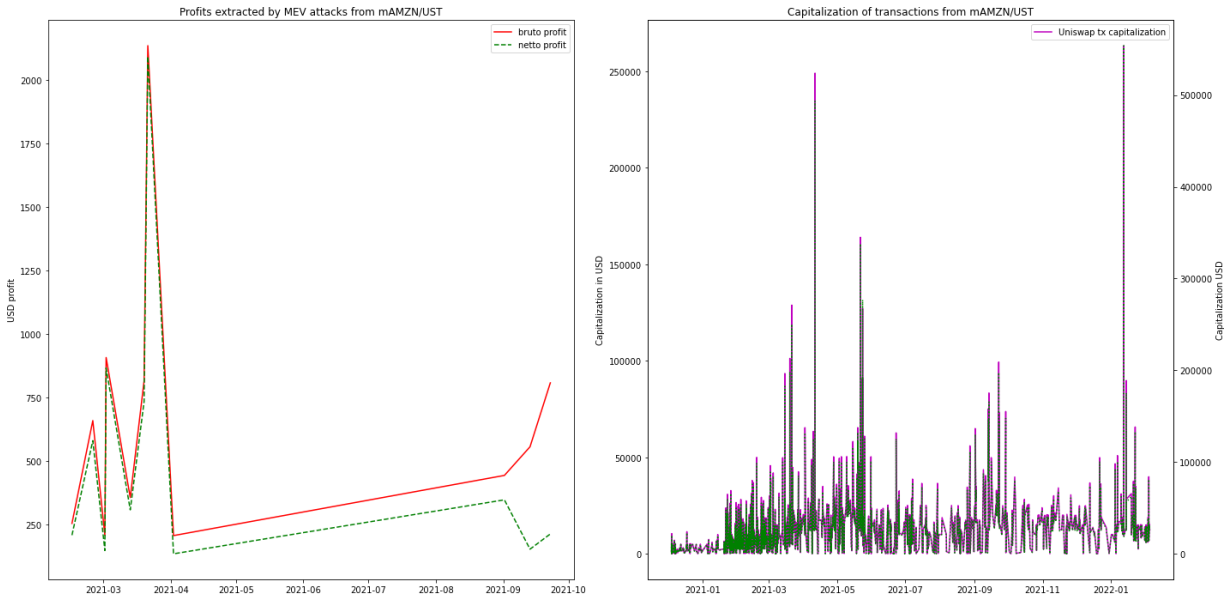
Picture X: profits and capitalization distributions from BPT/WETH

mAMZN/UST

Current pool statistics:

- Total brutto profit = 7 350,92 $;
- Total netto profit = 5 783,87 $;
- Total gas spendings = 1 567,05 $;
- Not profitable transactions count = 0;
- Coefficient of MEV transactions count to total transactions count = 0.0122087 (or 1.22087%);
- Brutto profit to total pool capitalization coefficient = 0.000326822 (or 0.0326822%);
- Netto profit to total pool capitalization coefficient = 0.000291986 (or 0.0291986%);
- MEV attacks capitalization to total pool capitalization coefficient = 0.0201124 (or 2.01124%).

Frequency of MEV-related transactions is relatively small and capitalization of the performed attacks considering their low count represent medium level of impact. Out of 1802 transactions there are only 24 MEV-related transactions, while extracted profit is higher than all previously reviewed STO pools. This is caused by higher recognition of the presented tokens and therefore their higher popularity.



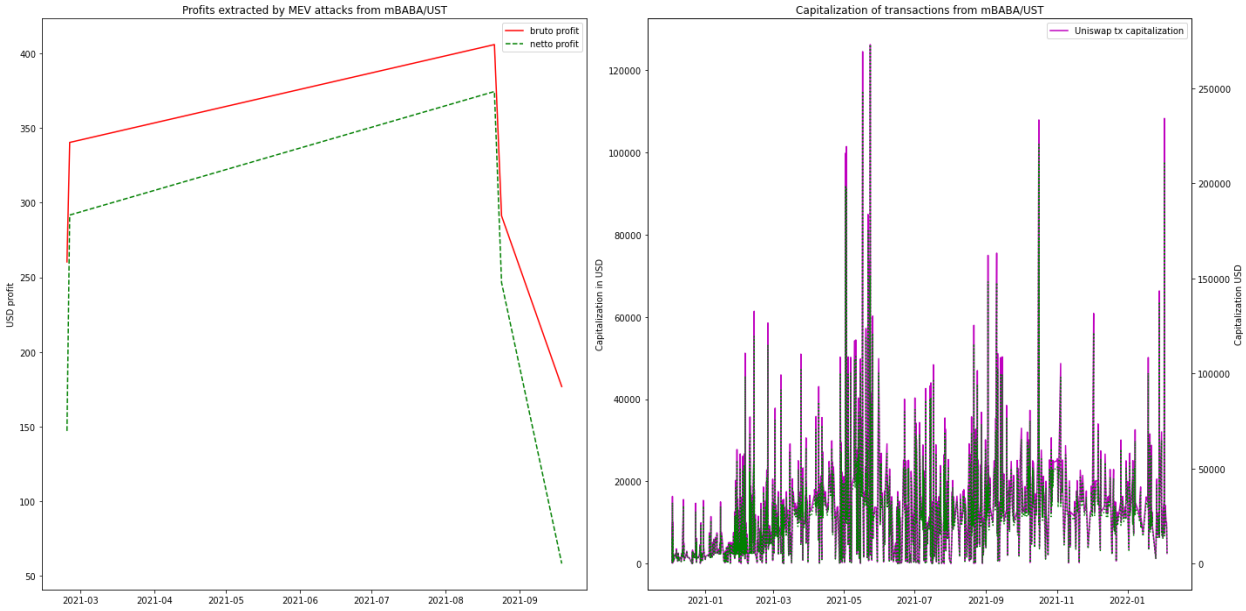
Picture X: profits and capitalization distributions from mAMZN/UST

Profitability of the performed attacks is medium level and gas spendings are not so high as in case of PERL/WETH and attractiveness of this pool is higher. Distribution of the extracted profits demonstrate that attacks are performed only during higher activity periods and higher activity was registered till rise of the gas spendings, when profitability of the attacks decreased heavily and therefore attacks are less frequent.

mBABA/UST

Current pool statistics:

- Total brutto profit = 1 474,38 $;
- Total netto profit = 1 117,88 $;
- Total gas spendings = 356,50 $;
- Not profitable transactions count = 0;
- Coefficient of MEV transactions count to total transactions count = 0.004914 (or 0.4914%);
- Brutto profit to total pool capitalization coefficient = 0.0000570042 (or 0.00570042%);
- Netto profit to total pool capitalization coefficient = 0.0000501125 (or 0.00501125%);
- MEV attacks capitalization to total pool capitalization coefficient = 0.0086331 (or 0.86331%).



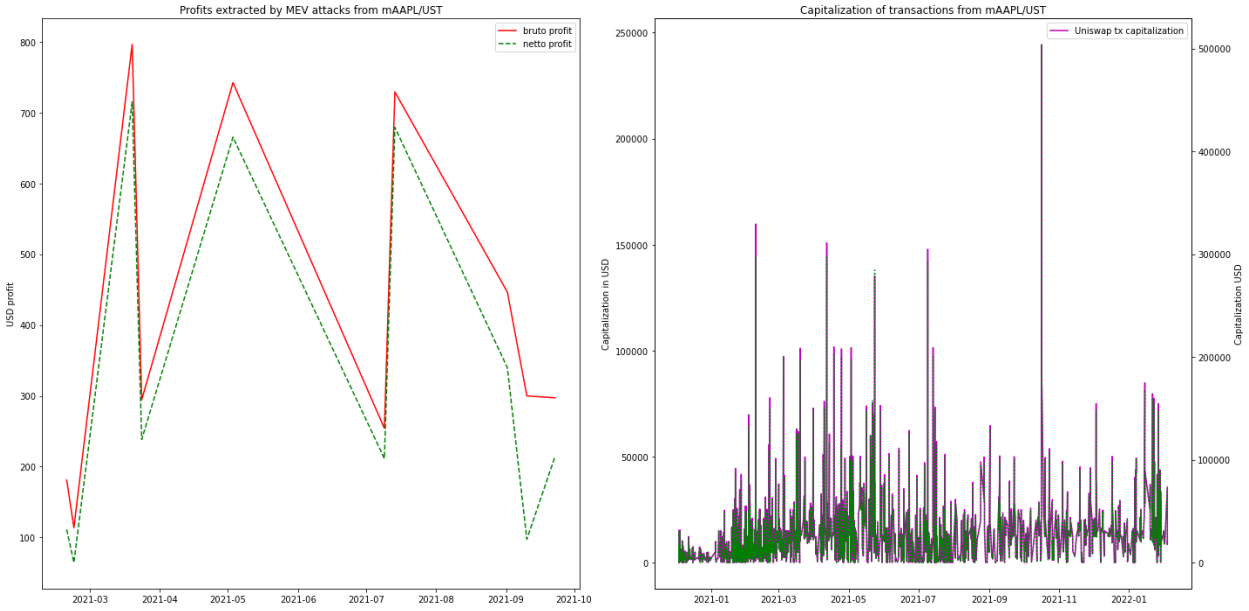
Picture X: profits and capitalization distributions from mBABA/UST

There are 10 MEV-related transactions out of 2035 transactions performed in the pool and compared to all previous pools has the lowest MEV attacks frequency and one of the smallest capitalization impacts on the pool. Profitability of the performed attacks is small, gas spendings are on medium level. Amount of the attacks performed is so small that there are almost no options in performing their analysis and giving some assumptions about them.

mAAPL/UST

Current pool statistics:

- Total brutto profit = 4 154,64 $;
- Total netto profit = 3 337,08 $;
- Total gas spendings = 817,60 $;
- Not profitable transactions count = 0;
- Coefficient of MEV transactions count to total transactions count = 0.0083438 (or 0.83438%);
- Brutto profit to total pool capitalization coefficient = 0.00014149 (or 0.014149%);
- Netto profit to total pool capitalization coefficient = 0.000127569 (or 0.0127569%);
- MEV attacks capitalization to total pool capitalization coefficient = 0.0100935 (or 1.00935%).

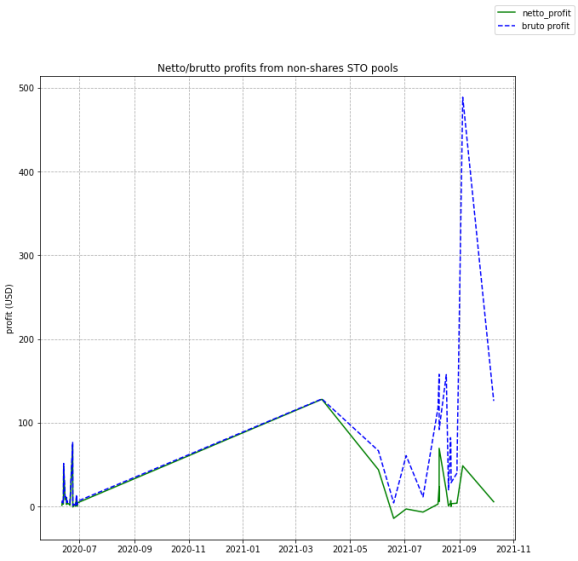


Picture X: profits and capitalization distributions from mAAPL/UST

There are 22 MEV-related transactions out of all 2397 transactions performed in the pool. Frequency of attacks is small, extracted profits are medium and compared to total capitalization of the activity in the pool can be seen that attacks capitalization is medium, while profits are small. Gas spendings are medium and profitability of the attacks is medium.

Overall situation of the MEV attacks in the STO pools

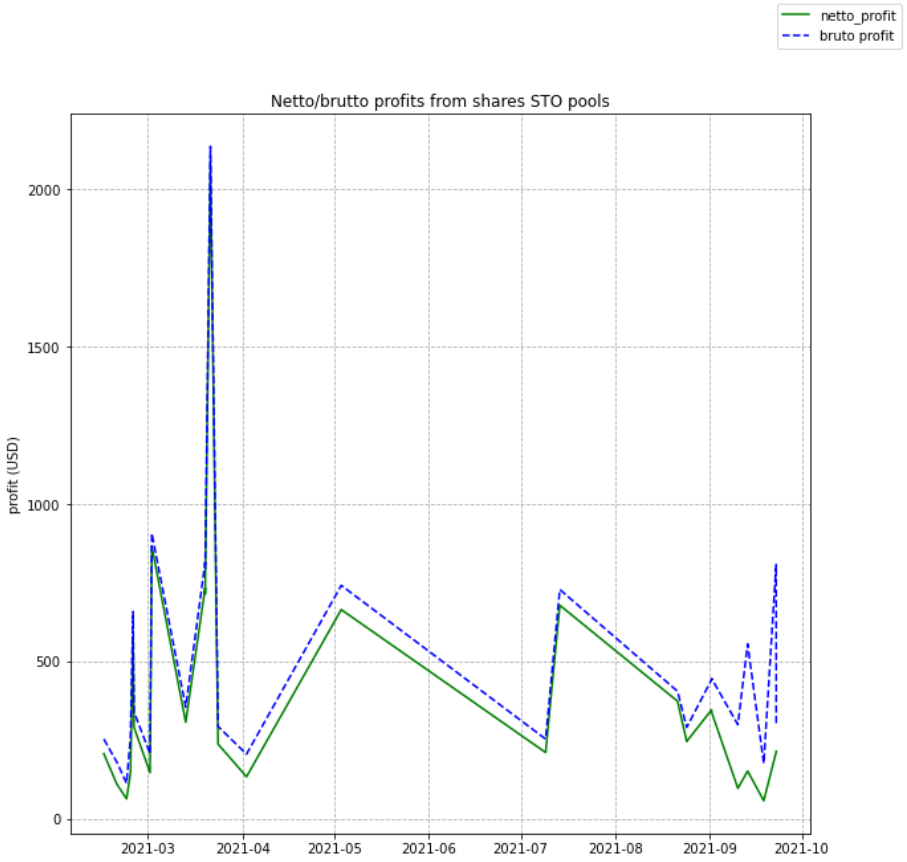
Considering metrics that were collected during analysis of the MEV attacks it is required to separate pools by 2 subtypes:



Picture X: profits distributions for non-shares STO

- Pools that represent simple STO tokens;
- Pools with STO tokens mirroring big companies shares.

This approach will clearly demonstrate the difference between those pools types. First, simple STO tokens. There are registered only 40 attacks and their profitability is small. They are happening with small frequency, small profitability and efficiency of those attacks is questionable. Possible reason for this problem is the small popularity of the tokens present in those pools.



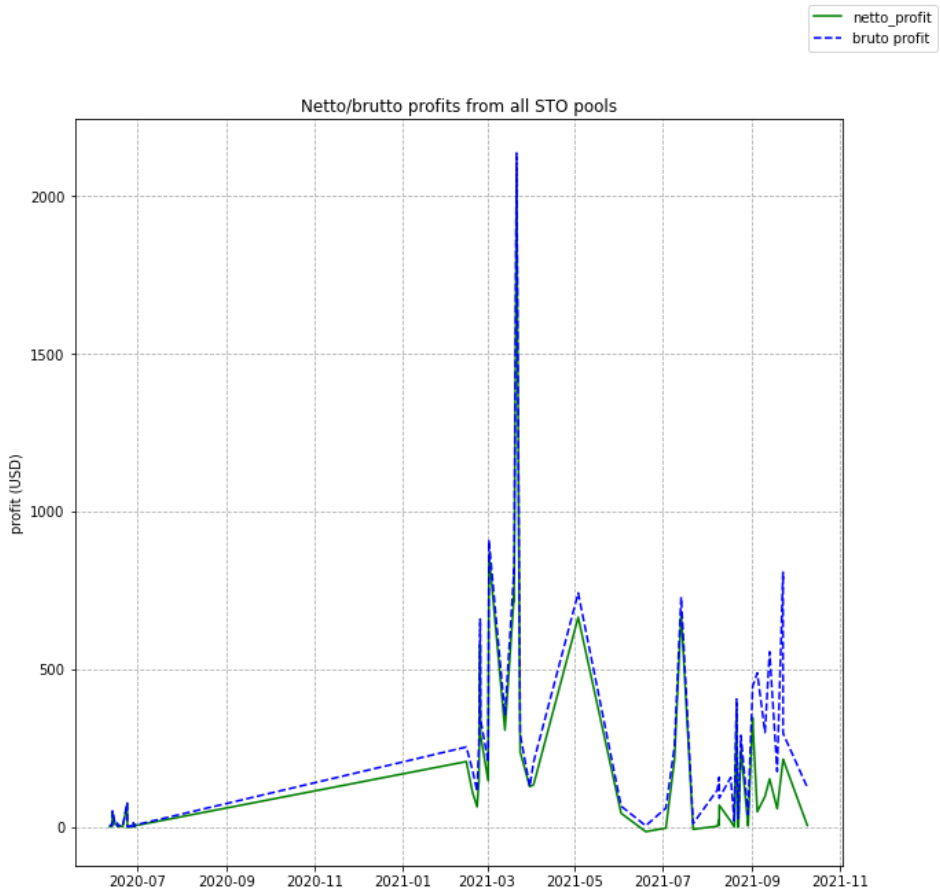
Picture X: profits distributions for shares-based STO

Profits distribution in this case demonstrate higher profits extracted by performing MEV attacks, which considering their smaller count show that those pools are more attractive for attackers but attack frequency demonstrates smaller attractiveness for attackers compared to the classic pools.

In the case of combining those two STO types, profits and frequency of the performed attacks are small, demonstrating that attackers are more interested in performing attacks over classic tokens, than STO ones. This can happen due to several important aspects:

- lower trading activity (lower transactions frequency);
- smaller deviations in tokens prices, meaning that token sales are happening with more stable price distribution;
- taken time intervals cover by 50% or bigger period after rise of the gas spendings, meaning that profitability of the attacks becomes lower and therefore low-profitable pools from brutto profits extraction approach have become even less attractive;
- recognition of the presented tokens is smaller compared to the case of classic tokens and their popularity is relatively low.

Further analysis of the NFT and meme tokens pools will demonstrate how high price deviation, bigger popularity of the tokens and bigger trades lead to bigger profits and MEV activity.



Picture X: profits distributions for all STO

Meme tokens pools (DOGE/WETH, ELON/WETH, SHIB/WETH, SQUID/WETH)

Meme pools represent the worst case of MEV attacks from the perspective of capitalization, profits, frequency and attacks count. There is only one pool without performing MEV attacks - SQUID/WETH pool. The problem with this pool is that it was dead from the start and there was almost no activity, meaning lack of attractiveness for attackers. Another reason for lack of MEV attacks is the case of fraud schemes with SQUID tokens (reference to “Squid Game” TV series) causing undesired risk for attackers.

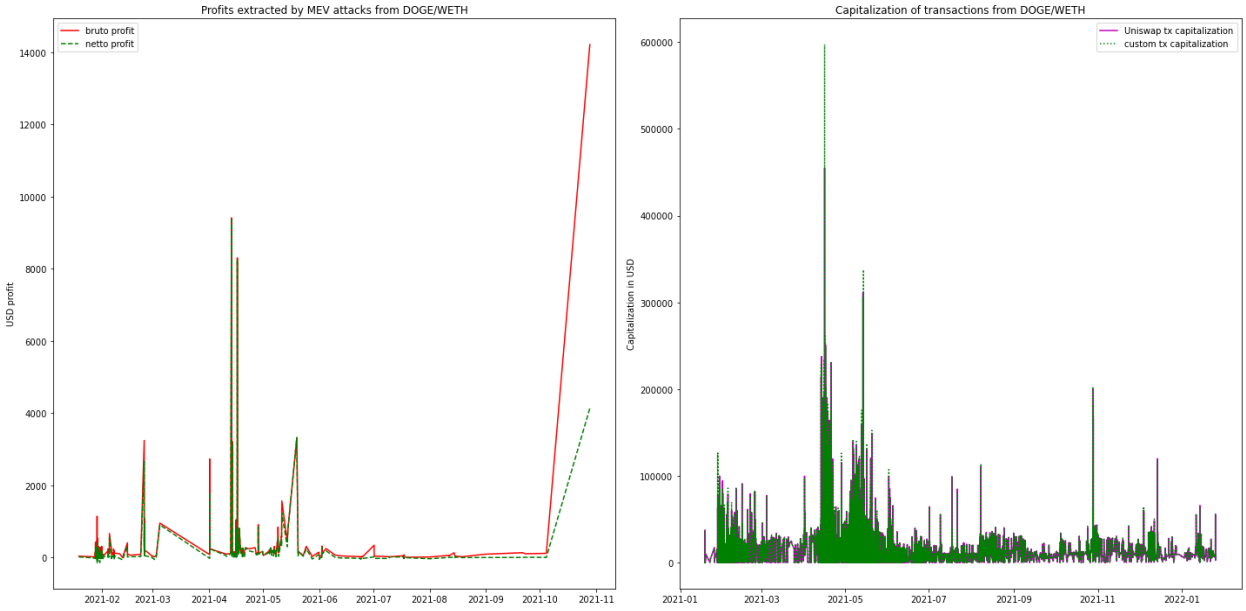
With 3 pools remaining, the amount of MEV attacks is extremely high and therefore this chapter will contain more details compared to previous cases of classic and STO pools.

DOGE/WETH

Current pool statistics:

- Total brutto profit = 109 603,81 $;
- Total netto profit = 69 876,36 $;
- Total gas spendings = 39 727,44 $;
- Not profitable transactions count = 33;
- Coefficient of MEV transactions count to total transactions count = 0.046155 (or 4.6155%);
- Brutto profit to total pool capitalization coefficient = 0.000388514 (or 0.0388514%);
- Netto profit to total pool capitalization coefficient = 0.000318103 (or 0.0318103%);
- MEV attacks capitalization to total pool capitalization coefficient = 0.0422148 (or 4.22148%).

There are 710 MEV-related transactions performed out of 14343 transactions through DOGE/WETH pool. Capitalization of the pool is high and therefore attractiveness of this pool is higher compared to cases of STO pools. Capitalization of attacks and their frequency is similar to the parameters of MEV attacks in classic tokens pools. Compared to classic tokens pools profits are higher, while gas spendings are relatively high (gas spendings reduced attackers profits by 36,25%).



Picture X: profits and capitalization distributions from DOGE/WETH

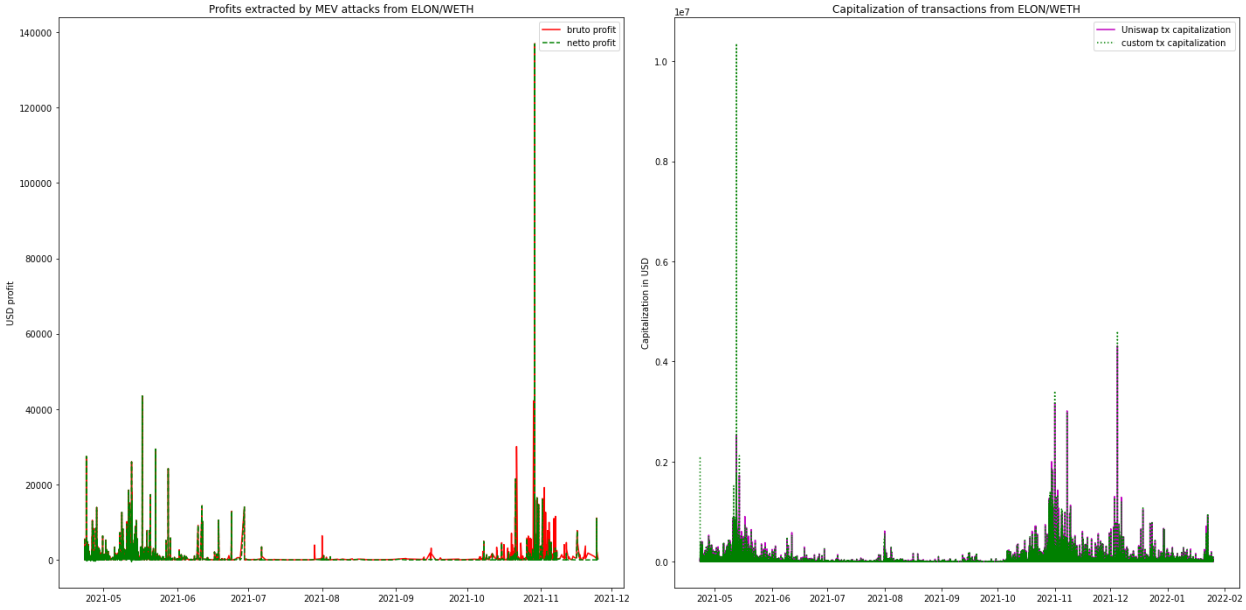
Compared to classic tokens pools amount of performed attacks are higher and sums of extracted profits are smaller than only WETH/USDC case (which until this moment has the highest extracted profits). Distribution of extracted profits show less stable distributions of profits compared to classic pools case and can be seen that there are several attacks with extremely high profits, making around half of entire extracted profits. Record of the WBTC/DAI case is not overcomed, due to extreme profit that attacker got in that case, but profits from current pool are high. Higher attack frequency is registered with increase of traders activity.

ELON/WETH

Current pool statistics:

- Total brutto profit = 3 726 029,22 $;
- Total netto profit = 2 918 241,68 $;
- Total gas spendings = 807 787,54 $;
- Not profitable transactions count = 26;
- Coefficient of MEV transactions count to total transactions count = 0.02185854 (or 2.185854%);
- Brutto profit to total pool capitalization coefficient = 0.00123266 (or 0.123266%);
- Netto profit to total pool capitalization coefficient = 0.00109904 (or 0.109904%);
- MEV attacks capitalization to total pool capitalization coefficient = 0.1976324 (or 19.76324%).

This pool demonstrates anomalous profits, amount of performed attacks and contains one of the biggest registered profits out of all. While MEV transactions frequency is relatively medium, capitalization of performed transactions is extremely big and form almost 20% out of entire pool capitalization. Extracted profits are anomalously high and gas spendings led to a loss of 21,68% of profit.



Picture X: profits and capitalization distributions from ELON/WETH

Distribution of profits are almost perfectly matching distribution of the capitalization meaning that rise of pool activity caused rise of MEV activity. On the MEV profits distributions is presented how rise of the gas spendings in the middle of 2021 caused decrease of the profits extracted from MEV attacks, but in this case it has not led to decrease of MEV attacks count, meaning that attackers are still able to extract profits, the problem is just in performing attacks more efficiently.

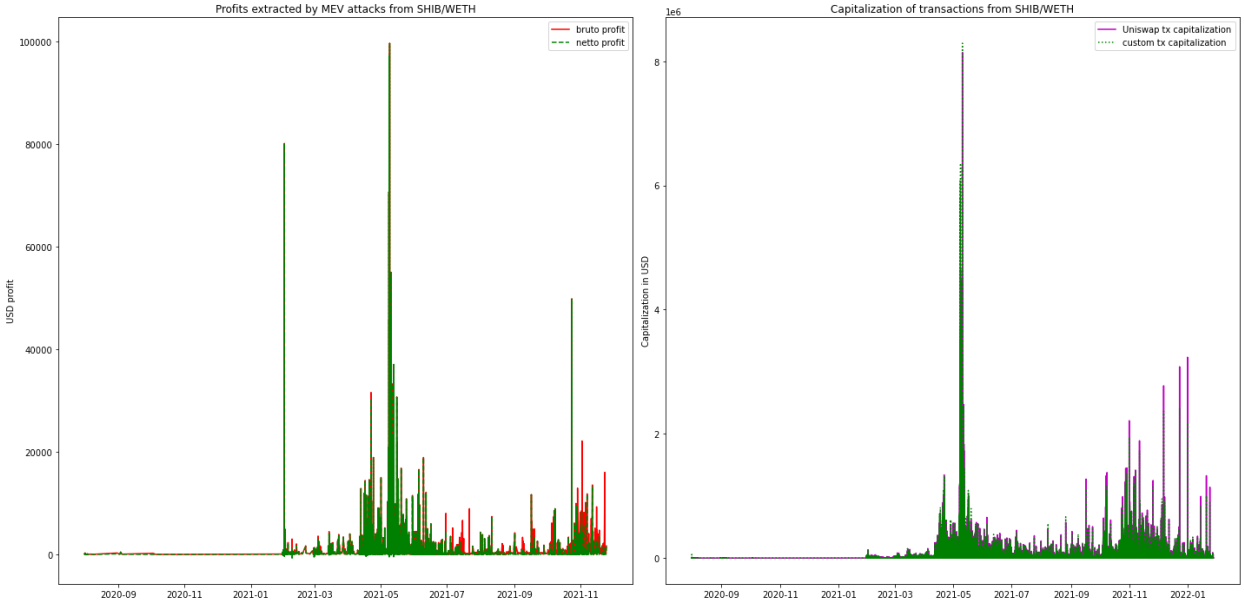
Possible reasons for such extreme profits may be caused by bigger deviation of the ELON token compared to the DOGE token. The second one has more stable distribution and contains a longer activity history, making this token more trustworthy, while the first one appeared not a long time ago, has reputation of a token with such a deviation in price that it is possible to raise high profits out of the price changes and possible “DOGE coin killer”. This led to higher exchange of tokens during token price rises and possible slippage disablement, considering that traders expected only positive price changes during their trading activity and therefore attackers may extract higher profits.

SHIB/WETH

Current pool statistics:

- Total brutto profit = 9 388 022,75 $;
- Total netto profit = 8 333 502,26 $;
- Total gas spendings = 1 054 520,49 $;
- Not profitable transactions count = 163;
- Coefficient of MEV transactions count to total transactions count = 0.0131234 (or 1.31234%);
- Brutto profit to total pool capitalization coefficient = 0.00107466 (or 0.107466%);
- Netto profit to total pool capitalization coefficient = 0.001014304 (or 0.1014304%);
- MEV attacks capitalization to total pool capitalization coefficient = 0.188628 (or 18.8628%).

This pool has the highest sum of netto and brutto profits collected out of the pool. Gas spendings are also one of the highest registered and attackers lost 11,23% of their profits. Capitalization of performed attacks is one of the biggest and forms around 19% of entire pool capitalization. Transaction frequency is medium.



Picture X: profits and capitalization distributions from SHIB/WETH

Profits distributions demonstrate correlation with capitalization of trades overall, meaning that MEV attacks are performed more frequently depending on traders activity. Distributions also

demonstrate how application of new gas fees strategy caused decrease of profits for MEV attackers, causing great difference in brutto and netto profits distributions.

Reasons of such a big MEV performance on this pool are almost identical to previous case of MEV performed for ELON/WETH pool. Activity, MEV profits distributions are correlating with distribution of the SHIB token price.

Overall situation of the MEV attacks in the STO pools

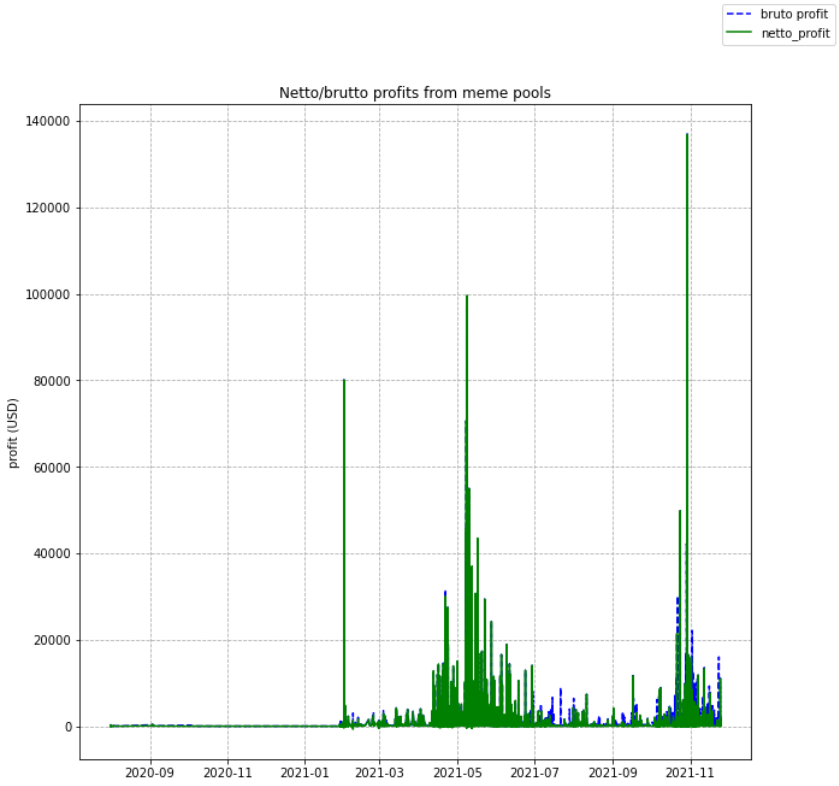
While classic tokens pools contain history of 6 pools, where each contained MEV attacks, and STO tokens pools contain history of 8 pools, where only 5 contained MEV attacks, meme tokens pools MEV attacks, where out of 4 pools only 3 contain MEV attack history, are outperforming results of both classic and STO pools.

Capitalization of performed attacks, their count and amount of extracted profits with highest-profits records in case of meme tokens are bigger than previous cases. From the presented results can be seen how attractive are those tokens for the attackers. This may be caused by extreme price deviations of those tokens. While classic tokens have become the most recognizable and demandable tokens with the highest prices on market, making their distributions more stable with changes happening only in case of powerful external influence, and STO tokens with less recognition and relatively stable with not so big activity are not attracting attackers, meme tokens deal with both attackers requirements - high activity, high price deviation and possible slippage removal (due to meme token possibility of strong price change even while performing trades). Statistics of all collected MEV attacks on meme tokens pools:

- Brutto profit = 13 223 655,77$;
- Netto profit = 11 321 620,31$;
- Gas spendings = 1 902 035,47$;
- Total meme pools capitalization = 12 040 671 161,57$;
- MEV attacks capitalization = 2 257 124 178,13$;
- MEV attacks capitalization coefficient = 0.187458 (or 18,7458%);
- Coefficient of MEV transactions out of all meme transactions = 0,015265 (or 1,5265%);

Distribution of MEV attacks profits on meme pools demonstrate extremely high profits, high activity, appeared difference between brutto and netto profits during period of raised gas

costs in the second half of 2021. Another interesting moment is that MEV activity is extremely high from around Spring 2021.



Picture X: profits distributions for all meme tokens pools

Capitalization of MEV attacks and extracted profits demonstrate that meme tokens are one of the main targets for MEV attackers. The problem with meme pools is in their regularization. Their activity is highly connected to price drops/rises caused by supply and demand changes on the market (even their recognition can influence those aspects) where application of any regularization (for example, mitigation mechanism application) can lead to impossibility of performing trades at specific time moment using close to market price, but because of "inertial" TWAP changes with some delay traders may lose possible profits and their interest in such a pool may greatly reduce.

NFT tokens pools (DOGE/WETH, ELON/WETH, SHIB/WETH, SQUID/WETH)

Principle behind NFT tokens is similar to the case of NFT pools, considering that any NFT price depends on the supply and demand mechanism with possible impact out of external events influencing demand of the token. Current case is unique, considering that it does not represent the case of fractionalized NFT, giving access for holders to a specific product or piece

of product. There are two cases of tokens taken from popular metaverse games (AXS/WETH and ALICE/WETH) and three cases of tokens representing tokens of platforms used for exchange, buy/sell and transfers of NFT products. Presented cases are interesting considering that the first two demonstrate concepts with rising popularity due to the new trend on metaverses at the moment of writing this document and three remaining demonstrate some form of combining STO with NFT.

All presented pools contain MEV attacks and here will be presented comparison with meme tokens pools situation.

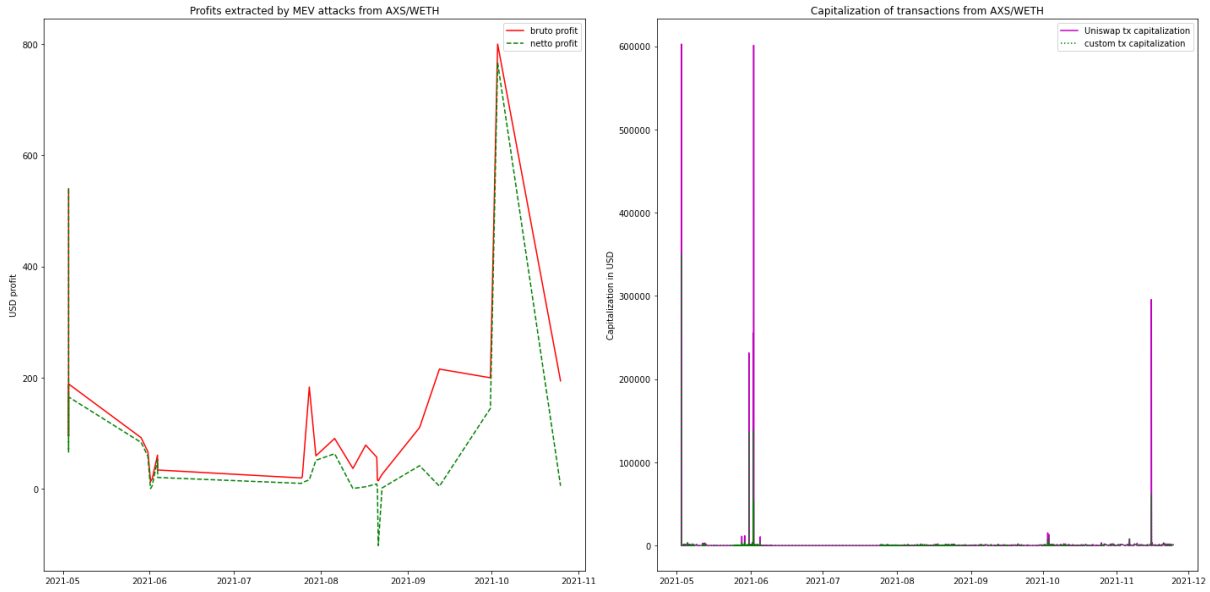
AXS/WETH

Current pool statistics:

- Total brutto profit = 3 224,66 $;
- Total netto profit = 2 016,40 $;
- Total gas spendings = 1 208,26 $;
- Not profitable transactions count = 1;
- Coefficient of MEV transactions count to total transactions count = 0.010897995 (or 1.0897995%);
- Brutto profit to total pool capitalization coefficient = 0.0007868449 (or 0.07868449%);
- Netto profit to total pool capitalization coefficient = 0.000639432 (or 0.0639432%);
- MEV attacks capitalization to total pool capitalization coefficient = 0.24157 (or 24.157%).

Frequency of MEV attacks is smaller than in case of meme tokens, but still on a medium level. Interesting moment about this case is that MEV attacks capitalization represent 24% out of entire pool capitalization. Extracted profits are relatively low and attackers lost 37,47% of their profits due to gas spendings.

Such a low profits and overall small amount of performed attacks demonstrate low interest of attackers on the presented pool. This may be caused by low popularity of the presented tokens in the pool, and unstable activity of the traders in this pool. Combination of those reasons decreases the attractiveness of the presented pool.



Picture X: profits and capitalization distributions from AXS/WETH

MANA/WETH

Current pool statistics:

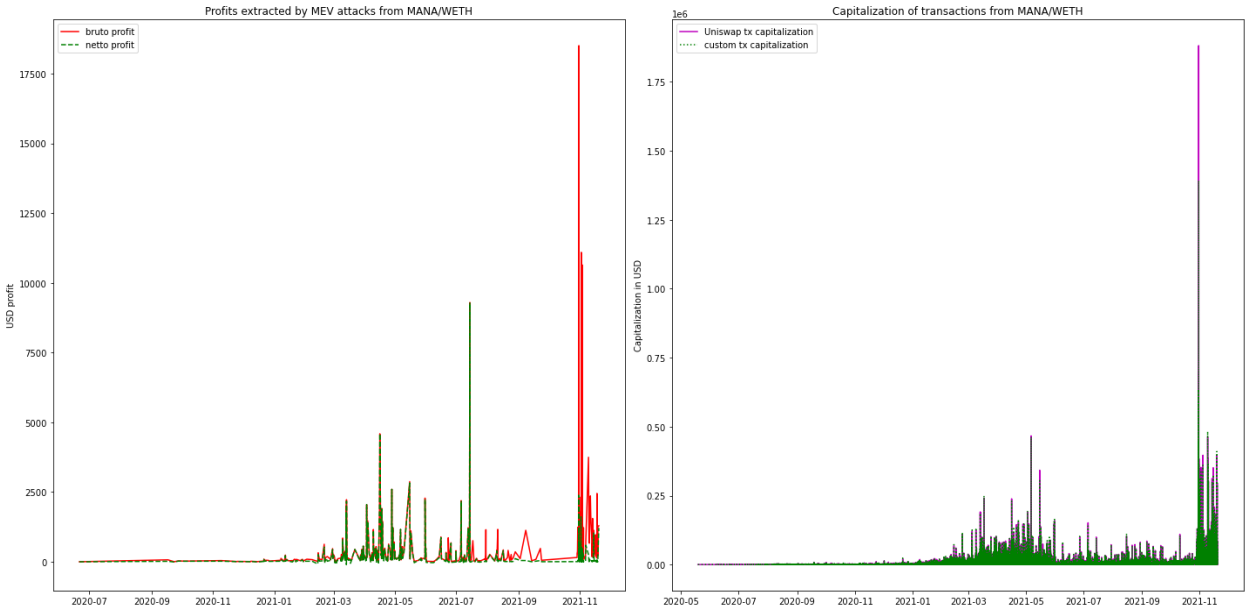
- Total brutto profit = 212 928,62 $;
- Total netto profit = 121 404,76 $;
- Total gas spendings = 91 523,85 $;
- Not profitable transactions count = 37;
- Coefficient of MEV transactions count to total transactions count = 0.0114446 (or 1.0114446%);
- Brutto profit to total pool capitalization coefficient = 0.00044719 (or 0.044719%);
- Netto profit to total pool capitalization coefficient = 0.0003197 (or 0.03197%);
- MEV attacks capitalization to total pool capitalization coefficient = 0.06781365 (or 6.781365%).

Frequency of performed attacks is almost identical to the AXS/WETH case, but the amount of extracted profits is extremely high compared to it. Gas spendings are extremely high relative to brutto profits collected from transactions. Gas caused a profit loss of 42,98%. Such a loss of profits demonstrates how impactful gas costs can be for attackers. Compared to previous case capitalization is much smaller, but still represents a medium size impact of MEV attacks.

Such a difference compared to the previous case can be explained that the presented token is different. It represents one of the most popular metaverse's tokens. The popularity of the

presented token causes higher popularity of the pool with this pool and higher attention from attackers due to higher demand of the token (therefore, higher liquidity of the token on market.

Interesting moment is that MEV attacks activity increased with trades activity after heavy marketing performed by Facebook around metaverses and declaring their decision to construct their own metaverse. This caused higher attention to the theme and higher demand for tokens used in such metaverses. Before this marketing company Decentraland (a game where MANA is used) was considered the biggest and most popular metaverse and therefore impact from the company was beneficial for this game. During this time period were performed one of the biggest brutto MEV profits and much bigger capitalization of performed activity.



Picture X: profits and capitalization distributions from MANA/WETH

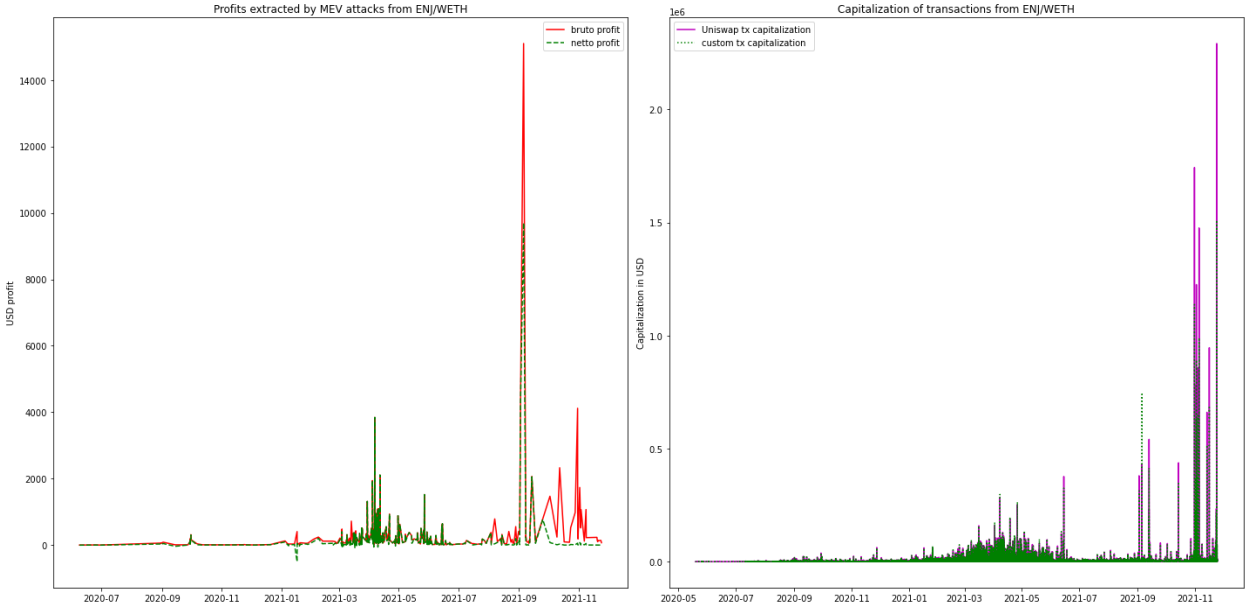
ENJ/WETH

Current pool statistics:

- Total brutto profit = 116 182,54 $;
- Total netto profit = 83 481,50 $;
- Total gas spendings = 32 701,03 $;
- Not profitable transactions count = 33;
- Coefficient of MEV transactions count to total transactions count = 0.010577488 (or 1.0577488%);
- Brutto profit to total pool capitalization coefficient = 0.00034133 (or 0.034133%);

- Netto profit to total pool capitalization coefficient = 0.000293295 (or 0.0293295%);
- MEV attacks capitalization to total pool capitalization coefficient = 0.0562248 (or 5.62248%).

Results of this pool are almost identical to the previous case with only one difference in gas spendings. Frequency of attacks is almost identical, demonstrating similarity between demand and popularity of those tokens, profits are smaller with almost identical amount of performed attacks and MEV attacks capitalization impact is also on medium level.



Picture X: profits of MEV attacks and capitalization of ENJ/WETH pool

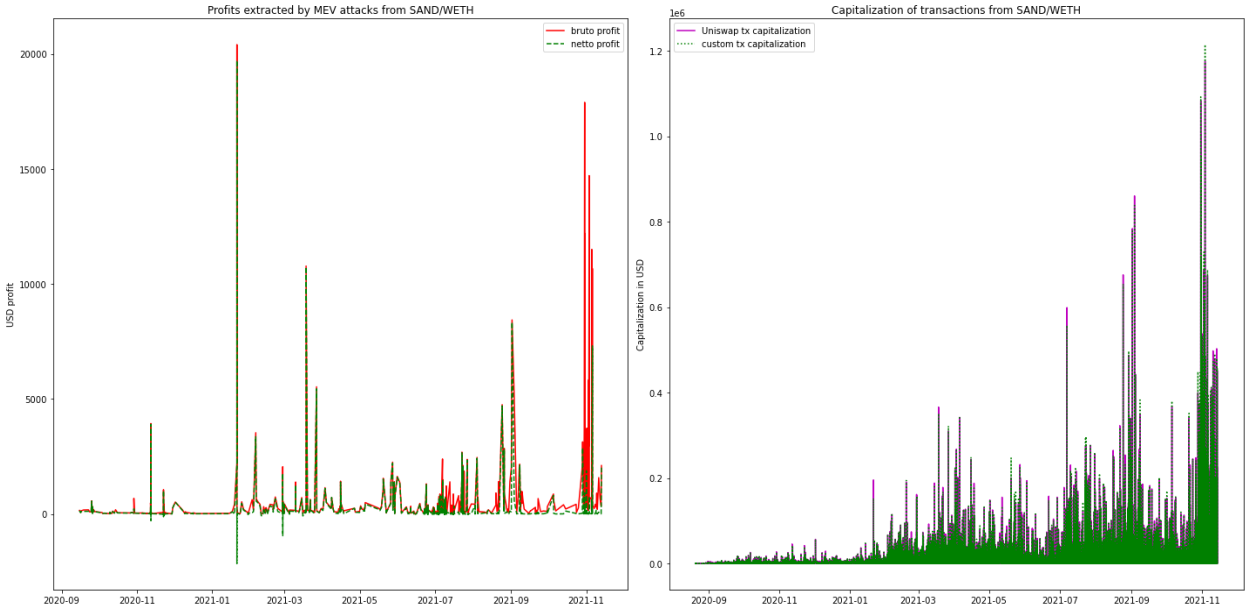
Performed attacks also demonstrate rise of the profits closer to the end 2021. Gas spendings are smaller and take from attackers 28,15% of extracted profits, demonstrating coefficient similar to the most of the cases. Reason why this token distribution is similar to the MANA/WETH and not AXS/WETH is in the recognition of the current token caused by a long history of the platform standing behind it, its relative recognition on the market and therefore liquidity of the token is higher.

SAND/WETH

Current pool statistics:

- Total brutto profit = 459 609,64 $;
- Total netto profit = 227 958,22 $;
- Total gas spendings = 231 651,42 $;

- Not profitable transactions count = 36;
- Coefficient of MEV transactions count to total transactions count = 0.0099543 (or 0.99543%);
- Brutto profit to total pool capitalization coefficient = 0.0003212421 (or 0.03212421%);
- Netto profit to total pool capitalization coefficient = 0.00024028627 (or 0.024028627%);
- MEV attacks capitalization to total pool capitalization coefficient = 0.0465316735 (or 4.65316735%).



Picture X: profits of MEV attacks and capitalization of SAND/WETH pool

Gas spendings cause catastrophic losses of profit for MEV attackers. 50,40% of received profits were lost due to high gas spendings. Even with this loss, netto profits extracted from SAND/WETH and brutto profits are one of the biggest out of the presented NFT pools. Frequency of attacks and their capitalization are similar to other cases of NFT pools. MEV activity correlates with activity of traders in SAND/WETH and can be seen that with the rise of activity MEV attacks are performed more frequently.

High gas spendings can be seen in the second half of the extracted profits from MEV attacks distributions, where the difference between netto and brutto profits rises. Activity of the traders increased closer to the end of 2021 due to the same reason as in other pools with tokens connected to metaverses - Facebook integration into metaverse community and started marketing

companies around this concept. SAND token is a token used in Sandbox platform, used for selling/exchanging, buying voxel models. Concept of this token is similar to the case of the ENJ token.

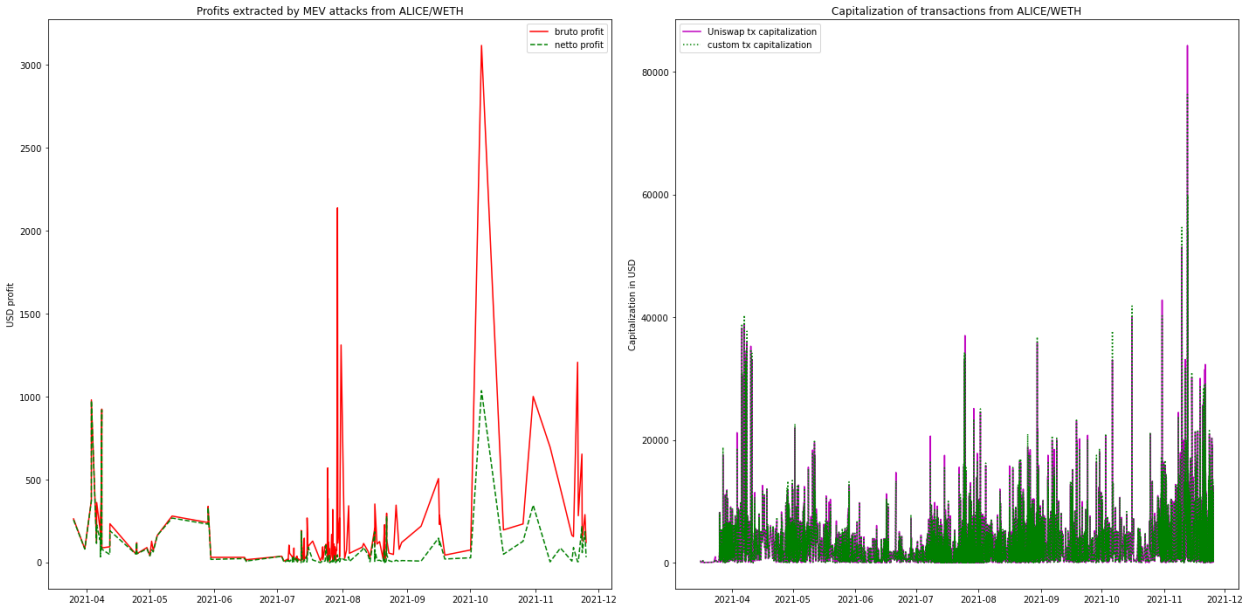
ALICE/WETH

Current pool statistics:

- Total brutto profit = 29 887,58 $;
- Total netto profit = 10 833,24 $;
- Total gas spendings = 19 054,34 $;
- Not profitable transactions count = 1;
- Coefficient of MEV transactions count to total transactions count = 0.039378484 (or 3.837884%);
- Brutto profit to total pool capitalization coefficient = 0.00109606168 (or 0.109606168%);
- Netto profit to total pool capitalization coefficient = 0.00074667355 (or 0.074667355%);
- MEV attacks capitalization to total pool capitalization coefficient = 0.0716006717 (or 7.16006717%).

ALICE/WETH has one of the highest gas fees considering that attackers lose 63,75% out of extracted profits and therefore efficiency of performed attacks is small. While brutto profit is representing a medium efficiency case, netto profits are one of the smallest registered out of all reviewed pools.

Most of the attacks are performed in the second half of 2021 when gas fees have raised and therefore efficiency of attackers will be smaller. It correlates with the activity performed in the pool. Another reason why MEV attacks were not performed with great profits - ALICE token is not so demandable and popular, because it is used in a small NFT game.



Picture X: profits of MEV attacks and capitalization of ALICE/WETH pool

Overall situation of the MEV attacks in the NFT pools

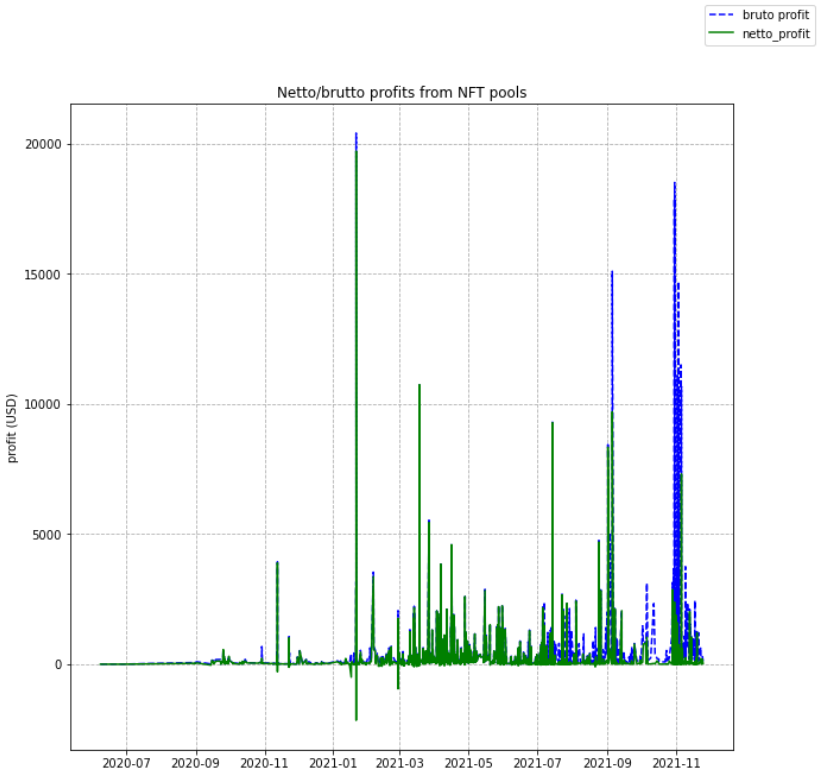
Frequency of attacks is similar to the case of meme pools and attackers activity in the presented pools is bigger than in the case of classic or STO pools. Netto profits are almost identical to the case of classic pools, which is a good factor considering the smaller number of considered pools compared to the case of classic pools, smaller activity and even smaller overall capitalization.

Still, attractiveness of NFT-related pools is bigger compared to STO pools and relatively close to attractiveness of performing attacks on classic pools. There is only one great problem with NFT-related pools - extremely high gas spendings. Those gas fees lead to extreme losses in profits of MEV attackers. It is required to consider that classic pools attacks were mostly performed during periods of smaller gas fees, but meme pools attacks were also performed with higher gas fees period, but proportion of gas spendings in meme pools attacks case is much smaller compared to NFT-related pools.

This can happen due to the rise of gas spendings in case of extremely rising activity in the pool, which considering the anomalous rise of NFT tokens demand several times could explain such losses on gas. Statistics of all collected MEV attacks on NFT-related pools:

- Brutto profit = 821 833,77$;
- Netto profit = 415 813,21$;
- Gas spendings = 406 019,82$;

- Total meme pools capitalization = 2 278 620 748,71$;
- MEV attacks capitalization = 120 943 641,56$;
- MEV attacks capitalization coefficient = 0.0530776 (or 5,30776%);
- Coefficient of MEV transactions out of all meme transactions = 0,01135611 (or 1,135611%).

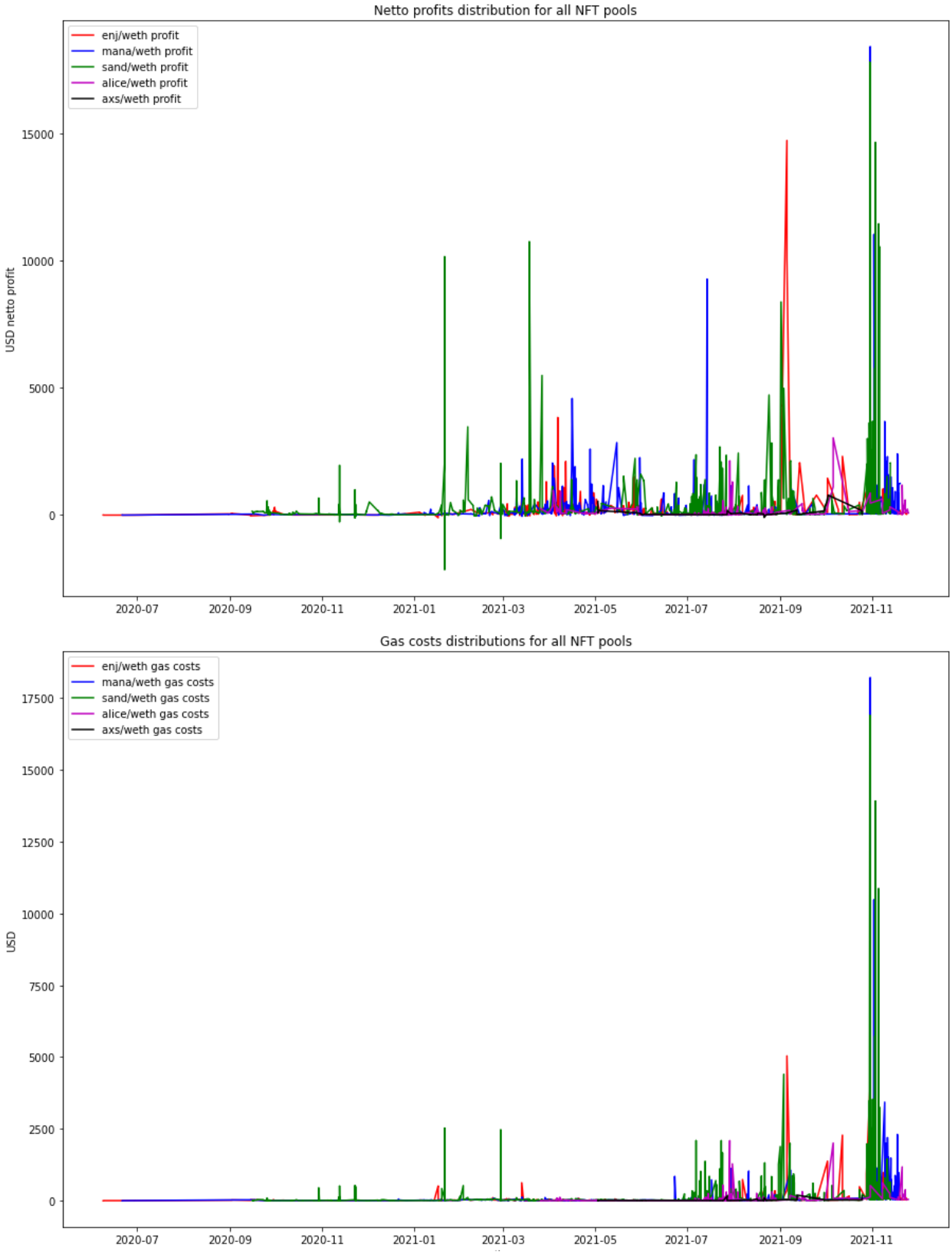


Picture X: profits of MEV attacks and capitalization of NFT related pools

Presented picture greatly demonstrates how the rise of gas fees in the second half of 2021 caused a drop in profitability of performed attacks and that their efficiency has been lowered. Therefore, out of all reviewed pools can be seen that MEV attacks are much better performed with meme pools.

Overall situation of the MEV attacks out of all reviewed pools

Overall distributions of all reviewed NFT-related pools are shifted to the right and can be seen how much of extracted profits has raised after the start of 2021, demonstrating the increasing attention of attackers to present on Uniswap pools for performing their attacks. Even with raised gas spendings can be seen how profits have raised closer to the end of 2021. This can be also connected to the rise of activity in NFT-related pools during 2021.

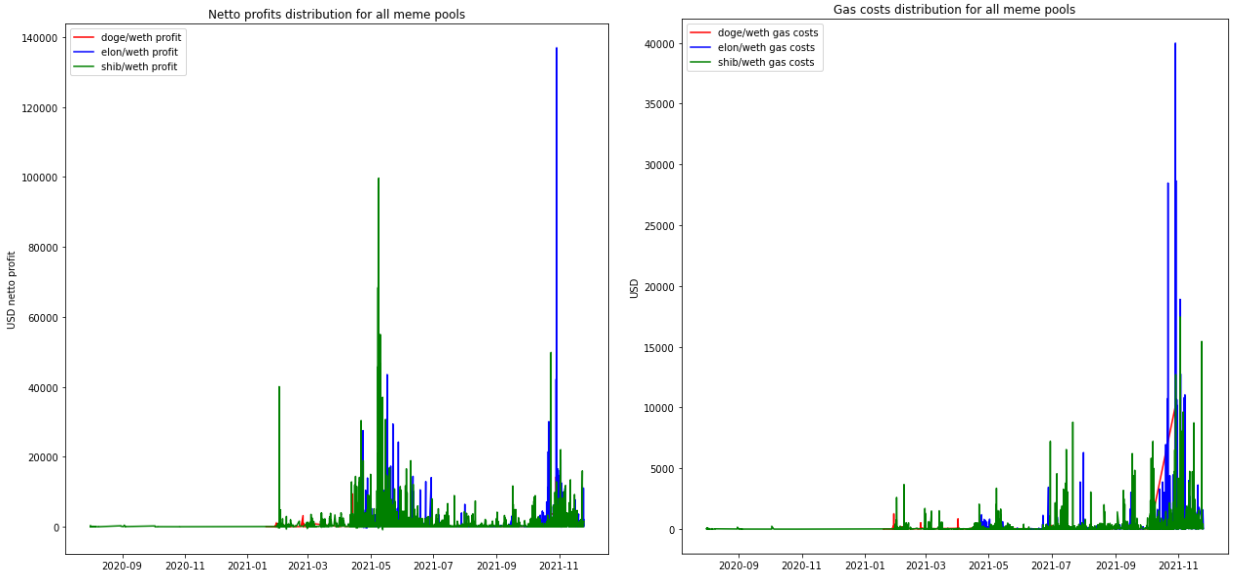


Picture X: netto profits distributions and gas spendings distributions for NFT-related pools

Presented distributions demonstrate high MEV activity for this category of pools and therefore it is required to pay higher attention to NFT-related pools from the perspective of MEV activity. NFT-related tokens have high price deviations like meme tokens. Price changes on those tokens stimulate a great increase of activity. Difference of this case from the rise of price on classic tokens and STO tokens is that in case a person misses a chance to sell a token with a raised price, or buy it while it is small, it means loss of profit. Size of lost profit depends on the difference between the new price and old one.

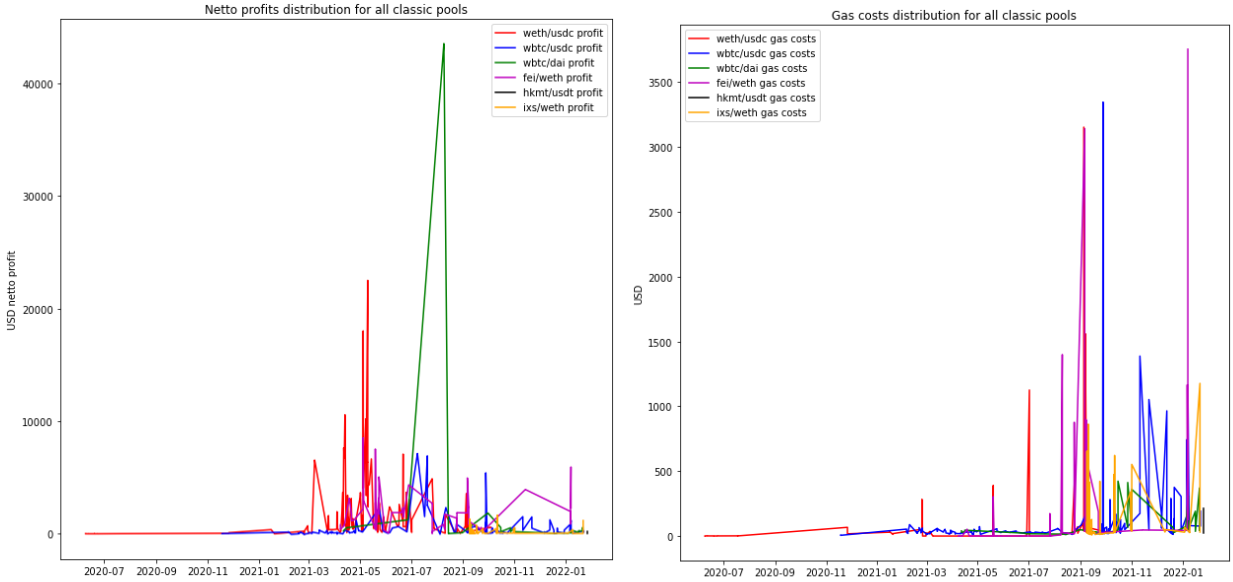
Why do classic tokens and STO represent different cases compared to meme and NFT tokens? Speculative nature of the last two token types. Ethereum and Bitcoin are now representing some sort of a standard in the world of cryptocurrency and their positions are more stable with higher chances of recovering after price fall due to recognition and demand on those tokens. They are becoming applicable in the real world for performing purchases and more financial institutes are starting to work with those cryptocurrency types. There are some unique cases of classic tokens connecting their price to some real-world value. STO tokens often stay behind organizations and their price with recognition depend on performed activity, on their lifecycle and reputation on market. Their price will be more stable and have extreme changes in case of heavy impact on work of a company. Moments of extreme price deviations for those token types are unlikely and rare. Therefore, traders that perform their activity with those tokens have lower chances of having extreme losses.

Meme and NFT tokens are highly dependent on demand and even small change on the market is able to cause high price deviation. For example, a tweet about a meme or NFT may cause high price change if it is performed by a popular person, while the same tweet about another cryptocurrency from classic or STO ones is unlikely to cause heavy impact. Another problem is the concept behind meme/NFT tokens. Classic tokens are oriented to be a currency used for performing financial operations on cryptomarket and perform unmonitored and untraceable purchases of goods/services, STO are used to support the company behind them, as an inner currency for exchange of goods/services provided by this company, connection to the real-world values. In most of the cases, NFT/meme tokens are not having any strong concept and real-life value for them. The first case may have connection to work of art (meaning that price depends on this art recognition), in-game goods purchase (depends on game recognition). The second case has no value staying behind them and their price is purely speculative.



Picture X: netto profits and gas spendings distributions for meme tokens pools

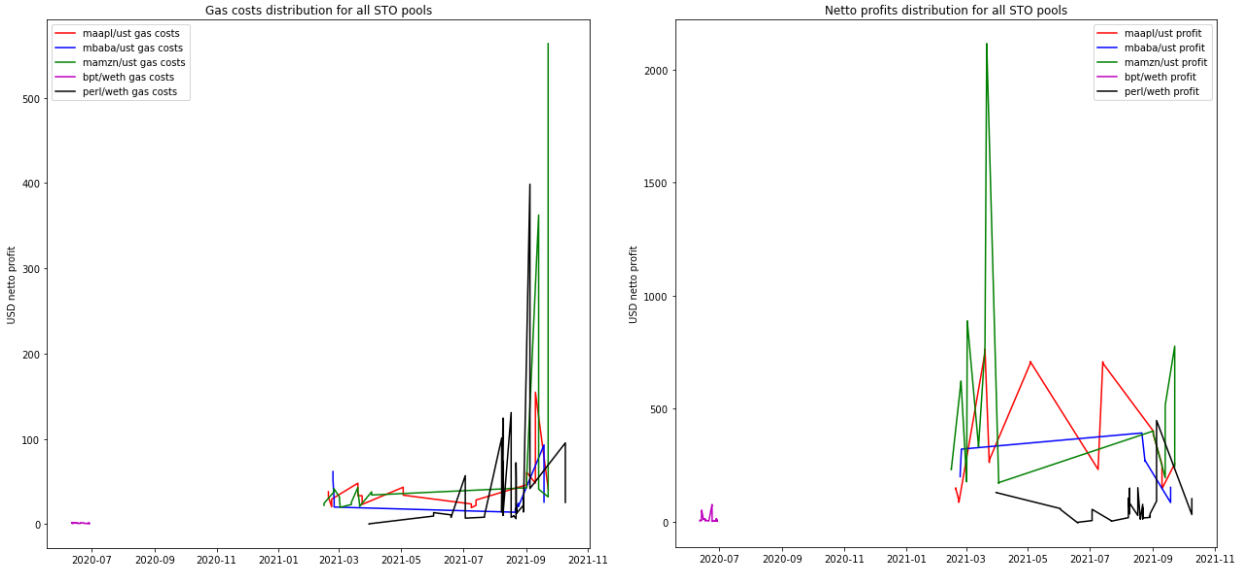
Purely speculative nature of meme tokens prices cause traders to use any possible chance to perform profitable trade, which is a perfect chance for MEV attackers to extract profits out of such desire. Traders will perform swaps with higher values, disabled slippage and as fast as possible, opening a chance for attackers to extract massive profits. Presented charts demonstrate how big profits can be and extracted profits are much higher compared to other token types.



Picture X: netto profits and gas spendings performed for classic tokens pools

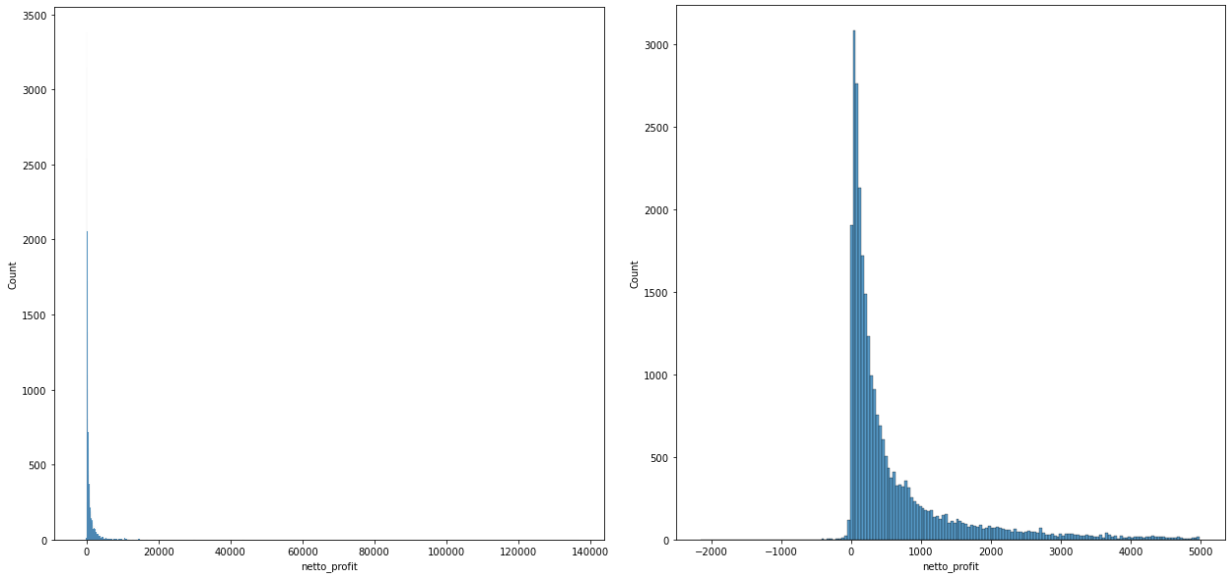
Classic tokens and STO tokens are less interesting for MEV attackers. It is possible to catch traders performing high exchange and rise of activity with change of token price, but

chance of getting such an option is smaller and traders are not exchanging such a big amount of tokens so easily compared to meme tokens and NFT.



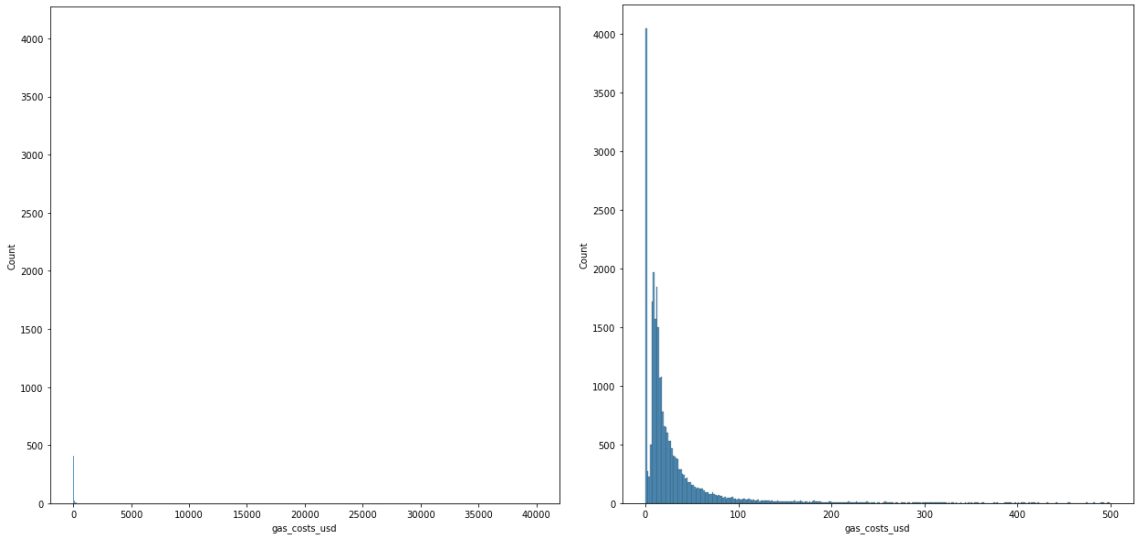
Picture X: netto profits and gas costs distributions for STO pools

Case of STO tokens attract lowest interest from MEV attackers due to small price changes and therefore more stable distributions from activity/price/capitalizations perspectives. The only case when MEV attackers will be attracted to those pools - big rise of activity performed by traders, meaning that risks are lower compared to other pool types, but still are present.



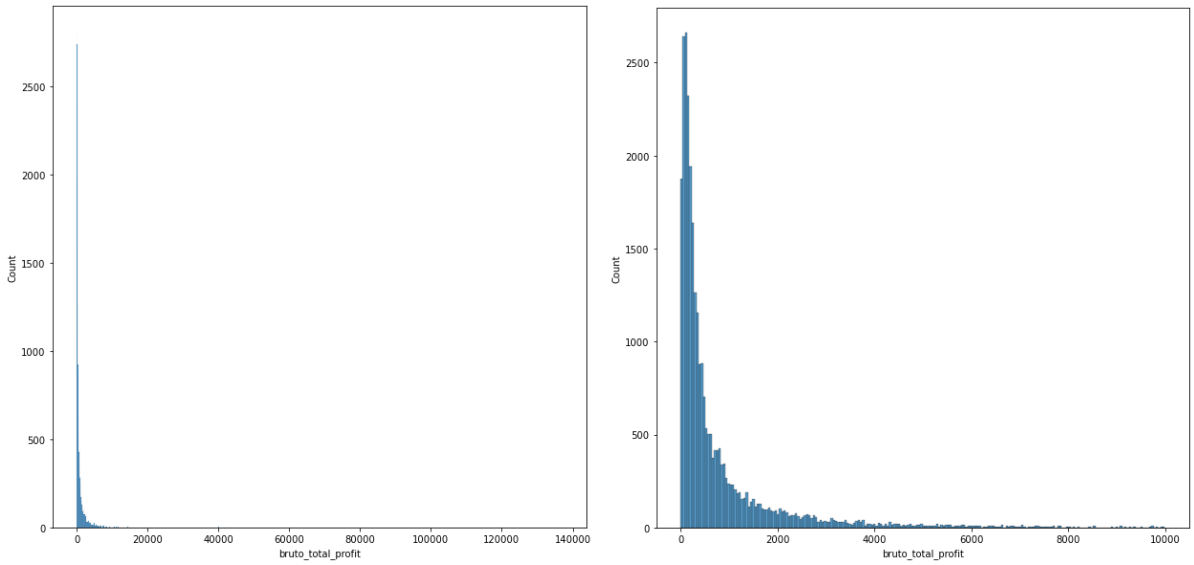
Picture X: entire netto profit distribution and with limit up to 5000 USD for all pools

Overall netto profits distribution looks extremely similar to the case of transaction values distribution, but there is one difference - while transaction values are only positive and profits can be negative. Transaction value generators can be also applied to the generating netto profits values or brutto profits values, but in this case there should be also applied gas costs values generators.



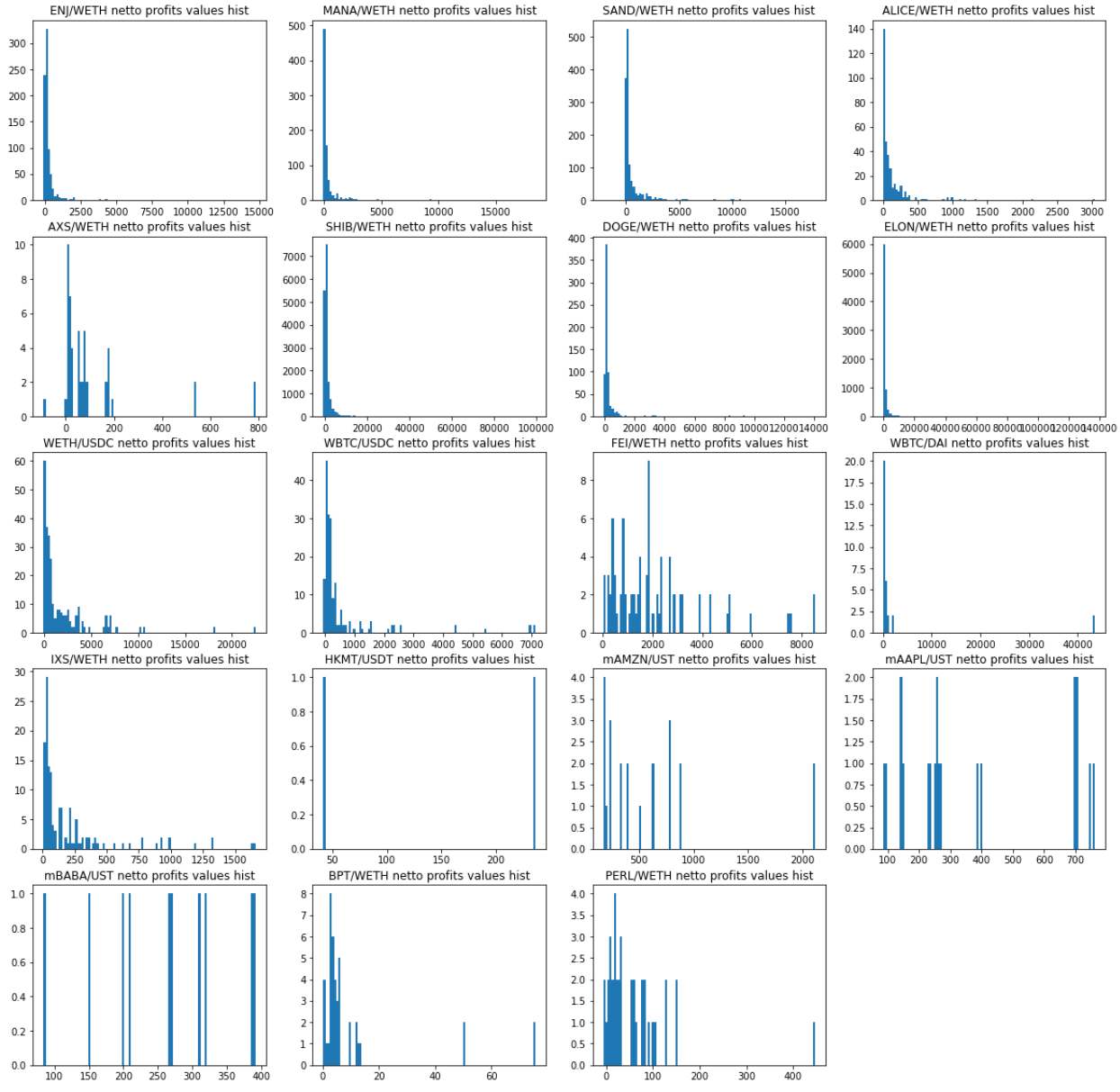
Picture X: entire gas costs distribution and with limit up to 500 USD for all pools

Gas costs distribution has a big range of values and in case of limiting gas costs values distribution up to 500 USD can be seen that values are similar to the exponential distribution and most likely models for generating transaction values can be used for gas costs values generation.



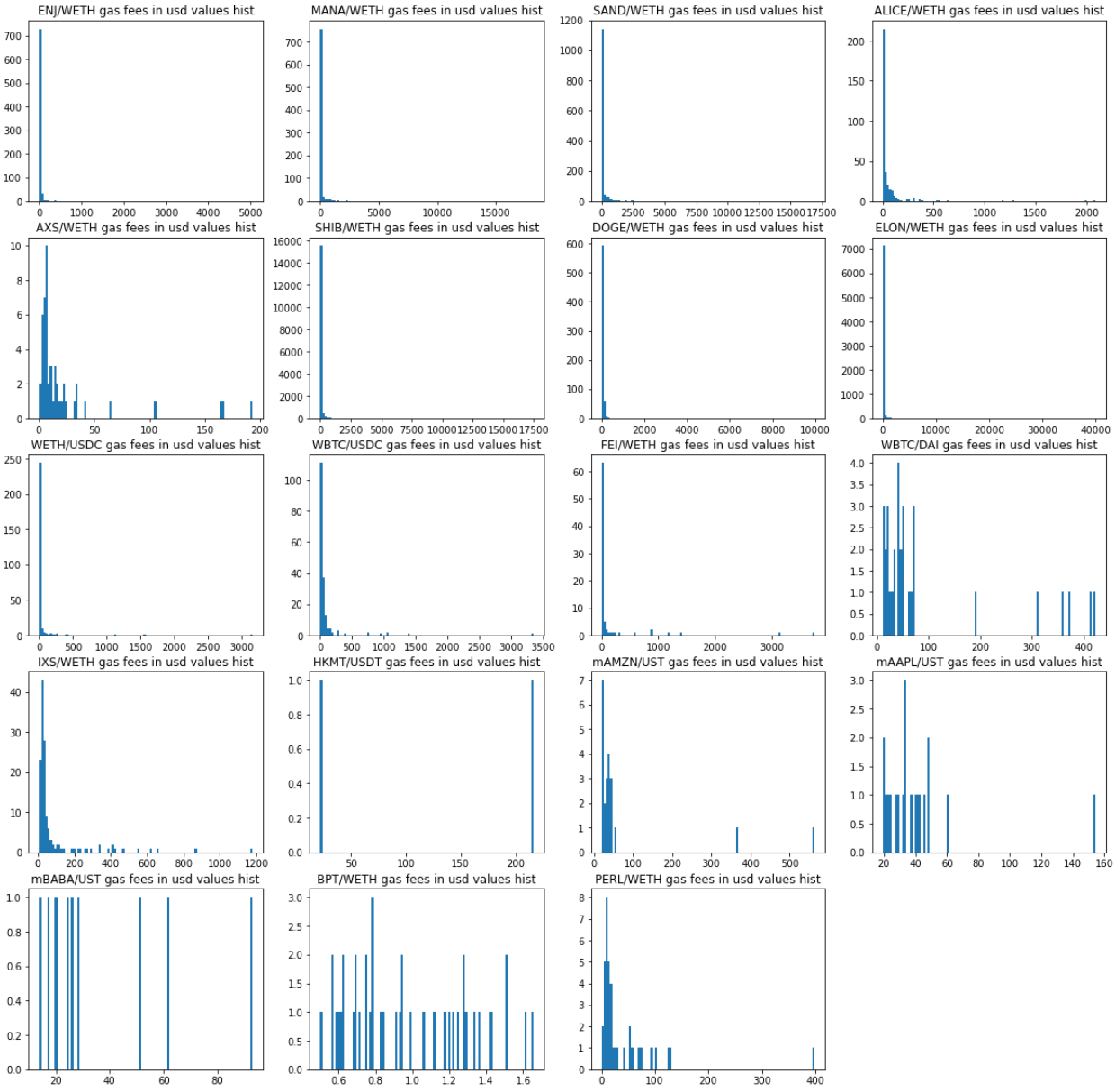
Picture X: entire brutto profit distribution and with limit up to 10000 USD for all pools

In case of plotting netto profits values distributions for each pool can be seen that meme pools and NFT-related pools converge to the exponential distributions and classic or STO pools contain unstable distributions with uninterpretable values distribution.



Picture X: netto profits values distribution for each of the reviewed pools

Gas cost values distributions also have exponential-like distribution in case of rich history. Meme pools contain the biggest gas costs registered due to the properties of the pool.

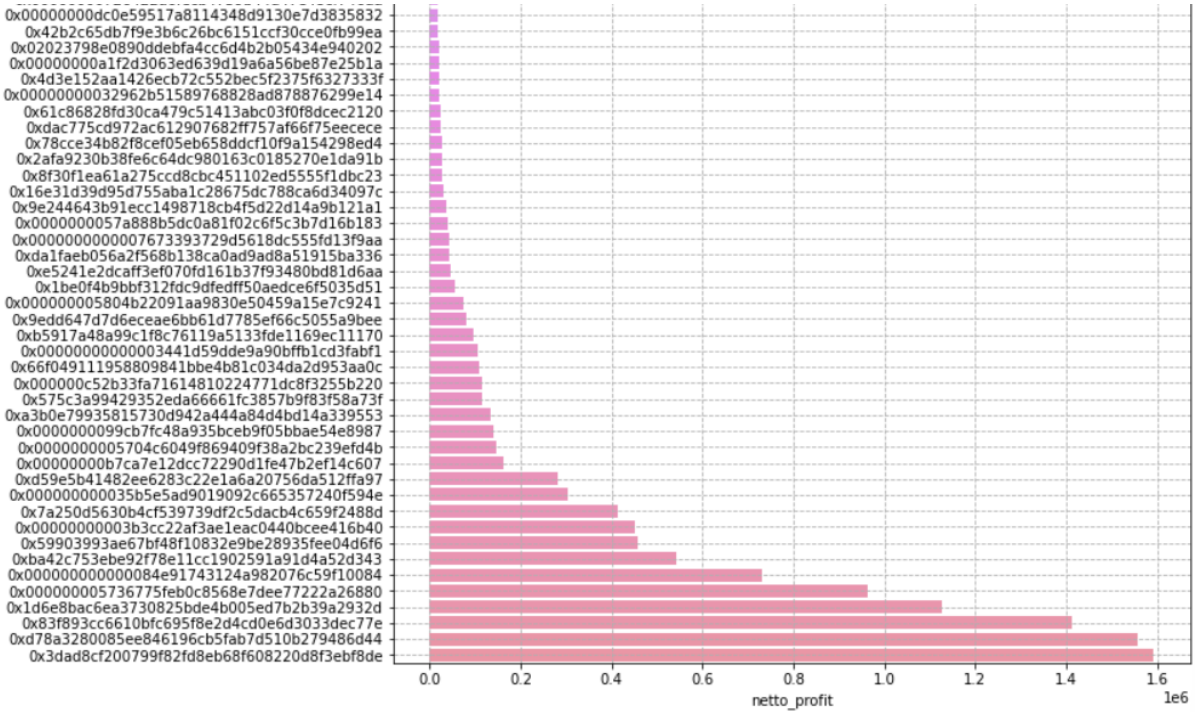


Picture X: gas costs values distributions for each pool

MEV attackers analysis

In process of MEV attacks analysis were observed multiple repeats of addresses that were indicated by the Uniswap services as “senders” of transactions, making it possible to consider them as addresses that performed MEV attack in the first place. Considering multiple repeats it was required to review those addresses closely from the perspective of how many attacks they performed, what pools were affected by their activity and profits extracted by them.

Review of profits extracted by addresses participating in MEV transactions as senders demonstrates that most of the profits were extracted by top 30 addresses by amount of extracted netto profits. Overall there were 242 addresses performing MEV transactions. Considering their amount and that most of the profits were extracted by top 30 addresses it is required to review them closer.



Picture X: netto profits extracted by addresses specified in “sender” section of the Uniswap transactions data (fragment represents top 30 attackers by amount of extracted netto profit)

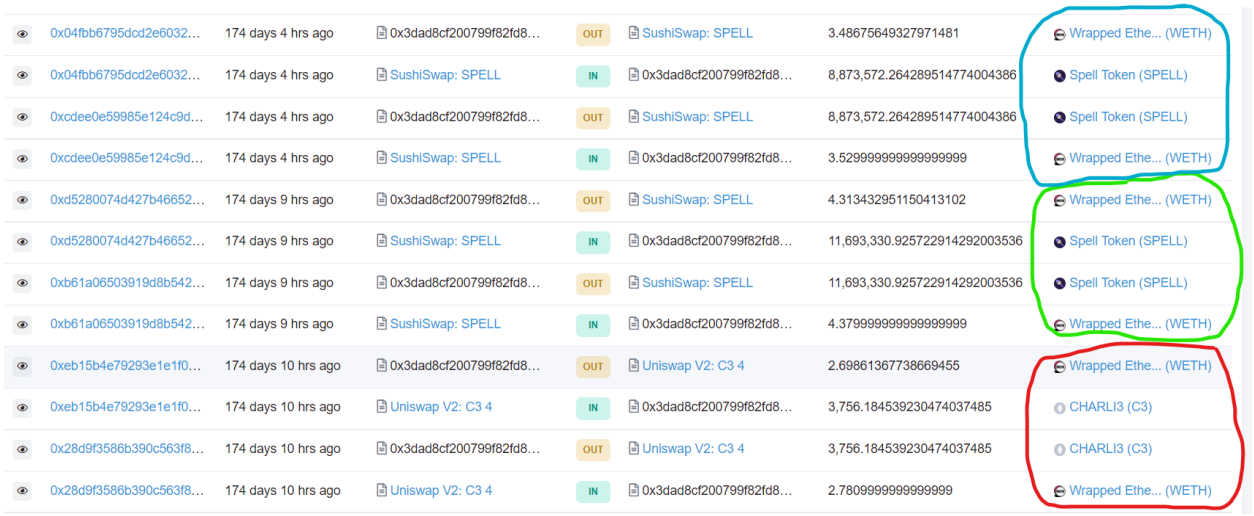
Reason why it is required to review senders closely is covered in the principle of how attackers perform their activity. In most of the cases, if reserves in the attacked pool are too high, the attacker gets a fast loan for performing the attack and then returns this loan. Both loaning and attacking are happening in the same block, making it possible that Uniswap transaction data will catch not the original sender of the transaction (not the original attacker), but the router service from another platform, eliminating option of preventing those attacks (because blocking those addresses will cause troubles for honest traders).

The biggest attacker

Above can be seen the biggest attacker from perspectives of extracted profits and performed attacks count with address 0x3dad8cf200799f82fd8eb68f608220d8f3ebf8de [link]. There is no specification of the presented address as router one and can be seen that performed

by this address transactions repeat pattern of the MEV attacks with 4 transactions sequence working by the next rule:

- Attacker loans tokens required for attack;
- Moves price to required direction to extract profit out of victim's losses;
- Extracts profit out of shifted by victim price of tokens (extract of profit close to victim's losses);
- Returns loaned tokens.



0x04fbb6795dcd2e6032...	174 days 4 hrs ago	0x3dad8cf200799f82fd8...	OUT	SushiSwap: SPELL	3.48675649327971481	Wrapped Ethe... (WETH)
0x04fbb6795dcd2e6032...	174 days 4 hrs ago	SushiSwap: SPELL	IN	0x3dad8cf200799f82fd8...	8,873,572.264289514774004386	Spell Token (SPELL)
0xcdee0e59985e124c9d...	174 days 4 hrs ago	0x3dad8cf200799f82fd8...	OUT	SushiSwap: SPELL	8,873,572.264289514774004386	Spell Token (SPELL)
0xcdee0e59985e124c9d...	174 days 4 hrs ago	SushiSwap: SPELL	IN	0x3dad8cf200799f82fd8...	3.529999999999999999	Wrapped Ethe... (WETH)
0xd5280074d427b46652...	174 days 9 hrs ago	0x3dad8cf200799f82fd8...	OUT	SushiSwap: SPELL	4.313432951150413102	Wrapped Ethe... (WETH)
0xd5280074d427b46652...	174 days 9 hrs ago	SushiSwap: SPELL	IN	0x3dad8cf200799f82fd8...	11,693,330.925722914292003536	Spell Token (SPELL)
0xb61a06503919d8b542...	174 days 9 hrs ago	0x3dad8cf200799f82fd8...	OUT	SushiSwap: SPELL	11,693,330.925722914292003536	Spell Token (SPELL)
0xb61a06503919d8b542...	174 days 9 hrs ago	SushiSwap: SPELL	IN	0x3dad8cf200799f82fd8...	4.379999999999999999	Wrapped Ethe... (WETH)
0xeb15b4e79293e1e1f0...	174 days 10 hrs ago	0x3dad8cf200799f82fd8...	OUT	Uniswap V2: C3 4	2.69861367738669455	Wrapped Ethe... (WETH)
0xeb15b4e79293e1e1f0...	174 days 10 hrs ago	Uniswap V2: C3 4	IN	0x3dad8cf200799f82fd8...	3,756.184539230474037485	CHARLI3 (C3)
0x28d9f3586b390c563f8...	174 days 10 hrs ago	0x3dad8cf200799f82fd8...	OUT	Uniswap V2: C3 4	3,756.184539230474037485	CHARLI3 (C3)
0x28d9f3586b390c563f8...	174 days 10 hrs ago	Uniswap V2: C3 4	IN	0x3dad8cf200799f82fd8...	2.7809999999999999	Wrapped Ethe... (WETH)

Picture X: example of transaction history covering 3 MEV attacks sequences

Etherscan data check ensures that the time interval when the presented address was active is between April 2021 and August 2021, which is also confirmed by first and last records of the MEV attacks performed by this address.

```
first record = 2021-04-12 12:35:43
last record = 2021-08-13 22:51:17
```

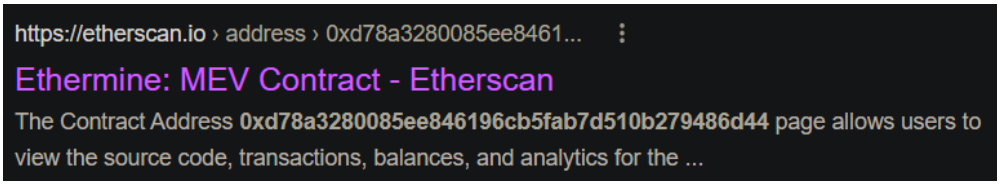
Picture X: first and last recorded MEV attacks by the given address

Conform available data address extracted 1683534,83$ netto profit out of reviewed pools in the presented time interval. Considering the presented time window, amount of performed attacks and structure of transactions available in the activity history of the presented address can be estimated that this is a MEV attacker with efficient scheme and performance of activity. Due to the last activity registered around half of a year ago (at the moment of writing this document) it is possible that this account finished its activity and has been disabled.

Out of all reviewed pools, the attacker performed its activity on only two pools - SHIB/WETH and ELON/WETH. Netto profit extracted from SHIB/WETH attacks is 1251265,52$ and netto profit extracted from ELON/WETH attacks is 432269,31$. There are only two meme tokens pools affected by activity of this attacker and it demonstrates clearly how profitable attacks on meme pools can be. The attacker performed 1787 MEV attacks on those pools.

The second attacker

The second place from the perspective of netto profit is taken by the attacker with address 0xd78a3280085ee846196cb5fab7d510b279486d44 [link]. The first sign demonstrating activity of the reviewed address is shown right after placing address in Google search.



Picture X: result of searching specified address

In case of reviewing performed activity it can be seen that history contains pure profit extractions, while review of each transaction demonstrates the same structure of MEV attacks sequence. Each attack extracts a small amount of Ethereum and therefore the attacker takes Ethereum as target token for extracting profits. This can be connected to the big rise of Ethereum price during spring of 2021.

Picture X: MEV attacks structure discovered in Etherscan history of transactions performed by reviewed address

There are 10 pools affected by activity of the presented address and profits extracted from each of them are listed below in increasing order:

1. AXS/WETH = 539,34$ after 1 attack (539,34$ mean profit);
2. ALICE/WETH = 588,46$ after 6 attacks (98,08$ mean profit);
3. SAND/WETH = 2 337,91$ after 7 attacks (333,99$ mean profit);
4. DOGE/WETH = 14 630,13$ after 48 attacks (304,79$ mean profit);
5. ENJ/WETH = 16 853,01$ after 68 attacks (247,84$ mean profit);
6. MANA/WETH = 19 054,70$ after 40 attacks (476,37$ mean profit);
7. FEI/WETH = 24 768,25$ after 12 attacks (2 064,02$ mean profit);
8. WETH/USDC = 79 234.91$ after 29 attacks (2 732,24$ mean profit);
9. ELON/WETH = 413 412,88$ after 542 attacks (762,75$ mean profit);
10. SHIB/WETH = 987 681,98$ after 800 attacks (1 234,60$ mean profit).

Again can be seen that most of the extracted profits were taken from meme tokens pools and the amount of extracted profits is much higher compared to NFT-related pools and classic tokens pools. Mean profits per transaction are highest in case of classic and meme tokens pools and can be seen that meme pools have been attacked much more frequently. Presented case greatly demonstrates how interested are attackers in performing their activity on meme pools.

```
first record = 2021-04-05 04:07:41
last record = 2021-05-25 11:26:13
```

Picture X: first and last recorded attacks performed by current address

This case is unique because of the active time of this bot and how much profit was extracted by this address. Two months of activity for this address led to almost the same results as the first and the third attackers by their profits while they were active for 5 months. This attacker extracted profits much faster.

The third attacker

The third place is taken by address 0x83f893cc6610bfc695f8e2d4cd0e6d3033dec77e [link] that performed activity between April and August 2021. During this time the attacker extracted 1418072,28$, but this attacker has 6-th place from the perspective of how many attacks

were performed by the address. There are 9 pools affected by attacks. All of them are presented below in increasing order:

1. ALICE/WETH = 14,68$ after 1 attack (14,68$ mean profit);
2. ENJ/WETH = 199,02$ after 1 attack (199,02$ mean profit);
3. SAND/WETH = 1 406,71$ after 1 attack (1 406,71$ mean profit);
4. FEI/WETH = 3 176,85$ after 1 attack (3 176,85$ mean profit);
5. MANA/WETH = 3 723,75$ after 6 attacks (620,63$ mean profit);
6. DOGE/WETH = 9 823,81$ after 8 attacks (1 227,98$ mean profit);
7. WETH/USDC = 74 349,49$ after 20 attacks (3 717,47$ mean profit);
8. ELON/WETH = 261 751,92$ after 69 attacks (3 793,51$ mean profit);
9. SHIB/WETH = 1 063 626,05$ after 395 attacks (2 692,72$ mean profit).

The attacker extracted most of the profits out of meme tokens pools and most of the attacks were directed to meme tokens pools. The principle of performed activity by this address is almost identical to the previous reviewed address, but the address was active for 4 months as the first reviewed address.

```
first record = 2021-04-14 23:21:58
last record = 2021-08-10 16:12:22
```

Picture X: first and last MEV attacks performed by the current attacker

Current address activity looks like a classic case of MEV bot because transaction history looks similar to MEV attacks sequences.

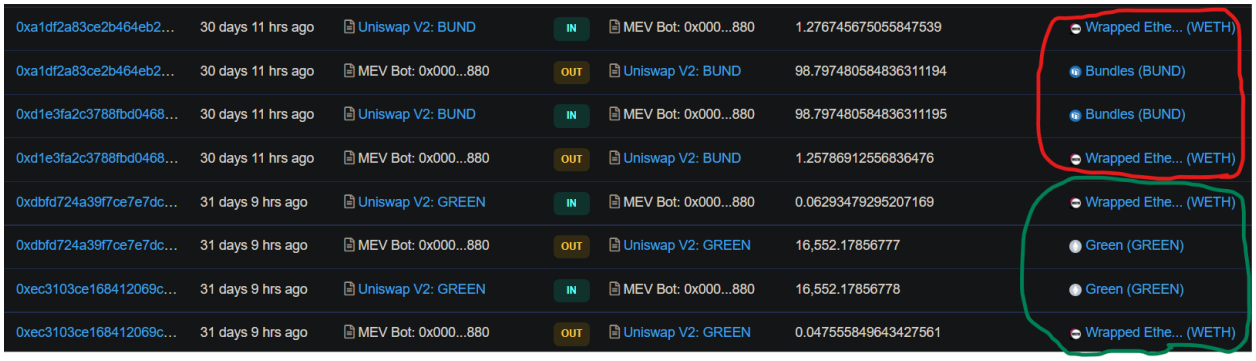
0x67d388f3db6a6aa747...	186 days 1 hr ago	Uniswap V2: NBU 2	IN	0x83f893cc6610bfc695f8...	2.308171555320223656	Wrapped Ethe... (WETH)
0x67d388f3db6a6aa747...	186 days 1 hr ago	0x83f893cc6610bfc695f8...	OUT	Uniswap V2: NBU 2	40,123.177058905806473685	Nimbus (NBU)
0x0c8e22f5c6f11e0d8b4...	186 days 1 hr ago	Uniswap V2: NBU 2	IN	0x83f893cc6610bfc695f8...	40,123.177058905806473685	Nimbus (NBU)
0x0c8e22f5c6f11e0d8b4...	186 days 1 hr ago	0x83f893cc6610bfc695f8...	OUT	Uniswap V2: NBU 2	2.251382883236364429	Wrapped Ethe... (WETH)
0xca32f36056b46a992c...	186 days 1 hr ago	0x83f893cc6610bfc695f8...	OUT	Uniswap V2: RNB	1,955.940597183144659155	Rentible (RNB)
0xca32f36056b46a992c...	186 days 1 hr ago	Uniswap V2: RNB	IN	0x83f893cc6610bfc695f8...	0.379695478391483761	Wrapped Ethe... (WETH)
0xb6d647aebfec6e6c8b...	186 days 1 hr ago	Uniswap V2: RNB	IN	0x83f893cc6610bfc695f8...	1,955.940597183144659155	Rentible (RNB)
0xb6d647aebfec6e6c8b...	186 days 1 hr ago	0x83f893cc6610bfc695f8...	OUT	Uniswap V2: RNB	0.366778901565179198	Wrapped Ethe... (WETH)
0x6fcfc43bd6cc3389d0a...	186 days 3 hrs ago	0x83f893cc6610bfc695f8...	OUT	Uniswap V2: GGTK 4	2,684.922662771732645065	GGToken (GGTK)
0x6fcfc43bd6cc3389d0a...	186 days 3 hrs ago	Uniswap V2: GGTK 4	IN	0x83f893cc6610bfc695f8...	1.022006331172630481	Wrapped Ethe... (WETH)
0xef7f00283282b1de4ce...	186 days 3 hrs ago	0x83f893cc6610bfc695f8...	OUT	Uniswap V2: GGTK 4	0.998126077770139769	Wrapped Ethe... (WETH)
0xef7f00283282b1de4ce...	186 days 3 hrs ago	Uniswap V2: GGTK 4	IN	0x83f893cc6610bfc695f8...	2,684.922662771732645065	GGToken (GGTK)

Picture X: Etherscan history of transactions by current address where can be seen principle of MEV attacks sequences

Taken transaction history demonstrates that after each attack a small value of WETH tokens is extracted. This is the same principle similar to the second and the first attackers.

The fourth attacker

The fourth attacker is address 0x000000005736775Feb0C8568e7DEe77222a26880 [link] and on Etherscan it is indicated as MEV bot, right from the start ensuring correct catch of the attacker. Structure of transactions present in the pool demonstrate classic MEV attack sequence.



0xa1df2a83ce2b464eb2...	30 days 11 hrs ago	Uniswap V2: BUND	IN	MEV Bot: 0x000...880	1.2767456750558475 39	Wrapped Ethe... (WETH)
0xa1df2a83ce2b464eb2...	30 days 11 hrs ago	MEV Bot: 0x000...880	OUT	Uniswap V2: BUND	98.797480584836311194	Bundles (BUND)
0xd1e3fa2c3788fbd0468...	30 days 11 hrs ago	Uniswap V2: BUND	IN	MEV Bot: 0x000...880	98.797480584836311195	Bundles (BUND)
0xd1e3fa2c3788fbd0468...	30 days 11 hrs ago	MEV Bot: 0x000...880	OUT	Uniswap V2: BUND	1.257869125568364 76	Wrapped Ethe... (WETH)
0xdbfd724a39f7ce7e7dc...	31 days 9 hrs ago	Uniswap V2: GREEN	IN	MEV Bot: 0x000...880	0.062934792952071 69	Wrapped Ethe... (WETH)
0xdbfd724a39f7ce7e7dc...	31 days 9 hrs ago	MEV Bot: 0x000...880	OUT	Uniswap V2: GREEN	16,552.17856777	Green (GREEN)
0xec3103ce168412069c...	31 days 9 hrs ago	Uniswap V2: GREEN	IN	MEV Bot: 0x000...880	16,552.17856778	Green (GREEN)
0xec3103ce168412069c...	31 days 9 hrs ago	MEV Bot: 0x000...880	OUT	Uniswap V2: GREEN	0.047555849643427561	Wrapped Ethe... (WETH)

Picture X: Etherscan transaction history of the current MEV attacker

While the Etherscan information shows that address is still active and performs attacks, taken pools contain activity records of this address from middle of April 2021 till end of November 2021.

```
first record = 2021-04-15 14:38:52
last record = 2021-11-24 15:27:53
```

Picture X: first and last performed attacks on the reviewed pools by the current attacker

Attacker affected 7 pools and total collected netto profit is equal to 1100027,78$. Profits extracted from pools are next (in increasing order by extracted profits):

1. AXS/WETH = 13,54$ after 1 attack (13,54$ mean profit);
2. PERL/WETH = 287,19$ after 5 attacks (57,44$ mean profit);
3. ENJ/WETH = 5 717,76$ after 22 attacks (259,90$ mean profit);
4. SAND/WETH = 17 022,27$ after 40 attacks (425,56$ mean profit);
5. MANA/WETH = 19 595,29$ after 40 attacks (489,88$ mean profit);

6. ELON/WETH = 358 982,32$ after 360 attacks (997,17$ mean profit);
7. SHIB/WETH = 698 409,41$ after 530 attacks (1 317,75$ mean profit);

This attacker also extracted most of the profits from meme tokens pools, meaning that the current attacker is also more interested in performing attacks on meme pools. Current attacker almost totally ignored classic tokens pools and STO pools.

The fifth attacker (something unique)

Current case is unique, because here transactions were called by a Uniswap Router V2 address 0x7a250d5630B4cF539739dF2C5dAcb4c659F2488D [link]. Total collected profit by this address is equal to 448167,80$ and there were 12 pools affected by those attacks (presented below in increasing netto profit order):

1. mBABA/UST = 519,70$ after 2 attacks (259,85$ mean profit);
2. ALICE/WETH = 1 175,16$ after 6 attacks (195,86$ mean profit);
3. mAAPL/UST = 1 257,08$ after 4 attacks (314,27$ mean profit);
4. DOGE/WETH = 5 003,10$ after 17 attacks (294,30$ mean profit);
5. mAMZN/UST = 5 307,47$ after 8 attacks (663,43$ mean profit);
6. MANA/WETH = 3 654,74$ after 27 attacks (135,36$ mean profit);
7. ENJ/WETH = 9 625,41$ after 26 attacks (370,21$ mean profit);
8. SAND/WETH = 9 869,17$ after 25 attacks (394,77$ mean profit);
9. FEI/WETH = 10 659,30$ after 2 attacks (5 329,65$ mean profit);
10. WETH/USDC = 18 388,56$ after 12 attacks (1 532,38$ mean profit);
11. ELON/WETH = 97 366,52$ after 114 attacks (854,09$ mean profit);
12. SHIB/WETH = 285 341,61$ after 366 attacks (779,62$ mean profit).

Again can be seen that meme tokens pools were the most affected ones by performed attacks, but considering that the presented address is referred to the Uniswap Router V2 means that more detailed analysis is required.

Review of transactions on the Etherscan platform demonstrates that overall behavior is not looking like a MEV one and performed transactions are simple trades. There are two possible reasons why this address appears in the Uniswap V2 transaction history:

- Attackers use Uniswap Router services to hide their attacks and therefore not to be shown on the transactions history;

- Uniswap performs some transactions using Router services to perform inner operations and therefore it is not possible to catch the real sender of the attack.

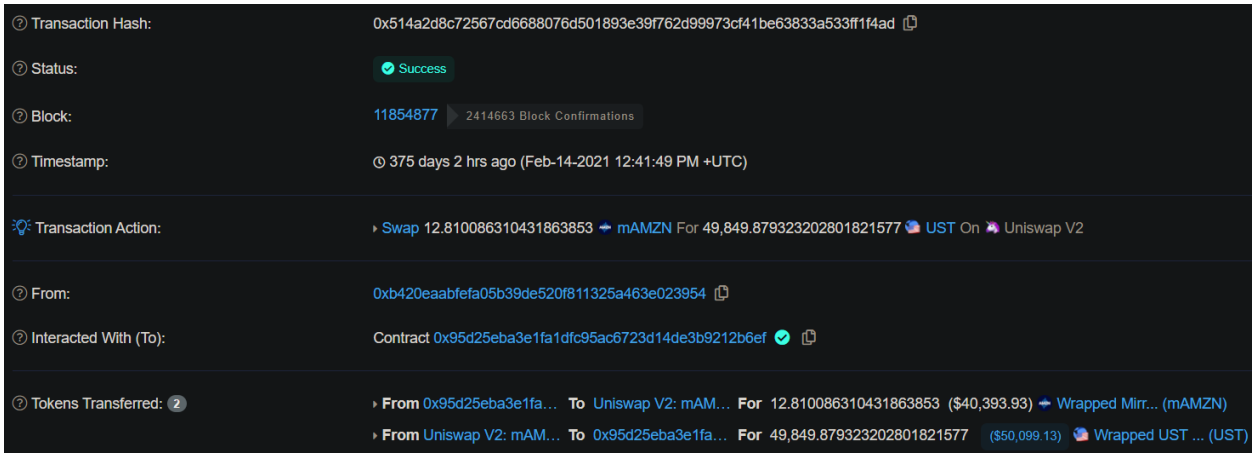
In both of those cases, it is not possible to estimate a real attacker using an Uniswap history, but there is an option of recovering addresses of possible attackers using Etherscan service, because a check of MEV transactions shows different addresses in the “From” field.

```
1  total_profits_df[total_profits_df['sender'] == '0x7a250d5630b4cf539739df2c5dacb4c659f2488d'].loc[0]
✓ 0.8s
```

timestamp	2021-02-14 12:41:49
sender	0x7a250d5630b4cf539739df2c5dacb4c659f2488d
amount_usd	NaN
to	0x95d25eba3e1fa1dfc95ac6723d14de3b9212b6ef
txd	0x514a2d8c72567cd6688076d501893e39f762d99973cf...
block	11854877.0
block_position	130.0
bruto_total_profit	254.103086
tx_fee	0.0
gas_usage_by_tx	110222.0
gas_costs_usd	21.935563
netto_profit	232.167522
pool_name	mAMZN/UST

Picture X: example of transaction taken for review

“From” field contains another address, different from Uniswap estimated one, but check of this transaction and next one ensures that it was a MEV attack performed on mAMZN/UST pool.



Picture X: the same transaction on Etherscan

Therefore, in case if it will be required to form a list of attackers for their further blocking it will be required to perform address filtering and verification to ensure that there will be no routers and inner services addresses blocked.

AMM simulations using generated transactions

Non-traded securities

The first examined use-case are pairs composed of a non-traded security (X) and stablecoin (Y). The primary assets taken into consideration are private equity and real estate assets.

Trading parameters

The stream of trades will come from a random process that "draws" trades from distributions. As in case of non-traded securities there are **no alternative markets** that would stimulate **arbitrage activity** in case of significant price differences, it's reasonable to assume that the behavior of traders for each side (those willing to exchange X on Y and vice-versa) can be described by **separate distributions**, varying the parameters of which it would be possible to model distinct trading behaviors.

The main parameters needed to describe the behavior of traders for each side are:

- Trade frequency - drawn from a poisson distribution with parameter Lambda (λ - is the expected rate of occurrences every minute)
- Trade size - the distribution allowing to describe the traders best is to be determined

Identification of best-fit trade size distribution

The identification of the best-fit trade size distribution is based on the analysis of the historical Uniswap v2 transactions. Particularly, the proposed method is to focus primarily on the transactions of exchanging the stablecoin on some other token. By determining the best fit distribution for each pool containing the stablecoin on one side, it would be possible to generalize the results, in order to highlight several **distinct trading behaviors** (which could be described by the parameters of the distribution). It was decided to focus initially only on the **stablecoin swap in transactions**, because the values of exchanging an alternative token are directly linked to it's price, which would significantly complicate the process of comparing the traders patterns across distinct pools.

To categorize the transactions into corresponding reserve ranges, one of the options would be to look at the exact reserve values right before the transaction was executed. However, this method would fail for swaps 'sandwiched' by MEV-bot transactions, and is susceptible to

other manipulatory scenarios. Another approach would be to consider the daily reserve values. The problem that arises now is the misclassification of transactions in case of significant mints or burns during the day, which would change the liquidity from one range to another. In this case, the transactions executed before the significant variation in reserves, would be classified into the wrong range (in case only the end of day reserves are considered). To avoid such scenarios, it was decided to consider only the transactions for which the end of day stablecoin reserves value didn't deviate by more than 30% compared to the previous day value.

The last important moment to consider before fitting the value to a distribution is **filtering MEV-bot transactions** and other **suspicious transaction types**, which **don't influence the reserves of the pool** outside of the block in which they are executed, and follow a distinct pattern from the usual ones.

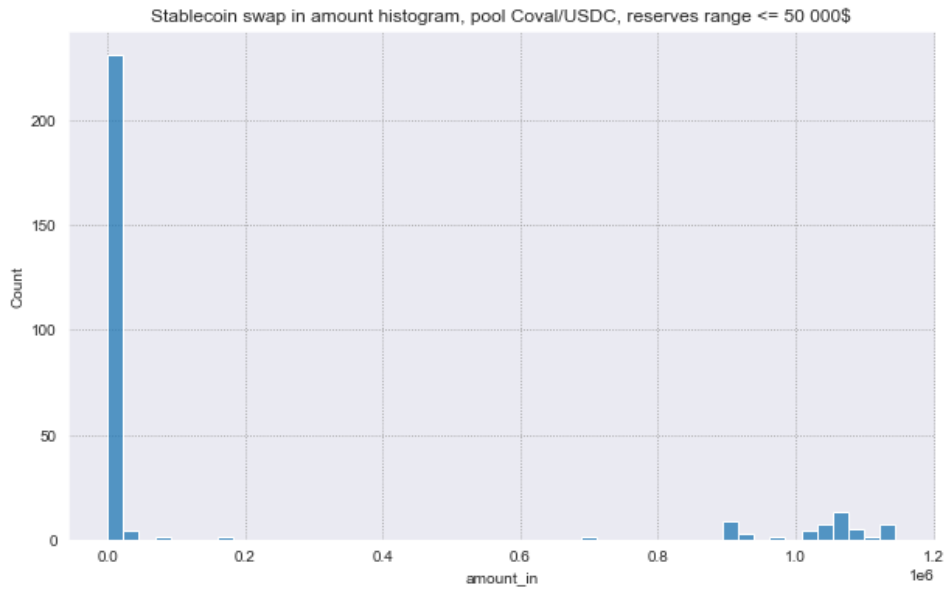


Figure X. Swap in stablecoin values

There was identified a high number of extremely big swap_in transactions (with values exceeding $1mln) inside the pool Coval / USDC. Considering that the reserves inside the pool at the moment the transactions were executed didn't exceed 50 000$, such high values certainly couldn't reflect usual trading behavior (even though they weren't detected by the MEV-bot transactions filter). By manually analyzing these transactions, it was established that most of them were executed either in order to extract the token, for a subsequent MEV-bot attack on another pool (containing this token), or represent some other kind of fraudulent actions. In the next transaction inside the same block, after executing the attack, the tokens are returned inside

the pool, with a small difference, the state of the pool remains the same. To filter out such transactions, an algorithm was written, detecting transaction pairs (distinct direction) inside the same block, initiated by the same sender and having a percentage difference of swap_out/swap_in values of less than 5%.

Considered distributions

In the analysis below, the distribution of swap-in stablecoin values (across each analyzed pool and for each corresponding reserve range separately), are compared against 4 distinct distributions: **LogNormal, Gamma, Weibull, HalfCauchy**.

To compare how well each of these distributions fit the data, 3 metrics have been chosen: SSE, MAE and AIC.

SSE and MAE are being computed based on the difference between the normalized histogram of the sample data and the PDF of the distribution estimated from the sample data using **maximum likelihood estimation** method. The number of bins at which to compute the error is selected in order to have a bin width of 1000, but cannot be less than 20 (number of bins = max(20, max(amount_in_values) / 1000).

AIC (Akaike Information Criterion) is another effective method for choosing the best-fit distribution, that deals with the trade-off between the goodness of fit of the model and the it's simplicity. The problem that it addresses is the tendency to overfit of the more complex models. The metric is computed based on the likelihood of the examined distribution, fitted using the MLE method, and the number of estimated parameters (which serves as a penalty to avoid overfitting). Compared to the previous 2 metrics, the absolute value of AIC is meaningless (as it's data specific) and can be used only to compare models fitted on identical samples. The smaller the AIC value, the better the model describing the data.

For all compared distributions, in order to estimate the parameters, the **location** parameter was **fixed to 0** (reflecting the fact that the swap amount should take positive values) and the remaining parameters have been computed using **maximum likelihood estimation** method.

Below, is presented the table of errors calculated based on the stablecoin swaps from the pool WBTC/DAI during reserve ranges 10 000 - 50 000 and 50 000 - 100 000.

pool	reserves_lower_limit	reserves_upper_limit	distribution	AIC	SSE	MAE
WBTC/DAI	10000	50000	Weibull	3050.12	4.53728e-06	0.00229391
WBTC/DAI	10000	50000	Gamma	3090.18	3.60944e-06	0.00211062
WBTC/DAI	10000	50000	LogNormal	3105.69	6.40064e-06	0.00281513
WBTC/DAI	10000	50000	HalfCauchy	3076.22	5.91532e-06	0.00260304
WBTC/DAI	50000	100000	Weibull	6210.87	1.09954e-07	0.000694919
WBTC/DAI	50000	100000	Gamma	6213.31	1.43639e-07	0.000755873
WBTC/DAI	50000	100000	LogNormal	6348.47	2.0174e-07	0.00108028
WBTC/DAI	50000	100000	HalfCauchy	6250.82	7.93179e-08	0.000710398

Figure X. Table of errors, pool WBTC/DAI, reserve ranges: [10 000, 50 000] and [50 000, 100 000], metrics: AIC, SSE, MAE

Weibull distribution shows the best performance according to AIC for both reserves ranges, and outperforms the other distributions according to MAE metric in the second reserve range. Gamma distribution has a better performance according to SSE and MAE metric in the first reserve range.

Considering all analyzed reserve ranges across the examined pools, the final table table of scores has been computed for each distribution. The score represents the number of cases the distribution outperformed the other ones according to the given metric.

distribution	AIC_score	MAE_score	SSE_score
Weibull	341	242	248
Gamma	205	188	176
LogNormal	71	86	94
HalfCauchy	18	119	117

Figure X. Final scores of each considered distribution, by metrics: AIC, SSE, MAE

Weibull distribution has the best fit in the majority of the cases, according to all examined metrics. The second best distribution is Gamma. Lognormal outperforms HalfCauchy based on AIC core, but shows a poorer score based on MAE and SSE.

Visual Methods

The examined metrics represent an effective way for model selection and filtering out bad-fit distributions, but they don't provide any additional information about where and how much the fitted distributions deviate from the real data. To address this issue, visual methods can be applied.

One of the ways to assess visually the quality of fit, is to overlay the distribution PDF on the histogram of the data.

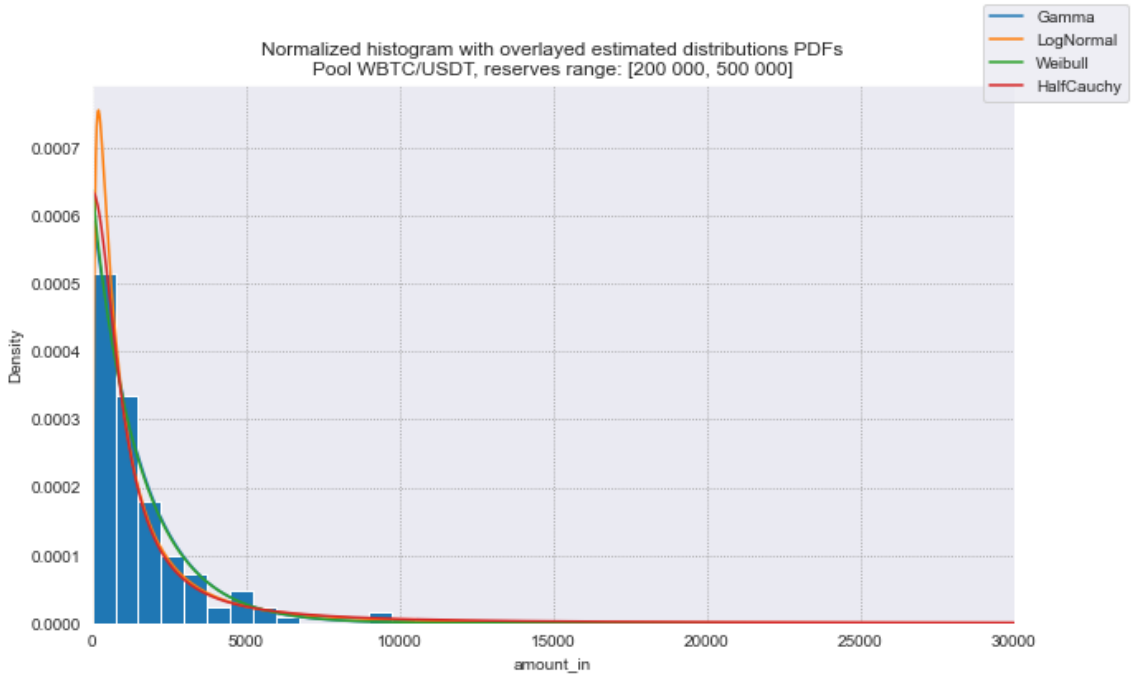


Figure X. Normalized histogram with overlaid estimated distributions PDFs, Pool WBTC/USDT, reserves range: [200 000, 500 000]

From the plot above, it seems that all of the selected distributions provide a really good approximation for the trade-size data, the Weibull distribution having a slightly better performance. However, there are several major downsides of the applied visual method for comparing similar distribution types. First of all, the histogram of the real data dependents too much on the number of bins. Particularly, if the number of bins would be increased, it would be visible that there is a decrease in the number of transactions having a very small amount, which is associated with high gas fees, that discourages users from performing very small trades. Now, these trades are being binned with the ones that are slightly greater and extremely frequent, and the mentioned aspect is being hidden. Also, it is not much clear what happens in the tail. As the

probability of high values is very small for all selected distributions, it's hard to identify the differences between them

A more effective way to determine visually whether the data follows a particular distribution is using Q-Q plots (quantile-quantile plots). To construct the graph, theoretical quantiles (on x axis) are plotted against sample quantiles (on y axis). If the data follows a straight line, the distribution is considered to fit the data well.

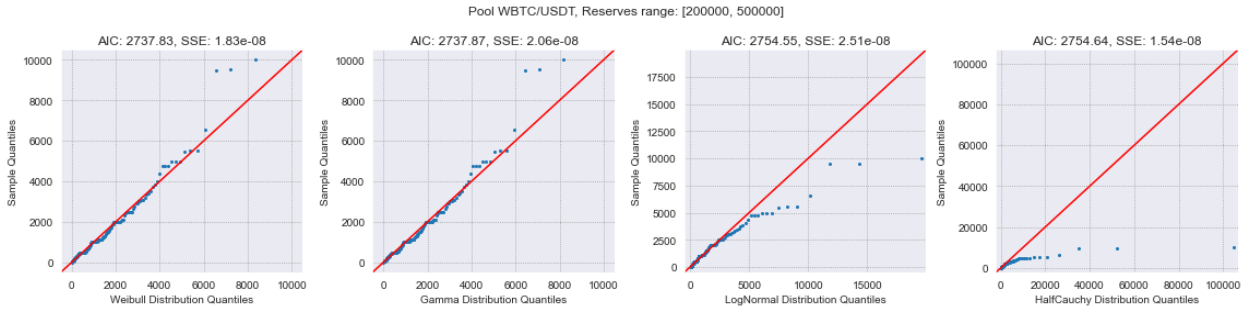


Figure X. QQ plots, stablecoin swap values, pool WBTC/USDT, reserve range [200 000, 500 000]

In the Q-Q plots above, the points represent how well each historical swap in value compares to the value that would be generated using the given distribution. In case the points lie above the straight line, it means that the values generated in the given range (OX axis) are too small compared to the historical data (OY axis). Contrary, if the points lie below the line, it means that the values are just too large. Slight deviations are acceptable, but in case they are too big and frequent, it signals that the given distribution describes the data poorly.

It can be seen that both Weibull and Gamma distributions provide a really good fit to the data. For the LogNormal distribution, starting from a given value, all of the generated points are much bigger compared to the historical value (notice the maximal sample value, which represents the historical data, is 10 000, while the theoretical generated maximal value is about 20 000). The HalfCauchy distribution , having a very fat tail, has the worst fit.

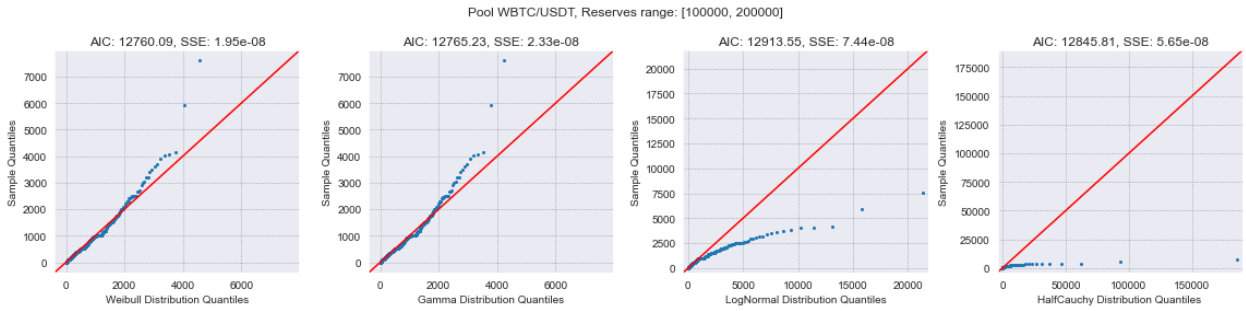


Figure X. QQ plots, stablecoin swap values, pool WBTC/USDT, reserve range [100 000, 200 000]

As Weibull distribution showed the best performance according to all of the considered metrics, and provides a good visual fit in the majority of the cases, it was decided to proceed further with Weibull distribution for trade-size distribution parameter estimation and generalization.

Weibull Distribution

The Weibull distribution is a continuous probability distribution, used extensively in a lot of distinct fields, due to its flexibility to model different shapes. The 2-parameter Weibull distribution is described by the shape and scale parameters. By increasing the scale parameter, the distribution is being stretched to the right. The shape parameter, unsurprisingly, determines the shape of the distribution. A smaller shape indicates a larger amount of extreme values, and increasing the shape parameter leads to a shift of the distribution mode to the right, and a consequent decrease of the tail thickness.

Previously, the fit of the distribution was assessed visually using QQ plots. One of the main downsides of applying QQ plots in order to assess the quality of fit for a heavy-tailed distribution is that the higher values (which represent only a small proportion from data), take up the majority of the space from the graph, the main concentration of points being squeezed in the bottom-left corner. Weibull probability plots, which are constructed on the log-scaled x axis, and y axis scaled according to a special formula, come to address this issue.

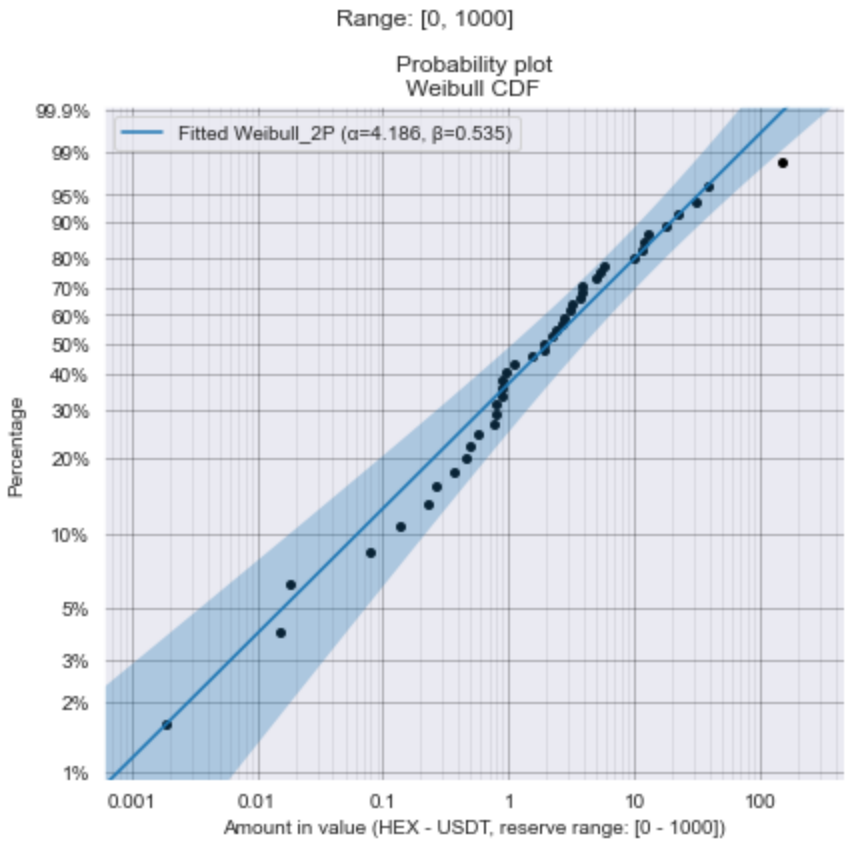


Figure X. Weibull Probability Plot. Stablecoin swap values, pool HEX/USDT, reserves range: [0, 1000]

Eliminating of bad-fit pools

Previously, it was established that the Weibull distribution models the best the trade-size in most of the analyzed pools. However, before proceeding to generalize the parameters, it's important to filter out the cases with a bad-fit, so that they wouldn't screw up the real picture. Considering that on the Weibull Probability Plot, ideally, the points should lie on a straight line, one of the ways to measure the quality of the fit is to compute the **correlation coefficient**. A value close to 1 suggests that the data follows the specified distribution. For the final estimations, the cases with a correlation coefficient below **0.95** have been filtered out.

Estimated parameters

In order to visualize the estimated parameters and understand how they vary as the liquidity changes, it was decided to construct a curve for each pool, X axis indicating the upper

limit of the reserve range used for parameter estimation and Y axis the value of the estimated parameter.

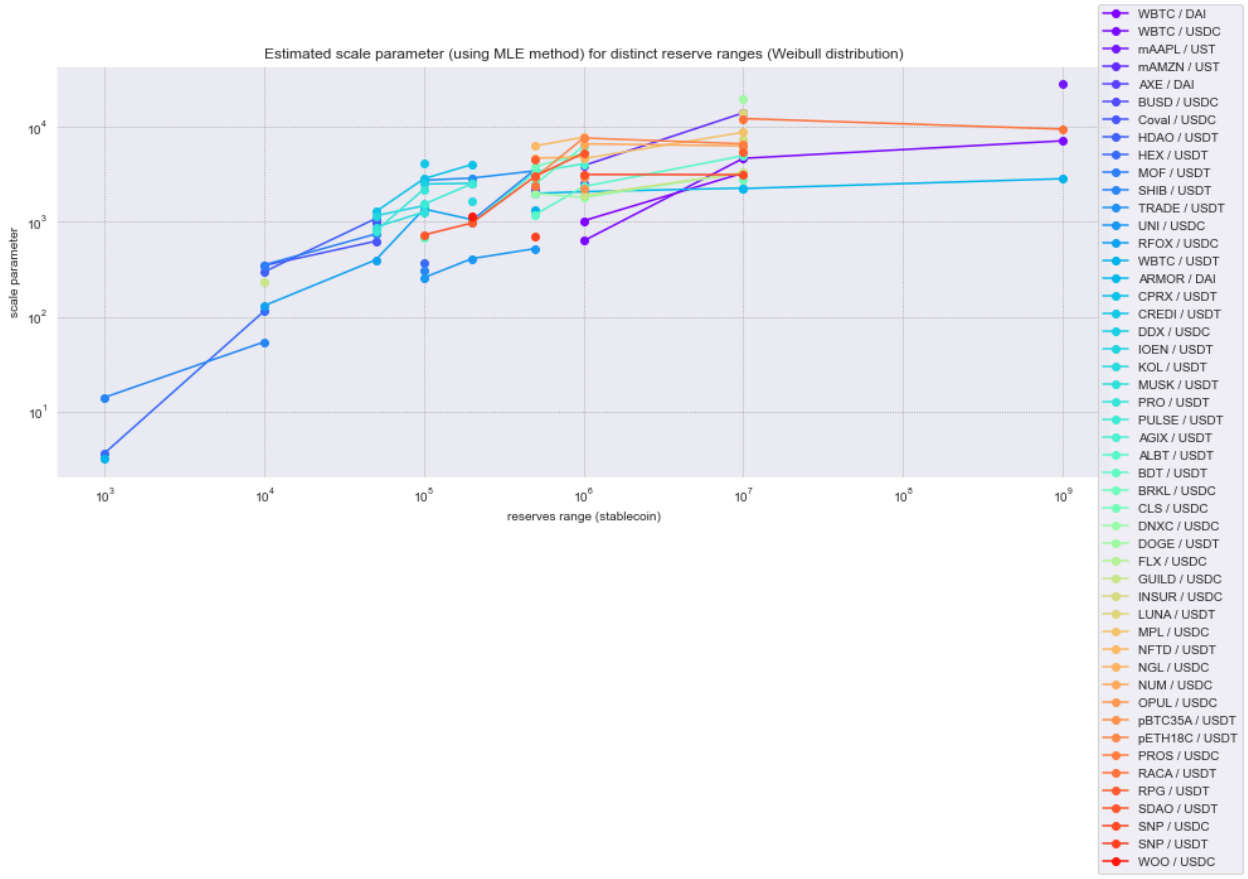


Figure X. Estimated *scale* parameters (using MLE method) for distinct reserve ranges (Weibull distribution). X axis represents the reserve range upper bound.

A common trend can be observed. As the range of the reserves increases, the estimated scale parameter also becomes bigger, indicating that for larger pool reserves, the average value of swaps rises.

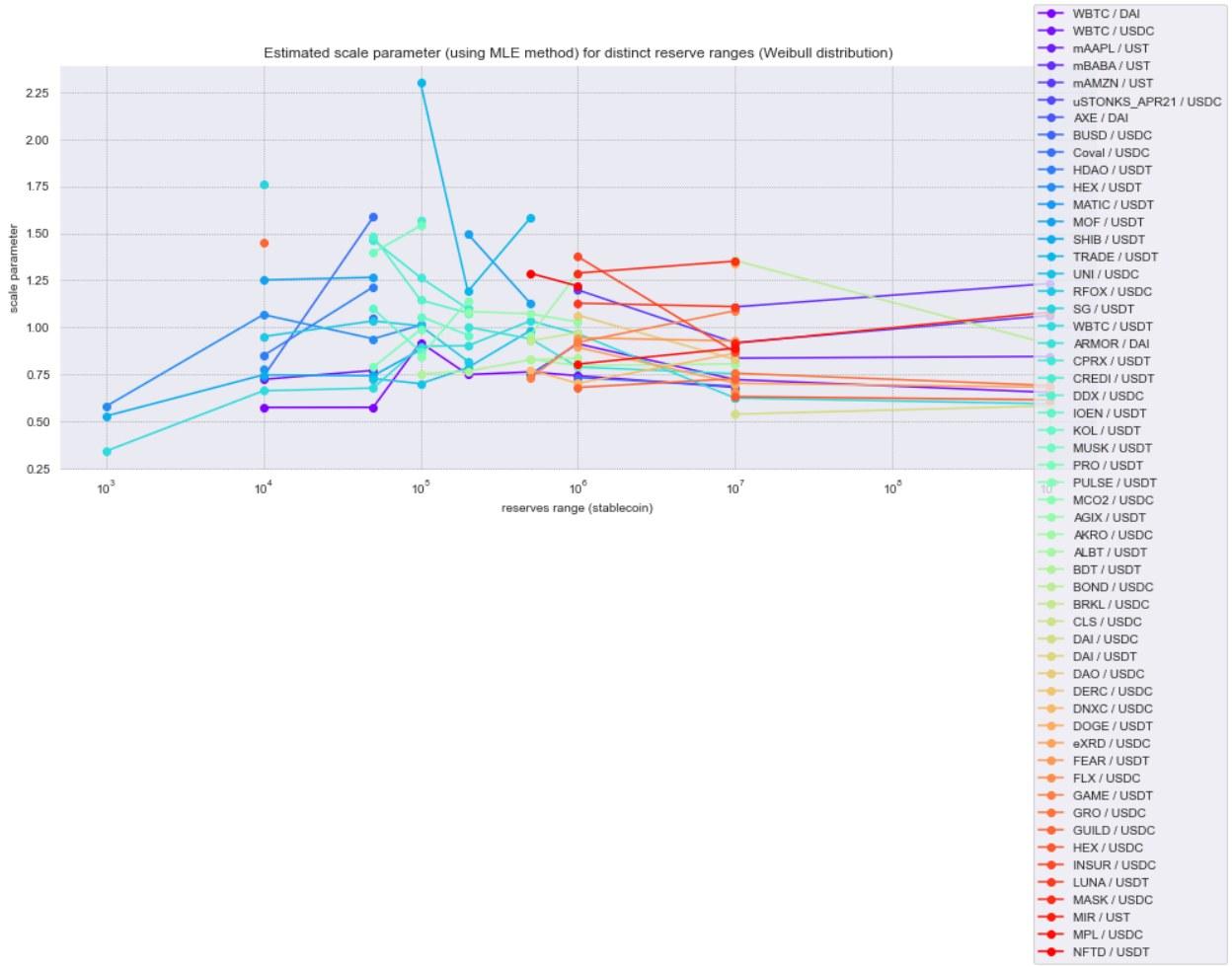


Figure X. Estimated *shape* parameters (using MLE method) for distinct reserve ranges (Weibull distribution). X axis represents the reserve range upper bound.

The shape parameter doesn't follow a monotonic pattern, but from the existing data it can be observed that it seems to increase toward the middle range of the reserves, followed by consequent smaller decrease till a certain point.

Below, are shown the curves computed by taking the arithmetic mean of the parameters for each range, across all of the analyzed pools.

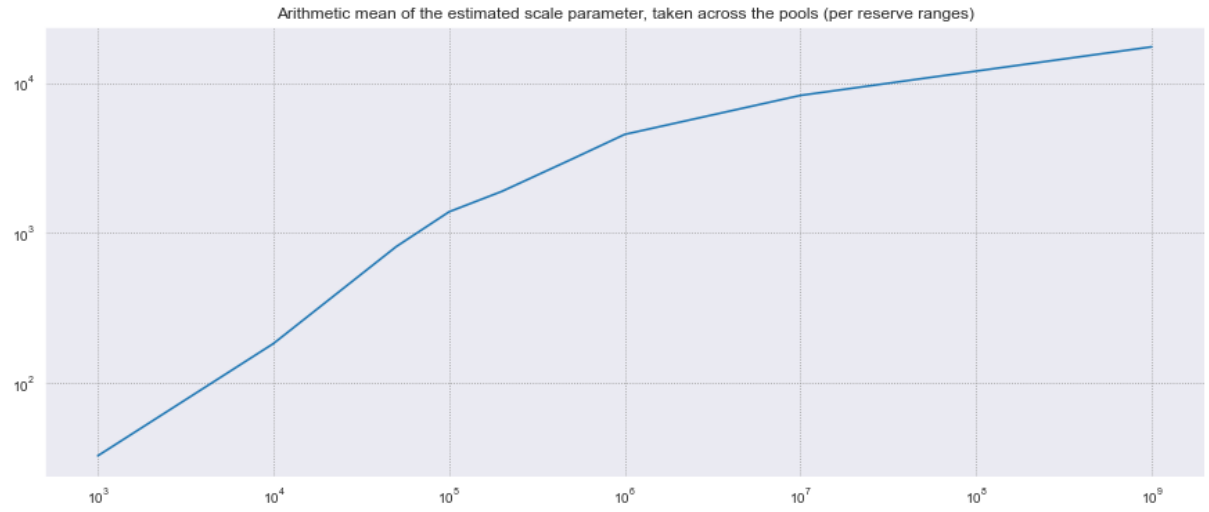


Figure X. Arithmetic mean of the estimated scale parameter, taken across the pool (per reserve ranges)

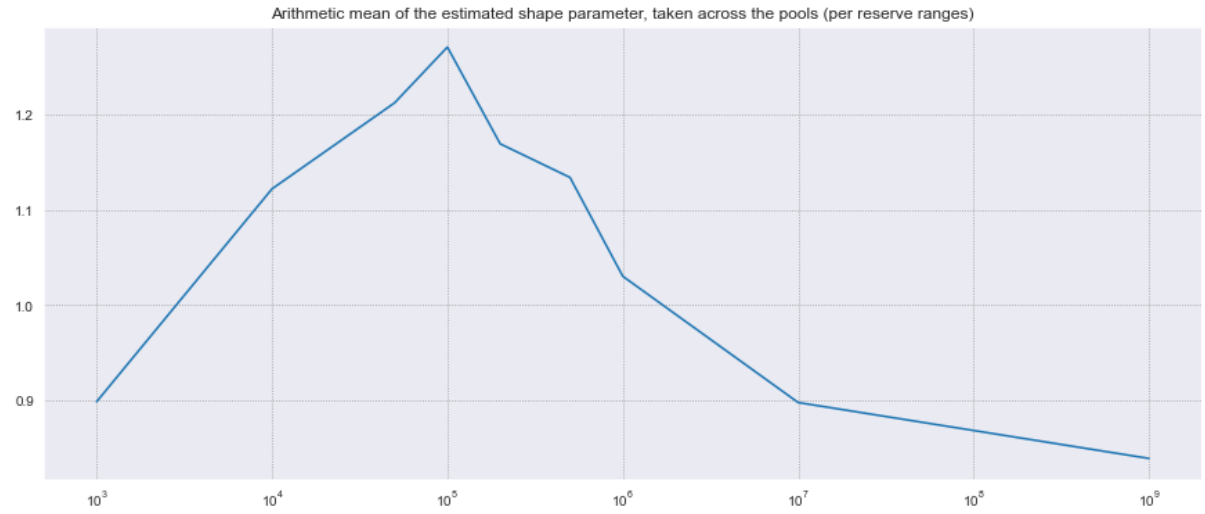


Figure X. Arithmetic mean of the estimated shape parameter, taken across the pool (per reserve ranges)

Generalizing trade-size distribution parameters

A naive way to generalize the estimated parameters, in order to select the ones for conducting the simulations, would be to consider the arithmetic mean of *scale* and *shape* across distinct pools at each distinct reserve range. However, this approach doesn't take into consideration the relationship between the params, and will certainly not be able to reflect different trading behavior patterns in pools falling inside the same reserve range.

To better understand the point, it's enough to analyze the relationship between the parameters by constructing a scatterplot of scale/shape values estimated for each pool.

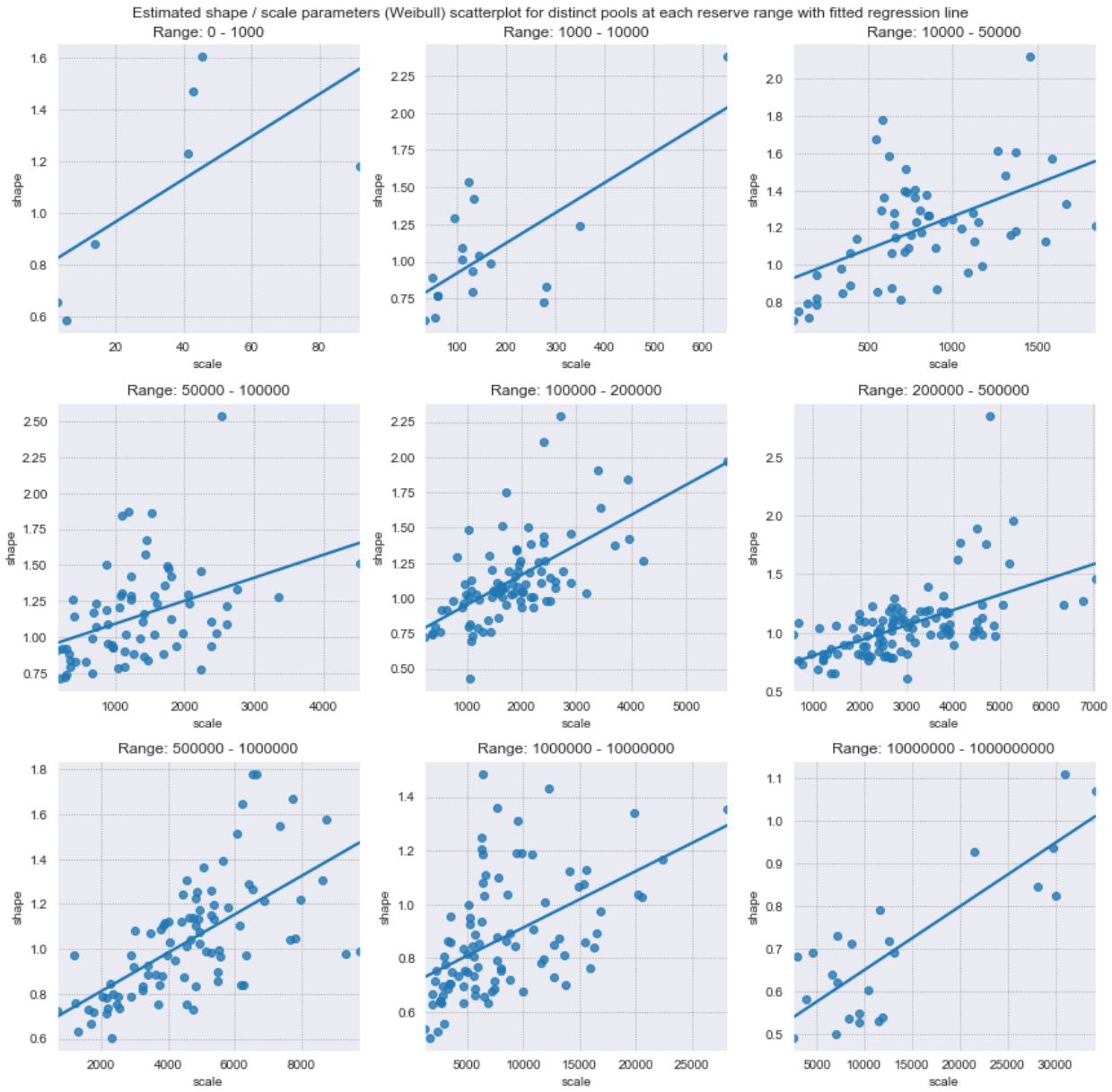


Figure X. Estimated scale/shape parameters (Weibull distribution) scatterplot for distinct pools, at each reserve range, with fitted regression line

There is a **positive correlation** between the shape and scale parameters. It can be explained taking into consideration the effects of the parameters on the distribution. The scale parameter stretches the distribution to the right, increasing the probability of higher values. Increasing the shape parameter not only leads to a shift of the distribution mode to the right, but also results in a thinner tail, decreasing the probability of extremely high values. By increasing the shape and scale parameters proportionally, the maximal generated values almost don't vary.

Having a high scale value with a low shape, contrary, results in unrealistically large generated values.

For selecting the final trade-size distribution parameters that would reflect distinct trading behaviors, 2 methods have been chosen.

The **first method** consists of computing the 4 equally spaced points both for the shape and scale parameters, between their minimum and maximum values across pools, and considering all possible pairs. This results in a grid of 4x4 possible combinations. However, this results in a lot of unrealistic scenarios (points in the upper left and lower right corners).

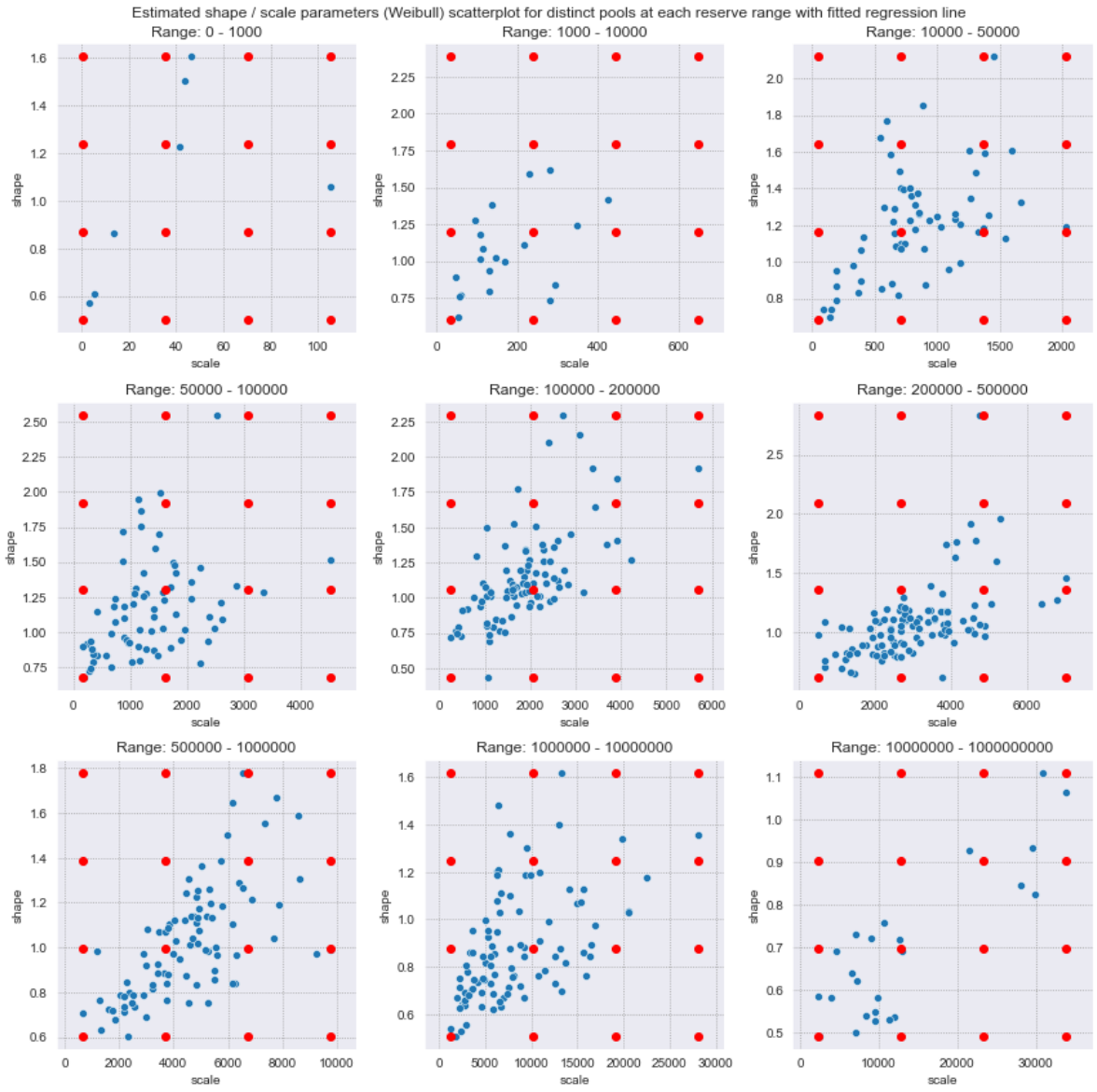


Figure X. Estimated scale/shape parameters (Weibull distribution) scatterplot for distinct pools, at each reserve range, with **generalized parameters (method I) highlighted in red**.

Below are presented the histograms of values sampled from the Weibull distribution, with the parameters corresponding to the highlighted points for the reserve range [50 000, 100 000].

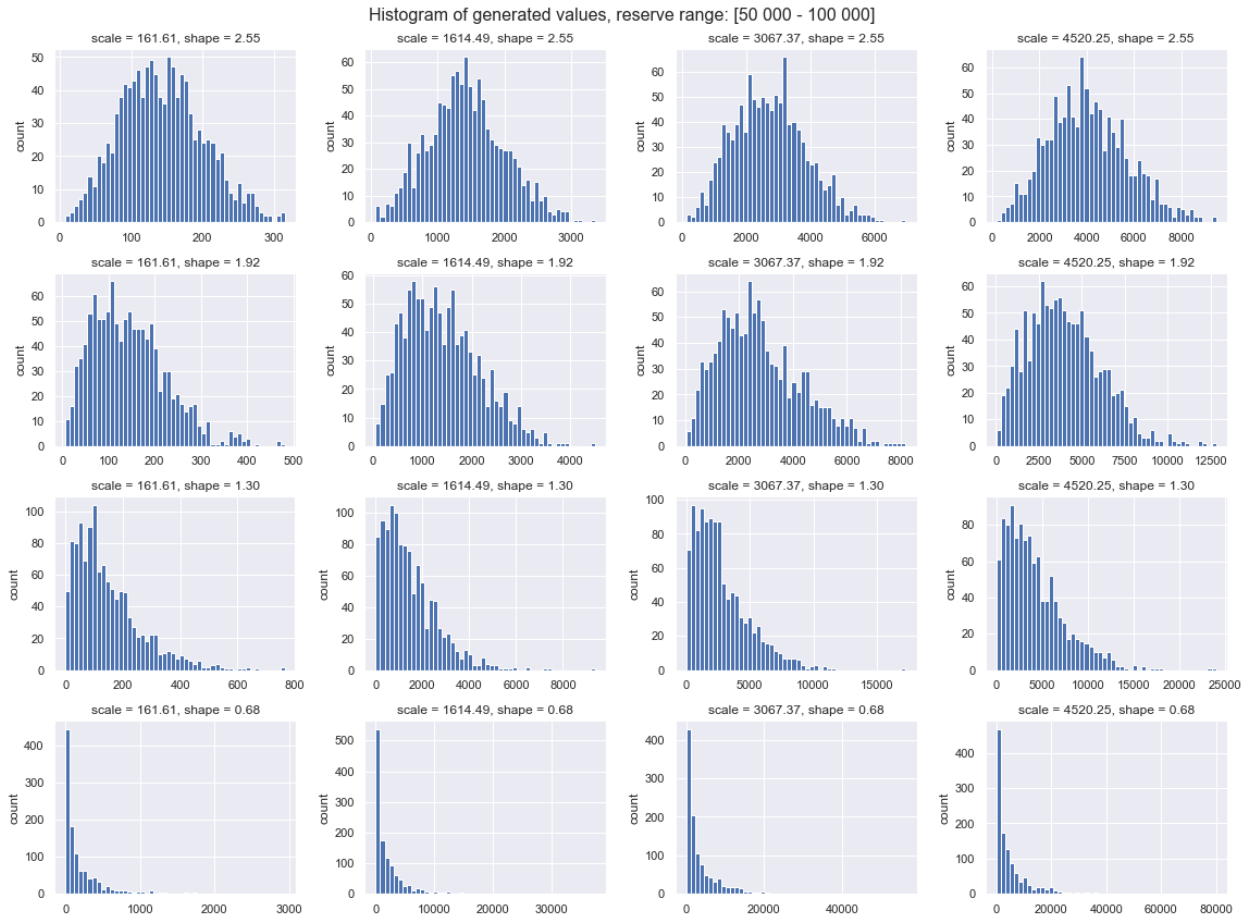


Figure X. Histograms of generated values. Weibull distribution.

By varying the shape and scale parameters, the overall shape of the generated values changes significantly. Each such combination describes different patterns in trading behavior. Notice that a smaller shape value, not only leads to the shift of the mode to the left, but also to a bigger amount of extreme (very large) generated values.

The **second method** consists of choosing generalized distribution parameters, only by considering realistic cases. The same procedure has been applied for each reserved range. Below are shown parameters which have been selected for each range.

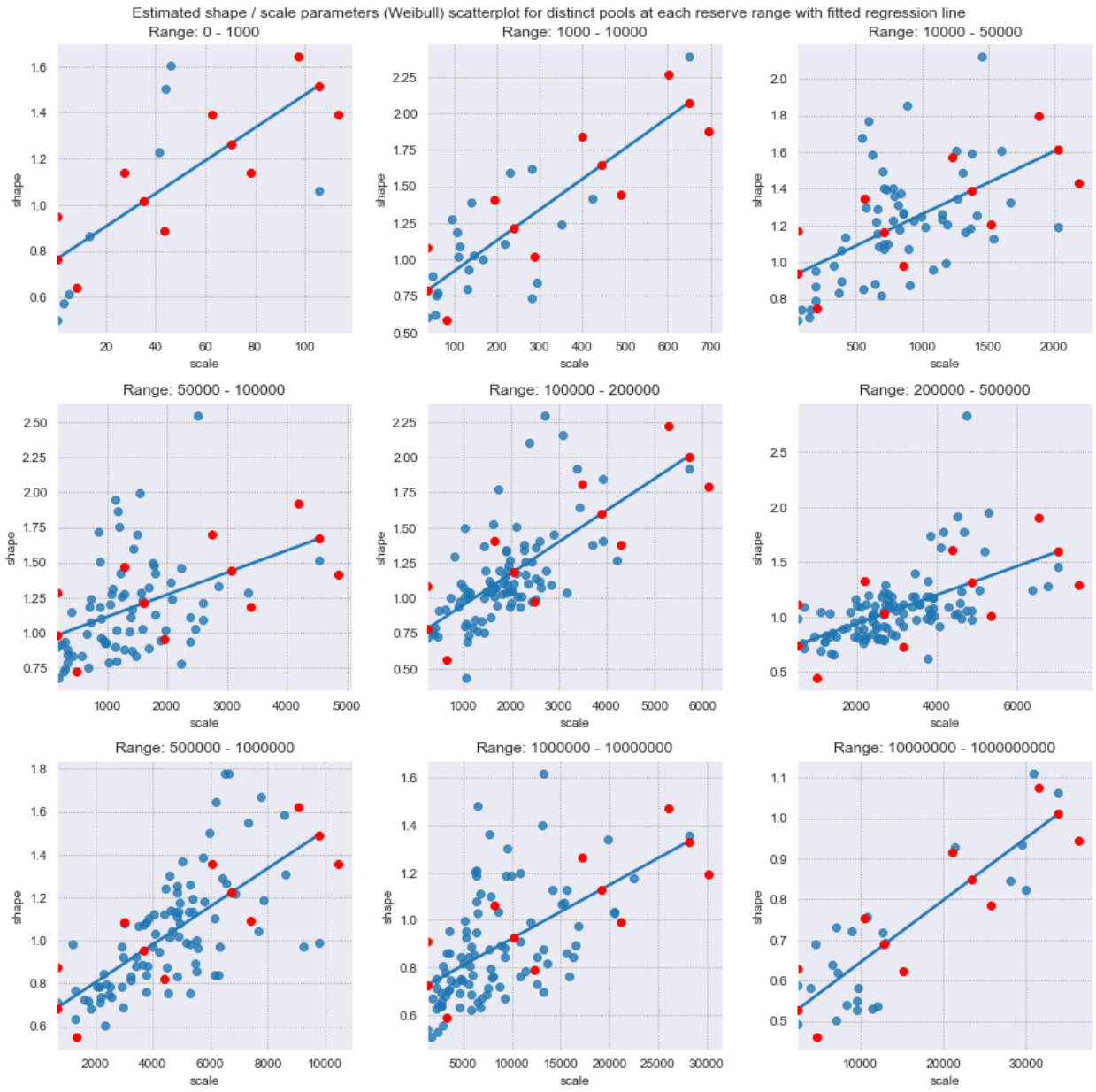


Figure X. Estimated scale/shape parameters (Weibull distribution) scatterplot for distinct pools, at each reserve range, with fitted regression line and **generalized parameters (method II) highlighted in red**

To select the generalized parameters, the same procedure has been applied for each reserve range. After fitting a regression line, the 4 equally spaced points (between the minimum and maximum scale value) had been computed. These points lie on the regression line and represent the distributions corresponding to the most common trading behaviors inside the pools. To cover the entire range of possibilities that may lead to different simulation results and reveal

additional insights, 4 points above and below the regression line have been computed according to the following principle: apply OX axis shift equal to ±0.15 * (x_max - x_min), compute the y value on the regression line, add apply an OY axis shift equal to ∓0.075 * (y_max - y_min).

Frequency of swaps per reserve ranges

It was decided to compute the median number of swaps based on daily reserve ranges at the moment of the swap. (For the following histograms, 2 additional constraints have been set: a pool is considered only if the number of days in the reserve range is not less than 10 and the total number of swaps inside the given pool/range is at least 250)

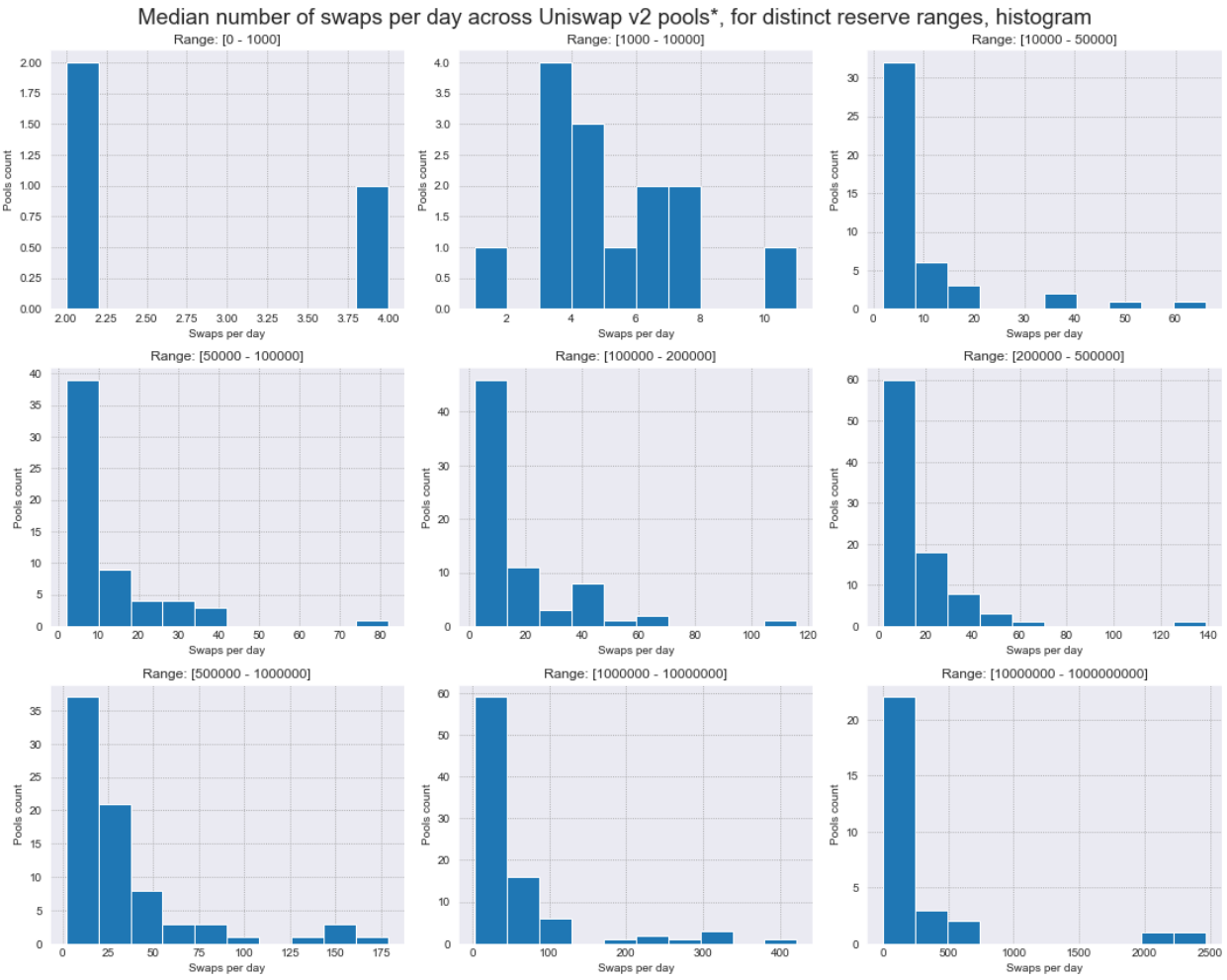


Figure X. Median number of swaps per day across Uniswap v2 pools*, for distinct reserve ranges, histogram

A clear pattern can be observed, the greater the reserve range, the higher the median daily frequency tends to be for the majority of the pools. The highest median swap frequency is registered for pools WETH/USDC and WETH/USDT at the highest reserve range, and is greater than 2000 swaps per day. Below, is presented the same histogram capped at 250.

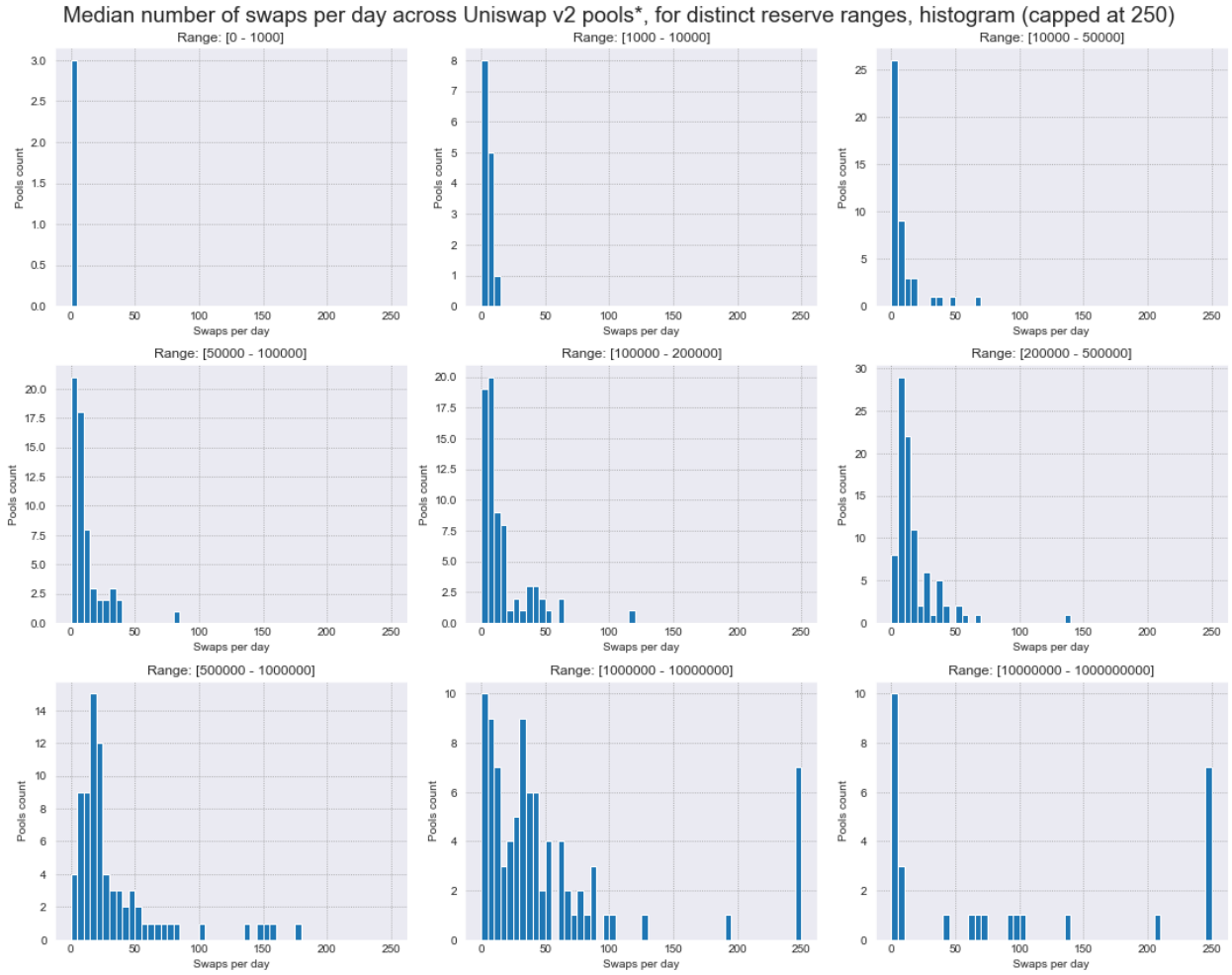


Figure X. Median number of swaps per day across Uniswap v2 pools*, for distinct reserve ranges, histogram (capped at 250)

Token in frequency ratio

During the initial analysis, it was established that the trading behavior across pools can differ significantly. In some particular markets, traders tend to perform many small-sized swaps in one direction, and fewer bigger swaps (in USD equivalent) in another direction. Below is presented the histogram of the token_in frequency ratio, constructed based on the extracted data.

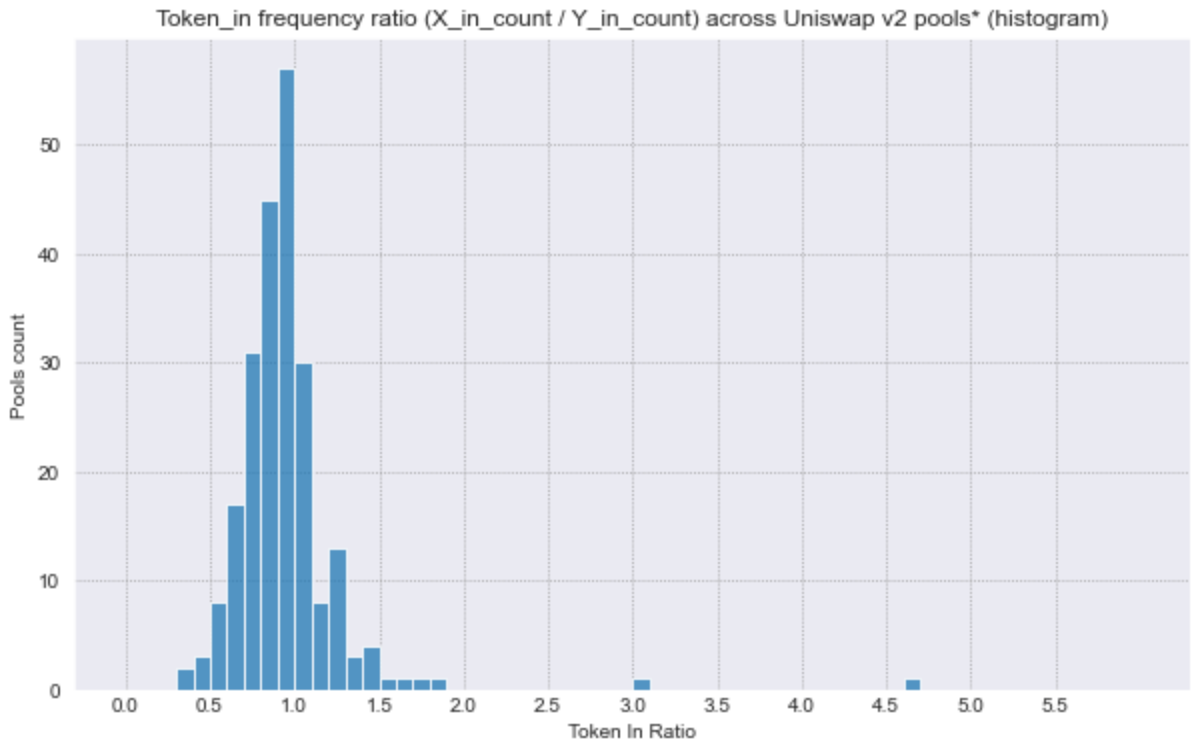


Figure X. Token_in frequency ratio (X_in_count / Y_in_count) across Uniswap v2 pools*, where Y - stablecoin, X - the remaining token in the pair

It can be seen that in the vast majority of the cases the ratio is 1, meaning that the number of swaps in each direction is the same.

Several extremes can be observed, particularly the ratio ~ 4.6, which corresponds to the pool FNK/USDT. FNK (Finiko) happens to be a financial pyramid scheme, whose price dropped by more than 100 times in a matter of several weeks, after a sudden price surge. Despite the price drop, there remains a pretty high liquidity of this token inside the Uniswap v2 pool, and people are still performing mainly swaps in order to exchange the token on the stablecoin, causing such a high token_in ratio.

On the other hand, the pool with token in ratio of about 3 corresponds to a healthy pool - DAI-UBI, where the difference in swap frequency for each side is natural and doesn't cause significant price variation in the long run, because of the differences in swap sizes (in USD equivalent) for each direction.

The token_in frequency ratio for the majority of the pools falls in the range 0.5 - 2.