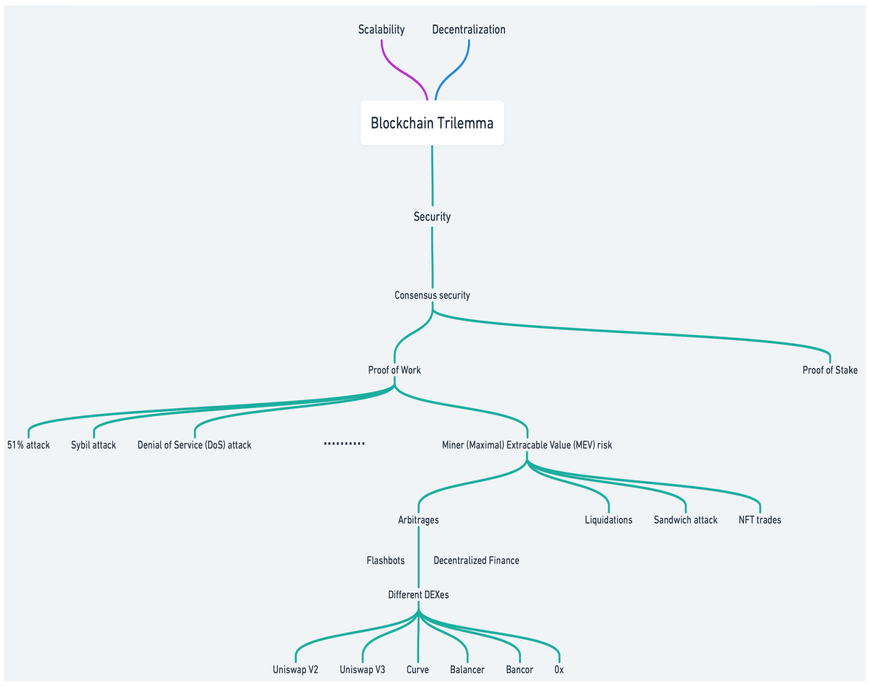
BLOCKCHAIN SECURITY: CATEGORIZATION AND QUANTIFICATION OF MINER EXTRACTABLE VALUE

Haoxin Yu

Data Science| Signature Work Class of 2022

Introduction



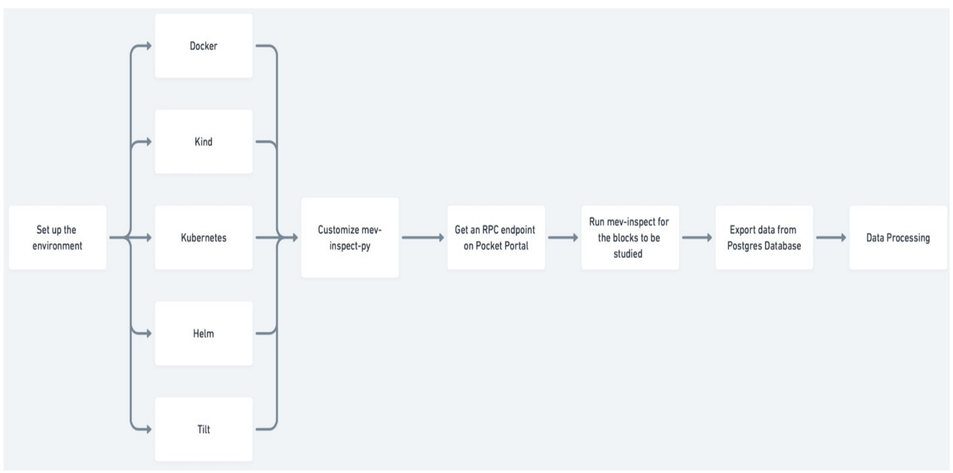
My general research question is that how we can measure blockchain security. Based on the background of blockchain trilemma, termed by Vitalik Buterin, it addresses the challenges that developers face in creating a blockchain that is scalable, decentralized, and secure, without compromising on any facet.

MEV was originally defined as the value that may be extracted directly from smart contracts as bitcoin profits by miners. Afterwards, a research and development organization Flashbots renamed MEV as *maximal* extractable value, broadening the scope to cover other blockchain architectures.

In the proposed research, we will explore how the arbitrage trading category was manifested in practical applications. The arbitrage revenue strategy was the most commonly seen strategy of MEV extraction, and there were almost no research works on arbitrage in the Decentralized Exchanges. Thus, we aim to quantify the MEV that happened through arbitrage trading, from both the searcher view and the miner view. Compared to the previous study, we extended our application scenario to a larger number of decentralized exchanges, including Uniswap v2, Uniswap v3, Curve, Balancer, Bancor, 0x.

Materials and Methods

Data Querying and Processing:



Arbitrage Inspection:

Conditions:

(1) Within an arbitrage, all tokens swap actions should take place in one single transaction, indirectly assuming that the arbitrageur uses atomic arbitrage to minimize his or her risk.

(2) Within one arbitrage trading, there must be more than one token swap action.

(3) An arbitrage's n swap activities s_1,..., s_n must generate a loop. Any swap action's input asset must be the same as the prior action's output asset, $in(s_i) = out(s_{i-1})$. The input asset for the first swap must be the same as the output asset for the last swap activity, $in(s_0) = out(s_n)$.

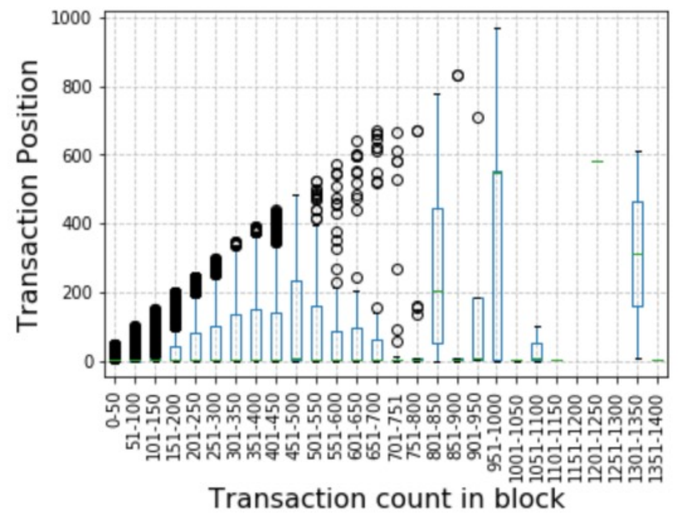
(4) The output amount of previous action must be larger than or equal to the input amount of corresponding swap action, $in(s_i) \leq out(s_{i-1})$.

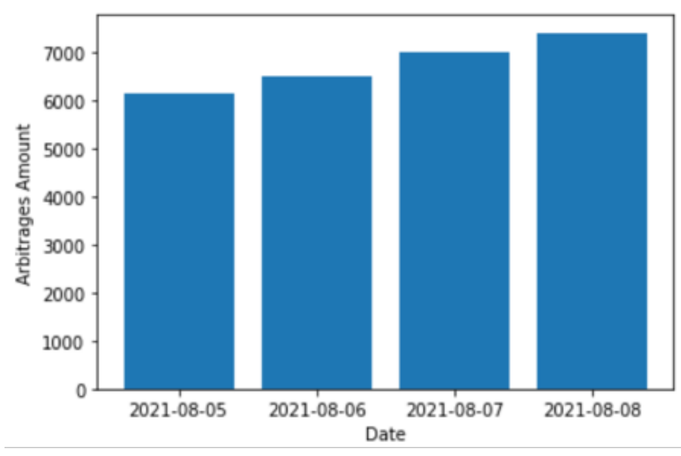
Gross profit, Miner payment, MEV:

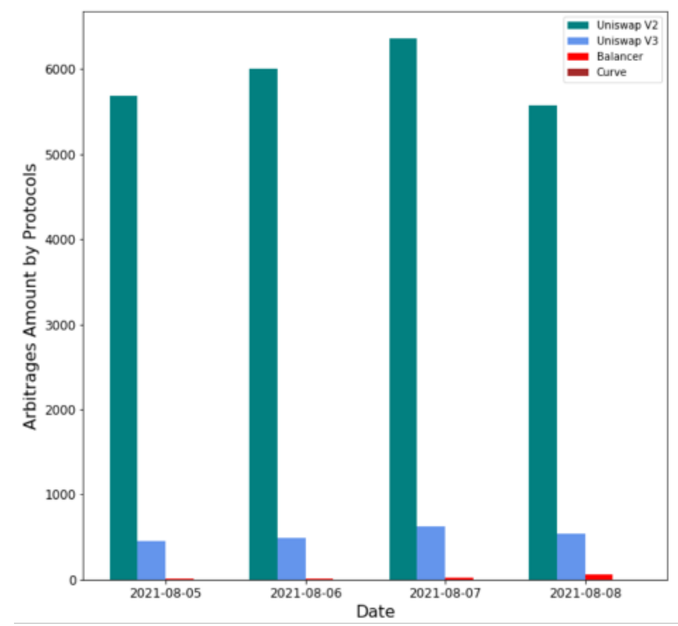
1. $Gross\_profit = (profit\_amount \cdot usd\_price) / 10^{18}$
2. $Miner\_payment = [(gas\_used \cdot gas\_price) + coinbase\_transfer] \cdot usd\_price / 10^{18}$
3. $MEV = gross\_profit - miner\_payment$

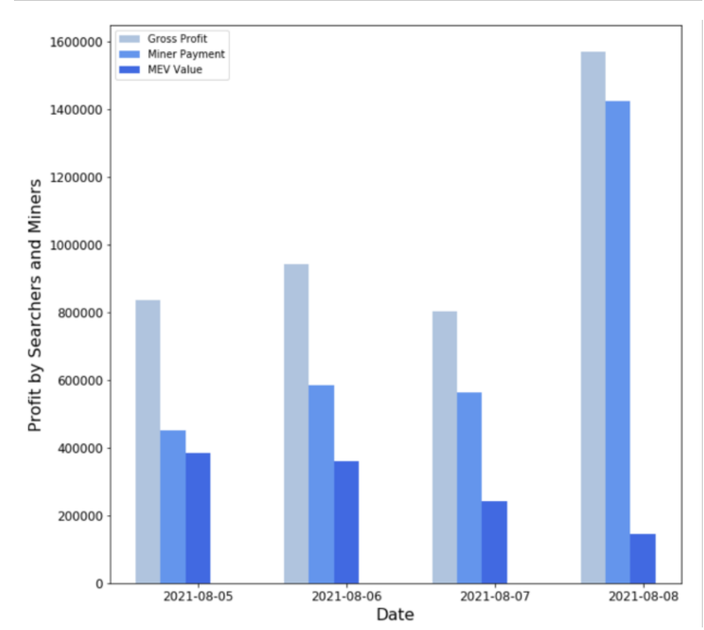
Results

/ Platforms / Markets	1	2	>= 3	Total
2	207 (0.8%)	10591 (41%)	None	10799 (41.8%)
3	6975 (27%)	5683 (22%)	413 (1.6%)	13072 (50.6%)
>= 4	1033 (4%)	775 (3%)	155 (0.6%)	1963 (7.6%)
Total	8215 (31.8%)	17049 (66%)	568 (2.2%)	25834 (100%)









Discussion

1. User Addresses, Smart Contracts
We find 125 distinct user (account) addresses and 1969 smart contracts executing 25834 arbitrages trades on Uniswap V2, Uniswap V3, Balancer, Curve, resulting in a profit of 1.132M USD. Based on our findings, there were 7612 arbitrage transactions (29.5%) that were communicated to miners on a private basis.

2. Markets and Platforms
The majority of traders or searchers choose to execute arbitrage trading involving two or three marketplaces. Only about 5% of traders used equal to or more than four markets to conduct their arbitrage. We also discovered that certain transactions combine two arbitrage opportunities into one. These behaviors may provide a bigger return because the gas price is lower.

3. Arbitrage Transaction Position
A high percentage of profitable arbitrage transactions are surprisingly located at the end of the blocks when displaying the arbitrage transaction positions in blocks. For example, out of 851 transactions in this block, one of the most profitable arbitrage deals we observed was at index 832.

4. Arbitrages Trading Amount
There is an increasing trend on total arbitrage amounts along the time series, which is consistent with previous research. Additionally, we found that the arbitrages that relevant to Uniswap V2 took the largest proportion of all arbitrage transactions, and the amount is much higher than that related to other DEXes.

5. Gross Profits and MEV value
We calculated the gross profits, which represent the revenue that traders expected to generate of synchronizing the prices of assets on several different markets, and the miner payment that miners received through paid gas and direct coinbase transfer from the traders. We can see a descending trend on the MEV profit along the time series.

Conclusion

Although blockchain has brought users benefits such as data transparency and decentralized trading platforms, many people still do not adopt it due to unexpected risks, which implies the significance of the lucid and quantified assessment of those risks. The proposed research could help illustrate the novel term MEV with real-world examples and application scenarios. Furthermore, it can support stakeholders, investors to choose low-risk products and assist developers manage the risks of their products. In addition, such findings could help assess the risks under different regulations from various regions, to determine the enforceability of the transactions.

The approach in the proposed research has an extension compared to the previous research. Based on the previous studies, we further investigate the actual application scenarios of defined categories of MEV. Additionally, we adopt a similar method of quantifying MEV on DeFi applications that are different from the examined Decentralized Exchanges (DEXes) previously.

In our research, we mainly examine the transactions running on the Ethereum blockchain, utilizing the proposed methods to identify the arbitrage transactions that fit for our purpose, and crawled the data correspondingly.

In future research, the researchers can further investigate the transactions based on other blockchains, or explore how miners and traders extract value from the DeFi applications other than the ones we have studied. In addition, they could further examine the MEV extraction that happened with other types of trading strategies, such as sandwich attacks, liquidations, and NFT trades.

昆山杜克大学
DUKE KUNSHAN UNIVERSITY