ISSN 2707-1898 (print)
Український журнал інформаційних технологій
Ukrainian Journal of Information Technology
http://science.lpnu.ua/uk/ujit
https://doi.org/10.23939/ujit2025.01.108
Article received 28.03.2025 p.
Article accepted 01.05.2025 p.
UDC 004.75/.62

Correspondence author
N.S. Cherkas
nazarii.s.cherkas@lpnu.ua

N. S. Cherkas, A. Y. Batiuk
Lviv Polytechnic National University, Lviv, Ukraine

METHODOLOGY FOR COMPARATIVE ANALYSIS OF MAXIMAL EXTRACTABLE VALUE (MEV) IN DECENTRALIZED EXCHANGE PROTOCOLS

The development of smart contracts in blockchain networks has enabled the creation of sophisticated decentralized finance (DeFi) protocols, encompassing decentralized exchanges, lending platforms, and algorithmic crypto-assets. Despite decentralization and transparency, blockchain networks do not guarantee a predictable transaction execution order, leading to the emergence of the phenomenon known as Maximal Extractable Value (MEV) – an additional profit extracted by certain network participants who influence transaction ordering.

This study focuses on the empirical analysis of MEV extraction across various DeFi protocols to identify critical factors influencing the frequency and extent of MEV attacks. The research introduces a comparative methodology for evaluating MEV extraction based on a modified version of the MEV Inspect Py software suite, enhanced by newly developed components: a Price Resolver for collecting and correcting cryptocurrency price data, and a Jupyter Notebook module for detailed data analysis, comparison and visualization. An evaluation of the total volume of sandwich and arbitrage-type MEV attacks was also developed, and a method for correcting cryptocurrency price data was implemented, which improved the quality of the obtained results.

The obtained results demonstrate that Uniswap V2 and Uniswap V3 are the primary targets for MEV extraction; however, their operational mechanisms create distinct conditions for attacks. A clear correlation was identified between concentrated liquidity, pricing algorithms, and the scale of MEV exploitation. Furthermore, the findings confirm that the architectural features of DeFi protocols significantly affect their vulnerability to MEV.

These results can be employed to enhance the resilience of decentralized exchange algorithms against MEV extraction and to develop mechanisms that minimize its negative impacts on both protocol efficiency and user fairness. Moreover, the insights from this research provide valuable guidance to DeFi protocol users seeking to reduce their exposure to MEV-related risks and make more informed decisions. Future research directions include extending the analysis to MEV exploitation in blockchain networks other than Ethereum and evaluating the effectiveness of existing and emerging protective strategies.

Keywords: blockchain, smart contracts, distributed systems, peer-to-peer networks, cryptography.

Introduction

Over time, blockchain networks have evolved to support programmable logic through smart contracts, which laid the foundation for the emergence of decentralized finance (DeFi) protocols – decentralized cryptocurrency exchanges, lending platforms, automated portfolio management systems, and algorithmic crypto-assets such as stablecoins and derivatives [1]. These protocols serve as decentralized analogues to traditional centralized financial services, which has rendered them susceptible to transaction ordering manipulation, similar to those observed in traditional finance, particularly in high-frequency trading (HFT) environments [2].

Such manipulations, or in fact attacks, have gained significant traction and were first formalized in [3] under the term Maximal Extractable Value (MEV) – the maximum value that network participants can extract by gaining preferential access to transaction ordering.

Researchers typically distinguish four primary categories of MEV attacks in blockchain systems [4]:

- frontrunning;
- backrunning;
- sandwich attacks;
- liquidations in decentralized lending protocols.

The exploitation of MEV has reached significant scale, initially started through uncoordinated priority gas auctions (PGAs), which eventually threatened the stability of the Ethereum network by incentivizing miners to rewrite blockchain history for additional profit. Later, after many blockchain networks including Ethereum transitioned to Proof-of-Stake (PoS) consensus, the MEV phenomenon influenced the role separation between network participants into Searchers, Block Builders, and Validators, alongside the introduction of the Protocol Builder Separation (PBS) scheme [5].

Consequently, MEV extraction must be recognized as a substantial systemic risk impacting the efficiency, fairness, and security of blockchain networks. Investigating this issue is particularly relevant amid the rapid growth of DeFi protocols, which demonstrate varying degrees of suscepti

bility to MEV attacks. This necessitates the use of empirical research methods capable of identifying and comparing vulnerabilities across different architectural models. The goal of this study is to formalize a methodology for comparative analysis of MEV exploitation in DeFi protocols and to identify the key factors that influence their resilience to such attacks.

The relevance of the MEV problem is driven by the range of risks it introduces: user profit loss within DeFi operations, increased network load due to surplus transactions, exploitation of consensus vulnerabilities, heightened censorship of on-chain activity, and broader centralization trends within blockchain infrastructure.

Researching MEV is non-trivial task due to the decentralized and dynamic nature of blockchain systems, the pseudonymity of participants, and the overall fragmentation of on-chain data. One of the most promising directions of inquiry is the empirical analysis of public blockchain data to assess the nature and scale of such attacks. Prior studies have focused either on live block monitoring or retrospective analysis of specific block ranges using a variety of methods and tools, such as those presented in [6], [7] (graph-theoretical approaches), [8], [9], [10] and [11].

Nevertheless, a gap remains in assessing the relationship between the implementation details of DeFi protocols and the extent of MEV exploitation. Our study focuses on comparing MEV extraction across DEX protocols and identifying potential correlations between their architectural design and their resilience or susceptibility to such attacks.

The object of this study is the process of MEV extraction within DeFi protocols and the architectural details of those protocols, specifically within the Ethereum blockchain.

The subject of this study is the set of algorithms, analytical techniques, and tooling used to evaluate MEV extraction, as well as the operational mechanics underlying DeFi protocol implementations.

The purpose of the study is to formulate and implement a methodology for comparative analysis of MEV exploitation across decentralized exchange protocols, with the goal of identifying key factors that affect their susceptibility or resistance to such attacks.

In order to achieve this goal, the following *research objectives* were defined:

To review existing empirical studies on MEV and its impact on DeFi protocols;

To modify and extend the MEV Inspect Py software framework to adapt it for comparative analysis of MEV extraction;

To develop additional components of the methodology, including a Jupyter Notebook analytics module and a Price Resolver component for retrieving and correcting crypto asset pricing data;

To collect and process MEV extraction data using the extended toolkit;

To investigate differences in MEV activity across the most popular DeFi protocols within selected categories;

To identify correlations between MEV extraction and other protocol metrics such as total value locked (TVL), trading volume, and liquidity distribution;

To summarize the findings and outline directions for further research.

Materials and methods. To collect and identify instances of MEV exploitation, this study employed the open-source project MEV Inspect Py (MIP) [12]. MIP is an Extract-Transform-Load (ETL) software framework that, based on a defined configuration, collects data from the Ethereum blockchain, decodes smart contract calls to DeFi protocols within transactions, classifies those calls, and detects MEV attacks using built-in patterns.

The MIP framework consists of the following components: a launcher container, a worker container, a PostgreSQL database [13], and a Redis caching layer configured in a master-slave setup [14]. The system is deployed using container orchestration tools based on Kubernetes [15], in conjunction with a local development cluster powered by Minikube [16] (Fig. 1).

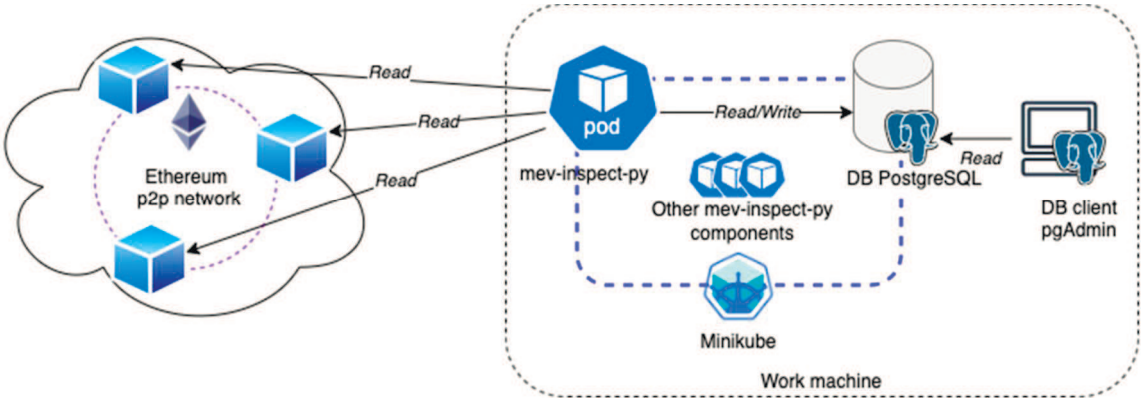

Fig. 1. Architecture of MEV Insepct Py

One of the main challenges in working with MIP is retrieving up-to-date prices for cryptocurrencies and tokens (hereafter referred to as crypto-assets). The built-in capabilities rely on paid external services such as Coingecko [17], which can be costly and may not always guarantee sufficient data accuracy. To address this issue, a set of custom Python scripts was implemented to fetch prices using the decentralized exchange API provided by Geckoterminal [18].

The analysis of differences in MEV extraction across various DeFi protocols and the generation of corresponding

analytical reports was carried out using the interactive Jupyter Notebook environment [19]. The analysis leveraged Python libraries including SQLAlchemy, Pandas, NumPy, and Matplotlib. Additionally, the Z-score method [20] was applied to detect anomalies in pricing data. This filtering allowed for the exclusion of distorted values caused by low liquidity in specific DEX pools, thus improving the quality and reliability of the resulting dataset.

Analysis of recent research and publications. The phenomenon of MEV in blockchain networks was first formalized in [3]. That study drew parallels between algorithmic high-frequency trading (HFT) in traditional stock markets and transaction ordering manipulation performed by automated bots and mining nodes within Ethereum blocks. It also investigated priority gas auctions (PGAs) using game theory [21] to model the behavior of participating bots, which allowed the authors to distinguish specific strategic patterns and analyze coordination mechanisms. Particular attention was given to systemic risks posed by MEV attacks conducted by miners. In such cases, miners, motivated by the potential for increased profits through transaction reordering, exploited vulnerabilities in the consensus algorithm to initiate blockchain reorganizations and capture portions of other users' profits. While this study made a significant contribution to the understanding of MEV, it focused primarily on spam-like PGA activity and did not explore the distribution of such attacks across different DeFi protocols.

The paper [10] presents an empirical analysis of transaction ordering manipulation in Ethereum and introduces a slightly different taxonomy of MEV attacks:

Displacement – when an attacker's transaction precedes the victim's transaction, altering its intended effect.

Insertion – a classic sandwich attack in which the attacker inserts transactions before and after the victim's to profit from price movements.

Suppression – when the attacker floods a block with high-fee transactions to exclude the victim's transaction from inclusion.

This study is notable for its depth in analyzing MEV execution and fits within earlier waves of MEV-related research.

The next study [6] offers a more in-depth examination of MEV exploitation across various types of DeFi protocols. The authors use a combination of heuristic algorithms and graph-based analysis to identify MEV attacks in large blockchain datasets. They trace transactions and apply clustering techniques to detect recurring behavioral patterns among MEV bots. Although the paper proposes improved techniques for MEV detection and examines their impact on the stability of DeFi protocols, it does not delve into differences between specific DEX implementations.

In [22], the authors examine the difficulty of MEV valuation and propose alternative methods for its estimation. They emphasize that due to the evolving nature of the market, changing trading mechanisms, and increasing reliance on private transaction channels, estimating the total value of MEV is extremely challenging. The study proposes a minimal-value estimation approach based on market analysis and observation of MEV actors' operational costs. While the methodological contribution is substantial, the work does not address differences in MEV exploitation across categories of DeFi protocols.

Another study [7] focuses on the role of Ethereum miners in block construction and transaction ordering for MEV extraction. It reveals that a significant portion of MEV activity occurs through private channels. Importantly, the paper highlights how miners maintain control over a large share of MEV profits. Although the study provides valuable insights into miner behavior and MEV dynamics, it does not investigate variation in MEV susceptibility across protocol categories – leaving room for further research into the relationship between protocol design and MEV extractability.

The study [23] presents a focused case study of MEV attacks on the Uniswap DEX, analyzing the USDC/WETH pool. The authors find that roughly 45% of daily trade volume in this pool involves MEV bots. The paper concentrates on arbitrage and sandwich attacks and demonstrates their impact on liquidity and price volatility. However, it limits its scope to a single DEX protocol and single exchange pool. Future research, therefore, could focus on cross-protocol comparison and evaluation of MEV resilience in a broader set of DeFi platforms.

In [24], the authors conduct a large-scale empirical analysis of sandwich and arbitrage MEV attacks on decentralized exchanges such as Sushiswap and Curve. Using a modified clustering algorithm and extensive transaction data, they show that liquidity structure and pricing mechanisms play a significant role in determining the frequency and profitability of MEV attacks. However, the study does not address systemic risks at the blockchain network level, nor does it perform a comparative analysis across a sufficiently broad set of DeFi protocols.

Finally, the study [25] explores MEV extraction within the Flashbots Bundle infrastructure. The authors introduce two novel analytical techniques – ActLifter and ActCluster, which enable the identification of MEV activities and the clustering of suspicious transactions to uncover the trading bot behavior patterns. This approach led to the discovery of previously undocumented rare MEV attack types. The authors also suggest several future research directions where these techniques may be applied.

In summary, MEV quantification has become a vibrant area of research in recent years, encompassing various aspects of its impact on blockchain ecosystems. A substantial portion of existing studies focus on profitability estimation, attack identification, and refinement of detection methods. However, despite this progress, a significant gap remains in understanding how MEV exploitation varies across categories of DeFi protocols and which protocols are most frequently targeted.

This direction of research is particularly relevant, as it may help identify the most vulnerable protocols and support the development of mitigation strategies. Moreover, such

comparative analysis can offer practical guidance for DeFi protocol developers seeking to minimize exposure to MEV threats in their systems.

Research results and their discussion

The results presented in this study are based on public data collected from the Ethereum blockchain between May 13 and May 19, 2024, using the modified version of the MEV Inspect Py (MIP) framework along with additional components developed as part of this work. The key quantitative characteristics of the resulting dataset are summarized in Table 1.

Table 1. Dataset from Ethereum network 13.05.2024 – 19.05.2024

Indicator	Value
Blocks	50 041
Swap method calls	1 707 482
Classified transaction traces	46 762 510
Sandwich attacks	66 125
Arbitrages	17 954
Liquidations	96
Unique decentralized exchanges involved	35

The data collection and processing workflow using the MIP framework includes the following stages:

1. Remote Procedure Calls (RPC) to a blockchain node to fetch blocks within the specified range. Retrieved data includes transactions, trace records, receipts, and other metadata.

2. Classification of transaction traces using the Application Binary Interface (ABI) of known decentralized exchanges (DEXs). This allows the identification of smart contract method calls relevant to MEV extraction.

3. Pattern matching among the classified method calls (e. g., swap) to detect known MEV attack types such as sandwich, arbitrage, or liquidation. For each identified MEV case, the system calculates the extracted profit, payments to miners or validators, and attaches relevant metadata.

The default version of the MIP framework contains several limitations that hinder more advanced analysis:

- lack of granular crypto-asset pricing data, which is essential for evaluating the volume and profitability of MEV extraction;
- absence of MEV volume metrics per attack type, which are important for estimating the scale of capital passing through MEV strategies;
- token balance mismatches between frontrun and backrun transactions in sandwich attacks which leaves some amount of profit unaccounted;
- no built-in functionality for comparing MEV metrics across different DEXs;
- lack of metadata on DEX protocols and the presence of certain processing bugs that distort the analysis results [12].

To address these limitations, this study introduces a comparative MEV analysis methodology designed to evaluate extraction patterns across different DeFi protocols using unified criteria. The methodology is implemented through the components described below.

Modified MEV Inspect Py (MIP) framework. The following extensions were introduced to enable richer quantitative analysis:

- expanded database schema to store token price data obtained from decentralized exchanges;
- implementation of rate limiting for external API calls;
- fixes for token balance mismatch in frontrun/backrun transactions in sandwich attacks;
- updated ABI configuration for the Uniswap protocol;
- bug fix for handling GBTC / WETH and other non-strict-check pools in Uniswap V3 [26], along with other minor fixes and improvements.

All modifications are publicly available in the GitHub repository [27].

Price resolver component for retrieving and correcting crypto-asset prices. This Python-based module supports granular historical price data collection using two sources – Coingecko [17] and Geckoterminal [18] APIs. While Coingecko provides aggregated price data for a limited number of tokens, Geckoterminal offers a broader dataset focused on DeFi protocols, particularly DEXs. If a token price is unavailable on Coingecko, the system searches for the token's pool on Geckoterminal and retrieves price data along with pool and token metadata.

Since Geckoterminal data may be distorted due to low liquidity in certain pools, the dataset may include anomalous price values. To filter out such anomalies, the *Z*-score method [20] is applied:

$$z = (x - \mu) / \sigma,$$

where z is the standardized score, x is the value being evaluated, μ is the sample mean and σ is the standard deviation.

This approach is applied to token price data obtained via Geckoterminal's API. Values with Z-scores above 3.0 are excluded, eliminating outliers and improving data quality. The component also retrieves additional pool metadata, including token decimals and relevant technical parameters.

Jupyter Notebook analytics module for comparing MEV extraction across protocols. This module serves as a post-processing layer for aggregating, comparing, and visualizing MEV extraction data across various DeFi protocols. When evaluating the impact of MEV on decentralized exchanges, it is important to assess not only the profitability of attacks but also the volume – the total adjusted amount of crypto-assets transferred through transactions involved in MEV attacks. The following formula is used to estimate MEV extraction volume:

$$V_{MEN} = \max(A_{out}, A_{in}) + R + F + L$$

where A_{in} – total assets spent by the attacker; A_{out} – total assets received by the attacker; R – residual unconverted assets; F – gas fees paid; L – losses due to failed transactions.

Comparative analysis of MEV extraction across different protocols also requires data aggregation by relevant dimensions such as attacker transaction pairs (frontrun-

backrun), block number, or date. In addition, the notebook module provides tools for statistical evaluation, filtering empty entries, and visualizing trends and relationships in the dataset. The baseline MIP implementation lacks these capabilities, so they were implemented as part of a Jupyter Notebook post-processing pipeline

Fig. 2 shows the architecture of the complete data collection and analysis system implementing the proposed methodology.

As illustrated in Fig. 2, the data collected by the MIP system is accessed via its built-in PostgreSQL database client. This architecture provides modularity and flexibility: pricing queries and analytics can be executed independently from MIP's core processing engine, and results generated in Jupyter Notebook can be exported in multiple formats, including CSV, PDF, and HTML.

Discussion of research results. The analytical module implemented using Jupyter Notebooks was applied to the dataset collected from the Ethereum blockchain between May 13 and May 19, 2024. Although a broad set of MEV-related metrics was calculated (extracted profit, validator payments, and others), this discussion focuses primarily on the number and volume of MEV extractions by type, as these metrics are the most indicative of the intensity and systemic footprint of MEV activity across protocols. The analysis is conducted across different decentralized exchanges, as these comparisons provide insights into the relative MEV activity and its impact on the examined protocols.

Fig. 3 presents the number of identified sandwich-type MEV attacks, grouped by the decentralized exchange on which they occurred.

As seen in the chart, the vast majority of sandwich attacks were executed on Uniswap V2, followed by a sharp drop in frequency across Uniswap V3 and other exchanges. A slightly different picture emerges in Fig. 4, which shows the volume of sandwich attacks over the same time period.

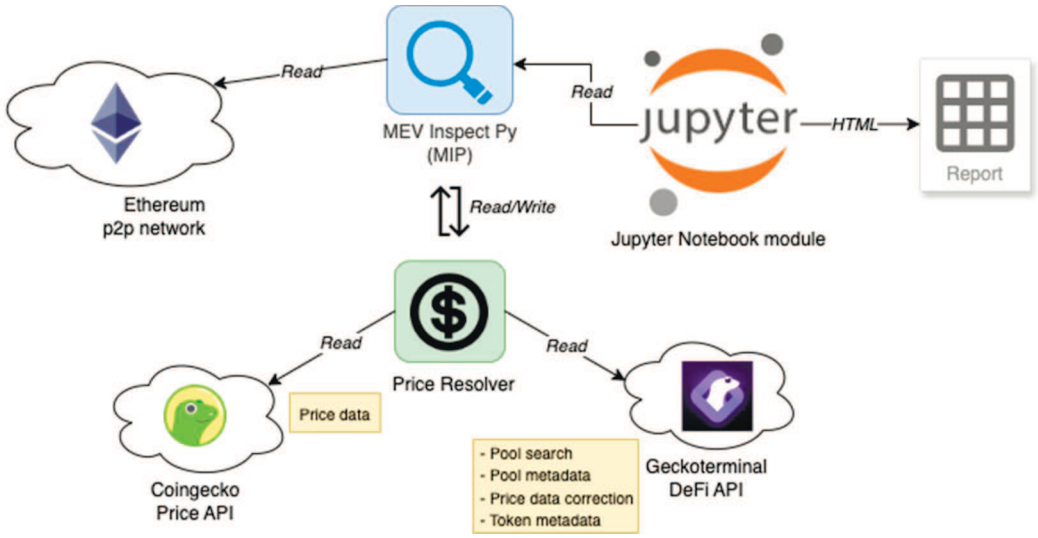

Fig. 2. Architecture of MEV data collection and comparative analysis

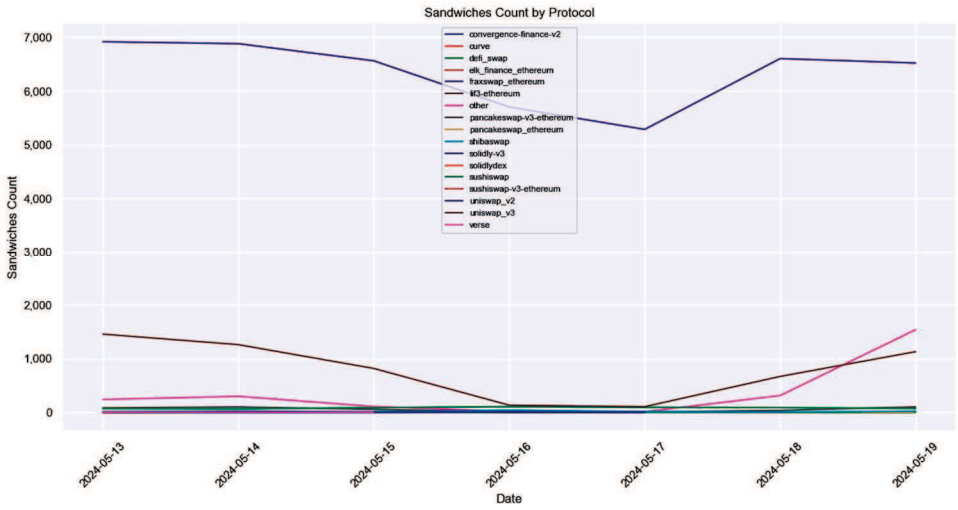

Fig. 3. MEV sandwich attacks count

A comparison of attack volume and count reveals that the total volume of crypto-assets involved in sandwich-type MEV extraction is similarly high for Uniswap V2, Uniswap V3, PancakeSwap, and Solidly V3. These results lead to several important observations. Uniswap V2, as shown in prior studies [28] and [23] employs a simple AMM

(Automated Market Maker) mechanism, which facilitates more flexible price manipulation in individual liquidity pools (e. g., WETH/USDC pairs) and easier execution of attacks. As a result, the number of attacks is higher, but their average volume tends to be lower. In contrast, Uniswap V3, PancakeSwap, and Solidly V3 use alternative mechanisms with distinctive characteristics. For example, Uniswap V3 utilizes concentrated liquidity [23], which makes sandwich attacks somewhat harder to perform but, due to liquidity fragmentation across price ranges, allows for greater financial gains per attack.

A similar pattern is observed when analyzing arbitrage-based MEV extraction on decentralized exchanges (Figs. 5–6).

Regarding MEV extraction during liquidations in lending protocols, the data collected shows a predictably small number of events (96 cases in total), limited to only two protocols – Compound V2 [29] and Aave [30]. Consequently, these cases are not analyzed in further detail.

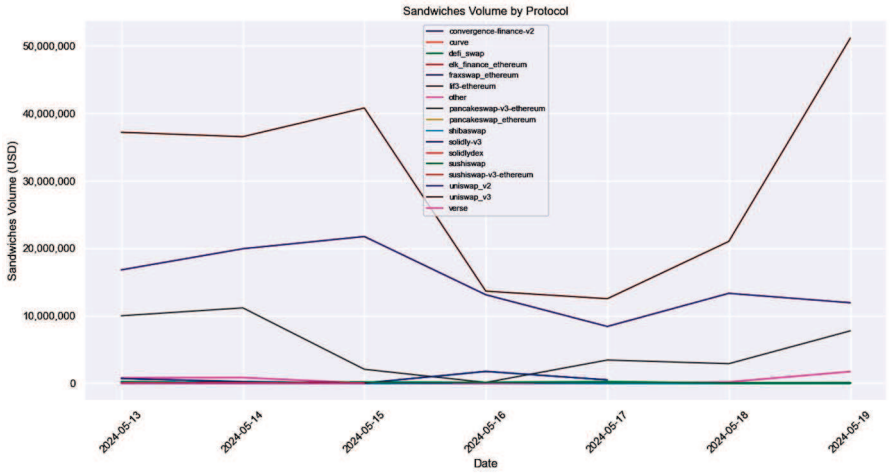

Fig. 4. MEV sandwich attacks volume

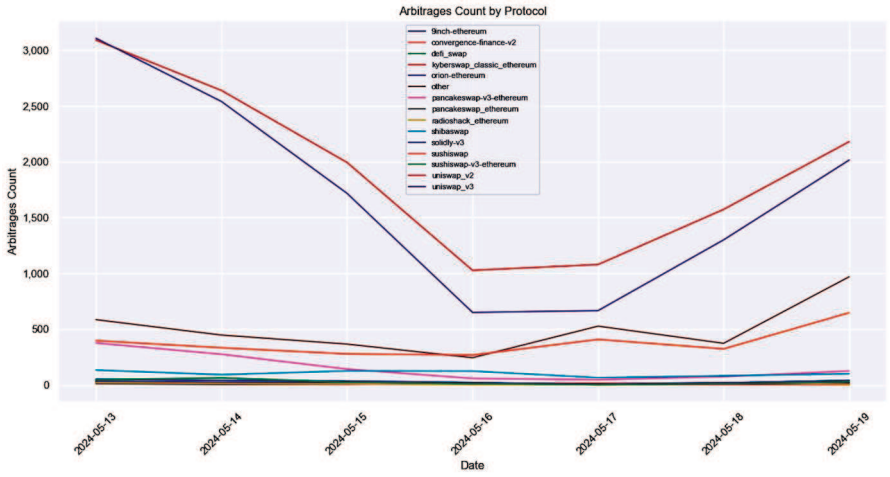

Fig. 5. MEV arbitrages count

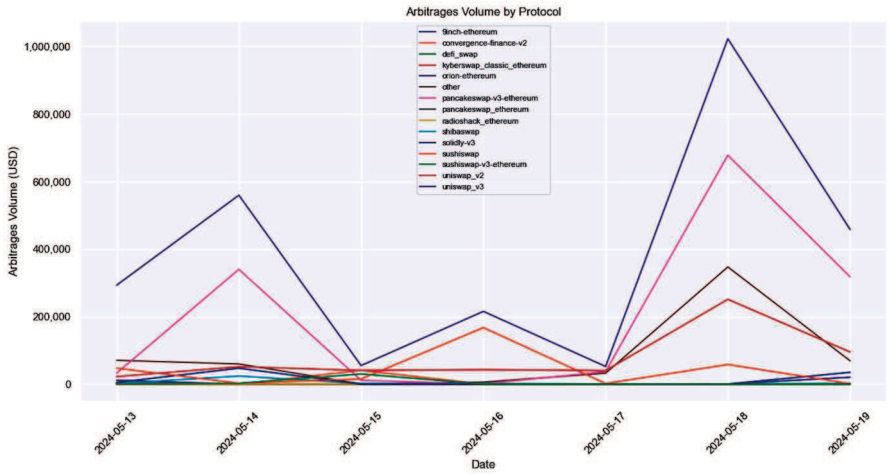

Fig. 6. MEV arbitrages volume

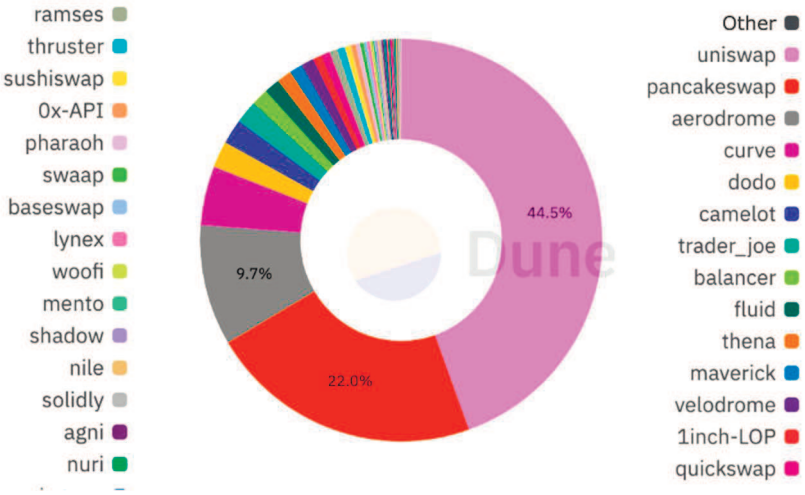

Fig. 7. DEXs volume, may 2024 [31]

It is also important to note that this study does not ignore the dependency between MEV extraction volume and overall trading volume on decentralized exchanges. To account for this factor, we implemented a custom SQL query using the Dune Analytics platform [31], which enables the estimation of trading volumes across leading DEX protocols for the target time period. The results are shown as a pie chart in Fig. 7, illustrating the distribution of trading volume across the most popular decentralized exchanges.

As we can see, trading volume does not fully explain the observed MEV distribution patterns, nor does it capture the distinct gap between the number and volume of MEV attacks revealed by our prior figures.

When comparing these findings to related studies, it is worth highlighting the work in [10], where the authors note that the highest frequency of MEV attacks tends to concentrate on protocols with high liquidity and significant trading activity – an observation corroborated by our results. However, our study further reveals substantial differences in the number and volume of attacks between different versions of the Uniswap protocol (V2 vs V3), attributed to their respective liquidity mechanisms (standard vs concentrated liquidity).

In addition, [6] emphasizes the role of priority gas auctions (PGAs) in shaping the scale of MEV activity. While our findings confirm this conclusion, we also provide quantitative comparisons across specific decentralized exchange protocols, which enhances the granularity of analysis.

Finally, the study [32], focuses on the structure of MEV attacks conducted through Flashbots auctions. Our results extend their conclusions by analyzing not only Flashbots-based attacks but also a wider range of transaction types, allowing us to examine more broadly how DeFi protocol design influences the extent of MEV exploitation.

Scientific contribution – this study introduces and applies a comparative methodology for analyzing Maximal Extractable Value (MEV) exploitation in decentralized exchange protocols. As part of this work, the open-source analytical framework MEV Inspect Py was modified, a Price Resolver component was developed to retrieve and normalize crypto-asset price data, and a Jupyter Notebook – based module was implemented for post-processing and visualization. The *Z*-score method was applied to detect and filter out anomalous pricing data. New metrics were proposed to assess the scale of MEV exploitation, including attack counts and the total volume of involved crypto-assets. The methodology enabled structured comparisons between Uniswap V2, Uniswap V3, PancakeSwap, and Solidly V3, and revealed clear correlations between architectural design and vulnerability to MEV attacks. The analysis also showed how differences in liquidity and pricing mechanisms affect both the nature and the magnitude of MEV activity, suggesting that the proposed approach may be applied to other protocols and blockchain ecosystems.

Practical significance and contribution – the proposed methodology and its components, including the customized version of MEV Inspect Py [12] and supporting modules can be reused by other researchers to obtain new insights into MEV dynamics in DeFi protocols. Additionally, the results of this study may be valuable to protocol developers and DeFi users alike. Developers can draw conclusions about potential improvements to protocol mechanisms, while users gain a better understanding of MEV-related risks across leading DeFi platforms.

Conclusions / Висновки

This study reviewed existing academic literature on the phenomenon of Maximal Extractable Value (MEV) and its empirical evaluation, revealing a notable lack of focus on the differences in MEV extraction across decentralized exchange protocols. This motivated the development of a dedicated comparative analysis methodology capable of identifying MEV events in public blockchain data, quantifying their frequency and volume, and enabling further processing and visualization.

To address this challenge, the open-source framework MEV Inspect Py was selected, although its default configuration proved insufficient for the study's objectives. Accordingly, the framework was modified and extended

through the development of two additional components – a Price Resolver for retrieving and correcting crypto-asset price data, and an analytics module based on Jupyter Notebook for post-processing and visualization.

To improve the quality of pricing data, the Z-score method was applied to detect and remove anomalies. Also, we introduced two new metrics – the number of attacks and the total volume (USD) of involved crypto-assets which help to assess the scale of MEV exploitation more accurately.

The analysis showed that Uniswap V2 and Uniswap V3 are the most active protocols in terms of MEV extraction. This is explained by their architectural differences: Uniswap V2 facilitates easier price manipulation via a classic AMM model ($x \cdot y = k$), while Uniswap V3, through its use of concentrated liquidity, creates conditions for higher per-attack profitability. Significant MEV volumes were also observed in PancakeSwap and Solidly V3, indicating that the internal design of a DEX plays a key role in the likelihood and profitability of MEV attacks. These results confirm that AMM model design and liquidity mechanics directly influence the scale and nature of MEV exploitation.

The proposed methodology and supporting tools provide scientific value as a unified approach for comparative analysis that can be adapted to other categories of DeFi protocols and blockchain networks. From a practical standpoint, the results may benefit protocol developers aiming to improve system design and end-users seeking to make better-informed decisions when interacting with DeFi infrastructure.

Future research directions may include:

- comparative MEV analysis across other blockchain networks;
- studying the temporal dynamics of MEV extraction and the impact of network and protocol updates on attack scale;
- deeper investigation of DeFi protocol implementations and their correlation with MEV frequency and profitability;
- evaluation of existing and development of new mitigation strategies to reduce the negative effects of MEV in decentralized finance protocols.

References

[1] Werner, S. M., Perez, D., Gudgeon, L., Klages-Mundt, A., Harz, D., & Knottenbelt, W. J. (2021). *SoK: Decentralized Finance (DeFi)*. https://doi.org/10.48550/arxiv.2101.08778

[2] *Amazon.com: Flash Boys: A Wall Street Revolt: 9780393351590: Lewis, Michael: Books* (n. d.). Retrieved August 13, 2023, from https://www.amazon.com/Flash-Boys-Wall-Street-Revolt/dp/0393351599

[3] Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., & Juels, A. (2019). *Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges*. https://doi.org/10.48550/arxiv.1904.05234

[4] Cherkas, N. S., & Batyuk, A. Ye. (2023). Maximal extractable value (mev) in blockchain networks and its impact on blockchain ecosystem. *Ukrainian Journal of Information Technology*, *5*(2), 60–71. https://doi.org/10.23939/ujit2023.02.060

[5] Heimbach, L., Kiffer, L., Torres, C. F., & Wattenhofer, R. (2023). *Ethereum's Proposer-Builder Separation: Promises and Realities*. http://arxiv.org/abs/2305.19037

[6] Qin, K., Zhou, L., & Gervais, A. (2021). *Quantifying Blockchain Extractable Value: How dark is the forest?* https://doi.org/ 10.48550/arxiv.2101.05511

[7] Piet, J., Fairoze, J., & Weaver, N. (2022). *Extracting Godl [sic] from the Salt Mines: Ethereum Miners Extracting Value*. https://doi.org/10.48550/arxiv.2203.15930

[8] Weintraub, B., Torres, C. F., Nita-Rotaru, C., & State, R. (2022). *A Flash(bot) in the Pan: Measuring Maximal Extractable Value in Private Pools*. https://doi.org/ 10.1145/3517745.3561448

[9] Eskandari, S., Moosavi, S., & Clark, J. (2019). *SoK: Transparent Dishonesty: front-running attacks on Blockchain*. https:// doi.org/ 10.48550/arxiv.1902.05164

[10] Torres, C. F., Camino, R., & State, R. (2021). *Frontrunner Jones and the Raiders of the Dark Forest: An Empirical Study of Frontrunning on the Ethereum Blockchain*. https://doi.org/ 10.48550/arxiv.2102.03347

[11] Wahrstätter, A., Zhou, L., Qin, K., Svetinovic, D., & Gervais, A. (2023). *Time to Bribe: Measuring Block Construction Markets*.

[12] *GitHub – flashbots/mev-inspect-py: an MEV inspector for Ethereum* (n. d.). Retrieved October 7, 2024, from https:// github. com/flashbots/mev-inspect-py

[13] *PostgreSQL: The world's most advanced open source database* (n. d.). Retrieved March 9, 2025, from https://www.postgresql.org/

[14] *Redis – The Real-time Data Platform* (n. d.). Retrieved March 9, 2025, from https://redis.io/

[15] *Kubernetes* (n. d.). Retrieved March 9, 2025, from https://kubernetes.io/

[16] *Welcome! / minikube* (n. d.). Retrieved March 9, 2025, from https://minikube.sigs.k8s.io/docs/

[17] *Cryptocurrency Prices, Charts, and Crypto Market Cap / CoinGecko* (n. d.). Retrieved March 9, 2025, from https:// www.coingecko.com/

[18] *DEX Tracker – Tool for Tracking Crypto Prices & Charts / GeckoTerminal*. (n. d.). Retrieved March 9, 2025, from https://www.geckoterminal.com/

[19] *Project Jupyter / Home* (n. d.). Retrieved October 7, 2024, from https://jupyter.org/

[20] *Z-Score: Meaning and Formula* (n. d.). Retrieved March 9, 2025, from https://www.investopedia.com/terms/z/zscore.asp

[21] Nisan, Noam (2007). *Algorithmic game theory*. Cambridge University Press.

[22] Judmayer, A., Stifter, N., Schindler, P., & Weippl, E. (2021). *Estimating (Miner) Extractable Value is Hard, Let's Go Shopping!* https://github.com/

[23] Choi, N., & Kim, H. (2024). Decentralized Exchange Transaction Analysis and Maximal Extractable Value Attack Identification: Focusing on Uniswap USDC3. *Electronics (Switzerland)*, *13*(6). https://doi.org/10.3390/ electronics 13061098

[24] Zhou, L., Qin, K., Torres, C. F., Le, D. V., & Gervais, A. (2020). High-Frequency Trading on Decentralized On-Chain Exchanges. *Proceedings – IEEE Symposium on Security and Privacy*, *2021, May*, 428–445. https://doi.org/10.1109/ SP40001.2021.00027

[25] Luu, L., Teutsch, J., Kulkarni, R., & Saxena, P. (2015). Demystifying incentives in the consensus computer. *Proceedings of the ACM Conference on Computer and*

Communications Security, *2015, October*, 706–719. https://doi.org/10.1145/ 2810103.2813659
[26] *Home / Uniswap Protocol* (n. d.). Retrieved August 13, 2023, from https://uniswap.org/
[27] *ncherkas/mev-inspect-py: Private fork of https://github.com/flashbots/mev-inspect-py* (n. d.). Retrieved March 9, 2025, from https://github.com/ncherkas/mev-inspect-py
[28] Xu, J., Paruch, K., Cousaert, S., & Feng, Y. (2023). SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols. *ACM Computing Surveys*, *55*(11). https://doi.org/10.1145/3570639
[29] *Compound* (n. d.). Retrieved March 9, 2025, from https://compound.finance/
[30] *Aave* (n. d.). Retrieved March 9, 2025, from https://aave.com/
[31] *DEX by volume May 2024* (n. d.). Retrieved March 9, 2025, from https://dune.com/queries/4824483/7994859
[32] Li, Z., Li, J., He, Z., Luo, X., Wang, T., Ni, X., Yang, W., Chen, X., & Chen, T. (2023). Demystifying DeFi MEV Activities in Flashbots Bundle. *CCS 2023 – Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, 165–179. https://doi.org/10.1145/3576915.3616590

Н. С. Черкас, А. Є. Батюк

Національний університет "Львівська політехніка", Львів, Україна

МЕТОДОЛОГІЯ ПОРІВНЯЛЬНОГО АНАЛІЗУ ЕКСТРАКЦІЇ MAXIMAL EXTRACTABLE VALUE (MEV) У ПРОТОКОЛАХ ДЕЦЕНТРАЛІЗОВАНИХ КРИПТОБІРЖ

Із розвитком смарт-контрактів у мережах блокчейн уможливилось створення складних децентралізованих фінансових (DeFi) протоколів, що охоплюють біржі, платформи кредитування та алгоритмічні криптоактиви. Незважаючи на децентралізованість та прозорість, блокчейн-мережі не гарантують прогнозованої послідовності виконання транзакцій, що привело до появи явища Maximal Extractable Value (MEV) – додаткової вигоди, яку отримують окремі учасники мережі завдяки впливу на впорядкування транзакцій.

Подане дослідження зосереджене на емпіричному аналізі масштабів явища MEV між різними DeFi-протоколами з метою визначення ключових факторів, що впливають на масштаби та частоту MEV-атак. У межах роботи запропоновано методологію порівняння екстракції MEV із використанням модифікованої версії програмного комплексу MEV Inspect Py та додатково реалізованих компонентів – Price Resolver для збирання та попереднього опрацювання цін на криптоактиви, та аналітичного модуля Jupyter Notebook для вивчення отриманих результатів. Крім того, запропоновано підхід до оцінювання загального обсягу MEV атак типу сендвіч та арбітраж, а також реалізовано метод виявлення та усунення аномалій у цінових даних, що поліпшило якість результатів аналізу.

Результати дослідження показали, що Uniswap V2 та Uniswap V3 є основними мішенями MEV екстракції, однак їхні механізми роботи створюють різні умови для атак. Виявлено кореляцію між концентрованою ліквідністю, алгоритмами ціноутворення та масштабами MEV-екстракції. Крім того, підтверджено, що архітектурні особливості DeFi-протоколів безпосередньо впливають на їхню вразливість до MEV.

Отримані результати можуть бути використані для підвищення стійкості алгоритмів децентралізованих бірж до MEV екстракції та розроблення механізмів мінімізації її негативного впливу. Дослідження може бути корисним також для користувачів DeFi-протоколів, які прагнуть зменшити ризики через явище MEV. Визначено напрями подальших досліджень, зокрема аналіз MEV-експлуатації в інших блокчейн-мережах та вивчення ефективності стратегій захисту.

Ключові слова: блокчейн, смарт-контракти, розподілені системи, однорангові мережі, криптографія.

Інформація про авторів:

Черкас Назарій Степанович, аспірант, кафедра автоматизованих систем управління. **Email:** nazarii.s.cherkas@lpnu.ua; https://orcid.org/0009-0007-9976-6530

Батюк Анатолій Євгенович, канд. техн. наук, доцент, кафедра автоматизованих систем управління. **Email:** anatolii.y.batiuk@lpnu.ua; https://orcid.org/0000-0001-7650-7383

Цитування за ДСТУ: Черкас Н. С., Батюк А. Є. Методологія порівняльного аналізу екстракції Maximal Extractable Value (MEV) у протоколах децентралізованих криптобірж. *Український журнал інформаційних технологій*. 2025, т. 7, № 1. С. 108–116.

Citation APA: Cherkas, N. S., & Batiuk, A. Y. (2025). Methodology for comparative analysis of Maximal Extractable Value (MEV) in decentralized exchange protocols. *Ukrainian Journal of Information Technology*, 7(1), 108–116. https://doi.org/10.23939/ujit2025.01.108