A Closer Look at Cross-Domain Maximal Extractable Value for Blockchain Decentralisation

Johan Hagelskjar Sjursen, Weizhi Meng, and Wei-Yang Chiu
SPTAGE Lab, Department of Applied Mathematics and Computer Science,
Technical University of Denmark, Kgs. Lyngby, Denmark

2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) | 979-8-3503-1019-1/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICBC56567.2023.10174971

***Abstract*—In the current literature, many solutions for solving blockchain scaling have been tried historically, whereas most of them usually may compromise the decentralisation. Ethereum has chosen to scale by switching to Proof of Stake consensus and adding data sharding to allow Layer 2 execution to be cheaper. However, in the light of cross-domain Maximal Extractable Value (MEV), even this strategy may have centralising forces built-in. In this work, we focus on cross-domain MEV and try to identify cross domain arbitrage. In particular, we extract Uniswap data from four different domains and provide an initial analysis of how to identify cross domain arbitrages.**

***Index Terms*—Blockchain, Decentralized Application, Maximal Extractable Value, Cross Domain, Ethereum**

I. Introduction

In 2008, the Bitcoin whitepaper [1] first described a peer-to-peer (P2P) network, which allowed for online payments without having to rely on financial institutions. Instead it relied on putting transactions into blocks linked with hashes in a manner, dubbed Proof of Work (PoW). This meant that users of the system could trust that their transactions would not be reverted as long as most of the participants in the network were not actively trying do undermine it [19]. Now blockchain technology has been studied in different domains such as security [21], [23], data sharing [14], 6G [17], vehicular [15], healthcare [20], smart city [22], [16] and more.

However in Bitcoin, there is a recent trend toward sacrificing decentralisation in order to achieve scale purpose. This trend has also been described as the scalability trilemma [24]. The idea behind is that one cannot meaningfully improve on one aspect of the trilemma (scalability, decentralisation, security) without compromising on another. As a solution, the Ethereum Roadmap is a set of upgrades to the Ethereum protocol that the Ethereum foundation is working along with client teams to actualise. The next two major expected upgrades are the merge (switching from PoW to Proof of Stake - PoS) and data sharding, where the former being a requirement for the latter. These upgrades aim to achieve all sides of the trilemma. In other words, they aim to build a decentralised and secure network that can settle a lot of transactions trustlessly.

In the last few years, awareness of Maximal Extractable Value (MEV) has grown steadily, which refers to the maximum value that can be extracted by blockchain miners from generating a block production in excess of the standard block reward and gas fees through including, excluding, and changing the order of transactions in a block [25]. Daian *et al.* [3] firstly proposed this issue, and figured out that high fees paid for priority transaction ordering may pose a systemic risk. For protection, Weintraub *et al.* [29] measured the impact of Flashbots [4] - a solution by creating a private transaction pool, and found some flaws existed. Churiwala and Krishnamachari [2] introduced a transaction protocol to eliminate MEV attacks by requesting an interaction token from the on-chain counter-party. Malkhi and Szalachowski [18] proposed Fino, a Directed Acyclic Graphs-based protocol that includes MEV-resistance features into an enhanced Byzantine fault tolerance (BFT) consensus without degrading the performance.

The landscape has moved from Priority Gas Auctions [8] to Flashbots bundles [9] and beyond, but there are still many open questions about its potential impact on decentralisation. With Ethereum's transition to Proof of Stake (PoS) consensus approaches, these questions are more pressing than ever, with new concerns about Cross-Domain MEV [28].

Contributions. In this work, we seek to find out if cross-domain MEV can be found. The contributions of this work can be summarized as: 1) we develop a tool that can extract Uniswap data [11] from different domains for traces of cross domain arbitrage, and 2) we perform an initial analysis and provide an example of how to identify cross domain arbitrages.

II. Data Collection and Extraction

There are many different types of MEV, and a long tail of exotic ways to extract values. The most obvious and most profitable way to extract values is through arbitrage. On Ethereum, there exist many different kinds of exchanges, but on other chains, the selection is more scarce. In the aspect of generated fees, the most popular DEX (decentralized exchange) by far is Uniswap [5]. Uniswap has multiple versions of their DEX'es deployed on the Ethereum mainnet, but only the third version v3 is deployed on different Layer 2. Uniswap [11] is also well documented, and their smart contracts emit events that make it a lot more feasible to find and organise swap data. Because of these factors, in this work, we mainly look at Uniswap data from different domains in order to keep the complexity of the problem under control.

In order to detect cross-domain MEV, we need to collect data from multiple domains. Transaction data for decentralised blockchains is public, whereas it does not mean it is readily available for average consumers. While running an Ethereum node and using it to extract data from Ethereum is relatively simple on consumers' hardware, if we want to run nodes for different blockchain networks, we need a lot of storage space.

The initial idea was to check cross-domain MEV between two domains, *Mainnet Ethereum* and *Arbitrum*, a Layer 2 (L2) scaling solution. Arbitrum [6] is also powered by the Ethereum Virtual Machine (EVM), which enables building software to analyse data on the two different chains easier. We rented a server in order to sync nodes and was successful. The storage requirements for running these nodes were however greater then expected, and this setup was costly when increasing the number of network and domains we could analyse.

An alternative solution is to host our own nodes using an infrastructure provider to supply the data. In our case, we adopted Infura [27], a service developed by Consensys [12] and much used in the Ethereum ecosystem. Infura API allows access to Ethereum data without running users' own node. Using Infura, we were able to do 100.000 request/day to their API for free, and extract data from Mainnet Ethereum, Arbitrum, Optimism [7] and Polygon PoS [10]. All these networks are EVM compatible and have an instance of Uniswap v3.

To limit the amount of data, we only extract from a certain period. We chose the range from the month of June as well as the first week of July 2022. This range was chosen partially to fall within the limits of how many transactions were allowed to the Infura API (100.000 per day) and partially to have enough space to store it comfortably.

III. Dataset and Analysis

In this section, we give an overview of the collected data and provide an initial analysis.

A. Data Overview

Firstly, we have to get an overview of the collected data. In total, we collected events from around 3.7 million swap events. The distribution of the swap events from different networks is shown in Figure 1.

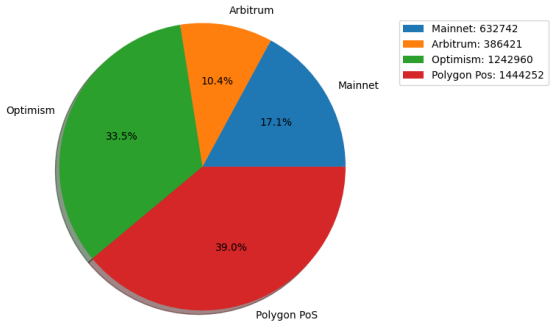

Fig. 1. Pie chart of distribution of events on the different networks

A certain number of swap events come from routers. This means that the user who made the transaction has used the web-interface that corresponds to the router in question, and is therefore most likely not used to extract cross-domain MEV. Table I shows the percentage of swap events initialised by routers belonging to 1inch [26] or the Uniswap Router.

TABLE I
Percentage of swap events initialised by routers.

Network	All Swap Events	Non-Router	Router Percentage
Mainnet	632742	343182	54.24 %
Arbitrum	386421	94714	24.51 %
Optimism	1242960	556892	44.80 %
Polygon PoS	1444252	547276	37.89 %
Total	3706375	1542064	41.60 %

B. Initial Analysis

To try and discover the extaction of cross-domain MEV, we first took the union of unique sender addresses from different networks. This yielded new sets of sender addresses that had interacted with Uniswap pools in different networks. These addresses were in turn inspected individually by using block explorers, in order to qualitatively discern whether or not they were engaging in cross-domain MEV extraction.

Regarding the transactions of this address, we found some cross domain arbitrages. Below is an example with steps:

1) The contract swaps 1.58 WETH for 1693.67 USDC by using a Uniswap V3 pool.
2) It then swaps the USDC gained in Step 1) for 5842.45 STRP tokens on a different DEX called Sushiswap.
3) Using the Arbitrum bridge, the STRP tokens are transferred to Arbitrum. Later the STRP tokens are transferred from the ERC20 gateway on Arbitrum to the same smart contract address that did the swaps from Step 1) and Step 2).
4) It then proceeds to swap the STRP tokens to 1701.59 USDC tokens through Sushiswap on Arbitrum.
5) Finally it swaps the USDC tokens for a total of 1.59 WETH tokens.

We can inspect these transactions on etherscan. Looking at the other transactions of this address on these public block explorers, we found that they also did cross domain arbitrage with Gnosis Chain (previously xDai), which is another EVM compatible domain [13]. We also found that this contract was created less than a month ago, and has less than a thousand transactions across all the domains we found it to be active. The profit of these transactions seemed to be low, around 0.1-0.2 WETH for the cases we manually checked.

IV. Conclusion

The current research on cross-domain MEV is still conducted at a very early stage, and it is even hard and complex to find relevant data. Motivated by this challenge, in this work, we tried to study cross-domain MEV in the wild, by sampling data from four different domains. Based on the collected data, we provided an initial analysis on how to identify cross domain arbitrages with an example. It is clear that cross-domain MEV and its extraction will become a bigger threat to Ethereum's decentralisation in the future.

Acknowledgment

This project is partially supported by H2020 DataVaults. The collected dataset will be available on request.

REFERENCES

[1] S. Nakamoto, "Bitcoin, A Peer-to-Peer Electronic Cash System", 2008.

[2] D. Churiwala and B. Krishnamachari, "CoMMA Protocol: Towards Complete Mitigation of Maximal Extractable Value (MEV) Attacks," CoRR abs/2211.14985, pp. 1-3, 2022.

[3] P. Daian, S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, L. Breidenbach, and A. Juels, "Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability," *In: IEEE Symposium on Security and Privacy*, pp. 910-927, 2020.

[4] Flashbots Docs. [Online; accessed 23. Nov. 2021]. https://docs.flashbots.net/flashbots-auction/overview

[5] Crypto fees. https://cryptofees.info/history/2022-07-25

[6] Offchain Labs, Arbitrum. https://arbitrum.io/

[7] OP Labs, Optimism. https://www.optimism.io/

[8] How Everything (and Nothing) Changes with Gas Fees: Blocknative ETHDenver – 2022 Recap. https://www.blocknative.com/blog/ethdenver-2022-recap-how-everything-and-nothing-changes-with-gas

[9] Bundling Transactions with Flashbots. https://spin.atomicobject.com/2023/01/28/bundle-transactions-flashbots/

[10] Polygon, Polygon pos. https://polygon.technology/solutions/polygon-pos/

[11] Uniswap Labs, Uniswap contract deployments. https://docs.uniswap.org/protocol/reference/deployments

[12] Consensys. https://consensys.net/

[13] Gnosis Chain. https://www.gnosis.io/

[14] W.Y. Chiu, W. Meng, and C.D. Jensen, "My Data, My Control: A Secure Data Sharing and Access Scheme over Blockchain," *Journal of Information Security and Applications* 63, 103020, 2021.

[15] W.Y. Chiu and W. Meng, "EdgeTC - A PBFT Blockchain-based ETC Scheme for Smart Cities," *Peer-to-Peer Networking and Applications* 14, pp. 2874-2886, 2021.

[16] W.Y. Chiu, W. Meng, W. Li and L.n Fang, "FolketID: A Decentralized Blockchain-based NemID Alternative against DDoS Attacks," *In: ProvSec 2022*, pp. 210-227, 2022.

[17] W. Li and W. Meng, "BCTrustFrame: Enhancing Trust Management via Blockchain and IPFS in 6G Era," *IEEE Network* 36(4), pp. 120-125, 2022.

[18] D. Malkhi and P. Szalachowski, "Maximal Extractable Value (MEV) Protection on a DAG," CoRR abs/2208.00940, pp. 1-10, 2022.

[19] W. Meng, E.W. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When Intrusion Detection Meets Blockchain Technology: A Review," *IEEE Access*, vol. 6, no. 1, pp. 10179-10188, 2018.

[20] W. Meng, W. Li, and L. Zhu, "Enhancing Medical Smartphone Networks via Blockchain-based Trust Management against Insider Attacks," *IEEE Transactions on Engineering Management* 67(4), pp. 1377-1386, 2020.

[21] W. Meng, W. Li, L.T. Yang, and P. Li, "Enhancing Challenge-based Collaborative Intrusion Detection Networks Against Insider Attacks using Blockchain," *International Journal of Information Security* 19(3), pp. 279-290, 2020.

[22] W. Meng, W. Li, S. Tug, and J. Tan, "Towards Blockchain-enabled Single Character Frequency-Based Exclusive Signature Matching in IoT-assisted Smart Cities," *Journal of Parallel and Distributed Computing* 144, pp. 268-277, 2020.

[23] W. Meng, W. Li, and J. Zhou, "Enhancing the Security of Blockchain-based Software Defined Networking through Trust-based Traffic Fusion and Filtration," *Information Fusion* 70, pp. 60-71, 2021.

[24] V. Buterin, "Why sharding is great: Demystifying the technical properties," https://vitalik.ca/general/2021/04/07/sharding.html

[25] Maximal Extractable Value (MEV). https://ethereum.org/en/developers/docs/mev/

[26] 1inch. https://1inch.io/

[27] Infura: The world's most powerful suite of high availability blockchain APIs and developer tools. https://infura.io/

[28] A. Obadia, A. Salles, L. Sankar, T. Chitra, V. Chellani, and P. Daian, "Unity is Strength: A Formalization of Cross-Domain Maximal Extractable Value," CoRR abs/2112.01472, pp. 1-13, 2021.

[29] B. Weintraub, C.F. Torres, C. Nita-Rotaru, and R. State, "A flash(bot) in the pan: measuring maximal extractable value in private pools," *In: IMC*, pp. 458-471, 2022.