CoMMA Protocol: Towards Complete Mitigation of Maximal Extractable Value (MEV) Attacks

Dev Churiwala  
Viterbi School of Engineering*  
University of Southern California  
Los Angeles, USA  
f20180602@goa.bits-pilani.ac.in

Bhaskar Krishnamachari  
Viterbi School of Engineering  
University of Southern California  
Los Angeles, USA  
bkrishna@usc.edu

Abstract—MEV attacks have been an omnipresent evil in the blockchain world, an implicit tax that uninformed users pay for using the service. The problem arises from the miners’ ability to reorder and insert arbitrary transactions in the blocks they mine. This paper introduces a 2-phased transaction protocol designed to mitigate MEV attacks in blockchain systems. The proposed protocol involves users obtaining interaction tokens from on-chain counter-parties, which act as preemptive measures against transaction reordering. The effectiveness of the CoMMA protocol in preventing MEV attacks is demonstrated and validated.

Index Terms—MEV, maximal extractable value, miner extractable value, distributed computing, blockchain, cryptography

I. INTRODUCTION

With the explosion in the adoption and use of cryptocurrencies, the underlying blockchain infrastructures handle copious amounts of transactions. In traditional distributed consensus algorithms, ‘miners’ insert these transactions into the blockchain ledgers. The miners pick unconfirmed transactions from the mempool, generally monetarily motivated, based on the profit they can make on the particular transaction. That said, nothing restricts the miners from including their transactions in the proposed block or from reordering the transactions in a way that is financially lucrative for them. The miner’s economic incentive and uninhibited power over the included transactions and order give rise to MEV attacks [1].

MEV bots exploit this vulnerability, targeting transactions for profit. Recent data shows that MEV bot-driven activities accounted for 46.1% of Uniswap V3’s transaction volume, equivalent to approximately $20 billion in a month [2], [3].

While MEV activities have been seen as market stabilizers, removing them aligns with economic principles and is unlikely to disrupt the equilibrium [4]. This study assesses MEV behavior and proposes an effective mitigation strategy.

II. RELATED WORKS

There has been much interest in mitigating MEV attacks recently. Zhou et al. proposed A2MM, which only targets insertion attacks [5]. Varun et al. suggest using machine learning to detect and mitigate MEV attacks [6]. Pillai proposes a new incentive structure for mitigating MEV activities [7]. Malkhi and Szalachowski propose an augmented BFT protocol [8]. Furthermore, drawing on traditional cryptography, one may even consider encrypting threshold values to prevent identification of target transactions [9].

However, most of these methods involve computational overhead or changes to the blockchain’s core. In contrast, our approach efficiently eliminates MEV attacks within the existing blockchain framework.

III. UNDERSTANDING MEV ATTACKS

In Fig. 1, a bot exploits a user, using a common scheme. The user submits transaction $T_{tgt}$ to the mempool for ledger inclusion. The bot’s role, indicated by the function $get_{tgt}()$ in the figure, is to continuously scan for ‘target’ transactions.

![Fig. 1: A transaction without the CoMMA protocol.](image)

Upon identifying an exploitable transaction (such as one with a high slippage tolerance), the bot selects it, like $T_{tgt}$, for the next block proposal. It supplements the block with transactions $T'$ and $T''$, arranging them as $\{T', T_{tgt}, T''\}$ to enclose the target transaction. When this block is accepted and executed, the ‘sandwiched’ transaction generates profit for the miner, achieving a successful MEV attack [10]. Alternatively, placing a transaction before $T_{tgt}$ can suffice for executing the attack [11].

IV. PROPOSED SOLUTION

A. CoMMA v1

MEV attacks are bound to occur as long as the malicious actors can monitor and identify transactions in the mempool. To combat this, we propose a 2-stage transaction architecture. We use a DEX as the on-chain counter-party to elucidate the
protocol, but an analogous protocol extends to all on-chain applications.

1) Users generate an ‘order request,’ $R_{q_{or}}$, for the DEX to signal an intended order.
2) This request becomes a transaction in the mempool.
3) A miner executes this transaction on the DEX since there’s no profit involved.
4) The DEX issues an ‘order token,’ $Tk_{or}$, to the user, marking their order queue position.
5) Users submit their orders, like $T_x$, which are executed as they reach the front of the queue.
6) DEX issues tokens ahead of time, not waiting for late transactions. Transactions not at the queue’s front lose their place and require a new ‘order request,’ $R_{q_{or}}$.

![CoMMA v1](image1)

Fig. 2: CoMMA v1

This protocol suppresses MEV attacks using an order queue. However, its verifiability is a limitation. Malicious actors can still attempt MEV attacks, but the associated costs, including transaction fees for unprofitable order requests targeting transactions with no profit, act as a deterrent.

B. CoMMA v2

To overcome this, we improve CoMMA v1 by integrating a one-way cryptographic hash, $H_{xT_x}$, into the initial ‘order request.’ This hash allows the DEX to verify the order’s validity before execution, deterring malicious MEV bots. Such attacks now demand predicting order details in the ‘order request’ phase, drastically reducing the likelihood of success and thereby minimizing the financial incentives for MEV attacks.

![CoMMA v2](image2)

Fig. 3: CoMMA v2

CoMMA v2 introduces slight latency and minor costs compared to conventional transactions. However, it effectively eradicates MEV attacks while upholding blockchain’s core principles—trustlessness, decentralization, and transparency.

V. FORMAL VERIFICATION

**Expectation:** CoMMA v2 eradicates MEV attacks while upholding trustlessness, decentralization, and transparency.

**Assumption:** The malicious actor is financially driven.

**Analysis:** We analyse CoMMA v2 under this assumption.

- **Case (i).** User Alice submits an order request to the mempool, indicating an intent to trade and providing a hash of the intended trade. The irreversible nature of the hash prevents Oscar from formulating an MEV attack. If Oscar were to acquire adjacent slots before and after Alice’s, he’d need to guess her trade for creating transaction hashes. This financial risk deters Oscar, allowing Alice’s transaction to be mined, and she receives an order token. Alice then submits her trade, along with the token and trade details. Without the required slots, Oscar can’t set up the described MEV attack. Thus, case (i) aligns with our expectation.

- **Case (ii).** In an alternate scenario, Oscar attempts to guess and obtain adjacent slots. However, statistical probabilities ensure he’s wrong most of the time, leading to financial losses in transaction fees. Since our assumption contradicts case (ii), we affirm CoMMA v2’s correctness.

VI. CONCLUSION

Blockchain’s high liquidity fosters numerous MEV attack opportunities, burdening ordinary users with substantial financial costs. While the overall impact of these attacks remains debatable, they pose a persistent concern. CoMMA v2 offers an efficient remedy, obviating the need for fundamental blockchain modifications. Its demonstrated correctness for financially motivated actors upholds core blockchain values. As a modular upgrade, CoMMA v2 holds promise for integration into existing protocols to effectively eliminate MEV attacks.

REFERENCES

[1] P. Daian, S. Goldfeder, T. Kell, Y. Li, X. Zhao, J. Bentov, L. Breidenbach, and A. Juels, “Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability,” in 2020 IEEE Symposium on Security and Privacy (SP), pp. 910–927, IEEE, 2020.

[2] H. Adams, N. Zinsmeister, M. Salem, R. Kefee, and D. Robinson, “Uniswap v3 core,” Tech. rep., Uniswap, Tech. Rep., 2021.

[3] D. Sui, “Uniswap v3 trades %, 30d by origination.” https://dune.com/queries/871679, 2022. Accessed: 2022-11-23.

[4] G. B. Richardson, “The theory of the market economy,” Revue économique, vol. 46, no. 6, pp. 1487–1496, 1995.

[5] L. Zhou, K. Qin, and A. Gervais, “A2mm: Mitigating frontrunning, transaction reordering and consensus instability in decentralized exchanges,” arXiv preprint arXiv:2106.07371, 2021.

[6] M. Varun, B. Palanisamy, and S. Sural, “Mitigating frontrunning attacks in ethereum,” in Proceedings of the Fourth ACM International Symposium on Blockchain and Secure Critical Infrastructure, pp. 115–124, 2022.

[7] B. Pillai, “Blockchain MEV minimisation solution with price guarantee reward,” 10 2022.

[8] D. Malkhi and P. Szalachowski, “Maximal extractable value (mev) protection on a dag,” arXiv preprint arXiv:2208.00940, 2022.

[9] V. Shoup and R. Gennaro, “Securing threshold cryptosystems against chosen ciphertext attack,” in International Conference on the Theory and Applications of Cryptographic Techniques, pp. 1–16, Springer, 1998.

[10] P. Züst, “Analyzing and preventing sandwich attacks in ethereum,” 2021.

[11] S. Eskandari, S. Moosavi, and J. Clark, “Sok: Transparent dishonesty: frontrunning attacks on blockchain,” in International Conference on Financial Cryptography and Data Security, pp. 170–189, Springer, 2019.