A theoretical basis for Blockchain Extractable Value

(Oral communication)

Massimo Bartoletti and Roberto Zunino
University of Cagliari, University of Trento

Abstract

Extractable Value refers to a wide class of economic attacks to public blockchains, where adversaries with the power to reorder, drop or insert transactions in a block can "extract" value from user transactions. Empirical research has shown that mainstream protocols, like e.g. decentralized exchanges, are massively targeted by these attacks, with detrimental effects on their users and on the blockchain network. Despite the growing impact of these attacks in the real world, theoretical foundations are still missing. We propose a formal theory of Extractable Value, based on a general, abstract model of blockchains and smart contracts. Our theory is the basis for formal proofs of security against Extractable Value attacks.

1 Motivations and overview

Most blockchain protocols delegate the construction of blocks to *consensus nodes* that can freely pick users' transactions from the mempool, possibly add their own, and propose blocks containing these transactions in a chosen order. This arbitrariness in the construction of blocks may turn consensus nodes into attackers, which exploit their transaction-ordering powers to maximize their gain to the detriment of users'. In the crypto jargon these attacks are suggestively referred to as "extracting" value from the mempool, and the gain that attackers can get is called *Maximal Extractable Value*, or MEV.

This issue is not purely theoretical: indeed, mainstream DeFi protocols like Automated Market Makers are common targets of MEV attacks, which overall have led to attacks worth more than 680 million dollars so far [2]. Notably, the profits derived from MEV attacks largely exceed those given by block rewards and transaction fees [10]. MEV attacks are so profitable that currently most of Ethereum network hashing power is controlled by Flashbots [1], a centralized private relay network which outsources the identification of MEV opportunities to anyone, and uses its large network of miners to include the MEV attack transactions in blocks. While this systematic MEV extraction has some benefits (e.g., it has decreased transaction fees for users at the expense of MEV seekers [19]), it is detrimental to blockchain decentralization, transparency, and network congestion [15].

Given the huge practical relevance of MEV, several research efforts have been made to improve its understanding. However, most approaches are preeminently empirical, as they focus on the definition of heuristics to extract value from certain classes of protocols [4, 11, 13, 22], on the quantification of their impact in the wild [16, 18, 20, 21], or on techniques to mitigate the effects of MEV attacks [6–9, 12]. There are only a few attempts to provide MEV with a rigorous definition [3, 14, 17], and the resulting notions are not completely satisfactory. In particular, all these approaches do not allow adversaries to craft blocks by combining their private knowledge with that of the transactions in the mempool, that can only be included verbatim, so losing some potential attacks. We believe that a general, formal definition of MEV and the construction of a rich theoretical apparatus supporting the definition are essential prerequisites to the design of *MEV-free* contracts that are provably secure against MEV attacks.

In this oral communication we discuss our ongoing work towards a general theory of MEV, which we have recently published as an ArXiV preprint [5]. In particular, in the talk we will touch the following points:

- we introduce a general, abstract model of contracts, equipped with key economic notions like wealth and gain;
- we show an instance of the abstract model as a bare-bone (yet Turing-complete) procedural language inspired by Solidity, the leading language to write contracts;
- we present an axiomatization of the transactions that a set of actors can deduce by exploiting their own knowledge and that of the mempool;
- we formally define MEV as the maximal value that a given set of actors can extract from the mempool. We outline our theoretical study of its main properties, like monotonicity, finiteness, and preservation under renamings;
- we propose a formal definition of *MEV-freedom*, the property enjoyed by contracts that are resistant to MEV attacks carried by any wealthy-enough set of actors regardless of their actual identity, as it happens for consensus nodes. Our definition is supported by a theoretical study of its main properties, and its application to formally prove the MEV-freedom (or its absence) of some archetypal contracts, like e.g. Automated Market Makers;
- we discuss and compare of our notion w.r.t. other formalization attempts [3, 14, 17].

References

[1] Flashbots, 2021. flashbots.net.

[2] MEV-explore: MEV over time, February 2023. explore.flashbots.net.

[3] K. Babel, P. Daian, M. Kelkar, and A. Juels. Clockwork finance: Automated analysis of economic security in smart contracts. In *IEEE Symposium on Security and Privacy*, pages 622–639. IEEE Computer Society, 2023.

[4] Massimo Bartoletti, James Hsin-yu Chiang, and Alberto Lluch-Lafuente. Maximizing extractable value from Automated Market Makers. In *Financial Cryptography*, volume 13411 of *LNCS*, pages 3–19. Springer, 2022.

[5] Massimo Bartoletti and Roberto Zunino. A theoretical basis for blockchain extractable value. *CoRR*, abs/2302.02154, 2023.

[6] Carsten Baum, Bernardo David, and Tore Kasper Frederiksen. P2DEX: privacy-preserving decentralized cryptocurrency exchange. In *Applied Cryptography and Network Security (ACNS)*, volume 12726 of *LNCS*, pages 163–194. Springer, 2021.

[7] Carsten Baum, James Hsin yu Chiang, Bernardo David, Tore Kasper Frederiksen, and Lorenzo Gentile. SoK: Mitigation of front-running in decentralized finance. Cryptology ePrint Archive, Report 2021/1628, 2021. https://ia.cr/2021/1628.

[8] Lorenz Breidenbach, Philip Daian, Florian Tramèr, and Ari Juels. Enter the Hydra: Towards principled bug bounties and exploit-resistant smart contracts. In *USENIX Security Symposium*, pages 1335–1352. USENIX Association, 2019.

[9] Michele Ciampi, Muhammad Ishaq, Malik Magdon-Ismail, Rafail Ostrovsky, and Vassilis Zikas. Fairmm: A fast and frontrunning-resistant crypto market-maker. In *Cyber Security, Cryptology, and Machine Learning (CSCML)*, volume 13301 of *LNCS*, pages 428–446. Springer, 2022.

[10] 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 Symp. on Security and Privacy*, pages 910–927. IEEE, 2020.

[11] Shayan Eskandari, Seyedehmahsa Moosavi, and Jeremy Clark. SoK: Transparent Dishonesty: Front-Running Attacks on Blockchain. In *Financial Cryptography*, pages 170–189. Springer, 2020.

[12] Lioba Heimbach and Roger Wattenhofer. Sok: Preventing transaction reordering manipulations in decentralized finance. 2022.

[13] Kshitij Kulkarni, Theo Diamandis, and Tarun Chitra. Towards a theory of maximal extractable value I: constant function market makers. *CoRR*, abs/2207.11835, 2022.

[14] Bruno Mazorra, Michael Reynolds, and Vanesa Daza. Price of MEV: towards a game theoretical approach to MEV. In *ACM CCS Workshop on Decentralized Finance and Security*, pages 15–22. ACM, 2022.

[15] Kaihua Qin, Liyi Zhou, and Arthur Gervais. Quantifying blockchain extractable value: How dark is the forest? In *IEEE Symp. on Security and Privacy*, pages 198–214. IEEE, 2022.

[16] Kaihua Qin, Liyi Zhou, Benjamin Livshits, and Arthur Gervais. Attacking the DeFi ecosystem with Flash Loans for fun and profit. In *Financial Cryptography*, volume 12674 of *LNCS*, pages 3–32. Springer, 2021.

[17] Alejo Salles. On the formalization of MEV, 2021. https://writings.flashbots.net/research/formalization-mev.

[18] Christof Ferreira Torres, Ramiro Camino, and Radu State. Frontrunner Jones and the Raiders of the Dark Forest: An empirical study of frontrunning on the Ethereum blockchain. In *USENIX Security Symposium*, pages 1343–1359, 2021.

[19] Ben Weintraub, Christof Ferreira Torres, Cristina Nita-Rotaru, and Radu State. A Flash(Bot) in the pan: Measuring maximal extractable value in private pools. In *ACM Internet Measurement Conference*, page 458–471. ACM, 2022.

[20] Sam M. Werner, Daniel Perez, Lewis Gudgeon, Ariah Klages-Mundt, Dominik Harz, and William J. Knottenbelt. SoK: Decentralized finance (DeFi). *CoRR*, abs/2101.08778, 2021.

[21] Liyi Zhou, Kaihua Qin, Antoine Cully, Benjamin Livshits, and Arthur Gervais. On the just-in-time discovery of profit-generating transactions in DeFi protocols. In *IEEE Symp. on Security and Privacy*, pages 919–936. IEEE, 2021.

[22] Liyi Zhou, Kaihua Qin, Christof Ferreira Torres, Duc V Le, and Arthur Gervais. High-Frequency Trading on Decentralized On-Chain Exchanges. In *IEEE Symp. on Security and Privacy*, pages 428–445. IEEE, 2021.