Who gets the Maximal Extractable Value? A Dynamic Sharing Blockchain Mechanism

Extended Abstract

Pedro Braga
King's College London
London, United Kingdom
pedro.braga@kcl.ac.uk

Georgios Chionas
University of Liverpool
Liverpool, United Kingdom
g.chionas@liverpool.ac.uk

Piotr Krysta*
Augusta University
Augusta, GA, USA
pkrysta@augusta.edu

Stefanos Leonardos
King's College London
London, United Kingdom
stefanos.leonardos@kcl.ac.uk

Georgios Piliouras
Singapore University of Technology and Design
Singapore
georgios@sutd.edu.sg

Carmine Ventre
King's College London
London, United Kingdom
carmine.ventre@kcl.ac.uk

ABSTRACT

Maximal Extractable Value (MEV) has emerged as a new frontier in the design of blockchain systems. MEV refers to any excess value that a block producer can realize by manipulating the ordering of transactions. In this paper, we propose to make the *MEV extraction rate* part of the protocol design space. Our aim is to leverage this parameter to maintain a healthy balance between block producers (who need to be compensated for the service they provide) and users (who need to feel encouraged to transact). We design a dynamic mechanism which updates the MEV extraction rate with the goal of stabilizing it at a target value. We analyse the evolution of this dynamic mechanism under various market conditions and provide formal guarantees about its long-term performance. The main take-away from our work is that the proposed system exhibits desirable behavior (near-optimal performance) even when it operates in out of equilibrium conditions that are often met in practice. Our work establishes, the first to our knowledge, dynamic framework for the integral problem of MEV sharing between extractors and users.

KEYWORDS

blockchain; maximal extractable value; out-of-equilibrium analysis; chaotic dynamical systems; markets; mechanism design

ACM Reference Format:
Pedro Braga, Georgios Chionas, Piotr Krysta, Stefanos Leonardos, Georgios Piliouras, and Carmine Ventre. 2024. Who gets the Maximal Extractable Value? A Dynamic Sharing Blockchain Mechanism: Extended Abstract. In *Proc. of the 23rd International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2024), Auckland, New Zealand, May 6 – 10, 2024*, IFAAMAS, 3 pages.

*P. Krysta is also affiliated with University of Liverpool, Liverpool, UK.

Proc. of the 23rd International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2024), N. Alechina, V. Dignum, M. Dastani, J.S. Sichman (eds.), May 6 – 10, 2024, Auckland, New Zealand.

1 INTRODUCTION

In smart contract blockchains, such as Ethereum [25], Cardano [17] and Tezos [12], *Maximal Extractable Value* (MEV) is any type of excess profit a block producer can obtain by adding, ordering, or censoring transactions [6]. In current smart-contract blockchains, MEV constitutes an integral source of concern. The reason is that even though MEV is produced by the economic activity of users (MEV generators), in most cases, the extracted amount goes to other agents of the system (MEV extractors). Resolving this tension is far from straightforward. Extreme solutions, in which all MEV goes to block producers, are shown to adversely affect the behaviour of the opposite group and end up compromising participation and system security [5, 6, 22].

Hence, the question of how to share the additional revenue between these two groups, i.e., users and block producers, constitutes a central problem in current blockchain research and practice [9, 11]. The current debate around MEV involves two main schools of thought. The first is the *anti-MEV* approach, which states that MEV is harmful and its exploitation must be prevented or mitigated [14–16]. The second is the *pro-MEV* approach which argues that, despite its negative externalities, MEV is inevitable in permissionless blockchains, and sometimes it could even improve the quality of routing transactions [9, 18] and could also alleviate some inflationary pressure that is required to incentivize staking [5].

Our Approach and Results. In this work, we take a neutral approach towards MEV and propose a mechanism to balance the two extreme positions by enshrining MEV sharing in the protocol design. The key element to achieve this is a variable MEV *extraction rate* that determines the fraction of MEV that is retained by block producers, with the rest going back to users.

The aim of the MEV extraction rate is to balance the participation of users and block producers, expressed in monetary terms, to a predetermined target ratio and is updated after every block following a dynamic update rule. The intensity of the updates is regulated by an *adjustment parameter* that is part of the design space of the mechanism. In simple terms, the rule increases (decreases, respectively) the MEV extraction rate if the ratio of block producer/user participation is lower (higher, respectively) than desired. We use as a proxy of the MEV extracted the winning bid of the auction held for the creation of the last block. The estimation of MEV is not *the* focus of our model. In any case, current research suggests that winning bids in MEV-boost auctions [8, 10] or experimental methods [1, 2, 13, 22] provide accurate estimates or tight lower bounds to the actual MEV. This dynamic update rule is inspired by the design principles of EIP-1559 that have proven successful in regulating transaction fee markets under similar conditions [19, 20, 23, 24].[1] Our work is also inspired by the trade-off between the goals of users (bidders) and block producers (auctioneers) as studied in the context of conventional auctions [7, 21].

Our objective in this paper is to study the evolution and performance of the above mechanism. In particular, our motivating questions are the following: (1) can a protocol-determined, dynamically-updated MEV extraction rate balance the conflicting participation incentives of users and block producers, and (2) can the design principles of EIP-1559 be useful in accomplishing this task? Our findings provide significant evidence that we can answer both questions affirmatively.

2 MODEL

We consider a two-sided market consisting of users (or MEV generators) who submit transactions on the one side and miners (or MEV extractors) who process these transactions on the other side. Here, the term *miners* is used as a general term to describe all MEV extractors including proposers, builders, searchers. The two sides are described in terms of their total participating stake, denoted by U for users and by M for miners, which correspond to the maximum potential participation of users and miners, respectively, measured in monetary terms (transaction volume for users and locked stake for miners) during the time-period under consideration.

The participation of users and miners in the market depends on the current MEV extraction rate, denoted by $\lambda \in [0, 1]$. Higher (lower) values of λ indicate more (less) aggressive extraction by miners. Equivalently, one may think of $1 - \lambda$ as the fraction of MEV that is returned to users. Each user and miner has a certain tolerance on λ. Thus, if a user (miner) sees an MEV extraction rate higher (lower) than what they can tolerate, they do not participate in the market. The *tolerance distributions* of users and miners are denoted by $F(\lambda)$ and $G(\lambda)$, respectively. Based on the above, the users that participate in the market for a given λ are $U \cdot \bar{F}(\lambda)$, where $\bar{F}(\lambda) := 1 - F(\lambda)$ and the miners are $M \cdot G(\lambda)$. We assume that the support of F, G is included in $[0, 1]$ and that both F, G are strictly increasing and differentiable.

To incorporate the MEV extraction rate as part of the protocol design space, we make the following design choices:

- The MEV extraction rate is dynamically updated after every block. This generates a sequence of MEV extraction rates, $(\lambda_t)_{t\geq 0}$, where t indicates the block height (time).
- The intensity of the updates between consecutive blocks is regulated by a parameter d that can be chosen by the designer.
- The designer can set a desired (optimal) balance between users and miners in the market denoted by T (target). This means that the designer is seeking to find a λ^* such that $U \cdot \bar{F}(\lambda^*) = T \cdot M \cdot G(\lambda^*)$.
- The boundary MEV extraction rates of $\lambda = 0$ and $\lambda = 1$ correspond to steady states in which the two-sided market collapses to having either only miners ($\lambda = 1$) or only users ($\lambda = 0$).

Based on the above desiderata, we consider the following dynamic update rule to govern the evolution of the MEV extraction rates, λ_t:

$$\lambda_{t+1} := \lambda_t + d\lambda_t(1 - \lambda_t) \cdot (U \cdot \bar{F}(\lambda_t) - T \cdot M \cdot G(\lambda_t)) \quad \text{(MEV-D)}$$

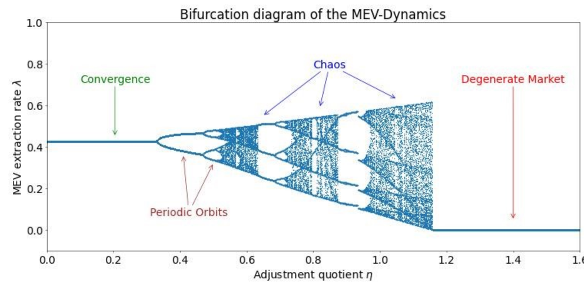

Figure 1: Our analysis of the long-term evolution of (MEV-D) **shows that the system exhibits one of the following behaviors depending on the value of the adjustment parameter: (i) *low* intensities: convergence to an optimal MEV extraction rate that achieves the target participation ratio, (ii) *intermediate* intensities: periodic behavior or provable chaos or (iii) *large* intensities: collapse to extraction rates of either 0 or 1 in which case one of the two groups of this two-sided economy abandons the system. Interested readers can refer to [3] for the full version of this article.**

3 CONCLUSION

Our work establishes the first to our knowledge dynamic framework for the integral problem of MEV sharing. Without arguing on whether MEV is desirable or not, this framework treats MEV as an unavoidable phenomenon of current blockchains and enables the market to decide dynamically on its exact level through a protocol-based implementation. Our work can be considered as a baseline framework for dynamic redistribution mechanisms, where a designer can add more granular definitions of λ, by accounting for different factors, such as congestion, bandwidth, etc. From a practical perspective, our results suggest that dynamic MEV extraction can achieve targets set by the protocol and can, thus, inform the ongoing discussion about actively enshrining MEV extraction in protocol designs.

ACKNOWLEDGMENTS

This research was supported in part by the National Research Foundation, Singapore and DSO National Laboratories under its AI Singapore Program (AISG Award No: AISG2-RP-2020-016), grant PIESGP-AI-2020-01, AME Programmatic Fund (Grant No.A20H6b0151) from A*STAR.

[1] It is worth highlighting that to measure deviations from its target and to adjust its updates accordingly, EIP-1559 uses as (on-chain) proxy of current demand the size of the last block [4].

REFERENCES

[1] K. Babel, P. Daian, M. Kelkar, and A. Juels. 2023. Clockwork Finance: Automated Analysis of Economic Security in Smart Contracts. In *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, Los Alamitos, CA, USA, 2499–2516. https://doi.org/10.1109/SP46215.2023.10179346

[2] M. Bartoletti, J.H-y. Chiang, and A. Lluch Lafuente. 2022. Maximizing Extractable Value from Automated Market Makers. In *Financial Cryptography and Data Security*, I. Eyal and J. Garay (Eds.). Springer International Publishing, Cham, 3–19. https://doi.org/10.1007/978-3-031-18283-9_1

[3] P. Braga, G. Chionas, S. Leonardos, P. Krysta, G. Piliouras, and C. Ventre. 2024. On the Redistribution of Maximal Extractable Value: A Dynamic Mechanism. arXiv:2402.15849 [cs.GT]

[4] V. Buterin, E. Conner, R. Dudley, M. Slipper, I. Norder, and A. Bakhta. 2019. EIP-1559: Fee market change for ETH 1.0 chain. https://eips.ethereum.org/EIPS/eip-1559

[5] T. Chitra and K. Kulkarni. 2022. Improving Proof of Stake Economic Security via MEV Redistribution. In *Proceedings of the 2022 ACM CCS Workshop on Decentralized Finance and Security* (Los Angeles, CA, USA) *(DeFi'22)*. Association for Computing Machinery, New York, NY, USA, 1–7. https://doi.org/10.1145/3560832.3564259

[6] P. Daian, S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, L. Breidenbach, and A. Juels. 2020. Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, USA, 910–927. https://doi.org/10.1109/SP40000.2020.00040

[7] I. Diakonikolas, C. Papadimitriou, G. Pierrakos, and Y. Singer. 2012. Efficiency-Revenue Trade-Offs in Auctions. In *Automata, Languages, and Programming*, A. Czumaj, K. Mehlhorn, A. Pitts, and R. Wattenhofer (Eds.). Springer, Berlin, Heidelberg, 488–499. https://doi.org/10.1007/978-3-642-31585-5_44

[8] Flashbots. 2022. MEV-Boost. https://boost.flashbots.net/

[9] Flashbots. 2022. The Future of MEV is SUAVE. https://writings.flashbots.net/the-future-of-mev-is-suave/

[10] Flashbots. 2023. MEV-Explore. https://explore.flashbots.net/

[11] Flashbots. 2023. MEV-Share: programmably private orderflow to share MEV with users. https://collective.flashbots.net.

[12] L.M. Goodman. 2014. Tezos—a self-amending crypto-ledger White paper. https://tezos.com/whitepaper.pdf

[13] L. Heimbach and R. Wattenhofer. 2022. Eliminating Sandwich Attacks with the Help of Game Theory. In *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security* (Nagasaki, Japan) *(ASIA CCS '22)*. Association for Computing Machinery, New York, NY, USA, 153–167. https://doi.org/10.1145/3488932.3517390

[14] M. Kelkar, S. Deb, and S. Kannan. 2022. Order-Fair Consensus in the Permissionless Setting. In *Proceedings of the 9th ACM on ASIA Public-Key Cryptography Workshop* (Nagasaki, Japan) *(APKC '22)*. Association for Computing Machinery, New York, NY, USA, 3–14. https://doi.org/10.1145/3494105.3526239

[15] M. Kelkar, S. Deb, S. Long, A. Juels, and S. Kannan. 2021. Themis: Fast, Strong Order-Fairness in Byzantine Consensus. Cryptology ePrint Archive, Paper 2021/1465. https://eprint.iacr.org/2021/1465

[16] M. Kelkar, F. Zhang, S. Goldfeder, and A. Juels. 2020. Order-Fairness for Byzantine Consensus. In *Advances in Cryptology – CRYPTO 2020: 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17–21, 2020, Proceedings, Part III* (Santa Barbara, CA, USA). Springer-Verlag, Berlin, Heidelberg, 451–480. https://doi.org/10.1007/978-3-030-56877-1_16

[17] A. Kiayias, A. Russell, B. David, and R. Oliynykov. 2017. Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. In *Advances in Cryptology – CRYPTO 2017*, Jonathan Katz and Hovav Shacham (Eds.). Springer International Publishing, Cham, 357–388.

[18] K. Kulkarni, T. Diamandis, and T. Chitra. 2023. Towards a Theory of Maximal Extractable Value I: Constant Function Market Makers. arXiv:2207.11835 [cs.GT]

[19] S. Leonardos, B. Monnot, D. Reijsbergen, S. Skoulakis, and G. Piliouras. 2021. Dynamical Analysis of the EIP-1559 Ethereum Fee Market. In *Proceedings of the 3rd ACM Conference on Advances in Financial Technologies* (Arlington, Virginia) *(AFT '21)*. Association for Computing Machinery, New York, NY, USA, 114–126. https://doi.org/10.1145/3479722.3480993

[20] S. Leonardos, D. Reijsbergen, B. Monnot, and G. Piliouras. 2022. Optimality Despite Chaos in Fee Markets. Financial Cryptography and Data Secutiry '23, Springer International Publishing. https://fc23.ifca.ai/preproceedings/127.pdf

[21] A. Likhodedov and T. Sandholm. 2004. Mechanism for Optimally Trading Off Revenue and Efficiency in Multi-unit Auctions. In *Agent-Mediated Electronic Commerce V. Designing Mechanisms and Systems*, P. Faratin, D. C. Parkes, J. A. Rodríguez-Aguilar, and W. E. Walsh (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 92–108. https://doi.org/10.1007/978-3-540-25947-3_6

[22] K. Qin, L. Zhou, and A. Gervais. 2022. Quantifying Blockchain Extractable Value: How dark is the forest?. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, Los Alamitos, CA, USA, 198–214. https://doi.org/10.1109/SP46214.2022.9833734

[23] T. Roughgarden. 2020. Transaction Fee Mechanism Design for the Ethereum Blockchain: An Economic Analysis of EIP-1559. arXiv:2012.00854 [cs.GT]

[24] T. Roughgarden. 2021. Transaction Fee Mechanism Design. In *Proceedings of the 22nd ACM Conference on Economics and Computation* (Budapest, Hungary) *(EC '21)*. Association for Computing Machinery, New York, NY, USA, 792. https://doi.org/10.1145/3465456.3467591

[25] V.Buterin. 2013. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.