Revisiting the Primitives of Transaction Fee Mechanism Design*

AADITYAN GANESH, Princeton University, USA
CLAYTON THOMAS, Microsoft Research, USA
S. MATTHEW WEINBERG, Princeton University, USA

Transaction Fee Mechanism Design—a rapidly-evolving research agenda initiated by Roughgarden [2021]—studies auctions run by untrusted miners for transaction inclusion in a blockchain. Under previously-considered desiderata, an auction is considered 'good' if, informally-speaking, each party (i.e., the miner, the users, and coalitions of both miners and users) has no incentive to deviate from the fixed and pre-determined protocol. In other words, previous works posit that a 'good' auction should be 'simple for users', 'simple for miners', and 'resistant to collusion'.

In this paper, we propose an alternative desiderata for Transaction Fee Mechanisms. We say that a TFM is *off-chain influence proof* when the miner cannot achieve additional revenue by running a separate auction off-chain. While the previously-highlighted mechanism EIP-1559 satisfies previously-considered desiderata (simplicity for miners and users, as well as collusion resistance), we show that it *does not* satisfy off-chain influence proof. Intuitively, this holds because a Bayesian revenue-maximizing miner can strictly increase profits by threatening to censor any bids that do not transfer a tip directly to the miner off-chain. We prove a strong impossibility result: no mechanism satisfies all previously-considered properties along with off-chain influence proof. On the other hand, we reconsider the Cryptographic (multi-party computation assisted) Second Price Auction mechanism [Shi et al., 2023]. We argue that the space of TFMs can be naturally expanded to solicit an input from the miner, for example, by asking them to set the reserve price of the auction. We show that in this model, the cryptographic second price auction satisfies simplicity for users and miners and off-chain influence proof, since it allows any Bayesian miner to maximize their revenue by posting an optimal reserve price.

CCS Concepts: • **Theory of computation** → **Algorithmic mechanism design**; • **Applied computing** → *Online auctions.*

Additional Key Words and Phrases: Transaction Fee Mechanism Design, Blockchain, Decentralized Finance, Simple Auctions

ACM Reference Format:
Aadityan Ganesh, Clayton Thomas, and S. Matthew Weinberg. 2024. Revisiting the Primitives of Transaction Fee Mechanism Design. In *The 25th ACM Conference on Economics and Computation (EC '24), July 8–11, 2024, New Haven, CT, USA.* ACM, New York, NY, USA, 1 page. https://doi.org/10.1145/3670865.3673621

Acknowledgments

This work is supported by a Ripple UBRI grant, and an NSF CAREER Award CCF-1942497. The authors also thank anonymous reviewers for valuable feedback during the review process.

*The full version of the paper can be found in https://aadityanganesh.in/revisiting-the-primitives-of-transaction-fee-mechanism-design/.

Authors' Contact Information: Aadityan Ganesh, aadityanganesh@princeton.edu, Princeton University, Princeton, NJ, USA; Clayton Thomas, thomasclay95@gmail.com, Microsoft Research, Boston, MA, USA; S. Matthew Weinberg, smweinberg@princeton.edu, Princeton University, Princeton, NJ, USA.

EC '24, July 8–11, 2024, New Haven, CT, USA

ACM ISBN 979-8-4007-0704-9/24/07
https://doi.org/10.1145/3670865.3673621