# Transaction Fee Mechanism Design

TIM ROUGHGARDEN
Columbia University

Demand for blockchains such as Bitcoin and Ethereum is far larger than supply, necessitating a mechanism that selects a subset of transactions to include “on-chain” from the pool of all pending transactions. EIP-1559 is a proposal to make several tightly coupled changes to the Ethereum blockchain’s transaction fee mechanism, including the introduction of variable-size blocks and a burned base fee that rises and falls with demand. These changes are slated for deployment in Ethereum’s “London fork,” scheduled for late summer 2021, at which point it will be the biggest economic change made to a major blockchain to date. This short note provides an overview of recent work by the author that formally investigates and compares the incentive guarantees offered by Ethereum’s current transaction fee mechanism and the new mechanism proposed in EIP-1559.

Categories and Subject Descriptors: F.0 [**Theory of Computation**]: General

General Terms: Economics; Security; Theory

Additional Key Words and Phrases: Mechanism Design, Blockchain, Cryptocurrencies, Ethereum

## 1. OVERVIEW

### 1.1 Background

Real estate on a major blockchain is a scarce resource. For example, Bitcoin [Nakamoto 2008] and Ethereum [Buterin 2013], the two biggest blockchains, process roughly 5 and 15 transactions per second on average, respectively. Demand for these blockchains is far larger, necessitating a mechanism that selects a subset of transactions to include “on-chain” from the pool of all submitted transactions.

Most blockchain protocols, including Bitcoin and Ethereum, employ a pay-as-bid transaction fee mechanism. Every transaction is submitted with a bid (in the blockchain’s native currency), the miner of a block decides which transactions should be included in it, and upon publication of that block, the bid of each included transaction is transferred from its creator to the miner. We follow blockchain convention and refer to this mechanism as a *first-price auction (FPA)*.

FPAs are natural enough and are currently the dominant paradigm in blockchain protocols, but are they really the best we can do? For example, could a different transaction fee mechanism offer stronger incentive guarantees?

These questions are addressed at length in a recent paper by the author [Roughgarden 2021]; this short note provides a brief overview of its primary contributions.[1]

### 1.2 Transaction Fee Mechanism Design

The first goal of the paper [Roughgarden 2021] is to frame the questions above as a mechanism design problem, while taking into account the many idiosyncrasies

[1]See also Roughgarden [2020] for a longer report written for a general audience.

Author’s email address: tim.roughgarden@gmail.com

of the blockchain setting relative to more traditional applications of the field. For example:

(1) The miner of a block has dictatorial control over its contents, and in particular may deviate from the allocation rule intended by the protocol designer.

(2) The miner of a block can costlessly include fake transactions that are indistinguishable from real transactions.

(3) Payments should be computable from "on-chain" data, which typically discloses no information about losing bids.

(4) Miners and users can easily collude off-chain to manipulate a transaction fee mechanism.

The sequential and repeated nature of the blockchain setting also offers some advantages to the mechanism designer. For example:

(5) The choice of mechanism (such as a reserve price) for a given block could be informed by the (publicly visible) outcomes for previous blocks.

(6) Revenue from a block need not be transferred directly to the block's miner and could instead be redirected, for example to the miners of future blocks.

### 1.3 Assessing EIP-1559

In addition to its scientific interest, the problem of transaction fee mechanism design is central to a debate that is currently raging over the future of the Ethereum blockchain (see e.g. Beiko [2020]). EIP-1559 is the name of a proposal, developed by Ethereum's founder [Buterin 2018], that suggests several tightly coupled changes to the transaction fee mechanism (which is currently an FPA), including the introduction of variable-size blocks and a burned "base fee" that acts as a reserve price and rises and falls with demand.[2] (See Roughgarden [2021] for a mathematical description of the proposed mechanism.) While not without critics, this mechanism is slated for deployment in Ethereum's "London fork," scheduled for late summer 2021, at which point it will be the biggest economic change made to a major blockchain to date. The second goal of the paper [Roughgarden 2021] is to formally investigate the game-theoretic properties of the transaction fee mechanism proposed in EIP-1559 and identify a precise sense in which it has superior incentive guarantees to the current FPA.[3]

### 1.4 Alternative Designs

The third goal of the paper is to explore two designs that offer benefits incomparable to those of the mechanism proposed in EIP-1559. One design—the tipless mechanism—strengthens the incentive-compatibility guarantee for users while sacrificing some resistance to off-chain collusion by miners and users. The second—the $\ell$-smoothed mechanism—pays base fee revenues forward rather than burning them, thereby favoring miners relative to passive holders of Ethereum's currency.

[2] "EIP" stands for "Ethereum improvement proposal."

[3] The framework proposed in this report can also be used to assess other transaction fee mechanisms that have been proposed in the literature, such as those in Basu et al. [2019] and Lavi et al. [2019].

## 2. A TASTE OF THE RESULTS

The paper [Roughgarden 2021] proposes three types of incentive-compatibility guarantees for transaction fee mechanisms: one for the creators of transactions; one for miners; and one for cartels of users and miners.

(1) *Dominant-strategy incentive-compatibility (DSIC).* This condition states that users should be incentivized to bid their true valuation for transaction inclusion.
(2) *Incentive-compatibility for myopic miners (MMIC).* This condition states that a miner of a block maximizes its revenue from that block by following the intended allocation rule.
(3) *OCA-proofness.* This condition states that there is never a way for a miner of a block to collude with the creators of outstanding transactions that strictly increases the cartel's joint utility. ("OCA" stands for "off-chain agreement.")

FPAs are, of course, not DSIC. The VCG mechanism is not MMIC, as a miner can typically boost its revenue under that mechanism through the creation and inclusion of fake transactions. Still other natural mechanism formats fail OCA-proofness. One of the main results in Roughgarden [2021] clarifies the extent to which the transaction fee mechanism proposed in EIP-1559 satisfies these incentive-compatibility guarantees:

**Theorem (Informal):** The transaction fee mechanism proposed in EIP-1559 is MMIC and OCA-proof, and is DSIC outside of periods of rapidly increasing demand.

When there is a sudden and sharp increase in demand for the Ethereum blockchain, the transaction fee mechanism proposed in EIP-1559 effectively reverts to a FPA while the mechanism's internally computed base fee increases to an appropriate level. An interesting open question is whether there is a transaction fee mechanism that always satisfies all three incentive-compatibility guarantees.

## 3. CONCLUSION

The work described in Roughgarden [2020; 2021] is only the tip of the iceberg for applications of mechanism design to blockchain protocol design, and there remain many opportunities for the SIGecom community to shape the evolution of the next generation of blockchains.

### REFERENCES

Basu, S., Easley, D., O'Hara, M., and Sirer, E. G. 2019. Towards a functional fee market for cryptocurrencies. arXiv:1901.06830. URL: https://arxiv.org/pdf/1901.06830.pdf.

Beiko, T. 2020. EIP-1559 community outreach report. URL: https://medium.com/ethereum-cat-herders/eip-1559-community-outreach-report-aa18be0666b5.

Buterin, V. 2013. Ethereum: A next-generation smart contract and decentralized application platform. Unpublished white paper. URL: https://ethereum.org/en/whitepaper/.

Buterin, V. 2018. Blockchain resource pricing. URL: https://ethresear.ch/uploads/default/original/2X/1/197884012ada193318b67c4b777441e4a1830f49.pdf.

Lavi, R., Sattath, O., and Zohar, A. 2019. Redesigning Bitcoin's fee market. In *Proceedings of the World Wide Web Conference (WWW)*. 2950–2956. URL: https://arxiv.org/pdf/1709.08881.pdf.

Nakamoto, S. 2008. Bitcoin: A peer-to-peer electronic cash system. Unpublished white paper. URL: https://bitcoin.org/bitcoin.pdf.

Roughgarden, T. 2020. Transaction fee mechanism design for the Ethereum blockchain: An economic analysis of EIP-1559. arXiv:2012.00854. URL: https://arxiv.org/pdf/2012.00854.pdf.

Roughgarden, T. 2021. Transaction fee mechanism design. In *Proceedings of the 22nd ACM Conference on Economics and Computation (EC)*. To appear.