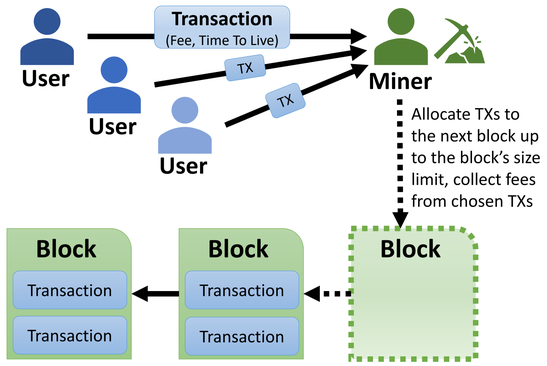
Greedy Transaction Fee Mechanisms for (Non-)myopic Miners

Yotam Gafni — Technion
Aviv Yaish — The Hebrew University

Transaction Fee Mechanisms (TFMs). Cryptocurrency users can create transactions (TXs) to transfer funds between each other and can incentivize quick processing of their TXs by including a *fee*, and specifying the TXs' *time to live*, after which they are no longer valid. The first miner to process a valid TX and allocate it to a block can **collect its fees** according to the revenue function of the cryptocurrency's TFM.



Bitcoin's TFM is pretty good. Existing literature has shown Bitcoin's TFM is not optimal in some senses, for example due to not being dominant strategy incentive compatible for users. We show that when relaxing this requirement to a Bayesian Incentive Compatibility (BIC) one, **Bitcoin's TFM performs quite well**, thus circumventing previous impossibility results.

Definition *(Pay-As-Bid Greedy Auction)*. In PABGA, miners "greedily" allocate TXs with the highest fees for the next block. Each TX pays its fee to the first miner to include it in a block, as in Bitcoin's TFM.

Theorem 1 (informal). PABGA with n bidders and B items **has at least $\frac{n-B}{n}$ of the revenue of the optimal auction** of B identical items.

Theorem 2 (informal). PABGA is **revenue optimal** in the class of ex-post budget balanced and individually rational block-size limited TFMs.

Claim 8 (informal). PABGA with n uniform bidders and **has a near-optimal Bayesian Nash equilibrium**.

Bitcoin's transaction fee mechanism is **pretty good!**

It is **Bayesian incentive compatible** for users, **incentive compatible** for myopic miners, **resistant** to user-miner collusion, and approximately **revenue & welfare optimal**.

If transactions can expire, non-myopic miners **can do better** than greedily allocating them solely by fees.

The impossible may be possible! Collusion notions previously conjectured to be equivalent **are different**, meaning that impossibility results relying on the equivalence are still open.

https://arxiv.org/abs/2210.07793

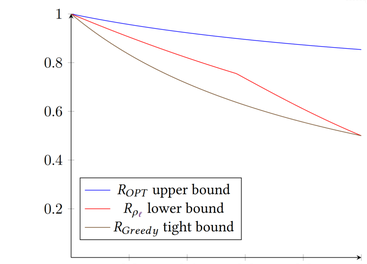
Non-myopic miners. Previous works focused on myopic miners. **We advance the literature by studying non-myopic miners** and the performance of non-myopic allocation rules of TXs to blocks which account for miners having some probability of mining more blocks in the future. We assume miners discount revenue from future blocks by a factor of λ per block.

Definition (*competitive ratio*). The competitive ratio of an allocation function x, denoted as R_x, is the ratio between its revenue and the revenue of the optimal function, when facing the worst possible adversarial user.

Lemma 2 (informal). The competitive ratio of the Greedy allocation function is $\frac{1}{1+\lambda}$.

Definition (l*-immediacy-biased allocation*). The allocation rule which picks the highest-fee TX with a TTL that is larger than 1 if its fee is at least l times higher than the fee of the highest-fee TX with a TTL of 1. If the fee ratio is less than l, it picks the highest-fee TX with a TTL of 1. We denote this rule as ρ_l.

Lemma 4 (informal). The competitive ratio of ρ_l with $l = \frac{1}{2}(\lambda + \sqrt{\lambda^2+4})$ is bounded by $\geq \frac{1}{\min\{\frac{1}{l'}, \frac{1}{1+\lambda^2}\}}$.



A comparison of the competitive ratio performance of various allocation rules.

Corollary 2 (informal). Any BIC mechanism that implements the greedy allocation rule has a social welfare of at least $\frac{1}{1+\lambda}$ of the optimum.

The impossible may be possible. Previous works have proved that TFMs cannot satisfy a certain desiderata of "good" features. We disprove the conjecture used to prove this.

Claim 4 (informal). **The OCA and 1-SCP notions of TFM collusion are not equivalent**, for example when using the third-price TFM. Intuitively, OCA compares the coalition of a miner and users to the coalition of winning users according to the TFM, whereas SCP compares a coalition to itself.

Acknowledgments. Yotam Gafni was supported by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (Grant No. 740435). Aviv Yaish was supported by a grant from the Ministry of Science & Technology.