No Transaction Fees? No Problem! Achieving Fairness in Transaction Fee Mechanism Design (Supplementary Material)

Anonymous Author(s)
Submission Id: 312

ACM Reference Format:
Anonymous Author(s). 2024. No Transaction Fees? No Problem! Achieving Fairness in Transaction Fee Mechanism Design (Supplementary Material). In *Proc. of the 23rd International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2024), Auckland, New Zealand, May 6 – 10, 2024,* IFAAMAS, 4 pages.

A PROOFS

A.1 Proof of Remark 1

Proof. Consider the following example where each transaction is of the same size. Let $n = 5$ such that the current block B_k can hold up to 8 transaction. Further, we have $\alpha = 3/4$. The miner must add (any) 2 transactions to the $1-\alpha$ section first, before greedily adding transactions to the α section. Whichever transactions from M the miner chooses to add to the $1-\alpha$ section, it can strictly increase its utility by adding 2 fake transactions instead. That is, by adding these fake transactions, the miner can add the real transactions of M to the α section. Thus, BitcoinF's allocation rule does not satisfy MIC. □

A.2 Proof of Claim 1

Proof. W.l.o.g., let the optimal set of bids (sorted in non-decreasing order) which maximizes miner's utility in Eq. 3 with $p_t = b_t$ and $q_t = 0,\ \forall t$ be $\{b_1, \ldots, b_c\}$. Then with $\alpha = \frac{k}{c}$ s.t. $k \leq c$, we can write BitcoinZF's bid set as $\{b_1, \ldots, b_k\}$ (since the miner will maximize utility in the "α" section of the block). Observe that,

$$\frac{OPT}{u_m^{BZ}} = \frac{b_1 + \ldots + b_c}{b_1 + \ldots + b_k} = 1 + \frac{b_{c-k+1} + \ldots + b_c}{b_1 + \ldots + b_k}$$
$$\leq 1 + \frac{(c-k)b_k}{k \cdot b_k} \leq 1 + \frac{c}{k} - 1 \leq \frac{c}{k} = 1/\alpha.$$

This completes the claim. □

A.3 Proof of Theorem 1

Proof. Consider the following example. Let the transaction bid and size pair in the mempool be denoted by $\mathcal{P} = [(b_i, s_i)] = \{(10,10), (10,10), (5,10), (0,10), (0,10)\}$. If the block B_k can admit a total transaction size of 30, then the miner can maximize its utility from 3 by selecting the first three transactions in $\mathcal{P}$. That is, $\mathbf{x}^{TFM} = \{1,1,1,0,0\}$ with $u_m^{TFM} = 25$. This implies that $\Pr(t_4 \in B_k) = \Pr(t_5 \in B_k) = 0$, thus, ZTi is not satisfied. □

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.

A.4 Proof of Theorem 2

Without considering the inclusion of fake bids from the miner, i.e., $F = \emptyset$, we first write the optimization of BitcoinZF as follows:

$$\left.\begin{aligned} &\max_{\mathbf{x}^{BZ}} \sum_{i \in M} x_i^{BZ} \cdot p_i^{BZ}(\mathcal{H}, B_k) \cdot s_i \\ &\text{s.t.} \sum_{t \in M, b_t \neq 0} s_t \cdot x_t^{BZ}(\mathcal{H}, M) \leq C_\alpha \\ &\quad \sum_{t \in M, b_t = 0} s_t \cdot x_t^{BZ}(\mathcal{H}, M) = C_{1-\alpha} \text{ and} \\ &\quad x_t^{BZ}(\mathcal{H}, M) \in \{0,1\}, \forall t \in M. \end{aligned}\right\} \quad \text{(B1)}$$

To show that BitcoinZF satisfies Monotonicity, we have to show that by increasing its bid b_i, agent i's transaction t_i has a higher probability of getting accepted in B_k. Indeed, this is the case in BitcoinZF, since increasing b_i to $b_i + \epsilon$ s.t. $\epsilon > 0$, can only increase the probability of t_i's inclusion in B_k. This is because of the KNAPSACK definition from Eq. B1.

Furthermore, since the miner receives no utility from any transaction in the "$1-\alpha$" section, it can uniformly sample zero-fee transactions in this section. There is a subtle point here: the miner does not get any utility by adding these transactions to the $1-\alpha$ section. It can in effect leave the section empty or add its own transactions. However, since such deviations will not yield the miner any increase in utility, we can state that BitcoinZF satisfies ZTi.

A.5 Proof of Theorem 3

Proof. We first prove that STFM satisfies Monotonicity irrespective of the payment and burning rules.

For this, we must show that $\forall t_i, t_j \in M$ s.t. $t_i \neq t_j$ if $b_i > b_j$, $\Pr(t_i \in B_k) > \Pr(t_j \in B_k)$. We remark that $\mathbf{x}^{STFM}$ admits transactions with a distribution generated by applying the softmax function on the transactions in M (refer Algorithm 1).

For sampling the first transaction, the probability distribution is $\Pr(t_i \in B_k) = \frac{\exp(b_i/\gamma)}{\sum_{i' \in M} \exp(b_{i'}/\gamma)},\ \forall i \in M$. Trivially, we have $\frac{\exp(b_i/\gamma)}{\sum_{i'} \exp(b_{i'}/\gamma)} > \frac{\exp(b_j/\gamma)}{\sum_{i'} \exp(b_{i'}/\gamma)}$ if $b_i > b_j$ and $\gamma > 0$, implying STFM satisfies Monotonicity in this case. Next, w.l.o.g., we assume a transaction t_l was sampled. The re-generated probability distribution becomes, $\Pr(t_i \in B_k) = \frac{\exp(b_i/\gamma)}{\sum_{i' \in M \setminus \{l\}} \exp(b_{i'}/\gamma)},\ \forall i \in M \setminus \{l\}$. Still, we have $\frac{\exp(b_i/\gamma)}{\sum_{i'} \exp(b_{i' \in M \setminus \{l\}}/\gamma)} > \frac{\exp(b_j/\gamma)}{\sum_{i'} \exp(b_{i' \in M \setminus \{l\}}/\gamma)}$ if $b_i > b_j$ and $\gamma > 0$. That is, Monotonicity still holds. Along similar lines, we can show that Monotonicity holds for each sampling stage.

Trivially, we can also show that STFM satisfies Zero-fee Transaction Inclusion (ZTi). For each $t_i \in M$ with $b_i = 0$, we have

$\Pr(t_i \in B_k) = \frac{\exp(b_i/\gamma)}{\sum_{i' \in M} \exp(b_{i'}/\gamma)} = \frac{1}{\sum_{i' \in M} \exp(b_{i'}/\gamma)} > 0$, irrespective of the size of M.

□

A.6 Proof of Theorem 4

Proof. For the proof, we have to show that for any non-trivial payment rule, the intended allocation $\mathbf{x}^{STFM}$ in $\mathcal{T}^{STFM}$ is such that the miner has an incentive to deviate.

Given the mempool M, denote $Z \subset M$ as the set of all zero-fee transactions, i.e., $Z = \{t_i \mid t_i \in M \text{ and } b_i = 0\}$. For all game instances of $\mathcal{T}^{STFM}$ where the block B_k's size C is less than the size of the transactions in $M - Z$, we have $\Pr(t_i \in B_k) = 0, \forall t_i \in Z$. That is, the miner has no incentive to add transactions in Z to B_k. This is because as the payment rule is increasing with the transaction fees, the miner's utility from greedily adding transactions from $M - Z$ will be strictly greater than including even a single transaction from Z. □

A.7 Proof of Theorem 5

Proof. Denote C and N as the block size and mempool size, respectively. Let OPT denote miner's utility from Eq. 3 with $p_t = b_t$ and $q_t = 0$, $\forall t$ and u_m^{STFM} denote miner's utility for $\mathcal{T}^{STFM}$. Let M comprise n transactions with fees $\{b_i\}_{i=1}^n$. W.l.o.g, we consider $b_1 \geq b_2 \geq \ldots \geq b_n$. Let c denote the maximum number transactions in a block. The block-size is C and for simplification we assume that transactions are of the same size.[1]

Miner's optimal utility from Eq. 3 is: $OPT = \sum_{i=1}^{c} b_i$. Let X denote the utility from sampling one transaction from M using $\mathcal{T}^{STFM}$. Then, $\mathbb{E}[X] = \sum_{i=1}^{n} \Pr(t_i \in B_k) \cdot b_i$. Further, if X_i is the utility from i^{th} sampled transaction, (out of total c transactions present in a block), then the expected utility is given by

$$\mathbb{E}[u_m^{STFM}] = \mathbb{E}[\sum_{x=1}^{c} X_x] = |c| \sum_{i=1}^{n} b_i \Pr(t_i \in B_k).$$

We get the last equation using linearity of expectations. Therefore, the ratio of utilities is,

$$\frac{OPT}{\mathbb{E}[u_m^{STFM}]} = \frac{\sum_{i=1}^{c} b_i}{|c| \sum_{i=1}^{n} b_i \Pr(t_i \in B_k)}$$

For maximizing $\frac{OPT}{\mathbb{E}[u_m^{STFM}]}$ we need to maximize numerator and minimize denominator. This is achieved by taking $b_1 = b_2 = \ldots = b_c = b$ and $b_{c+1} = b_{c+2} = \ldots = b_n = 0$. That is,

$$\frac{OPT}{\mathbb{E}[u_m^{STFM}]} = \frac{c \cdot b}{c(\sum_{i=1}^{c} b \cdot \frac{e^{\frac{b}{\gamma}}}{n-c+c \cdot e^{\frac{b}{\gamma}}} + 0)}$$

$$\frac{OPT}{\mathbb{E}[u_m^{STFM}]} = \frac{n - c + c \cdot e^{\frac{b}{\gamma}}}{c \cdot e^{\frac{b}{\gamma}}} = \frac{n}{c} + 1 - e^{-\frac{b}{\gamma}}$$

Upper bound on utility-loss ($\frac{OPT}{\mathbb{E}[u_m^{STFM}]}$) is found when $b \to \infty$ and is equal to $\frac{n}{C} + 1$. □

[1] if N and C are large enough, then with very high probability, number of transactions n (or c) in a pool (or block) of size N (or C) will deviate from n (or c) negligibly. This observation follows from Chernoff bound.

A.8 Proof for Theorem 7

Proof. To show that the TFMs satisfy MIC, we remark that the selecting between the optimal and zero-fee transactions (refer Algorithm 2) is carried out by the blockchain in a trusted manner (Eq. 8). As the miner has no control over the random outcome of $O(\text{Hash}(B_k), \phi)$ (Remark 5), its strategy involves (i) optimally selecting the transactions and (ii) either adding the zero-fee transactions or keeping them empty. For (i), we know that both EIP-1559 and FPA payment rules satisfy MIC. For (ii), both strategies result in zero utility for the miner; that is, rTFM is MIC for the miner. □

A.9 Proof for Theorem 8

Proof. By construction, $\mathbf{x}^{\text{rTFM}}$ implies that (i) with probability $1 - \phi$, the miner optimally selects transactions (Eq. 3) satisfying Monotonicity and (ii) with probability ϕ, the blockchain selects zero-fee transactions to be included in the block. □

B SOFTMAX TFM: TUNING γ FOR INCREASED MINER UTILITY

We observe that satisfying our fairness notions with STFM reduces a miner's utility. Naturally, each miner of a block will prefer to increase its utility. We now discuss the role of the temperature parameter γ in improving the miner's utility while simultaneously retaining the fairness guarantees.

STFM at $\gamma \to \infty$. Observe that, from (6), as γ increases, the softmax probability distributions tend toward the uniform distribution. When $\gamma \to \infty$, the distribution becomes Uniform, i.e., all transactions are included with the same probability. That is, at $\gamma \to \infty$, STFM does not satisfy Monotonicity, and the miner's utility loss is at its maximum.

STFM at $\gamma \to 0$. In contrast to the previous scenario, when $\gamma \to 0$, STFM's allocation mimics the optimal allocation from (3). That is, at $\gamma \to 0$, STFM does not satisfy ZTi, and the miner's utility loss is approximately zero.

An Improved Trade-off. In Appendix C.2, we show how to derive an ideal value of $\gamma^\star$ with regards to CoF and number of zero-fee transactions included. More concretely, we first derive the expression of the ratio of the probability of the optimal set of transactions (from Eq. 3) being included to the block with probability of some $\alpha \in [0, 1]$ fraction of block comprising transactions with zero-fees (say $\frac{pr_{\text{CoF}}}{pr_{\text{ZF}}}$). Then, we solve for $\gamma^\star$ s.t. $\frac{pr_{\text{CoF}}}{pr_{\text{ZF}}} \leq \phi$. Here, ϕ is a target ratio that the miner can choose. E.g., if $\phi = 2$, the miner weighs the probability of accepting the optimal transactions twice more than accepting an α fraction of zero-fee transactions.

C SIMULATIONS

We now empirically validate STFM's performance with regards to the loss in miner's utility and the fraction of zero-fee transactions included in the block.

C.1 Experimental Setup & Performance Measures

To simulate STFM, we need to configure the size of the mempool M, block size C, temperature parameter γ, each agent's transaction fees

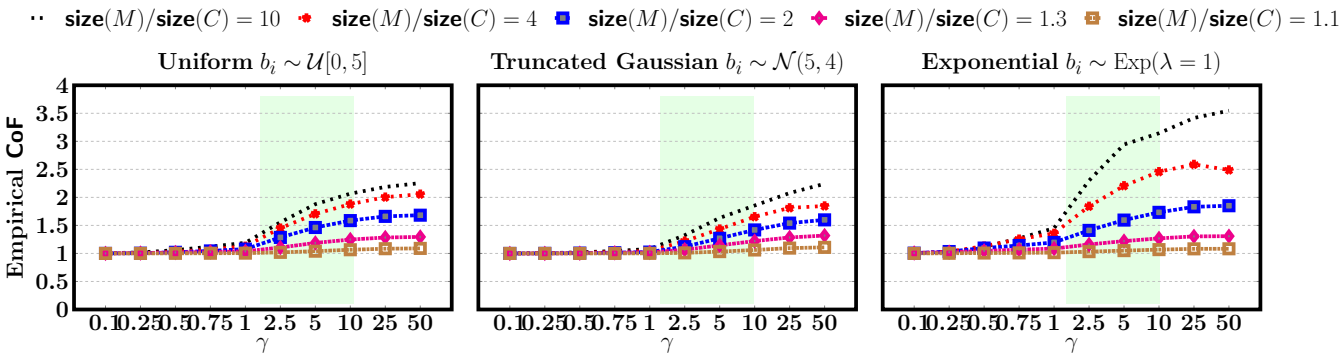

Figure C1: Empirical CoF for the distributions: (D1) Uniform, (D2) Truncated Gaussian and (D3) Exponential.

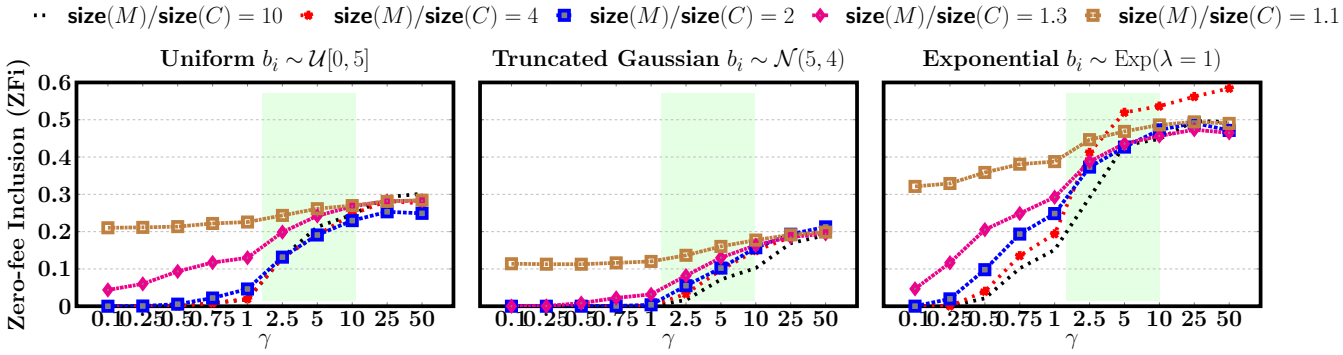

Figure C2: Zero-fee Inclusion (ZFi) for the distributions: (D1) Uniform, (D2) Truncated Gaussian and (D3) Exponential.

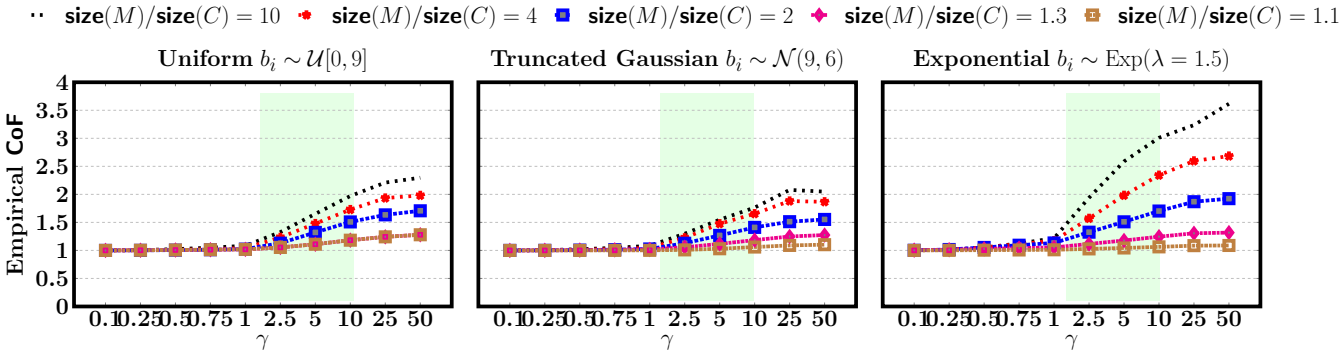

Figure C3: Empricial CoF: Miner's Utility Ratio for the distributions: (D1) Uniform, (D2) Truncated Gaussian and (D3) Exponential

and their sizes. In our experiments, we vary the ratio of the sizes of the mempool and block size, say $\frac{\text{size}(M)}{\text{size}(C)}$, in the set $\{1.1, 1.3, 2, 4, 10\}$ and $\gamma \in [0.1, 50]$. To concretely mimic all possible real-world scenarios, for each $t_i \in M$, the agent i samples its bid b_i from the following three distributions[2]: (D1) Uniform, i.e., $b_i \sim \mathcal{U}[0,5]$, (D2) Truncated Gaussian, i.e., $b_i \sim \mathcal{N}(5,4)$, and (D3) Exponential, i.e., $b_i \sim \text{Exp}(\lambda = 1)$.

Likewise, for each $t_i \in M$, the agent i samples the transaction's size $s_i \sim \text{Exp}(\lambda = 1)$. This choice is reasonable since smaller transactions (e.g., payer-payee token transfer) are more common than

[2]We observe similar trends for other distribution parameters.

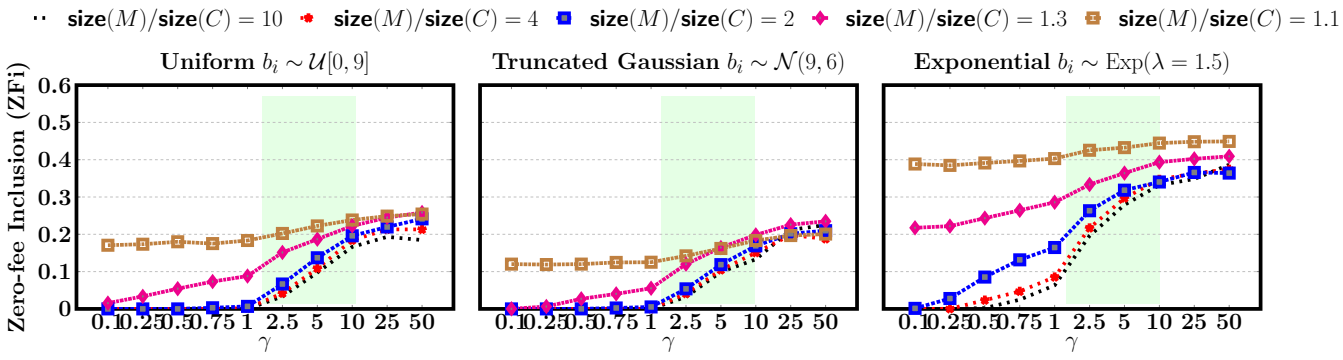

Figure C4: Zero-fee Inclusion (ZFi) for the distributions: (D1) Uniform, (D2) Truncated Gaussian and (D3) Exponential

larger transactions (e.g., smart contract deployment). To measure STFM's performance, we also define the following measures.

(1) Empirical CoF. This is the ratio of miner's utility by greedily adding transactions to the block with the utility from STFM's allocation. Smaller the CoF, the better.
(2) Zero-fee Inclusion (ZFi). ZFi is the ratio of the size of zero-fees transactions in the block with the total size of all the transactions in the block.

For each $\frac{\text{size}(M)}{\text{size}(C)}$ and γ, we sample the agent's bids based on D1, D2 and D3. We simulate the resulting game instances 100 times and report the average CoF and ZFi values. The codebase is available with the accompanying supplement.

C.2 Results & Discussion

Figure C1 and Figure C2 depict our results. Details follow.

Empirical CoF: Miner's Utility Ratio. We first discuss the change in CoF with varying γs and $\frac{\text{size}(M)}{\text{size}(C)}$ values for D1, D2 and D3. For all three distributions, we observe a consistent increase in CoF as γ increases, i.e., $\gamma \uparrow \implies u_m \downarrow$. For $\gamma \in (0, 1)$, CoF is < 1.5 implying that miner's utility drop is > 0.67 times OPT. For $\gamma \geq 1$ CoF increases, but remains < 2.5 for D1, D2 and < 3.5 for D3. E.g., for $\gamma = 5$ and the worst-case value of $\frac{\text{size}(M)}{\text{size}(C)} = 10$, CoF values are 1.88 (D1), 1.63 (D2) and 2.93 (D3).

Furthermore, one way to interpret decreasing $\frac{\text{size}(M)}{\text{size}(C)}$ is an increase in the block size, $\text{size}(C)$. As $\text{size}(C) \to \text{size}(M)$, the randomized allocation adopted with STFM plays a lesser role as the block gets large enough to accommodate most transactions. From Figure C1, we see that decreasing $\frac{\text{size}(M)}{\text{size}(C)}$ decreases CoF, i.e., an increase in the miner's utility.

Zero-fee Inclusion (ZFi). We empirically show that STFM admits zero-fee transactions with Figure C2. For varying γ, we plot the ratio of the size of zero-fees transactions included in the block with the total block size (aka ZFi). We make five major observations. First, for $\gamma \in (0, 1]$ and high $\frac{\text{size}(M)}{\text{size}(C)}$, ZFi values are ≈ 0. Second, ZFi consistently increases as γ decreases. Third, for $\gamma > 5$, ZFi values almost saturates at ≈ 0.3 (D1, D2) and ≈ 0.6 (D3) for all values of $\frac{\text{size}(M)}{\text{size}(C)}$. Fourth, as $\frac{\text{size}(M)}{\text{size}(C)}$ decreases, we observe significant ZFi even for $\gamma \in (0, 1)$. This is because smaller $\frac{\text{size}(M)}{\text{size}(C)}$ implies enough room for most of the available transactions. Lastly, since with D3, there is a greater chance of sampling lower b_is, its ZFi values are greater than D1 and D2.

The green shaded region depicts the range of γ with a practical CoF-ZFi trade-off. Specifically, for $\gamma \in (2, 10)$, we observe CoF < 2 and ZFi > 0.1, for all three distributions.