TRANSACTION FEE MECHANISM FOR PROOF-OF-STAKE PROTOCOL

WENPIN TANG AND DAVID D. YAO

Abstract. We study a mechanism design problem in the blockchain proof-of-stake (PoS) protocol. Our main objective is to extend the transaction fee mechanism (TFM) recently proposed in [7], so as to incorporate a *long-run* utility model for the miner into the burning second-price auction mechanism $\texttt{BSP}(\gamma)$ proposed in [7] (where γ is a key parameter in the strict γ-utility model that is applied to both miners and users). First, we derive an explicit functional form for the long-run utility of the miner using a martingale approach, and reveal a critical discontinuity of the utility function, namely a small deviation from being truthful will yield a discrete jump (up or down) in the miner's utility. We show that because of this discontinuity the $\texttt{BSP}(\gamma)$ mechanism will fail a key desired property in TFM, c-side contract proofness (c-SCP). As a remedy, we introduce another parameter θ, and propose a new $\texttt{BSP}(\theta)$ mechanism, and prove that it satisfies all three desired properties of TFM: user- and miner-incentive compatibility (UIC and MIC) as well as c-SCP, provided the parameter θ falls into a specific range, along with a proper "tick" size imposed on user bids.

Key words: Blockchain, proof of stake, transaction fee mechanism, cryptocurrency, incentive compatibility, utility, martingale.

1. Introduction

A blockchain is a digital ledger that facilitates the secure exchange and execution of transactions in a distributed network without an intermediary, hence achieving *decentralization*. The past decade has witnessed impressive advances of the blockchain technology in a wide range of applications including cryptocurrency [19, 33], healthcare [17, 30], supply chain [6, 23], non-fungible tokens [9, 32], and (more recently) crypto exchanges for the stock market [16], among many others.

There are two primary parties in a blockchain, the users and the miners. Below is a brief highlight of the two parties' activities and interactions.

- The users, who submit transactions to the blockchain for processing, seek to have their transactions settled and published on the blockchain network in a timely fashion by the miners. Since each block has a limited size or capacity, most blockchains adopt an auction mechanism that requires the users to submit bids to have their transactions processed by the miners. In this regard, the blockchain transaction is similar to an auction system, with the miners acting like the auctioneer, and the users as bidders.
- The miners select a subset of transactions from the mempool (according to the bids), include them in a block, and then position the block into an ever-growing public ledger. At the core of this "mining" process is a *consensus protocol*, a set of rules governing the whole process, including both the selection of the miner and the detailed

Date: August 26, 2023.

mechanics (e.g., the "longest chain") to form the public ledger. The most popular protocols are *Proof of Work* (PoW) [19] and *Proof of Stake* (PoS) [13, 33]. In both protocols, the miners compete with each other (to be selected to do the work) by either solving a hashing puzzle (PoW) or bidding with their stakes/coins (PoS). The winner will be selected to attach a new block (i.e. mine the block) to the blockchain. The selected miner will then receive transaction fees from the users, along with a separate reward from the blockchain.

See Figure 1 for an illustration of the miner-user activities under the PoS protocol, which is the focus of this study.

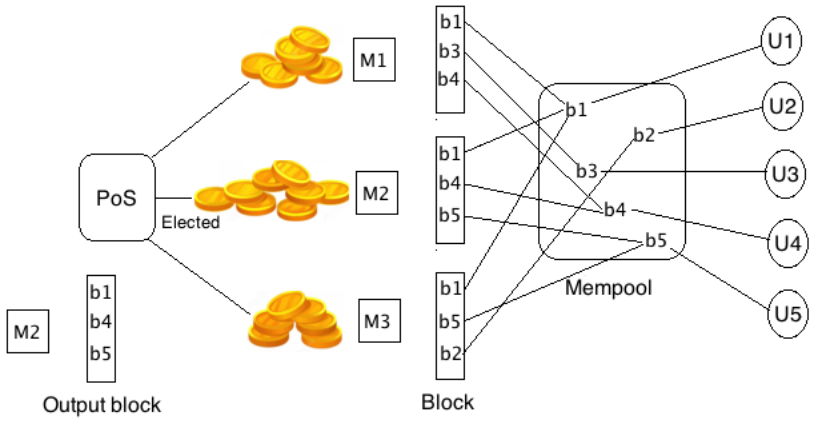


FIGURE 1. Miner-user activities under the PoS protocol.

A central design issue for the PoS protocol is to come up with a reliable and efficient *transaction fee mechanism* (TFM) so as to incentivize all participants, users and miners, to act honestly or truthfully. Most work in the general area of mechanism design (see [14, 18]) assumes that the auctioneer will honestly follow the prescribed mechanism, so the only concern is the strategic behavior of bidders. In blockchains, however, the miners (similar to the auctioneer) may also deviate from being truthful based on ex-post information. For instance, a miner may inject fake transactions so as to collect a larger payment, or collude with some users (possibly after examining all the bids) so as to improve their joint utility. What's more, [2] showed that the Vickrey auction [31], known to be user incentive compatible, fails to be incentive compatible for the miners.

To address the above problems, [7, 15, 22] proposed three desired properties for a transaction fee mechanism:

- *User incentive compatibility* (UIC): the users bid truthfully given that the miners implement the mechanism honestly.
- *Miner incentive compatibility* (MIC): the miners follow the prescribed mechanism honestly.
- *Miner-user side contract proofness* (c-SCP): any collusion between the miner and up to c users cannot improve their joint utility by deviating from being truthful.

Refer to Section 3 for more details. See also [1, 5, 11, 34] for discussions on (how to circumvent) the miner or auctioneer's strategic behaviors. Recently, [8] proposed the notion of *maximal extractable value* (MEV) to formally quantify and analyze the strategic behaviors in the blockchain generation, along with the so-called *proposer-builder separation* (PBS) [3] as an early attempt to reduce the miner's MEV.

In 2019, Ethereum proposed a TFM EIP-1559 [4], which achieves all three properties above, as shown in [22], under the condition that there is no congestion, i.e. the block size is unlimited, while leaving open (unanswered) the congestion case. A recent breakthrough [7] provides a negative answer to this: when the block size is limited, as it is in practice, no TFM can achieve UIC, MIC and c-SCP simultaneously under the so-called *current utility*, i.e., the utility applies only to the immediate gain/loss. Specifically, a miner or a user may submit untruthful or fake bids, which may not be included in the current block (and hence cost nothing) but, once submitted and registered in the blockchain may still be included in a (possibly near) future block. This strategic behavior is not accounted for in the current utility model.

As a remedy, [7] proposes a *strict γ-utility*, where the parameter $\gamma > 0$ (strictly positive) serves as a discount factor that will be applied to any unconfirmed bids. Based on this, [7] also proposes a randomized TFM, called the *burning second-price auction*, and shows it satisfies all the three properties under the strict γ-utility. The essence of the strict γ-utility is to account for the future cost of any strategic gain, and thus mitigating the myopia in the current utility (via neglecting the future cost).

The objective of our work here is to further generalize this idea, by taking into account not only the future cost but also the difference between a miner's perspective of the "future" and that of a user's, particularly in terms of *time scale*. Any user, by definition a minor player in the blockchain system, may only use the blockchain occasionally, to request the execution of a transaction (e.g., a buy/sell order). So it is reasonable to assume that the users primarily focus on the current or near-term interests in terms of their utilities. In contrast, the miners are the major players performing the dual role of verifying the transactions and updating the blockchain (refer to Figure 1). Thus, a miner's utility is long-term based; and this is even more so in the PoS protocol, where the probability for a miner to be selected to mine a new block (and earn the associated transaction payment and blockchain reward) is proportional to the number of stakes that the miner can afford to put forth to bid (see [21, 27, 29], and [28] for a review on the PoS wealth evolution.) Thus, the more profit (or stakes) a miner can accumulate over time, the more likely is the miner's chance to win the bid to mine the next block and thereby make yet more profit. In this regard, the miner's time scale, in terms of formulating a proper miner's utility model, should be very different from that of a typical user's.

In this paper, our main objective is to extend the TFM of [7], so as to incorporate a long-run utility model for the miner into the burning second-price auction mechanism of [7], denoted $\texttt{BSP}(\gamma)$, where γ is the parameter (discount factor) in the strict γ-utility model. In particular, we bring out a critical feature of such a long-run utility model (for the miner), a discontinuity in the sense that a small deviation from being truthful will yield a discrete jump, either up or down, in the miner's utility (Theorem 2.2). This discontinuity calls for a substantial modification of the $\texttt{BSP}(\gamma)$ mechanism. Specifically, we show the $\texttt{BSP}(\gamma)$

mechanism cannot achieve c-SCP due to the discontinuity of the miner's utility (Proposition 3.3).

To overcome this handicap, we need to introduce another parameter θ, which characterizes the randomized confirmation rule (which selects a subset of top bids to be confirmed for inclusion into a new block). In addition, a minimal "tick" size Δ needs to be imposed on every bid submitted by the users, i.e., a bid can only be multiples of Δ. Based on these two devices, we propose a new $\texttt{BSP}(\theta)$ mechanism, and prove that it satisfies all three desired properties, UIC, MIC and c-SCP, under the PoS protocol, provided the parameter θ falls into a specific range, along with a proper tick size Δ. Refer to details in Theorem 4.2.

The rest of the paper is organized as follows. In Section 2, we provide background and preliminary materials on the TFM in the context of the PoS protocol, define the utility functions and discuss the relevant strategic behaviors. In particular, in Section 2.2, we define the long-run utility for the miner mentioned above, explicitly derive its functional form, and reveal a crucial discontinuity in the miner's revenue (i.e., payment collected from the users whose bids are confirmed). In Section 3, we propose a new burning second-price auction mechanism, denoted $\texttt{BSP}(\theta)$ as highlighted above. We then show in Section 4, that the $\texttt{BSP}(\theta)$, along with a minimum tick size and a proper parametric range for θ, achieves all three properties, UIC, MIC and c-SCP, for the PoS protocol. We conclude with Section 5.

2. Transaction fee mechanism, strategy and utility

In a transaction fee mechanism, a miner acts like an auctioneer, while users will bid to have their transactions included and confirmed in a block and published in the blockchain.

Let B be the number of slots in a block (i.e., the block size), and assume without loss of generality that there are more bids than slots. The mechanism operates under the following rules:

- An *inclusion rule* (executed by the miner) that decides which of the bids to include in the block. Only included bids can be accessed by the blockchain.
- A *confirmation rule* (executed by the blockchain) that selects a subset of the included bids to confirm. Only confirmed bids are considered final, i.e., settled transactions.
- A *payment rule* (executed by the blockchain) that specifies how much each confirmed bid should pay.
- A *(miner) revenue rule* (executed by the blockchain) that specifies how much the miner should be paid.

There are several important facts to keep in mind. To start with, only the first rule above, the inclusion rule, involves human decisions – from the users (how much to bid) and the miners (which bids to include); the other three rules concerning confirmation, user payment and miner revenue are all hard-coded into and executed by the blockchain protocol. The specification of these rules (all four) constitutes the main task of the mechanism design.

Notably, however, since the inclusion rule interfaces with human decisions, the design of all four rules need to anticipate and account for possible strategic behaviors of both the users and the miners. Thus, in addition to the inclusion rule (executed by the miners), there's the confirmation rule (executed by the system), i.e., not all bids included by a miner will be confirmed. The other two rules specify how much a confirmed bid should pay, which need

not be the same as what the user originally bids (e.g., similar to the second-price auction mechanism); and how much the miner should receive, which need not be the sum total of the payments from all confirmed bids. More detailed discussions are provided below.

2.1. **Strategic behaviors and utilities.** As mentioned above, a good mechanism design is supposed to steer all participants away from strategic (i.e., dishonest) behavior, so that they stay with their true (i.e., honest) values. There are five sources of strategic behavior in the PoS protocol: those originate from (i) a user, (ii) a miner, (iii) miner-user collusion, (iv) user-user collusion; and (v) miner-miner collusion.

The impact of (iv), user-user collusion, is negligible, since the users are minor players in a blockchain network, and it is difficult for them to collude. So, below we shall ignore (iv). As to (v), observe that under the PoS protocol, a miner's strategic decision will depend a priori on the number of stakes the miner owns, which determines the miner's chance to be selected to process the transaction. Thus, a miner-miner collusion can be reduced to the strategic behavior of a single representative miner, who owns all the stakes (i.e., of the entire collusion group). So, below we shall implicitly assume there's a single ("super") miner in the system.

Specifically, we will consider the following possible strategic behaviors of the miner and the users:

- *Strategically forming the inclusion list.* A strategic miner or a miner-user collusion may not follow the inclusion rule, as long as the included bids satisfy the block validity rules enforced by the blockchain.
- *Injecting fake transactions.* The miner, users or a miner-user collusion may inject fake transactions, possibly after examining other users' bids in the mempool.
- *Bidding untruthfully.* The users or a miner-user collusion can bid untruthfully, possibly after examining other users' bids in the mempool.

Specifically, we shall adopt an *ex-post* auction (see [20]) in the transaction fee mechanism detailed below. To do so, we need to first specify the utilities of the miner and the users.

Definition 2.1 (Strict γ-utility for the PoS)**.** *For a bid b (real or fake), denote by v and p its true value and required payment. Let $\gamma \in (0,1]$ be a (given) parameter.*

- *The strict γ-utility of the user is defined as the expected value of*
$$\sum_{b \text{ confirmed}} (v-p) - \sum_{b \text{ unconfirmed}, b>v} \gamma(b-v). \tag{2.1}$$
- *The strict γ-***return** *of the miner, denoted by $\mathcal{R}_\gamma$, is defined as the expected value of*
$$\textit{miner's revenue} + \sum_{b \text{ confirmed}} (0-p) - \sum_{b \text{ unconfirmed}, b>v} \gamma(b-0), \tag{2.2}$$
where a fake bid has value $v=0$. The strict γ-utility of the miner is
$$\mathcal{U}_m(\mathcal{R}_\gamma), \quad \textit{where } \mathcal{U}_m(\cdot) \textit{ is given by (2.7) below.} \tag{2.3}$$

We shall simply refer to (2.1) *as the user's utility, and to* (2.2)–(2.3) *as the miner's return and utility, i.e., implicitly assume a positive ("strict") $\gamma > 0$.*

Several remarks are in order. An honest user's bid satisfies $b = v$, whereas $b \neq v$ corresponds to a strategic user. A confirmed bid returns to the user its true value v (even if $b \neq v$),

for which the user will pay p (to be specified by the mechanism below). This explains the first summation in (2.1). Moreover, as mentioned above, if a user's bid is not confirmed in the current block, it is still recorded in the blockchain and may very well be confirmed in a future (often near-term) block. The second summation in (2.1) accounts for the cost/penalty the strategic user will pay for overbidding ($b > v$). (There's no penalty for underbidding.)

The miner's total return (or net profit) $\mathcal{R}_\gamma$ is specified in the expression in (2.2), where the first term is the revenue (the miner's receivable, to be specified by the mechanism below); while the other two terms are the same as the user's return (utility) in (2.1), which allows for modeling the miner's possible strategic behavior of injecting fake transactions into the system.

As to the miner's utility function $\mathcal{U}_m(\mathcal{R}_\gamma)$, the modeling details will be specified in the next subsection.

2.2. **Miner's long-run utility.** To properly model the miner's utility, one must recognize and acknowledge that the miner and the users differ fundamentally in their *time scales*. In the context of capturing their strategic behaviors, users are often more myopic and focus on their short-term gains; while the miner is concerned with long-term returns, particularly so once we aggregate all the miners into a single representative miner. Recall, under the PoS protocol, in addition to the return/profit the miner earns for processing the transactions, the miner can also include the return as part of the stake used to earn rewards (in the form of stakes) associated with validating a block (and handed out separately by the protocol). Hence, the more profit the miner receives in each round of processing transactions, the more likely the miner will be selected to validate a new block in the future, which in turn will generate more profit. This *"more leads to more"* incentive is simply not present in a user's bidding process.

As mentioned earlier, the miner's revenue comes from two sources: payment from processing the user transactions and the reward from the blockchain. To earn both, the miner needs to be selected by the PoS protocol to mine the block; if not the miner gets nothing. Assume the users' payment p is a constant, which is consistent with our focus on formulating a long-run utility for the miner. (Not to add, in practice a stationary flow of transactions over a long period is expected in a healthy payment ecosystem.) For $t \geq 1$, let R_t be the number of stakes handed out as reward by the PoS protocol at time t. Let $(M_t,\, t \geq 0)$ be the number of stakes owned by the miner; hence,

$$M_t = M_{t-1} + (p + R_t)\, 1_{\{\text{the miner is selected at time } t\}}. \tag{2.4}$$

It is important to note that here the payment p may or may not be honest, which allows for modeling the miner's strategic behavior.

Now, if the miner is not selected to mine a block, then some other miner will be selected to do so. The latter will receive a payment p_h, an honest one. This way, the other miner is used as a reference point to pin down any possible strategic gain or loss in the utility of the miner we are focusing on. Let $(N_t,\, t \geq 0)$ be the total number of stakes owned by all the miners. We have

$$N_t = N_{t-1} + (p + R_t)\, 1_{\{\text{the miner is selected at time } t\}} + (p_h + R_t)\, 1_{\{\text{the miner not selected at time } t\}}, \tag{2.5}$$

where the probability that the miner is selected at time t given the past is M_{t-1}/N_{t-1}. Denote by $\{\mathcal{F}_t\}_{t\geq 0}$ the filtration generated by the process (M_t, N_t). Combining (2.4) and (2.5), we

obtain the dynamics of (M_t, N_t):

$$(M_t, N_t) \,|\, \mathcal{F}_{t-1} = \begin{cases} (M_{t-1} + p + R_t, N_{t-1} + p + R_t) & \text{with probability} \quad M_{t-1}/N_{t-1}, \\ (M_{t-1}, N_{t-1} + p_h + R_t) & \text{with probability} \quad 1 - M_{t-1}/N_{t-1}. \end{cases} \tag{2.6}$$

Define the miner's long-run utility by

$$\mathcal{U}_m(p) := \liminf_{t\to\infty} \frac{\mathbb{E}M_t}{t}. \tag{2.7}$$

It is worth mentioning that long-run payoffs (though different) were also used in [12, 24] to analyze strategic behaviors in PoW blockchain mining.

To simplify the presentation, below we shall assume that the reward $R_t = R \geq 0$ is constant throughout. The next theorem derives the miner's long-run utility $\mathcal{U}_m(p)$ using a martingale approach.

Theorem 2.2. *Let $\pi_0 := M_0/N_0$ be the miner's initial share, and $\mathcal{U}_m(\cdot)$ be defined by (2.7). Assume that $0 < \pi_0 < 1$. Then*

$$\mathcal{U}_m(p) = \begin{cases} \pi_0(p_h + R) & \text{for} \quad p = p_h, \\ p + R & \text{for} \quad p > p_h, \\ 0 & \text{for} \quad p < p_h. \end{cases} \tag{2.8}$$

Refer to Figure 2 for a plot of $\mathcal{U}_m(p)$.

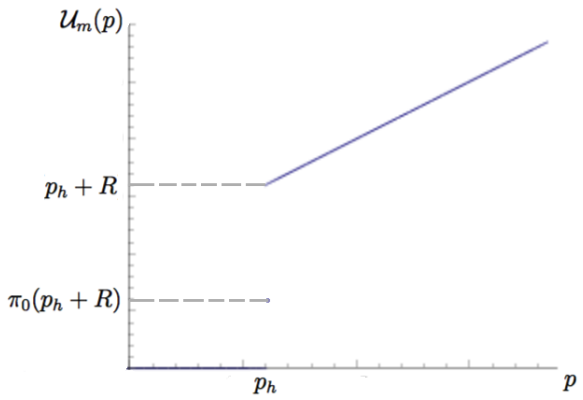


FIGURE 2. Plot of $\mathcal{U}_m(\cdot)$.

Proof. Denote $G := p + R$ and $G_h := p_h + R$, so the dynamics in (2.6) can be expressed as

$$(M_{t+1}, N_{t+1}) \,|\, \mathcal{F}_t = \begin{cases} (M_t + G, N_t + G) & \text{with probability} \quad M_t/N_t, \\ (M_t, N_t + G_h) & \text{with probability} \quad 1 - M_t/N_t. \end{cases} \tag{2.9}$$

We distinguish two cases: $p = p_h$ and $p \neq p_h$.

Case 1: $p = p_h$ (i.e., the miner is honest). In this case,

$$M_{t+1} \,|\, \mathcal{F}_t = \begin{cases} M_t + G_h & \text{with probability} \quad M_t/N_t, \\ M_t & \text{with probability} \quad 1 - M_t/N_t. \end{cases} \tag{2.10}$$

where $N_t = N_0 + G_h t$ is non-random. It is easy to see from (2.10) that

$$\mathbb{E}M_{t+1} = \left(1 + \frac{G_h}{N_t}\right) \mathbb{E}M_t = \frac{N_{t+1}}{N_t} \mathbb{E}M_t,$$

which yields $\mathbb{E}M_t = \pi_0 N_t$ for $t \geq 0$. (In fact, $(M_t/N_t,\, t \geq 0)$ is a martingale.) As a result,

$$\frac{\mathbb{E}M_t}{t} = \pi_0 \frac{N_t}{t} \longrightarrow \pi_0 G_h, \quad \text{as } t \to \infty.$$

Case 2: $p \neq p_h$ (i.e., the miner is strategic). Set $c := M_0 + \frac{G}{G_h - G} N_0$. It is straightforward from (2.9) that

$$M_{t+1} + \frac{G}{G_h - G} N_{t+1} = M_t + \frac{G}{G_h - G} N_t + \frac{G G_h}{G_h - G},$$

so

$$M_t + \frac{G}{G_h - G} N_t + \frac{G G_h}{G - G_h} t = c, \tag{2.11}$$

and

$$\mathcal{U}_m(p) = \frac{G}{G - G_h} \liminf_{t \to \infty} \frac{\mathbb{E}N_t}{t} + \frac{G G_h}{G_h - G}. \tag{2.12}$$

By (2.9) and (2.11), we obtain the dynamics of N_t:

$$N_{t+1} = \begin{cases} N_t + G & \text{with probability} \quad \left(\frac{G}{G - G_h} N_t + \frac{G G_h}{G_h - G} t + c\right) / N_t, \\ N_t + G_h & \text{with probability} \quad 1 - \left(\frac{G}{G - G_h} N_t + \frac{G G_h}{G_h - G} t + c\right) / N_t. \end{cases}$$

First assume that $p > p_h$ (so $G > G_h$). Let $L_t := N_t - G_h t$, and the dynamics of L_t is:

$$L_{t+1} = \begin{cases} L_t + (G - G_h) & \text{with probability} \quad \left(\frac{G}{G - G_h} L_t + c\right) / (L_t + G_h t), \\ L_t & \text{with probability} \quad 1 - \left(\frac{G}{G - G_h} L_t + c\right) / (L_t + G_h t). \end{cases}$$

Note that

$$\left(\frac{G}{G - G_h} L_t + c\right) / (L_t + G_h t) \leq 1 \Longrightarrow L_t \leq (G - G_h) \left(t - \frac{c}{G_h}\right). \tag{2.13}$$

We have

$$\begin{aligned} \mathbb{E}\left(L_{t+1} \,|\, \mathcal{F}_t\right) &= L_t + \frac{G L_t + c(G - G_h)}{L_t + G_h t} \\ &\geq \left(1 + \frac{1}{t - \frac{G - G_h}{G G_h} c}\right) L_t + \frac{c(G - G_h)/G}{t - \frac{G - G_h}{G G_h} c}. \end{aligned} \tag{2.14}$$

By setting

$$I_t := \frac{L_t + c(G - G_h)/G}{t - \frac{G - G_h}{G G_h} c},$$

the inequality (2.14) yields $\mathbb{E}(I_{t+1} \,|\, \mathcal{F}_t) \geq I_t$. That is, $(I_t,\, t \geq 0)$ is a sub-martingale. By (2.13), we have $\limsup_{t \to \infty} \mathbb{E}(I_t) \leq G - G_h$. The martingale convergence theorem (see [10, Theorem 4.2.11]) implies that as $t \to \infty$,

$$I_t \to I_\infty \text{ a.s. and in } L^1, \quad \text{with } 0 < I_\infty \leq G - G_h \text{ a.s.}$$

So $L_t/t \to I_\infty$ a.s. and in L^1. Again by (2.14), we get $\lim_{t\to\infty} \mathbb{E}L_{t+1} - \mathbb{E}L_t = \mathbb{E}\left(\frac{GI_\infty}{I_\infty+G_h}\right)$, which yields

$$\mathbb{E}I_\infty = \mathbb{E}\left(\frac{GI_\infty}{I_\infty+G_h}\right).$$

We then have $\mathbb{E}\left(\frac{(G-G_h-I_\infty)I_\infty}{I_\infty+G_h}\right) = 0$, so $I_\infty = G - G_h$ a.s. and $\mathbb{E}L_t/t = G - G_h$. Therefore, $\mathbb{E}N_t/t \to G$ as $t \to \infty$, and by (2.12), we get $\mathcal{U}_m(p) = \frac{G}{G-G_h}G + \frac{GG_h}{G_h-G} = G$ if $p > p_h$.

Similarly, if $p < p_h$, we can show that $\mathbb{E}N_t/t \to G_h$ as $t \to \infty$, and hence, $\mathcal{U}_m(p) = \frac{G}{G-G_h}G_h + \frac{GG_h}{G_h-G} = 0$. □

Let's make several remarks. First, the formula in (2.8) shows that the miner's utility $\mathcal{U}_m(\cdot)$ is discontinuous at the true value $p = p_h$. If the miner is strategic so as to be overpaid with $p = p_h + \varepsilon$, then

$$\mathcal{U}_m(p) - \mathcal{U}_m(p_h) = (p + R) - \pi_0(p_h + R) = \varepsilon + (1 - \pi_0)(p_h + R),$$

i.e., the miner's utility is overshot by a fixed amount $(1 - \pi_0)(p_h + R)$ plus the ε increment (above p). Similarly, if $p = p - \varepsilon$, then

$$\mathcal{U}_m(p) - \mathcal{U}_m(p_h) = 0 - \pi_0(p_h + R) = -\pi_0(p_h + R),$$

i.e., the miner's utility is undershot by a fixed amount $\pi_0(p_h + R)$. As will be clear in the following section, these "gaps" (the overshot and the undershot) will become a key obstacle to apply the (raw) burning second-price auction of [7], in particular when there's a miner-user collusion.

Second, the assumption $0 < \pi_0 < 1$ excludes two extremal cases: $\pi_0 = 0$ and $\pi_0 = 1$. If $\pi_0 = 0$, the miner has no stake at hand, hence is effectively a user. If $\pi_0 = 1$, then the miner controls the entirely blockchain, an extreme case that rarely happens. In that case, the miner's utility is always $\mathcal{U}_m(p) = p+R$, whatever the value of p is, simply because there's no other miner as a competitor.

Finally, the assumption that R_t is constant may be relaxed. If $p = p_h$, the same argument in the proof shows that

$$\mathcal{U}_M(p_h) = \pi_0\left(p_h + \liminf_{t\to\infty} \frac{\sum_{k=1}^t R_k}{t}\right).$$

However determining $\mathcal{U}_M(p)$ for $p \neq p_h$ with a time-dependent reward R_t seems to be involved.

3. Burning second-price auction

Here we start with defining the three desired properties of a transaction fee mechanism.

Definition 3.1. *Let $c \geq 1$ be a positive integer parameter. A transaction fee mechanism is said to be:*

- *user incentive compatible (UIC), if a user's utility is maximized when biding honestly (i.e., with $b = v$), independent of how the other users bid;*
- *miner incentive compatible (MIC), if the miner's utility is maximized while honestly implementing the inclusion rule, given any bids from the users;*

- *c-side contract proofness (c-SCP), if the joint utility of the miner and one or up to c (colluding) users is maximized when the miner follows the inclusion rule honestly and the colluding users bid honestly, independent of how the other users bid.*

While Definition 3.1 certainly applies to general utility functions, here we focus on the strict γ-utility in Definition 2.1, with a given value of $\gamma \in (0, 1]$.

Next, we introduce a one-parameter family of the burning second-price auctions, which naturally extends the burning second-price auction in [7].

Definition 3.2 (Burning second-price auction)**.** *Let B be the block size, and $c \geq 1$ be the (maximum) colluding size. Set $\frac{2c}{2c+1}B \leq k < B$. Define the burning second-price auction with parameter $\theta \in (0, 1]$ by the following set of rules:*

- *Inclusion rule: Choose the B highest bids to include in the block, breaking ties arbitrarily. Let $(b_1, ..., b_B)$ denote the included bids ranked in decreasing order.*
- *Confirmation rule: Randomly select a subset $S \subset \{b_1, ..., b_k\}$ of size $\lfloor \frac{\theta k}{c} \rfloor$. All bid in the set S are confirmed, and all other bids $\{b_1, \dots, b_B\} \setminus S$ are unconfirmed.*
- *Payment rule: Each confirmed bid pays $p = b_{k+1}$; unconfirmed bids pay nothing.*
- *Miner's revenue: The miner is paid $\theta(b_{k+1} + \cdots + b_B)$ if $\lfloor \frac{\theta k}{c} \rfloor \geq 1$, and 0 otherwise. Burn the remaining payment collected from the confirmed bids.*

Let $\texttt{BSP}(\theta)$ denote this transaction fee mechanism.

First note that a random subset of the included bids are confirmed. This can be implemented by trusted on-chain algorithms, e.g. multi-party computation (see [25]). Second, if the size of this subset $\lfloor \frac{\theta k}{c} \rfloor = 0$, then no transaction is confirmed and the miner is paid nothing (the trivial mechanism). Hence, we will only need to consider the case $\lfloor \frac{\theta k}{c} \rfloor \geq 1$:

$$\left\lfloor \frac{\theta k}{c} \right\rfloor b_{k+1} \geq \frac{\theta k}{2c} b_{k+1} \geq \theta(b_{k+1} + \cdots + b_B), \tag{3.1}$$

where the left side is the total payment collected from the users, and the right side is the miner's revenue. The second inequality in (3.1) follows from the fact that $b_{k+1} \geq \cdots \geq b_B$ and $k \geq \frac{2c}{2c+1}B$. Thus, $\texttt{BSP}(\theta)$ is a valid transaction fee mechanism.

More importantly, whereas it might appear that when $\theta = \gamma$, $\texttt{BSP}(\theta)$ reduces to the $\texttt{BSP}(\gamma)$ mechanism in [7], there is a crucial difference between the two: While both mechanisms apply the strict γ-utility to the miner, as well as to every user, the $\texttt{BSP}(\gamma)$ mechanism in [7] further applies the same time scale to both miner and user. In contrast, in the $\texttt{BSP}(\theta)$ mechanism here, a different time scale, *long-run average*, is applied to the miner's utility following (2.7), and more explicitly in (2.8). Consequently, we need an extra parameter θ so as to overcome the discontinuity of the miner's utility highlighted at the end of the last section. To appreciate this, first note a negative (impossibility) result in the following proposition.

Proposition 3.3. *c-SCP cannot be achieved by $\texttt{BSP}(\theta)$ for any $\theta \in (0, 1]$ under the strict γ-utility for the PoS.*

Proof. Without loss of generality, assume $c = 1$. Let $(v_1, \dots, v_B)$ be the honest bids ranked in decreasing order, with $v_k > v_{k+1}$. Consider the case where the miner and user $k + 1$ collude. Note that user $k + 1$'s utility is 0 since v_{k+1} is not confirmed.

Now, suppose user $k+1$ increase the bid to $b_{k+1} := v_{k+1} + \varepsilon$, with $\varepsilon < v_k - v_{k+1}$. So b_{k+1} is still unconfirmed. Then, user $k+1$'s utility decreases from 0 to $-\gamma\varepsilon$. The miner's utility increases from $\pi_0 \left(\theta \sum_{\ell=k+1}^{B} v_\ell + R\right)$ to $\theta \left(\sum_{\ell=k+1}^{B} v_\ell + \varepsilon\right) + R$. Thus, the change in the joint utility of the miner and user $k+1$ is

$$(1-\pi_0)\left(\theta \sum_{\ell=k+1}^{B} v_\ell + R\right) + (\theta - \gamma)\varepsilon. \tag{3.2}$$

By making ε sufficiently small ($\varepsilon \downarrow 0$), the first term above will be the dominant, and thus the change will be positive. That is, the miner can collude with user $k+1$ to get a higher joint utility, which violates 1-SCP. □

In the above proof, c-SCP fails because a small increase in a user's bid can trigger an overshoot $(1-\pi_0)\left(\theta \sum_{\ell=k+1}^{B} v_\ell + R\right)$ in the miner's utility. One way to prevent this from happening is to put some constraints on ε (the bid increment), and also on the bids $(v_1, \ldots, v_B)$; specifically, a lower bound on ε, and an upper bound on $\sum_{\ell=k+1}^{B} v_\ell$. Yet even more importantly, we need to impose an upper limit on θ, so as to rule out $\theta - \gamma \geq 0$. Because if $\theta \geq \gamma$, then the change to the joint miner-user utility in (3.2) will always be positive; i.e., c-SCP will always fail, even with the constraints on bids and bid increments.

4. Burning second-price auction with minimum tick

Based on the observations following the proof of Proposition 3.3, we make the following assumption.

Assumption 4.1.

(i) The bids are in multiples of $\Delta > 0$, i.e. taking values from the discrete set $\in \{0, \Delta, 2\Delta, \ldots\}$.

(ii) Let $(v_1, \ldots, v_B)$ be honest bids ranked in decreasing order. Then, there exists a constant $\kappa > 0$ such that $\sum_{\ell=k+1}^{B} v_\ell \leq \kappa$.

The assumption in (i) imposes a (minimum) bid increment $\Delta > 0$, or "tick" size, which is common in practice (e.g., auction, stock markets, etc). It is a block validity rule, so is part of the inclusion rule of the transaction fee mechanism. The assumption (ii) gives an upper bound for the miner's revenue $\theta \sum_{\ell=k+1}^{B} v_\ell$ if all participants are honest. A sufficient condition is that

$$\sum_{\ell=1}^{B} v_\ell \leq \kappa,$$

i.e. the total amount of top (honest) bids is bounded. This is related to the idea of *bounded rationality* [26], where the users bid rationally. So the bid flow is expected to stabilize, or close to stationarity. In practice, the upper bound κ can be inferred or estimated from the bid-stream data.

The next theorem confirms that under Assumption 4.1, $\texttt{BSP}(\theta)$ satisfies UIC, MIC and c-SCP for a suitable choice of θ.

Theorem 4.2. *Let Assumption 4.1 hold. Then, for* $0 < \pi_0 < 1$, $\Delta > (1-\pi_0)R/\gamma$, *and*

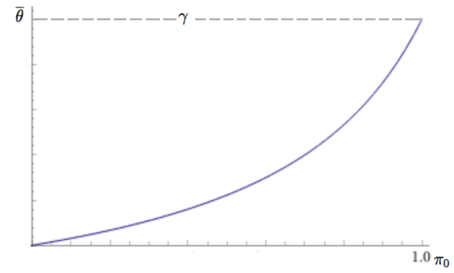
$$\theta \le \overline{\theta} := \min\left(\frac{\pi_0 R}{(1-\pi_0)\kappa}, \frac{\gamma\Delta - (1-\pi_0)R}{(1-\pi_0)\kappa + \Delta}\right), \tag{4.1}$$

$\mathtt{BSP}(\theta)$ achieves UIC, MIC and c-SCP under the strict γ-utility for the PoS.

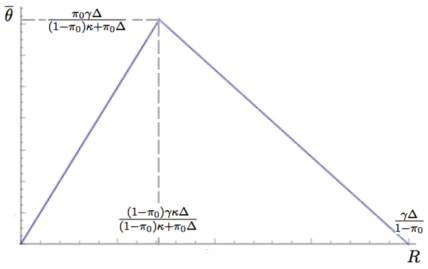
Several remarks are in order before we prove Theorem 4.2. First, observe the dependence of $\overline{\theta}$ on the parameters $(\pi_0, R, \Delta, \kappa)$ as specified below, and also refer to Figure 3 for illustration:

- $\overline{\theta}$ is increasing in Δ, and $\overline{\theta} \to 0$ when $\Delta \to (1-\pi_0)R/\gamma$, and $\overline{\theta} \to \min\left(\frac{\pi_0 R}{(1-\pi_0)\kappa}, \gamma\right)$ when $\Delta \to \infty$.
- $\overline{\theta}$ is decreasing in κ, and $\overline{\theta} \to \gamma - (1-\pi_0)R/\Delta$ when $\kappa \to 0$, and $\overline{\theta} \to 0$ when $\kappa \to \infty$.
- $\overline{\theta}$ is increasing in π_0, and $\overline{\theta} \to 0$ when $\pi_0 \to 0$, and $\overline{\theta} \to \gamma$ when $\pi_0 \to 1$.
- $\overline{\theta}$ increases from 0 to $\frac{\pi_0\gamma\Delta}{(1-\pi_0)\kappa+\pi_0\Delta}$ when $R \in \left[0, \frac{(1-\pi_0)\kappa\gamma\Delta}{(1-\pi_0)\kappa+\pi_0\Delta}\right]$; and then decreases to 0 when $R \in \left(\frac{(1-\pi_0)\kappa\gamma\Delta}{(1-\pi_0)\kappa+\pi_0\Delta}, \frac{\gamma\Delta}{1-\pi_0}\right)$.

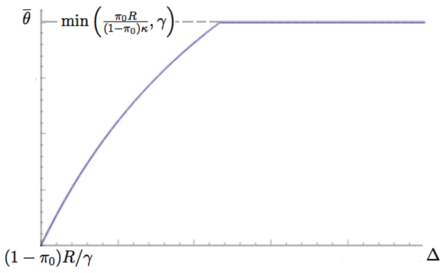
Second, as we will see in the proof below, $\mathtt{BSP}(\theta)$ satisfies UIC for any θ, and satisfies MIC for any $\theta \le \gamma$. (Note that $\theta \le \overline{\theta} \le \gamma$ as observed above.) The condition in (4.1) is required for c-SCP, where the bound $\frac{\pi_0 R}{(1-\pi_0)\kappa}$ is to offset the undershoot gap in the miner's utility, while the bound $\frac{\gamma\Delta-(1-\pi_0)R}{(1-\pi_0)\kappa+\Delta}$ is to offset its overshoot gap.



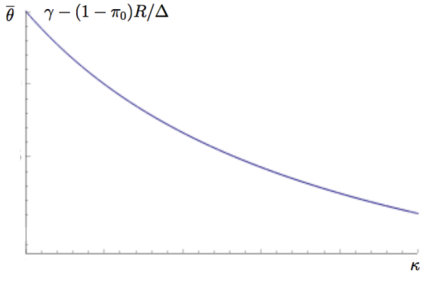
(A) Plot of $\pi_0 \to \overline{\theta}$.



(B) Plot of $R \to \overline{\theta}$.



(C) Plot of $\Delta \to \overline{\theta}$.



(D) Plot of $\kappa \to \overline{\theta}$.

FIGURE 3. Plots of $\overline{\theta}(\pi_0, R, \Delta, \kappa)$.

Following Theorem 4.2, we know that $\mathtt{BSP}(\theta)$ achieves UIC, MIC and c-SCP as long as $\theta \le \overline{\theta}$. Recall $\mathtt{BSP}(\theta)$ confirms a θ-portion of the top k bids; hence, it is desirable to take $\theta = \overline{\theta}$

so as to attain the best efficiency. After all, the blockchain is used to confirm transactions, so the more it confirms in each block, the more efficient the mechanism is.

As indicated in Section 2.1, Theorem 4.2 can be readily extended to the miner-miner collusion. To do so, it suffices to replace π_0 with π_0^{gr} in (4.1), where π_0^{gr} is the total share of the miner collusion group. In this case it is possible, albeit highly unlikely, that $\pi_0^{\text{gr}} = 1$ (i.e., a group of miners control the entire blockchain). Then $\mathcal{U}_m(p) = p + R$ for all p; refer to the earlier remarks after Theorem 2.2. In this case, the condition in (4.1) reduces to $\theta \le \overline{\theta} = \gamma$, and the raw $\texttt{BSP}(\gamma)$ achieves all the desired properties.

We are now ready to prove Theorem 4.2. We split the proof into three separate lemmas, each proving one of the three properties UIC, MIC and c-SCP. This split allows us to bring out the specific conditions required for each property; in particular, note that the range of θ in (4.1) can be relaxed (extended) for UIC and MIC, and Assumption 4.1 is only needed for establishing c-SCP.

Lemma 4.3 (UIC)**.** *For any $\theta > 0$, $\texttt{BSP}(\theta)$ achieves UIC.*

Proof. Any user i who submits an honest bid, i.e., $b_i = v_i$, obtains a utility of $v_i - v_{k+1}$, with $p = v_{k+1}$ being the payment, if the bid is confirmed; or a utility of 0, if the bid is unconfirmed.

Now, suppose user i changes the bid to $b_i \neq v_i$. There are two cases:

Case 1: $i \le k$. If b_i is among the top k bids, the utility remains unchanged at $v_i - v_{k+1}$ if the bid is confirmed; the utility is $-\gamma(b_i - v_i)^+ \le 0$ if the bid is unconfirmed. In both cases, the utility cannot exceed that of the honest bid. If b_i drops out of the top k bids, the utility is 0 – no greater than the original utility.

Case 2: $i > k$. If b_i is not among the top k bids, the bid is unconfirmed and the utility is $-\gamma(b_i - v_i)^+ \le 0$. If b_i joins the top k bids, the payment changes to $p = v_k$. The user's utility is $v_i - v_k \le 0$ if the bid is confirmed, and is $-\gamma(b_i - v_i)^+ = -\gamma(b_i - v_i) \le 0$ if the bid is unconfirmed.

The above also covers the case of injecting a fake transaction, i.e., one with $v_i = 0$ and $b_i > 0$. □

Lemma 4.4 (MIC)**.** *For any $\theta \le \gamma$, $\texttt{BSP}(\theta)$ achieves MIC.*

Proof. The miner can deviate from being honest by either not including the highest B bids, or injecting fake bids. Recall, given the bid vector $(b_1, \ldots, b_B)$ in decreasing order, the miner's utility $\mathcal{U}_m(\cdot)$ is non-decreasing in the miner's receivable (i.e., revenue) $\theta \sum_{\ell=k+1}^{B} b_\ell$. Hence, it is impossible for the miner not to include the highest B bids.

As to injecting fake bids, this amounts to the miner changing some bid b_i to f (a fake one). Again, as the miner's utility $\mathcal{U}_m(\cdot)$ is non-decreasing in the miner's total return (revenue minus payment/cost), it suffices to examine the changes to the miners total return.

There are two cases:

Case 1: Suppose f is confirmed (hence, f must be among the top k bids).

(1a) If $i \le k$, then f replaces b_i in the original set of k bids. Thus, the miner needs to pay b_{k+1} for the confirmed (fake) bid, while the miner's own revenue remains unchanged. So, the net change to the miner's total return is $-b_{k+1} < 0$.

(1b) if $i > k$, then f joins the set of top k bids, replacing b_k, which in turn replaces b_{k+1} as payment; and this is also the miner's payment for the confirmed (fake) bid. Accordingly, the change to the miner's revenue is $\theta(b_k - b_i)$. Thus, the net change is $-b_k + \theta(b_k - b_i) < 0$, as $\theta \le 1$.

Case 2: Suppose f is not confirmed. The fake bid costs the miner zero payment, but incurs a negative amount $-\gamma f < 0$ (since the fake bid has zero value). In addition, there are changes to the miner's revenue:

(2a) Suppose f is among the top k bids. If b_i is also among the top k bids, then, there's no change to the miner's revenue. If b_i is not among the top k bids, i.e., $i > k$, then similar to (1b) above, the change to the miner's revenue is $\theta(b_k - b_i)$. Thus the net change (to the miner's total return) is $-\gamma f + \theta(b_k - b_i) = (\theta b_k - \gamma f) - \theta b_i < 0$, since $\theta \le \gamma$ and $b_k \le f$.

(2b) Suppose f is not among the top k bids. If b_i is among the top k bids, then replacing b_i by f will result in moving b_{k+1} into the top k set. The change to the miner's revenue is $\theta(f - b_{k+1})$; hence, the net change is $-\gamma f + \theta(f - b_{k+1}) < 0$, since $f \le b_{k+1}$. If b_i is also not among the top k bids, then replacing b_i by f, the change to the miner's revenue is $\theta(f - b_i)$; hence, the net change is $-\gamma f + \theta(f - b_i) = -(\gamma - \theta)f - \theta b_i < 0$ since $\theta \le \gamma$.

Since the miner's total return will be (strictly) reduced in all cases, the miner will have no incentive to inject any fake bids. □

Lemma 4.5 (c-SCP)**.** *Under the assumptions in Theorem 4.2,* `BSP`(θ) *achieves c-SCP.*

Proof. A collusion between a miner and the users may one of the three strategies: the miner does not include the highest bids; the miner injects fake bids; some users bid untruthfully. Denote by C the set of the colluding users, with cardinality $|C| \le c$. Equivalently, assume that the miner and the users collude in the following order:

- Step 1. The miner includes bids strategically. This is the same as the miner deleting the (real) bids one by one, and then including the highest bids.
- Step 2. The miner replaces some real bids (not in the set C) with fake bids.
- Step 3. Some users in C change their bids untruthfully.

Step 1. Let $(v_1, \dots, v_B, \dots)$ denote the honest bids ranked in decreasing order. Suppose v_i with $i > k+1$ is deleted. This will not affect either the miner's utility or any user's utility.

Suppose v_i with $i \le k+1$ is deleted. Then, the miner's revenue changes from $\theta \sum_{\ell=k+1}^{B} v_\ell$ to $\theta \sum_{\ell=k+2}^{B+1} v_\ell$. This change will be a net decrease, in which case the miner's utility drops to 0 and stays at 0; unless $v_{k+1} = v_{B+1}$, in which case there's no change to the miner's revenue. On the other hand, any user's utility can increase by at most $\frac{\theta}{c}(v_{k+1} - v_{k+2})$. If the miner deletes one more bid, any user's utility can increase by at most $\frac{\theta}{c}(v_{k+2} - v_{k+3})$, accumulating to $\frac{\theta}{c}(v_{k+1} - v_{k+3})$, and so forth. Thus, any user's utility can increase by at most $\frac{\theta}{c} v_{k+1}$. Since there are at most c colluding users, the joint utility of the colluding users can increase by at most θv_{k+1}. So the change in the joint utility of the miner and the colluding users is at most

$$-\pi_0 \left(\theta \sum_{\ell=k+1}^{B} v_\ell + R \right) + \theta v_{k+1} \le (1 - \pi_0)\theta\kappa - \pi_0 R \le 0, \tag{4.2}$$

since $v_{k+1} \le \sum_{\ell=k+1}^{B} v_\ell \le \kappa$ by Assumption 4.1, and $\theta \le \frac{\pi_0 R}{(1-\pi_0)\kappa}$ by (4.1).

Step 2. From the proof of Lemma 4.4, it is shown that replacing a (real) bid with a fake one cannot increase the miner's utility in any scenario. Furthermore, it is clear that no user's utility can increase if the fake bid f is among the top k bids, as this may increase the payment (from v_{k+1} to v_k). Hence, we only need to consider case (2b) in the proof of Lemma 4.4. In that case, the net change to the miner's total return (revenue minus cost) is < 0; hence the miner's utility will drop to 0 and stay at 0. Moreover, following the argument in Step 1 above, a user's utility can increase by at most $\frac{\theta}{c}\left(v_{k+1} - \max\{f, v_{k+2}\}\right)$, where $\max\{f, v_{k+2}\}$ represents the $(k+1)$-th bid (i.e. the largest unconfirmed bid) after the replacement. If the miner replace one more bid by another fake f', any user's utility can further increase by at most $\frac{\theta}{c}\left(\max\{f, v_{k+2}\} - \max\{f', \min(f, v_{k+2})\}\right)$, where the max term is the $(k+1)$-th bid after replacement. Repeating this argument will lead to the same inequality in (4.2).

Step 3. Recall that $(v_1, \ldots, v_B)$ are the honest bids ranked in decreasing order. Without loss of generality, assume that the colluding users change their bids in an ascending order; i.e. the one with the lower true value changes first. Suppose user i replaces v_i with $b_i \ne v_i$.

Case 1: $i > k$.

(1a) b_i is among the top k bids. In this case, we have $v_k \ge v_i$ and $b_i > v_k$; moreover, v_k becomes the $(k+1)$-th bid (i.e. the largest unconfirmed bid). Then, user i's utility changes from 0 to $v_i - v_k \le 0$ if b_i is confirmed, and to $-\gamma(b_i - v_i) < 0$ if unconfirmed. Thus, user i's utility change is

$$\begin{aligned} -\left(1-\frac{\theta}{c}\right)\gamma(b_i - v_i) - \frac{\theta}{c}(v_k - v_i) &\le -\left(1-\frac{\theta}{c}\right)\gamma\left(v_k - v_i\right) - \frac{\theta}{c}\gamma(v_k - v_i) \\ &= -\gamma(v_k - v_i), \end{aligned} \tag{4.3}$$

with the inequality following from $b_i > v_k \ge v_i$ and $\gamma \le 1$.

The miner's revenue changes from $\theta \sum_{\ell=k+1}^{B} v_\ell$ to $\theta\left(\sum_{\ell=k}^{B} v_\ell - v_i\right)$. So, the change to the miner's utility is

$$\pi_0\left(\theta \sum_{\ell=k+1}^{B} v_\ell + R\right) \longrightarrow \theta\left(\sum_{\ell=k}^{B} v_\ell - v_i\right) + R. \tag{4.4}$$

Thus, the change to the joint utility of the miner and the colluding user is at most

$$\begin{aligned} & (1-\pi_0)\left(\theta \sum_{\ell=k+1}^{B} e_\ell + R\right) - (\gamma - \theta)(v_k - v_i) \\ \le\ & (1-\pi_0)(\theta\kappa + R) - (\gamma - \theta)\Delta \le 0, \end{aligned} \tag{4.5}$$

where the first inequality follows from $\sum_{\ell=k+1}^{B} e_\ell \le \kappa$ and $v_k - v_i \ge \Delta$ by Assumption 4.1, and the second inequality follows from $\theta \le \frac{\gamma\Delta - (1-\pi_0)R}{(1-\pi_0)\kappa + \Delta}$ by (4.1).

(1b) b_i is not among the top k (hence, unconfirmed). The miner's revenue changes from $\theta \sum_{\ell=k+1}^{B} v_\ell$ to $\theta\left(\sum_{\ell=k+1}^{B} v_\ell + b_i - v_i\right)$. For the users who are among the top k, let their payment be v'_{k+1} (if confirmed). There are two possibilities.

- If $b_i > v_i$ (overbidding), then $v'_{k+1} \geq v_{k+1}$. Then, user i's utility decreases from 0 to $-\gamma(b_i - v_i) < 0$, whereas all other users' utilities do not increase (as their payment my increase). The miner's utility increases, and the change is the same as in (4.4). Thus, the change in the joint utility is at most $(1 - \pi_0)\left(\theta \sum_{\ell=k+1}^{B} e_\ell + R\right) - (\gamma - \theta)(b_i - v_i) \leq 0$ for the same reason as in (4.5).
- If $b_i < v_i$ (underbidding), then $v'_{k+1} \leq v_{k+1}$. So user i's utility is unchanged (at 0); the utility of any other user among the top k increases by at most $\frac{\theta}{c}\left(v_{k+1} - v'_{k+1}\right)$; all other users are unaffected. Thus, the joint utility of the colluding users can increase by at most $\theta(v_{k+1} - v'_{k+1}) \leq \theta v_{k+1}$; while the miner's utility drops to 0. This reduces to the scenario in (4.2), and hence the joint utility of the miner and the colluding users cannot increase.

Case 2: $i \leq k$.

(2a) b_i remains among the top k. So user i's utility change is equal to 0 if confirmed, and equal to $-\gamma(b_i - v_i)^+ < 0$ if unconfirmed. All other users' utilities and the miner's utility remain unchanged. So it is obvious that the joint utility of the miner and the colluding users cannot increase.

(2b) b_i drops out of the top k, which means $b_i \leq v_{k+1}$. Then, the miner's utility either remains unchanged (if $b_i = v_{k+1}$) or drops to 0 (if $b_i < v_{k+1}$). The utility of the colluding user(s) can increase by at most $\theta(v_{k+1} - \max(b_i, v_{k+2})) \leq \theta v_{k+1}$, following the same argument as in Step 2. So, this leads again to the scenario in (4.2), and hence the joint utility of the miner and the colluding users cannot increase.

Finally, consider the case of further replacements by the colluding users.

(3a) Suppose the miner's revenue increases from $\theta \sum_{\ell=k+1}^{B} v_\ell$ to $\theta\left(\sum_{\ell=k+1}^{B} v_\ell + \varepsilon^{\uparrow}\right)$, with $\varepsilon^{\uparrow} > 0$. A closer inspection of the previous analysis on cases when the miner's revenue increases, case (1a) and case (1b) with overbidding, implies that the joint utility of the colluding users will decrease by at least Thus, the change to the joint utility of the miner and the colluding users is at most

$$(1 - \pi_0)\left(\theta \sum_{\ell=k+1}^{B} v_\ell + R\right) + (\theta - \gamma)\varepsilon^{\uparrow} \leq 0,$$

for the same reason as in (4.5), taking into account that $\varepsilon^{\uparrow} > \Delta$.

(3b) Suppose the miner's revenue decreases from $\theta \sum_{\ell=k+1}^{B} v_\ell$ to $\theta\left(\sum_{\ell=k+1}^{B} v_\ell - \varepsilon^{\downarrow}\right)$, with $\varepsilon^{\downarrow} > 0$. Then, the miner's utility drops to 0. From the previous analysis on cases when the miner's revenue decreases, case (1b) with underbidding and case (2b), we know the joint utility of the colluding users increases by at most $\theta\varepsilon^{\downarrow}$. So the joint utility of the miner and the colluding users is at most

$$-\pi_0\left(\theta \sum_{\ell=k+1}^{B} v_\ell + R\right) + \theta\varepsilon^{\downarrow} \leq 0,$$

for the same reason as in (4.2). (Clearly, $\varepsilon^{\downarrow} \leq \sum_{\ell=k+1}^{B} v_\ell$.)

□

5. Conclusions

In this paper, we consider the transaction fee mechanism design for the PoS protocol. Motivated by the miner's long-term objective, we propose a long-run utility for the miner, and demonstrate that it exhibits discontinuity. While the raw burning second price-auction recently proposed in the TFM literature fails to satisfy c-SCP under this long-run utility, a one-parameter generalization along with a minimum tick size achieves all three desired properties (UIC, MIC and c-SCP) for TFM.

There are several directions to extend this work. An obvious one is to consider the TFM for the PoW protocol, where the computational cost (and the R&D cost) needs to be taken into account. Second, one can also consider other types of strategic behaviors such that splitting a bid into small ones. This resorts to the study a combinatorial auction. Finally, some recent work proposed the notion of maximal extractable value (MEV) in the context of Flash Boys [8], and the proposer-builder separation (PBS) solution [3]. It would be interesting to analyze the TFM in these contexts.

Acknowledgements: We thank Elaine Shi for introducing and explaining to us the strict γ-utility. W. Tang gratefully acknowledges financial support through NSF grants DMS-2113779 and DMS-2206038, and through a start-up grant at Columbia University. David Yao's work is part of a Columbia-CityU/HK collaborative project that is supported by the InnoHK Initiative, The Government of the HKSAR and the AIFT Lab.

References

[1] M. Akbarpour and S. Li. Credible auctions: a trilemma. *Econometrica*, 88(2):425–467, 2020.

[2] S. Basu, D. Easley, M. O'Hara, and E. G. Sirer. Towards a functional fee market for cryptocurrencies. 2019. arXiv:1901.06830.

[3] V. Buterin. Proposer/block builder separation-friendly fee market designs. 2021. Available at `https://ethresear.ch/t/proposer-block-builder-separation-friendly-fee-market-designs/9725`.

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

[5] X. Chen, D. Simchi-Levi, Z. Zhao, and Y. Zhou. Bayesian mechanism design for blockchain transaction fee allocation. *arXiv e-prints*, 2022. arXiv:2209.13099.

[6] J. Chod, N. Trichakis, G. Tsoukalas, H. Aspegren, and M. Weber. On the financing benefits of supply chain transparency and blockchain adoption. *Manag. Sci.*, 66(10):4378–4396, 2020.

[7] H. Chung and E. Shi. Foundations of transaction fee mechanism design. In *Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 3856–3899. SIAM, Philadelphia, PA, 2023.

[8] P. Daian, S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, L. Breidenbach, and A. Juels. Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 910–927, 2020.

[9] M. Dowling. Is non-fungible token pricing driven by cryptocurrencies? *Finance Res. Lett.*, 44:102097, 2022.

[10] R. Durrett. *Probability: theory and examples*, volume 31 of *Cambridge Series in Statistical and Probabilistic Mathematics*. Cambridge University Press, Cambridge, fourth edition, 2010.

[11] M. V. Ferreira and S. M. Weinberg. Credible, truthful, and two-round (optimal) auctions via cryptographic commitments. In *Proceedings of the 21st ACM Conference on Economics and Computation*, pages 683–712, 2020.

[12] A. Kiayias, E. Koutsoupias, M. Kyropoulou, and Y. Tselekounis. Blockchain mining games. In *Proceedings of the 2016 ACM Conference on Economics and Computation*, pages 365–382, 2016.

[13] S. King and S. Nadal. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. 2012. Available at https://decred.org/research/king2012.pdf.
[14] V. Krishna. *Auction theory*. Academic Press, 2002.
[15] R. Lavi, O. Sattath, and A. Zohar. Redesigning bitcoin's fee market. *ACM Trans. Econ.*, 10(1):1–31, 2022.
[16] J. Mccrank and N. Nishant. Fidelity readies new spot bitcoin ETF filing, report says. 2023. Avalialbe at https://www.reuters.com/technology/fidelity-preparing-submit-spot-bitcoin-etf-filing-block-2023-06-27/.
[17] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He. Blockchain in healthcare applications: Research challenges and opportunities. *J. Netw. Comput. Appl.*, 135:62–75, 2019.
[18] R. B. Myerson. Optimal auction design. *Math. Oper. Res.*, 6(1):58–73, 1981.
[19] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, page 21260, 2008.
[20] J. G. Riley. Ex post information in auctions. *Rev. Econom. Stud.*, 55(3):409–429, 1988.
[21] I. Roşu and F. Saleh. Evolution of shares in a proof-of-stake cryptocurrency. *Manag. Sci.*, 67(2):661–672, 2021.
[22] T. Roughgarden. Transaction fee mechanism design for the Ethereum blockchain: An economic analysis of EIP-1559. 2020. arXiv:2012.00854.
[23] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen. Blockchain technology and its relationships to sustainable supply chain management. *Int. J. Prod. Res.*, 57(7):2117–2135, 2019.
[24] A. Sapirshtein, Y. Sompolinsky, and A. Zohar. Optimal selfish mining strategies in Bitcoin. In *Financial Cryptography and Data Security*, volume 9603 of *Lecture Notes in Comput. Sci.*, pages 515–532. Springer, Berlin, 2017.
[25] E. Shi, H. Chung, and K. Wu. What can cryptography do for decentralized mechanism design. 2022. arXiv:2209.14462.
[26] H. A. Simon. Bounded rationality. In *Utility and Probability*, pages 15–18. 1990.
[27] W. Tang. Stability of shares in the Proof of Stake protocol – concentration and phase transitions. 2022. arXiv:2206.02227.
[28] W. Tang. Trading and wealth evolution in the Proof of Stake protocol. 2023. arXiv:2308.01803.
[29] W. Tang and D. D. Yao. Trading under the proof-of-stake protocol–a continuous-time control approach. *Math. Finance*, 2023. arXiv:2207.12581. Available at https://onlinelibrary.wiley.com/doi/10.1111/mafi.12403.
[30] S. Tanwar, K. Parekh, and R. Evans. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *J. Netw. Comput. Appl.*, 50:102407, 2020.
[31] W. Vickrey. Counterspeculation, auctions, and competitive sealed tenders. *J. Finance*, 16(1):8–37, 1961.
[32] Q. Wang, R. Li, Q. Wang, and S. Chen. Non-fungible token (NFT): Overview, evaluation, opportunities and challenges. 2021. arXiv:2105.07447.
[33] G. Wood. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, 151:1–32, 2014.
[34] K. Wu, E. Shi, and H. Chung. Maximizing miner revenue in transaction fee mechanism design. 2023. arXiv:2302.12895.

Department of Industrial Engineer and Operations Research, Columbia University.
Email address: wt2319@columbia.edu

Department of Industrial Engineer and Operations Research, Columbia University.
Email address: yao@columbia.edu