Collusion-Resilience in Transaction Fee Mechanism Design

Hao Chung
Carnegie Mellon University
haochung@andrew.cmu.edu

Tim Roughgarden
Columbia University and a16z crypto
tim.roughgarden@gmail.com

Elaine Shi
Carnegie Mellon University
runting@cs.cmu.edu

Abstract

Users bid in a transaction fee mechanism (TFM) to get their transactions included and confirmed by a blockchain protocol. Roughgarden (EC'21) initiated the formal treatment of TFMs and proposed three requirements: user incentive compatibility (UIC), miner incentive compatibility (MIC), and a form of collusion-resilience called OCA-proofness. Ethereum's EIP-1559 mechanism satisfies all three properties simultaneously when there is no contention between transactions, but loses the UIC property when there are too many eligible transactions to fit in a single block. Chung and Shi (SODA'23) considered an alternative notion of collusion-resilience, called c-side-constract-proofness (c-SCP), and showed that, when there is contention between transactions, no TFM can satisfy UIC, MIC, and c-SCP for any $c \geq 1$. OCA-proofness asserts that the users and a miner should not be able to "steal from the protocol" and is intuitively weaker than the c-SCP condition, which stipulates that a coalition of a miner and a subset of users should not be able to profit through strategic deviations (whether at the expense of the protocol or of the users outside the coalition).

Our main result is the first proof that, when there is contention between transactions, no (possibly randomized) direct-revelation TFM satisfies UIC, MIC, and OCA-proofness. This result resolves the main open question in Roughgarden (EC'21). We also suggest several relaxations of the basic model that allow our impossibility result to be circumvented.

Contents

1 Introduction

Real estate on the blockchain is scarce, and blockchain users bid in an auction called the transaction fee mechanism (TFM) to have their transactions included and confirmed on the blockchain. The original Bitcoin adopted a simple first-price auction, where the top k bids win and they each pay their bid. However, the first-price auction is known to incentivize untruthful bidding. Therefore, a line of subsequent works [LSZ19, Yao, BEOS19, BCD+, Rou20, Rou21, FMPS21, CS23, SCW23, WSC24, GY22, ZCZ22, BGR23, TY23, KKLP23, XFP23, CMW23, LRMP23, Ndi23] explored what is the dream TFM for blockchains. Most works [Rou20, Rou21, CS23, SCW23, WSC24, GY22, GY22, ZCZ22, BGR23, TY23] agree on roughly the same set of desiderata, that is, a dream TFM should provide incentive compatibility not just for an individual user, but also for the miner of the block. Further, a dream TFM should provide resilience against miner-user collusion.

Roughgarden [Rou21] was the first to formally define the aforementioned requirements for TFM, which he referred to as *user incentive compatibility*[1], (myopic) *miner incentive compatibility*, and *OCA-proofness*, where OCA stands "off-chain agreement" and refers to colluding strategies between the miner and a set of users that allow offchain transfers. Roughgarden [Rou21] also showed that the simple "posted price auction with all fees burnt", which corresponds to the behavior of Ethereum's EIP-1559 auction [BCD+] when there is no congestion, satisfies all three properties. However, the posted price auction with all fees burnt works only when the block size is infinite (i.e., when there is no congestion). In practice, however, congestion does happen especially when there are major events such as an NFT mint or price fluctuations — for example, in Ethereum, roughly 2.3% of the blocks experience congestion.[2] When congestion happens, approximately speaking, Ethereum's EIP-1559 mechanism falls back to the first-price auction which violates user incentive compatibility. Therefore, an interesting question is whether we can design a dream TFM satisfying all three properties for finite block sizes.

Chung and Shi [CS23] considered an alternative notion of collusion-resilience, called side-constract-proofness. Unfortunately, they proved that no (even randomized) TFM can simultaneously satisfy user incentive compatibility and side-constract-proofness. Since side-constract-proofness is stronger than OCA-proofness, the question raised by Roughgarden [Rou21] that whether we can have a dream mechanism satisfying all three properties under his notions is still open.

Two notions of miner-user collusion resilience. Here we examine the two notions of miner-user collusion resilience proposed by Roughgarden [Rou21] and Chung and Shi [CS23] in more detail.

- **OCA-proofness**: Roughgarden's notion, henceforth referred to as OCA-proofness, requires that there exists a bidding strategy, denoted σ, that maps a private valuation to a bid such that σ maximizes the joint utility of the global coalition (consisting of the miner of the present block and all users), and satisfies a set of natural properties: 1) it does not involve modifying the inclusion rule; 2) it is individually rational; 3) it requires each bidder to bid independently without looking at others' true values; and 4) each user submits only a single bid and does not inject fake bids. In particular, the truth-telling strategy where each user submits a single truthful bid simultaneously satisfies all of the above constraints — however, Roughgarden [Rou21] found

[1] User incentive compatibility (UIC) is usually called dominant-strategy incentive compatible (DSIC) in mechanism design literature.

[2] From Jan 1, 2024 to Feb 5, 2024, there are 256595 blocks have been produced on Ethereum, and 5840 blocks among them are full, where we say a block is full if more than 99.9% of the gas limit (30M) is used.

it helpful to allow the globally optimal strategy σ to be a non-truthful strategy, which explains his definitional choice.

- **c-SCP**: Chung and Shi's notion [CS23], henceforth called c-SCP (where SCP stands for side-contract-proofness), requires that the honest strategy (i.e., all users follows the honest bidding rule and the miner honestly implements the inclusion rule) is the profit-maximizing strategy for any coalition consisting of the miner of the present block and at most c users. For direct-revelation mechanisms, the honest bidding rule is just the truth-telling, while for non-direct-revelation mechanisms, the bidding rule can be more general (See Section 2.1 for the formal definition). Chung and Shi's notion in fact matches standard notions used in a line of work at the intersection of game theory and cryptography [HT04, KN08, ADGH06, OPRV09, AL11, ACH11, GKM+13, GKTZ15, GTZ15, Kat08, DR07, GLR10, CGL+18, WAS22, CCWS21, PS17, KMSW22, FW20, EFW22].

Philosophical considerations. The two notions of collusion resilience are meant to capture different philosophical considerations. OCA-proofness captures the intuitive requirement that the users and miners *should not be able to steal from the protocol* through strategic deviations — for this reason, Roughgarden's notion considered *only the global coalition* consisting of the miner and all users. By contrast, the c-SCP notion captures the intuitive idea that a miner-user coalition's best response is to act honestly, and that no strategic deviations can allow the coalition to *steal from other users or steal from the protocol*.

Relations between the two notions. Finally, it is worth noting the relationship between the two notions. A mechanism that is c-SCP for any c incentivizes any miner-user coalition (including the global coalition) to behave honestly. In this sense, a mechanism that is c-SCP for any c must be OCA-proof as well, where the global coalition's optimal strategy σ is simply the honest strategy. Moreover, the aforementioned "posted price mechanism with all fees burnt" satisfies c-SCP for any c, and therefore, it satisfies OCA-proofness, too.

1.1 Our Contributions

As explained, both Roughgarden's and Chung and Shi's collusion resilience notion captures meaningful incentive compatibility considerations. Recognizing their differences, one natural question arises: does Chung and Shi's finite-block impossibility still hold if we adopt the original OCA-proofness notion of Roughgarden in lieu of SCP? Notably, no existing TFM construction [LSZ19, Yao, BEOS19, BCD+, Rou20, Rou21, FMPS21, CS23, SCW23, WSC24, GY22, ZCZ22, BGR23, TY23, KKLP23, XFP23, CMW23, LRMP23, Ndi23] can simultaneously satisfy user incentive compatibility, miner incentive compatibility, and OCA-proofness under finite block size.

Main impossibility result. In our work, we give an affirmative answer to the above question. We show that indeed, an analog of Chung and Shi's finite-block impossibility still holds when we replace SCP with OCA-proofness. More specifically, we prove the following theorem.

Theorem 1.1. *Suppose the block size is finite. Then, no possibly randomized, direct-revelation TFM can simultaneously satisfy user incentive compatibility (UIC), miner incentive compatibility (MIC), and OCA-proofness. Further, this impossibility holds even when the globally optimal strategy σ need not be individually rational.*

Notice that in a direct-revelation TFM, a user is expected to bid truthfully, so if the mechanism satisfies UIC, a user's utility is maximized when it just reports its true value. However, OCA-proofness allows the global coalition to adopt a non-truthful bidding strategy σ even for direct-revelation mechanisms.

Our Theorem 1.1 is intuitively stronger but technically incomparable in comparison with Chung and Shi's impossibility, who showed that no TFM can simultaneously satisfy UIC and 1-SCP for finite block sizes. Interestingly, Chung and Shi's impossibility does not rely on MIC; however, MIC is necessary for our Theorem 1.1 to hold. Specifically, a simple second-price auction with no burning (see Remark 2) satisfies both UIC and OCA-proofness, but does not satisfy MIC since the miner may benefit by injecting a fake $(t+1)$-th bid where t is the number of confirmed bids, since the $(t+1)$-th bid sets the price for confirmed bids.

Global SCP. We suggest an analog of OCA-proofness called **global SCP**, which also intuitively captures the requirement that strategic users and miners cannot steal from the protocol. In our work, global SCP is not only a technical *stepping stone* towards proving Theorem 1.1, but also of *independent interest* as we explain later. Specifically, global SCP is almost the same as OCA-proofness, except for requiring σ to be the honest bidding strategy indicated by the mechanism. In other words, a mechanism satisfies global SCP, iff the honest strategy is profit-maximizing for the global coalition. It is easy to see that for a direct revelation mechanism, c-SCP for any c implies global SCP, which in turn implies OCA-proofness. To prove Theorem 1.1, we first prove the following theorem:

Theorem 1.2. *Suppose that the block size is finite. Then no possibly randomized TFM can simultaneously satisfy user incentive compatibility (UIC), miner incentive compatibility (MIC), and global SCP. Further, the impossibility holds even for non-direct-revelation mechanisms.*

We now explain why the global SCP notion is of independent interest. One advantage of global SCP is that the *revelation principle* holds for any TFM that satisfies UIC, MIC, and global-SCP, which we formally prove in Section 8. In other words, given any TFM that is UIC, MIC, and global-SCP, there is an equivalent direct-revelation mechanism that simulates it. For this reason, Theorem 1.2 rules out even non-direct-revelation TFMs that simultaneously satisfy UIC, MIC, and global-SCP.

By contrast, Theorem 1.1 holds only for direct-revelation mechanisms. In particular, in Section 6.1, we show a non-direct-revelation mechanism that simultaneously satisfies UIC, MIC, and OCA-proof. The mechanism is contrived and may not be practical, but it demonstrates the subtlety and the technical challenges when modelling the notion of collusion-resilience. This also suggests that the revelation principle does not hold for mechanisms that satisfy UIC, MIC, and OCA-proofness, partly because in such a mechanism, the bidding strategie used to establish UIC and the one used to establish OCA-proofness may be different.

Ways to circumvent the impossibilities. We suggest ways to circumvent the impossibility results. The impossibility of Theorem 1.1 can be circumvented as long as we make a relaxation in one of the following directions: 1) allowing non-direct revelation mechanisms; or 2) allowing users to coordinate in bidding in the globally optimal strategy σ. We provide more details in Section 7. In the same section, we also raise an open question regarding whether it is possible to use cryptography (e.g., the MPC-assisted model of Shi et al. [SCW23]) and Bayesian notions of incentive compatibility to circumvent the impossibilities.

2 Definitions

2.1 Transaction Fee Mechanism

In this work, we assume all transactions have the equal size, and we define the *block size* to be the maximal number of transactions that can be included in a block. If there exists a finite number k such that a block can include at most k transactions, we say the block size is *finite*;[3] otherwise, we say the block size is *infinite*. Additionally, we assume that the users' utilities are independent of the order of the transactions in a block. In practice, transactions may have different sizes and the order of the transactions matters. For example, the size is measured in "gas" in Ethereum, and the prices for trading may depend on the order of the transactions. However, for our impossibility results, these assumptions only make them stronger.

We use the notation $\mathbb{R}_{\geq 0}$ to denote non-negative reals. A transaction fee mechanism (TFM) consists of the following possibly randomized algorithms:

- **Bidding rule** (executed by the user): takes in the user's true valuation $v \in \mathbb{R}_{\geq 0}$ for getting its transaction confirmed, and outputs a vector of a nonnegative number real-valued bids. Without loss of generality, we assume that at most one bid in the output vector may correspond to the user's actual transaction[4] which has a true value of v (henceforth called the *primary* bid), and the remaining bids are *fake bids* with a true value of 0. For a *direct revelation* mechanism, the honest bidding rule asks the user to submit a single primary bid that reports its true value. Our formulation is more general and admits non-direct-revelation mechanisms, too.[5]

- **Inclusion rule** (executed by the miner): takes a bid vector $\mathbf{b} = (b_1, \ldots, b_t) \in \mathbb{R}^t$ as input, and outputs a subset of $S \subseteq \mathbf{b}$ indicating which bids to be included in the block. When the block size k is *finite*, it must be that $|S| \leq k$.

- **Confirmation rule** (executed by the blockchain): takes as input a block $\mathbf{B}$, i.e., a vector of included bids, and outputs a subset of $\mathbf{B}$ to be confirmed. In general, not all transactions included in the block must be confirmed, and only the confirmed transactions are executed.[6]

- **Payment rule** (executed by the blockchain): given a block $\mathbf{B}$ as input, outputs the payment of each bid. We require *individual rationality*, i.e., for any vector of true values $\mathbf{v} = (v_1, \ldots, v_t)$, if all users execute the honest bidding rule, and we then execute the honest inclusion, confirmation, and payment rules, then the following holds with probability 1: for every user $i \in [t]$, if its primary bid is not confirmed, then its total payment is zero; else if its primary bid is confirmed, then its total payment is at most its true value v_i. Here, a user's total payment is the sum of the payment of all bids it has submitted.

- **Miner revenue rule** (executed by the blockchain): given a block $\mathbf{B}$ as input, outputs how much revenue the miner gets. We require *budget feasibility*, i.e., the miner's revenue is at most the total payment collected from all confirmed bids. When the miner revenue is strictly smaller

[3] The finite block size regime in this work and [CS23] corresponds to the case in [Rou21] where the base fee in the EIP-1559 or tipless mechanisms is *excessively low*, i.e. the number of transactions willing to pay the base fee exceeds the maximum block size (c.f. Definition 5.6 in [Rou21]).

[4] The blockchain protocol can always suppress conflicting or double-spending transactions.

[5] Throughout the paper except Section 8, we only focus on the bidding rules that output a single bid. In Section 8, we consider general bidding rules, and they may output multiple bids.

[6] Roughgarden [Rou21] assumes that all included transactions are confirmed. However, Chung and Shi [CS23] show that allowing unconfirmed transactions in a block enlarges the design space. For example, some mechanisms require that a block to contain some unconfirmed transactions (See Section 7 in [CS23]).

than the total payment, the difference between the total payment and the miner revenue is said to be *burnt*, i.e. eliminated from the circulation.

We say a TFM is *trivial* if the confirmation probability of all transactions is zero for any bid vector assuming the miner honestly follows the inclusion rule; otherwise, it is called *non-trivial*.

A strategic miner or miner-user coalition may deviate from the honest inclusion rule. On the other hand, since the confirmation, payment, and miner revenue rules are executed by the blockchain, they are always implemented honestly.

We focus on mechanisms that are *weakly symmetric*, i.e., mechanisms that do not make use of the bidders' identities or other auxiliary information (e.g., timestamp, transaction metadata), except for tie-breaking among equal bids. More formally, we define weak symmetry as below.

Definition 1 (Weak symmetry)**.** A mechanism is called *weakly symmetric* if the mechanism can always be equivalently described in the following manner: given a bid vector $\mathbf{b}$ where each bid may carry some extra information such as identity or timestamp, the honest mechanism always sorts the vector $\mathbf{b}$ by the bid amount first. During the sorting step, if multiple bids have the same amount, then arbitrary tie-breaking rules may be applied, and the tie-breaking can depend on the extra information such as timestamp, identity, or random coins. After this sorting step, the inclusion rule and the confirmation rules should depend only on the amount of the bids and their relative position in the sorted bid vector.

The above weak symmetry definition is equivalent to the following: for two bid vectors $\mathbf{b}$ and $\mathbf{b}'$ of length n that are equivalent up to a permutation, then the distribution of the mechanism's outcomes on $\mathbf{b}$ and $\mathbf{b}'$ are identically distributed — assuming that the outcome is encoded in the form of $\left(\mu, \mathsf{sorted}(\{(v_i, x_i, p_i)\}_{i\in[n]})\right)$ sorted in descending order of v_i, where μ encodes the the miner's revenue, each tuple (v_i, x_i, p_i) indicates that some user with bid v_i had the confirmation outcome $x_i \in \{0, 1\}$, and paid p_i.

Strategy space. A strategic user can deviate from the honest bidding rule and post an arbitrary bid vector with zero to multiple bids. Without loss of generality, we may assume that in the strategic bid vector, at most one bid can correspond to the user's actual transaction which has a non-zero true value; all other bids must be fake bids with zero true value. A strategic miner can deviate from the honest inclusion rule, and instead create an arbitrary block (subject to the block size limit) that includes any subset of the bid vector as well as any number of fake bids that it chooses to inject. A strategic miner-user coalition can adopt a combination of the above strategies.

Utility and social welfare. In this work, we consider a single-parameter environment, where each user has a true value $v \in \mathbb{R}_{\geq 0}$. For a user with true value v, let $x \in \{0, 1\}$ be the indicator whether its primary bid is confirmed or not, let p denote its total payment, then the user's utility is $x \cdot v - p$. The miner's utility is simply its revenue. The social welfare is defined to be the sum of everyone's utilities, including all users and the miner.

Notice that we allow the miner revenue to be smaller than the sum of users' payment, since the coins can be burnt. When calculating the social welfare, the payments among the users and the miner are cancelled out, so the social welfare is independent of the payment; however, the amount of burnt coins decreases the social welfare. For example, suppose there is only one user, and let p be the user's payment and q be the amount of burnt coins. In this case, the user's utility is $x \cdot v - p$, the miner revenue is $p - q$, and the social welfare is $(x \cdot v - p) + (p - q) = x \cdot v - q$.

2.2 Incentive Compatibility Notions

Definition 2 (User incentive compatible (UIC))**.** A TFM is said to be *user incentive compatible (UIC)*, iff the following holds: for any user i, for any bid vector $\mathbf{b}_{-i}$ that corresponds to the bids posted by all other users, user i's expected utility is always maximized when it follows the honest bidding rule (assuming that the miner executes the inclusion rule honestly). Notice that for a direct-revelation mechanism, the bidding rule is just truth-telling, so following the honest bidding rule simply means submitting the value truthfully; for a non-direct-revelation mechanism, a bidding rule may ask a user to submit a bid other than its true value.

Definition 3 (Miner incentive compatible (MIC))**.** A TFM is said to be *miner incentive compatible (MIC)*, iff given any bid vector $\mathbf{b}$, the miner's expected utility is maximized when the miner does not inject any fake bid and creates a block indicated by the honest inclusion rule.

Definition 4 (c-side-contract-proof (c-SCP))**.** A TFM is said to be c-side-contract-proof (c-SCP), iff for any coalition C consisting of the miner and between 1 and at most c users, and for any bid vector $\mathbf{b}_{-C}$ that corresponds to the bids posted by all users not in C, the coalition's joint utility is always maximized when it adopts the honest strategy, i.e., all users in the coalition bid according to the honest bidding rule, and the miner follows the honest inclusion rule.

Definition 5 (Global-side-contract-proof (global-SCP))**.** A TFM is said to be *global-side-contract-proof (global-SCP)*, iff given any vector of true values $\mathbf{v}$, the expected social welfare is maximized when the all users bid according to the honest bidding rule, and the miner follows the honest inclusion rule, where the maximization is taken over all the coordinated strategies that the coalition consisting of the miner and all users can adopt.

Definition 6 (OCA-proof)**.** A TFM is said to be *OCA-proof* iff there exists an individually rational bidding strategy $\sigma : \mathbb{R}_{\geq 0} \to \mathbb{R}$ such that the expected social welfare is maximized when the all users bid according to σ, and the miner creates a block indicated by the inclusion rule, where the maximization is taken over all the coordinated strategies that the coalition consisting of the miner and all users can adopt.

In the definitions above, the expectation is taken over the randomness of the TFM. More explicitly, in Definition 2, the expectation is taken over the randomness of the inclusion/confirmation/payment rules; in Definitions 3 to 6, the expectation is taken over the randomness of the inclusion/confirmation/payment/miner revenue rules.

Note that in the OCA-proofness definition, σ is required to output a single real-valued bid. A canonical example of σ is scaling; that is, $\sigma(v) = \gamma v$ for some $\gamma \in [0, 1]$ (c.f. Corollary 5.12 and 5.14 in [Rou21]).

3 Preliminary: Myerson's Lemma

In a single-parameter environment, if a direct-revelation TFM satisfies UIC, then for any user, its confirmation probability and the payment must satisfy the famous Myerson's lemma [Mye81]. It is an important ingredient for proving our impossibilities, and we review it in this section. Formally, given a bid vector $\mathbf{b} = (b_1, \ldots, b_t)$, let $x_i(\mathbf{b}) \in [0, 1]$ denote the probability that user i's bid is confirmed, and let $p_i(\mathbf{b})$ denote user i's expected payment assuming the miner implements the mechanism honestly. For any vector $\mathbf{b}$, let $\mathbf{b}_{-i}$ denote a vector when we remove i-th coordinate in $\mathbf{b}$. With these notations, Myerson's lemma can be stated as follows.

Lemma 3.1 (Myerson's lemma [Mye81])**.** *In a single-parameter environment, for any direct-revelation TFM that satisfies UIC, it must be*

- *For any user i, bid vector $\mathbf{b}_{-i}$, and b_i, b_i' such that $b_i' > b_i'$, it must be $x_i(\mathbf{b}_{-i}, b_i') \geq x_i(\mathbf{b}_{-i}, b_i)$.*
- *For any user i, bid vector $\mathbf{b}_{-i}$ from other users, and bid b_i from user i, user i's expected payment must be*

$$p_i(\mathbf{b}_{-i}, b_i) = b_i \cdot x_i(\mathbf{b}_{-i}, b_i) - \int_0^{b_i} x_i(\mathbf{b}_{-i}, t)dt,$$

with respect to the normalization condition: $p_i(\mathbf{b}_{-i}, 0) = 0$, i.e. user i's payment must be zero when $b_i = 0$.

When the mechanism is deterministic, the confirmation probability x_i is either 0 or 1. In this case, user i's payment can be simplified as

$$p_i(\mathbf{b}_{-i}, b_i) = \begin{cases} \inf\{z \in [0, b_i] : x_i(\mathbf{b}_{-i}, z) = 1\}, & \text{if } x_i(\mathbf{b}_{-i}, b_i) = 1; \\ 0, & \text{if } x_i(\mathbf{b}_{-i}, b_i) = 0. \end{cases}$$

Conceptually, user i must pay the minimal price which makes its bid confirmed.

4 Warmup: Impossibility of UIC + MIC + Global SCP for Deterministic Mechanisms

As a warmup, we first show a finite-block impossibility for UIC + MIC + global SCP for *deterministic* mechanisms. Recall that a TFM is said to be trivial if everyone's confirmation probability is zero for any bid vector assuming the miner follows the inclusion rule. In this case, everyone's utility is always zero in an honest execution. We will show that no non-trivial mechanism can satisfy all three properties simultaneously. Later in Section 5, we extend the impossibility to randomized mechanisms. Due to the revelation principle we prove in Section 8, if we can prove the impossibility for direct-revelation mechanisms, the impossibility immediately extends to non-direct mechanisms as well. Therefore, in this section, we shall assume direct-revelation mechanisms.

Lemma 4.1. *For any global-SCP mechanism, the confirmed bids must correspond to the highest bids.*

Proof. Suppose in some scenario, Alice bids her true value b and Bob bids his true value $b' < b$; however, Bob's bid is confirmed and Alice's is not. Now, we can have Alice and Bob swap their bids. The miner creates the same block as before in which the position originally corresponding to Bob now has Alice's bid of b'. Since the mechanism is weakly symmetric (Definition 1), Alice's bid is confirmed. This way, the social welfare increases by $b - b'$ in comparison with the honest case, and this violates global SCP. □

Lemma 4.2. *For any global-SCP mechanism, the amount of burnt coins depends only on the number of confirmed bids.*

Proof. Suppose in two different scenarios, when everyone acts honestly, the blocks made are $\mathbf{B}$ and $\mathbf{B}'$ respectively, the confirmed bids are $\mathbf{b} \subseteq \mathbf{B}$ and $\mathbf{b}' \subseteq \mathbf{B}'$ respectively where $\mathbf{b}$ and $\mathbf{b}'$ are of the same length, and the burnt amount in the two scenarios are q and q' respectively, where $q < q'$. Now, suppose we are actually in the second scenario. A global coalition can adopt the following strategy: create a block identical to $\mathbf{B}$ in which the confirmed bids correspond to the users with

the highest true values and the rest can be fake bids. Observe that the social welfare is the sum of the true values of all confirmed bids (where fake bids have a true value of 0) minus the total coins burnt. Therefore, the above strategy achieves strictly higher social welfare than the honest case. □

Theorem 4.3. *No non-trivial deterministic TFM can simultaneously satisfy UIC, MIC, and global SCP when the block size is finite.*

Proof. Since the block size is finite, there must exist a scenario that maximized the number of confirmed bids. Suppose in this scenario, the block created is $\mathbf{B}$ and the confirmed bids contained in $\mathbf{B}$ are $\mathbf{b} = (b_1, \ldots, b_m)$ sorted from high to low. Since the mechanism is non-trivial, we have $m \geq 1$. Given Lemma 4.2, we can use q_i to denote the amount of burnt coins when exactly i bids are confirmed.

First, we show that in any scenario with at least m users whose true values are sufficiently large w.r.t. $q_0, q_1, \ldots, q_m$, if everyone acts honestly, the mechanism must confirm m bids — by Lemma 4.1, they must also be the m highest bids. Suppose this is not the case, say, $m' < m$ bidders are confirmed — by Lemma 4.1, they must be the m' highest bids. Now, the global coalition can create the block $\mathbf{B}$ where the m confirmed bids correspond the users with the highest true values, and the rest can just be fake bids. In comparison with the honest case, the increase in social welfare is $\sum_{i=m'+1}^{m} (v_i - (q_i - q_{i-1}))$ which is positive as long as users' true values v_i's are sufficiently large. This violates global SCP.

Imagine a scenario with at least $m+1$ users whose true values are sufficiently high, and $v_1 \geq \cdots \geq v_m > v_{m+1}$. By Lemma 4.1, it must be $v_1, \ldots, v_m$ are confirmed. Because the mechanism is UIC, by Myerson's lemma, all m confirmed bids must pay v_{m+1}. However, such a mechanism violates MIC, because the miner can pretend that there is a fake bid $v' \in (v_{m+1}, v_m)$. Because the burnt amount is fixed to q_m, the miner will get more revenue if every confirmed bid pays v' instead of v_{m+1}. □

5 Impossibility of UIC + MIC + Global SCP for Randomized Mechanisms

In this section, we extend the finite-block impossibility of UIC + MIC + global SCP to even randomized mechanisms. Recall that a TFM consists of five rules as defined in Section 2.1, and a randomized TFM may use randomness in any of the five rules. Since the confirmation, the payment, and the miner revenue rules are executed by the blockchain, the strategic players can only bias the randomness in and deviate from the bidding rule and the inclusion rule. Again, due to the direct revelation principle proven in Section 8, it suffices to consider direct-revelation mechanisms.

5.1 Proof Roadmap

A new challenge in the randomized setting is that whether a bid is confirmed becomes probabilistic, and the arguments in Section 4 no longer hold. Here we give a brief roadmap of our new proof. The key idea of the proof is captured in Lemma 5.4, which says that if there are i equal bids $(\underbrace{b, \ldots, b}_{i})$, followed by other bids $(b_{i+1}, \ldots, b_{k+1})$ that are strictly smaller than b, then $b_{i+1}, \ldots, b_{k+1}$ must be unconfirmed with probability 1, and moreover, all the b-bids must pay b when confirmed, i.e., the total user utility is 0 — throughout, we use k to denote the block size. Since Lemma 5.4 imposes

a very strong constraint on the TFM, using it to lead to the final impossibility is not too hard (see Theorem 5.6).

We therefore give an intuition of the proof of Lemma 5.4. Specifically, we get this lemma through an inductive proof. The base case is the scenario $(\underbrace{b, \ldots, b}_{k}, b_{k+1})$ where $b_{k+1} < b$. Using global SCP and the fact that the block size is only k, we show that the b_{k+1} must be unconfirmed with probability 1. Then, we show that the k bids at b must pay b if they are confirmed. To show this, we first argue that in a TFM that is MIC and global SCP, the total user utility is equivalent if b_{k+1} is anything below b (see Lemma 5.3). We then consider a scenario where the $(k+1)$-th bid $b_{k+1} < b$ is arbitrarily close to b, and consider lowering one of the first k bids (say, the first bid) to $b_{k+1} - \delta$ — in this case, we argue that the first bid will become unconfirmed using global SCP. Finally, by Myerson's lemma, we conclude that in the original scenario $(\underbrace{b, \ldots, b}_{k}, b_{k+1} < b)$, first bid must pay b when confirmed.

Once we prove the base case, we now do an induction for $i = k-1, k-2, \ldots, 1$. The induction step is similar in structure to the base case, except that we first need to use the induction hypothesis that in the scenario $(\underbrace{b, \ldots, b}_{i}, b_{i+1} < b, \ldots)$, all the b bids pay b when confirmed, to conclude that in the scenario $(\underbrace{b, \ldots, b}_{i-1}, b_i < b, \ldots)$, b_i is unconfirmed with probability 1 — this follows due to Myerson's lemma. From this point on, the rest of the proof for the induction step is similar to the base case.

5.2 Formal Proofs

In the rest of this section, we present the formal proofs.

Lemma 5.1. *Suppose the mechanism satifies global SCP. Then, for any bid vector $\mathbf{b} = (b_1, \ldots, b_t)$, if $b_i > b_j$, it must be that $x_i(\mathbf{b}) \geq x_j(\mathbf{b})$ where $x_i(\mathbf{b})$ and $x_j(\mathbf{b})$ denote user i and j's confirmation probabilities, respectively.*

Proof. For the sake of contradiction, suppose there exists two integers i, j such that $b_i > b_j$ and $x_i(\mathbf{b}) < x_j(\mathbf{b})$. The global coalition can swap user i's and user j's bids. Concretely, user i should bid b_j and user j should bid b_i. Since the bid vector is the same as before (though b_i represents user j's bid, and b_j represents user i's bid), the expected burning is the same as before. However, since the mechanism is weakly symmetric, the social welfare increases by $(b_i \cdot x_j(\mathbf{b}) + b_j \cdot x_i(\mathbf{b})) - (b_i \cdot x_i(\mathbf{b}) + b_j \cdot x_j(\mathbf{b})) > 0$, which violates global-SCP. □

Lemma 5.2. *Suppose the mechanism satisfies global SCP and let the block size be k. Consider any bid vector satisfying $b_1 \geq b_2 \geq \ldots \geq b_k > b_{k+1}$. Then, it must be that b_{k+1} has 0 probability of confirmation.*

Proof. Suppose for the sake of contradiction that b_{k+1} has non-zero probability of confirmation. This means it must be included in the block with some non-zero probability p, and conditioned on being included, it has a non-zero probability p' of confirmation. A global coalition whose true values are $b_1, \ldots, b_{k+1}$ can play the following strategy. First, run the honest mechanism in its head including flipping any coins required by the inclusion rule assuming everyone bids honestly, and let $\mathbf{B}$ be the resulting block. If $b_{k+1} \notin \mathbf{B}$, just have everyone bid truthfully and build the block $\mathbf{B}$. Else, if $b_{k+1} \in \mathbf{B}$, then let $b_i > b_{k+1}$ be one bid that is left out of the block — such a bid must exist because the block size is only k. The coalition will have the i-th user actually bid b_k and build the

same block $\mathbf{B}$ where the b_{k+1} actually corresponds to user i's strategic bid. With this strategy, the coalition's expected gain in utility is $p \cdot p' \cdot (b_i - b_{k+1}) > 0$, which violates global SCP. □

Lemma 5.3. *Suppose the mechanism satisfies MIC and global SCP. Let* $\mathbf{a}$ *be an arbitrary vector of positive length, and let* $\mathbf{b}, \mathbf{b}'$ *arbitrary vectors —* $\mathbf{b}$ *and* $\mathbf{b}'$ *may or may not be of the same length, and their lengths are allowed to be* 0*. Consider two scenarios with bid vectors* $(\mathbf{a}, \mathbf{b})$ *and* $(\mathbf{a}, \mathbf{b}')$ *respectively. Suppose that* $\mathbf{b}$ *and* $\mathbf{b}'$ *have 0 confirmation probability in each of the two scenarios, respectively. Then, both scenarios enjoy the same expected miner utility, total social welfare, and total user utility.*

Proof. We first prove that expected miner utility is the same in both scenarios. Suppose this is not true, and without loss of generality, suppose expected miner utility is higher in scenario 1. Then, the miner can ignore the bids $\mathbf{b}$, inject the fake bids $\mathbf{b}'$, pretend that the bid vector is $(\mathbf{a}, \mathbf{b}')$, and run the honest mechanism. Since the confirmation probability of $\mathbf{b}'$ is 0, the miner need not pay any cost for the fake bids. Therefore, the miner gets higher expected utility by taking the above strategy which violates MIC.

The proof of global SCP is similar. Suppose, without loss of generality, that the expected total social welfare in scenario 1 is higher. Then, the global coalition can inject fake bids $\mathbf{b}'$ and pretend that the bid vector is $(\mathbf{a}, \mathbf{b}')$, thus allowing it to increase its expected social welfare. This violates global SCP.

The equivalence in total user utility follows directly from the above, since total user utility is the difference between the social welfare and the miner utility. □

Lemma 5.4. *Suppose the mechanism satisfies UIC, MIC and global SCP, and the block size is* k*. Let* $\mathbf{b} = (b_1, \ldots, b_{k+1})$ *be any vector where* $b_1 = b_2 = \cdots = b_i > b_{i+1} > \cdots > b_{k+1}$*. Then, under the bid vector* $\mathbf{b}$*, the following hold: 1) users* $i+1, \ldots, k+1$ *have* 0 *confirmation probability; and 2) the total user utility is* 0 *assuming every one is bidding their true value.*

Proof. We prove both statements by induction. Henceforth, given a bid vector $\mathbf{b} = (b_1, \ldots, b_{k+1})$, we use $x_i(\mathbf{b})$ to denote the confirmation probability of the i-th user under $\mathbf{b}$.

Base case. The base case is when $i = k$; that is, there are $k+1$ users with valuations $\mathbf{b} = (b_1, \ldots, b_{k+1})$ where $b_1 = \cdots = b_k > b_{k+1}$. By Lemma 5.2, we have $x_{k+1}(\mathbf{b}) = 0$. Next, we show that the joint utility of all users must be zero. By Lemma 5.3 and Lemma 5.2, the total user utility under $\mathbf{b} = (\underbrace{b, \ldots, b}_{k}, b_{k+1})$ is the same as under $\mathbf{b}' = (\underbrace{b, b, \ldots, b}_{k}, b - \delta)$ for any arbitrarily small $\delta > 0$ — in both cases, the last user must have 0 confirmation probability. Now, consider the scenario $\mathbf{b}' = (\underbrace{b, b, \ldots, b}_{k}, b - \delta)$. If one of the b-bidders denoted $i \in [k]$ lowered its bid to less than $b - \delta$ (and everyone else's bids stay the same), its confirmation probability would become 0 by Lemma 5.2. Since the mechanism is UIC, by Myerson's lemma, under $(b, b, \ldots, b, b - \delta)$, user i's expected payment must be at least $(b - \delta) \cdot x_i(\mathbf{b}')$. Therefore, user i's expected utility is at most $\delta \cdot x_i(\mathbf{b}')$. Therefore, the expected total user utility under $\mathbf{b}'$ is at most $k \cdot \delta \cdot x_i(\mathbf{b}') \leq k \cdot \delta$. This means that under $\mathbf{b} = (b_1, \ldots, b_{k+1})$, the expected total user utility is at most $k \cdot \delta$ for any arbitrarily small $\delta > 0$, i.e., the expected total user utility is at most 0. Finally, by the individual rationality of the payment rule, each user's utility is non-negative when it bids truthfully. Therefore, the expected total user utility is 0.

Inductive step. Fix any $i \in \{2, \ldots, k\}$, suppose the lemma statement holds. We will show that the lemma also holds for any vector $\mathbf{b} = (b_1, \ldots, b_{k+1})$ where $b_1 = b_2 = \cdots = b_{i-1} > b_i > b_{i+1} > \cdots > b_{k+1}$.

We first show that all users $i, \ldots, k+1$ are unconfirmed. Consider the vector $\underbrace{b, b, \ldots, b}_{i}, b_{i+1}, \ldots, b_{k+1}$. By our induction hypothesis, i users can have non-zero confirmation probability and moreover, the total user utility is 0. Because of individual rationality, each user's utility must be non-negative, so every user's utility is also 0. In this case, whenever a bid is confirmed, the payment is equal to the bid (and hence the true value). By UIC and Myerson's lemma, it means that if the i-th user lowers its bid to $b_i < b$ (which becomes the scenario $\mathbf{b}$ we care about), then user i's confirmation probability becomes 0. By Lemma 5.1, users $i+1, \ldots, k+1$ must have 0 confirmation probability under $\mathbf{b}$ too.

Next, we show that the joint utility of all users is zero under $\mathbf{b}$ and assuming everyone bids truthfully. By Lemma 5.3, the total user utility under $\mathbf{b}$ is the same as under the scenario $\mathbf{b}' = (\underbrace{b, b, \ldots, b}_{i-1}, b-\delta, b-2\delta, \ldots, b-(k+2-i)\delta)$ for an arbitrarily small $\delta > 0$ — since in both scenarios, users $i, \ldots, k+1$ have 0 confirmation probability. Under $\mathbf{b}'$, if any b-bidders denoted j lowers its bid to less than $b-(k+2-i)\delta$, its confirmation probability becomes 0 by Lemma 5.2. By UIC and Myerson's lemma, j's expected payment under $\mathbf{b}'$ is at least $(b-(k+2-i)\delta) \cdot x_j(\mathbf{b}')$. This means that the total user utility under $\mathbf{b}'$ is at most $(k+2-i)\delta \cdot x_j(\mathbf{b}') \cdot (i-1) \leq k^2\delta$. Therefore, under $\mathbf{b}$, the total user utility is at most $k^2\delta$ for any arbitrarily small $\delta > 0$. This means that the total user utility under $\mathbf{b}$ is at most 0. Finally, by the individual rationality of the payment rule, each user's utility is non-negative when it bids truthfully. Therefore, the expected total user utility is 0. □

Lemma 5.5. *Suppose the mechanism satisifies UIC, MIC and global SCP, and the block size is k. Let a be any positive real number. Consider a scenario with only one bid a. Then, the only user's utility is zero assuming it bids its true value.*

Proof. Fix $a_1 > 0$. Consider any vector $\mathbf{a} = (a_1, a_2, \ldots, a_{k+1})$ such that $a_1 > a_2 > \cdots > a_{k+1}$. By Lemma 5.4, under $\mathbf{a}$, all users except the first user must have 0 confirmation probability, and moreover, the first user has utility 0. By Lemma 5.3, the total expected user utility under $\mathbf{a}$ and under a single bid a_1 are the same. Therefore, under a single bid a_1, the user's utility is also 0. □

Theorem 5.6. *No non-trivial, possibly randomized TFM can simultaneously satisfy UIC, MIC, and global SCP when the block size is finite.*

Proof. For the sake of contradiction, suppose the mechanism satisfies UIC, MIC, and global SCP. Since the mechanism is non-trivial, there must exist a scenario $\mathbf{b} = (b_1, \ldots, b_t)$ such that some user i has positive confirmation probability. Let $a > \sum_{j=1}^{t} b_j$. Then, under a scenario with only one bid a, we argue that the user must achieve positive expected utility assuming it is bidding truthfully, thus contradicting Lemma 5.5. To see this, suppose for the sake of contradiction that the user has 0 utility when bidding truthfully at a. Now, consider the following strategy which strictly increases its utility and thus violating UIC: replace its bid with b_i, inject the fake bids $\mathbf{b}_{-i}$, and pretend that the bid vector is $\mathbf{b}$. This way, the user would get positive confirmation probability and since its payment is at most $\sum_{j=1}^{t} b_j$, including considering b_i and the injected bids $\mathbf{b}_{-i}$, its expected utility is positive.

□

6 Feasibility and Impossibility of UIC + MIC + OCA-Proof

We can generalize the proof in Section 5, and rule out UIC, MIC, and OCA-proof (rather than global SCP) for direct-revelation mechanisms. Recall that for a direct-revelation mechanism, the difference between OCA-proof and global SCP is that global SCP insists that the optimal strategy of the global coalition is the truthful strategy, whereas OCA-proofness allows it to be some other strategy in which each user acts independently and bids the outcome of some function $\sigma(\cdot)$.

Interestingly, if we allow the bidding rule to be not truth-telling, i.e. considering non-direct-revelation mechanisms, we can have a mechanism that satisfies UIC, MIC, and OCA-proof. We present the feasibility for non-direct mechanisms in Section 6.1, and we prove the impossibility of UIC + MIC + OCA-proof for direct-revelation mechanisms in Section 6.2. Notice that because of the feasibility in Section 6.1, we must require the bidding rule to be truth-telling to reach an impossibility in Section 6.2.

6.1 A Non-Direct Mechanism with UIC + MIC + OCA-Proof

The rationale of the design is to signal to the mechanism when everyone is adopting the globally optimal strategy σ (as opposed to the bidding rule used to establish UIC). When the mechanism detects that everyone is behaving according to σ, it adopts a different behavior to optimize social welfare. We use the range $[0, 1)$ to encode the actual bid, and use the range $[1, \infty)$ for signalling. While the resulting mechanism is somewhat contrived and not necessarily meaningful from a practical point of view, it clarifies which notions of collusion-resilience most accurately capture the intended modeling goals and illustrates some technical challenges involved in the proof in Section 6.2. Consider the following TFM:

- **Globally optimal strategy** $\sigma(v)$: Given a true value v, output a bid $v + 1$.
- **Bidding rule**: Given a true value v, output a bid $1/(v + 2)$.
- **Inclusion rule**: Let S be the set of all pending bids that are in $[0, 1)$. If $|S| > k$, then randomly select k bids from S to include. If $1 \leq |S| \leq k$, then include all bids in S. If $|S| = 0$, choose the top up to k bids to include.
- **Confirmation, payment, and miner revenue rules**: All included bids are confirmed. Each confirmed bid pays nothing, and the miner gets nothing.

Obviously, this mechanism is non-trivial.

Claim 6.1. *The above mechanism satisfies UIC, MIC, and OCA-proofness.*

Proof. For UIC, notice that if a user follows the bidding rule, its bid is always in $[0, 1)$. If there is no bid in $[0, 1)$ before a user submits its bid, then bidding $1/(v + 2)$ always guarantees user's bid to be included and confirmed, where v denote the true value. If there is already some bids in $[0, 1)$ before a user submits its bid, then bidding $1/(v + 2)$ is a dominant strategy since it guarantees the user's bid is added to S, the set of all bids in $[0, 1)$, which is the best a user can do. Next, MIC holds since the miner revenue is always zero. Finally, if all users follows the globally optimal strategy σ, everyone's bid is at least 1. The honest inclusion rule will include the top up to k bids, which maximizes the social welfare. Thus, OCA-proofness holds. □

Remark 1. We can try to apply revelation principle, and bake the bidding rule into the mechanism so that the resulting mechanism is direct-revelation. For example, whenever seeing a bid b, the

miner and the mechanism view it as $1/(b+2)$. The modified mechanism, however, does not satisfy OCA-proofness anymore. This is not a coincidence as we will show that it is impossible to have a non-trivial direct-revelation mechanism satisfying UIC, MIC, and OCA-proofness in the next section.

6.2 Impossibility of UIC + MIC + OCA-Proof for Direct Mechanisms

The structure of the proof in this section is similar to the proof in Section 5. In fact, Lemmas 6.2, 6.3 and 6.5 to 6.7 and Theorem 6.8 are the analogies of Lemmas 5.1 to 5.5 and Theorem 5.6, respectively, except that we need to work on the images of σ in order to apply OCA-proofness. Before diving into the proof, we make a few remarks.

- A key step in Section 5 is to prove a user with true value v must have zero utility, and we prove it by making an unconfirmed bid arbitrarily close to v (see Lemma 5.4). To extend the similar idea to OCA-proofness, we require σ to be strictly increasing and continuous. In fact, we show that being strictly increasing is a consequence of UIC and OCA-proofness (Lemma 6.4). To make our proofs easier to follow, we assume that σ is continuous, and we prove our main result, Theorem 6.8. Later on, in Corollary 6.9, we explain how we remove the assumption of continuity; specifically, the fact that σ is strictly increasing implies that there exists a point where σ is continuous at.

- As we have seen a feasibility for non-direct mechanisms in Section 6.1, we must require the bidding rule to be truth-telling to reach an impossibility. Indeed, the proofs of Lemmas 6.4, 6.6 and 6.7 and Theorem 6.8 rely on Myerson's lemma, and Myerson's lemma requires the mechanism to be direct-revelation. Notice that the mechanism in Section 6.1 does not satisfy the requirements of Myerson's lemma. If we apply the revelation principle to make the mechanism become direct-revelation so that Myerson's Lemma could apply, it breaks OCA-proofness (see Remark 1).

- Notice that OCA-proofness requires σ to output a single real-valued bid. In fact, if we allow σ to output multiple bids, we can have a (somewhat contrived) mechanism that satisfies UIC, MIC, and OCA-proof (see Section 7.2). In particular, Lemma 6.4 requires σ only outputs a single real number.

- The original definition of OCA-proofness also requires σ to be individually rational, but this will not be needed for the impossibility proof.

Given any vector $\mathbf{b} = (b_1, \ldots, b_t)$ of the length t, let $\sigma(\mathbf{b})$ denote the element-wise application of σ, i.e. $\sigma(\mathbf{b}) = (\sigma(b_1), \ldots, \sigma(b_t))$.

Lemma 6.2. *Suppose the mechanism satisfies OCA-proofness with the globally optimal strategy σ. Then, for any bid vector $\sigma(\mathbf{b}) = (\sigma(b_1), \ldots, \sigma(b_t))$, if $b_i > b_j$, it must be that the confirmation probability of the bid $\sigma(b_i)$ is at least as high as that of $\sigma(b_j)$.*

Proof. Imagine that t players each have true values $b_1, \ldots, b_t$, and they all bid according to the globally optimal strategy σ. Let x_i, x_j denote the confirmation probabilities of $\sigma(b_i)$ and $\sigma(b_j)$ respectively. Suppose for the sake of contradiction that $b_i > b_j$, and $x_j > x_i$. The global coalition can engage in the following OCA: have users i and j swap their bids, that is, user i who has true value b_i bids $\sigma(b_j)$, and user j who has true value b_j bids $\sigma(b_i)$. The set of bids are the same as before, therefore, the expected burning amount does not change. The expected social welfare thus increases by $b_i x_j + b_j x_i - (b_i x_i + b_j x_j) = (b_i - b_j)(x_j - x_i) > 0$. This violates OCA-proofness and the fact that σ is the social-welfare-maximizing-strategy of the global coalition. □

Lemma 6.3. *Suppose the mechanism satisfies OCA-proofness with the globally optimal strategy σ, and let the block size be k. Given $b_1 \geq b_2 \geq \ldots \geq b_k > b_{k+1}$, then, under the bid vector $\sigma(b_1), \sigma(b_2), \ldots, \sigma(b_k), \sigma(b_{k+1})$, it must be that $\sigma(b_{k+1})$ have 0 probability of confirmation.*

Proof. Imagine that $k+1$ players each have true values $b_1, \ldots, b_{k+1}$, and they all bid according to the globally optimal strategy σ. It suffices to show the following: suppose $\sigma(b_{k+1})$ has a non-zero probability p of being included in the block, then conditioned on being included, its probability of confirmation must be 0. Suppose this is not true, and conditioned on being included, $\sigma(b_{k+1})$ has probability $p' > 0$ of being confirmed. Then, the global coalition can adopt the following OCA: run the honest inclusion rule in the head including flipping any coins required by the inclusion rule, and let $\mathbf{B}$ denote the resulting block. If $\sigma(b_{k+1})$ is not included in $\mathbf{B}$, simply output the block $\mathbf{B}$. Else if $\sigma(b_{k+1})$ is included in $\mathbf{B}$, then let $\sigma(b_i)$ be some bid that is left out — such a bid must exist because the block size is only k. Now, have the i-th user bid $\sigma(b_{k+1})$ and make an actual block $\mathbf{B}$ where the bid $\sigma(b_{k+1})$ corresponds to user i's bid. The expected increase in social welfare relative to everyone adopting σ is $p \cdot p' \cdot (b_i - b_{k+1}) > 0$ which violates OCA-proofness and the fact that σ is the social-welfare-maximizing strategy. □

Lemma 6.4. *Suppose a direct-revelation mechanism satisfies UIC and OCA-proofness with the globally optimal strategy σ, and let the block size be k. Then, there exists a constant c^* such that for any real numbers z, z' satisfying $z > z' > c^*$, it must be $\sigma(z) > \sigma(z')$. Conceptually, σ must be strictly increasing for large inputs.*

Proof. Since the mechanism is non-trivial, there exists a bid vector $(b_1, \ldots, b_t)$ such that the total confirmation probability is positive. Let b_i be the bid with the highest confirmation probability among $b_1, \ldots, b_t$. Let x be the confirmation probability of b_i and let c^* be any real number larger than $\sum_{j=1}^{t} b_j / x$. We will show that for any $z > z' > c^*$, $\sigma(z) > \sigma(z')$.

Consider a scenario where there are $k+1$ users all with the true value z. Suppose they form a global coalition and follow the bidding strategy σ so that the bid vector is $\mathbf{s} = (\underbrace{\sigma(z), \ldots, \sigma(z)}_{k+1})$. There are two possible cases.

First, there exists a user j with positive confirmation probability assuming the miner honestly follows the inclusion rule and select from the bid vector $\mathbf{s}$. Because the mechanism satisfies UIC, by Myerson's lemma, if user j increases its bid, the confirmation probability must be non-decreasing. Thus, if $\sigma(z) \leq \sigma(z')$, and user j increases its bid from $\sigma(z)$ to $\sigma(z')$, its confirmation probability is still positive. However, if user j bids $\sigma(z')$, the resulting bid vector will become $(\underbrace{\sigma(z), \ldots, \sigma(z)}_{k}, \sigma(z'))$. By Lemma 6.3, the bid $\sigma(z')$ has zero confirmation probability, which leads to a contradiction. Consequently, it must be $\sigma(z) > \sigma(z')$.

Second, if everyone's confirmation probability is zero assuming the miner honestly follows the inclusion rule and select from the bid vector $\mathbf{s}$, following σ will lead to zero social welfare. We argue that this case is impossible by showing an alternative strategy of the global coalition that achieves positive social welfare, contradicting the fact that σ is social-welfare-maximizing. Specifically, the alternative strategy works as follows: the global coalition pretends that the bid vector is $(b_1, \ldots, b_t)$ where the bid b_i corresponds to the primary bid of any user, say, the first user. Recall that the first user's true value is z. Thus, social welfare is at least $z \cdot x - p$, where p is the expected payment of all users. Since b_i has the highest confirmation probability among $b_1, \ldots, b_t$, p is at most $x \cdot \sum_{j=1}^{t} b_j$. Because $z > c^* > \sum_{j=1}^{t} b_j / x$, the social welfare is positive.

□

Lemma 6.5. *Suppose the mechanism satisfies MIC and OCA-proofness with the globally optimal strategy σ. Let $\mathbf{a}, \mathbf{b}, \mathbf{b}'$ be arbitrary vectors. Consider two scenarios $(\sigma(\mathbf{a}), \sigma(\mathbf{b}))$ and $(\sigma(\mathbf{a}), \sigma(\mathbf{b}'))$. Suppose that $\sigma(\mathbf{b})$ and $\sigma(\mathbf{b}')$ have 0 confirmation probability in each of the two scenarios, respectively. Then, both scenarios enjoy the same expected miner utility, social welfare, and total user utility.*

Proof. The equivalence in expected miner utility follows directly from MIC and the fact that the miner can change from $\mathbf{b}$ to $\mathbf{b}'$ for free, or vice versa, since these bids are unconfirmed.

The equivalence in social welfare follows from OCA-proofness, and the fact that σ maximizes social welfare. Suppose, for example, the social welfare under $(\sigma(\mathbf{a}), \sigma(\mathbf{b}))$ is strictly greater than $(\sigma(\mathbf{a}), \sigma(\mathbf{b}'))$. Then, under the scenario where the users' true values are $(\mathbf{a}, \mathbf{b}')$, everyone following σ will not maximize social welfare, since there is an OCA that have the users bid $(\sigma(\mathbf{a}), \sigma(\mathbf{b}))$ instead which strictly increases the social welfare.

The equivalence in total user utility follows directly from the above, since total user utility is the difference between the social welfare and the miner utility. □

Below, we will first prove the impossibility assuming that σ is a continuous function, and we will then discuss how to remove this assumption.

Lemma 6.6. *Suppose the direct-revelation mechanism satisfies UIC, MIC and OCA-proofness with the globally optimal strategy σ, and the block size is k. Suppose σ is a continuous function. Then, there exists a constant c^* such that for any $i \in [k]$, the following holds.*

- *Consider a scenario with the arbitrary bid vector $\mathbf{s} = (\underbrace{\sigma(b), \ldots, \sigma(b)}_{i}, \sigma(b_{i+1}), \ldots, \sigma(b_{k+1}))$, where $b > b_{i+1} > b_{i+2} > \ldots > b_{k+1} > c^*$. Then, the bids $\sigma(b_{i+1}), \ldots, \sigma(b_{k+1})$ have 0 confirmation probability.*
- *Moreover, if there are $k+1$ users with the true value $\mathbf{s}$, the expected total user utility is 0 when all users bid truthfully.*

Proof. By Lemma 6.4, there exists a constant c^* such that for any real numbers z, z' satisfying $z > z' > c^*$, it must be $\sigma(z) > \sigma(z')$. Throughout this proof, we assume $b_{k+1} > c^*$ so that σ is strictly increasing for any input larger than b_{k+1}. We will prove the lemma by induction.

Base case. The base case is when $i = k$; that is, there are $k+1$ users with the true values $\mathbf{s} = (\underbrace{\sigma(b), \ldots, \sigma(b)}_{k}, \sigma(b_{k+1}))$. Notice the true value is $\sigma(b)$ instead of b for the first k users. By Lemma 6.3, $\sigma(b_{k+1})$ has 0 confirmation probability. By Lemma 6.5, the total user utility under $\mathbf{s}$ is the same as under $\mathbf{s}' = (\underbrace{\sigma(b), \ldots, \sigma(b)}_{k}, \sigma(b-\delta))$ where $\delta > 0$ can be arbitrarily small — since in both scenarios, the last bid is unconfirmed. Now, suppose the bid vector is $\mathbf{s}'$. Fix any user with the true value $\sigma(b)$, say the first user. If it lowered its bid to anything less than $\sigma(b-\delta)$, its confirmation probability must be 0 by Lemma 6.3. Since the mechanism is UIC, by Myerson's lemma, the payment of the first user is at least $\sigma(b-\delta) \cdot x_1(\mathbf{s}')$. In this case, the first user's utility is at most $(\sigma(b) - \sigma(b-\delta)) \cdot x_1(\mathbf{s}') \leq \sigma(b) - \sigma(b-\delta)$. Therefore, the total user utility under $\mathbf{s}'$ (and hence under $\mathbf{s}$) is at most $k \cdot (\sigma(b) - \sigma(b-\delta))$. Since σ is continuous, and the above holds for any $\delta > 0$, the total user utility under $\mathbf{s}$ is at most 0. By the individual rationality of the payment rule, each user's utility is non-negative when it bids truthfully. Therefore, the expected total user utility is 0.

Inductive step. Fix any $i \in \{2, \ldots, k\}$, and suppose the lemma holds. We want to show that the lemma also holds for any $\mathbf{s}_{i-1} = (\underbrace{\sigma(b), \ldots, \sigma(b)}_{i-1}, \sigma(b_i), \sigma(b_{i+1}), \ldots, \sigma(b_{k+1}))$. Start from the scenario $\mathbf{s}_i = (\underbrace{\sigma(b), \ldots, \sigma(b)}_{i}, \sigma(b_{i+1}), \ldots, \sigma(b_{k+1}))$, and imagine that the i-th bid lowers from $\sigma(b)$ to $\sigma(b_i)$. Since the i-th user has 0 utility under $\mathbf{s}_i$, by UIC and Myerson's lemma, its confirmation probability must become 0 when it lowers its bid to $\sigma(b_i) < \sigma(b)$. By Lemma 6.2, the bids $\sigma(b_{i+1}), \ldots, \sigma(b_{k+1})$ must have 0 confirmation probability too.

We next show that under $\mathbf{s}_{i-1}$, total user utility is 0. Consider another bid vector $\mathbf{s}' := (\underbrace{\sigma(b), \ldots, \sigma(b)}_{i-1}, \sigma(b-\delta), \ldots, \sigma(b-(k+2-i)\delta))$ for some $\delta > 0$. By the argument above, the bids numbered $i+1, \ldots, k+1$ are not confirmed. By Lemma 6.5, the total user utility under $\mathbf{s}_{i-1}$ is the same as under the scenario $\mathbf{s}'$. In scenario $\mathbf{s}'$, if any of the $\sigma(b)$ bidders, say the first bidder, lowers its bid from $\sigma(b)$ to anything less than $\sigma(b-(k+2-i)\delta)$, its confirmation probability becomes 0 by Lemma 6.3. By UIC and Myerson, the first user's payment under $\mathbf{s}'$ is at least $\sigma(b-(k+2-i)\delta) \cdot x_1(\mathbf{s}')$, and its utility is at most $(\sigma(b) - \sigma(b-(k+2-i)\delta)) \cdot x_1(\mathbf{s}') \le \sigma(b) - \sigma(b-(k+2-i))\delta$. Therefore, the total user utility under $\mathbf{s}'$ (and also under $\mathbf{s}_{i-1}$) is upper bounded by $k \cdot (\sigma(b) - \sigma(b-(k+2-i)\delta))$. Since σ is continuous and the above holds for any arbitrarily small $\delta > 0$, it means that the total user utility under $\mathbf{s}_{i-1}$ is at most 0. By the individual rationality of the payment rule, each user's utility is non-negative when it bids truthfully. Therefore, the expected total user utility is 0. □

Lemma 6.7. *Suppose the direct-revelation mechanism satisfies UIC, MIC and OCA-proofness with the globally optimal strategy σ which is a continuous function, and the block size is k. Then, there exists a constant c^* such that for any $a > c^*$, if there is only a single user with the true value $\sigma(a)$, its utility is zero when it bids truthfully.*

Proof. By Lemma 6.6, there exists a constant c^* such that under the scenario $\mathbf{a} := (\sigma(a), \sigma(a_2), \ldots, \sigma(a_{k+1}))$ where $a > a_2 > \ldots > a_{k+1} > c^*$, the utility of the first user is 0 assuming it is bidding truthfully. Moreover, all users except the first user must have 0 confirmation probability. By Lemma 6.5, the total expected user utility under $\mathbf{a}$ and under a single bid $\sigma(a)$ are the same. Therefore, under a single bid $\sigma(a)$, the user's utility is also 0. □

Theorem 6.8. *No non-trivial, possibly randomized direct-revelation TFM can simultaneously satisfy UIC, MIC, and OCA-proofness (for a continuous σ) when the block size is finite.*[7]

Proof. We will show that under any sufficiently large a, the confirmation probability under a single bid $\sigma(a)$ is non-zero. If we can show this, then we can show a contradiction to UIC and the Myerson's lemma. Specifically, consider $b > a$ and both sufficiently large. By Lemma 6.7, under both scenarios, the user utility is 0 (assuming the bid, $\sigma(a)$ or $\sigma(b)$, is the same as the user's true value). By Lemma 6.4, for sufficiently large a, we have $\sigma(b) > \sigma(a)$. However, by Myerson's lemma, if the confirmation probabilities under a single $\sigma(a)$ and under a single $\sigma(b)$ are both non-zero, it cannot be that in both cases the user's utility is 0. Otherwise, the user with the true value $\sigma(b)$ can underbid $\sigma(a)$. Since the confirmation probability is non-zero and the payment is at most $\sigma(a)$, the user enjoys positive utility, which violates UIC.

We now show that the confirmation probability under a single bid $\sigma(a)$ for a sufficiently large a is non-zero assuming the miner honestly follows the inclusion rule. Suppose this is not true for the sake of a contradiction; that is, when the bid vector is just $\sigma(a)$ and the miner is honest, no one has

[7] We can remove the assumption that σ is continuous. See Corollary 6.9.

positive confirmation probability, so the social welfare is zero. Since the mechanism is non-trivial, there exists a scenario $\mathbf{b} = (b_1, \ldots, b_t)$ such that the total confirmation probability is non-zero, and let $x > 0$ be the confirmation probability of some bid b_i in $\mathbf{b}$. Consider $a > \sum_{j\in[n]} b_j/x$, and suppose there is only one user with the true value a. We will show that the strategy $\sigma(a)$ does not maximize social welfare which contradicts to the fact that σ is social-welfare-maximizing-strategy. Specifically, the user can post the bids $(b_1, \ldots, b_t)$ instead where position i corresponds to the user's primary bid and all others are fake bids. Note that under $\mathbf{b}$, the total user payment is at most $\sum_{j\in[n]} b_j$. Since the user's true value is greater than $\sum_{j\in[n]} b_j/x$ and its confirmation probability is x, the total user utility (and thus the social welfare) is positive under this new bidding strategy. □

Remark 2. Notice that Chung and Shi [CS23] showed that no TFM can simultaneously satisfy UIC and 1-SCP when the block size is finite. Their impossibility does not rely on MIC, while MIC is necessary for proving Theorem 6.8. Specifically, consider *the second-price auction without burning* defined as follows. Given the block size k, the miner includes the top up to k bids in the block. If the number of included bids is less than k, then all included bids are confirmed, and pay nothing. If the number of included bids is k, then the top $k-1$ bids are confirmed, while the k-th bid is unconfirmed (break tie arbitrarily). All confirmed bids pay the k-th bid, and all the payments go to the miner. This mechanism satisfies UIC since the confirmation and the payment satisfy the requirements of Myerson's lemma. The mechanism also satisfies OCA-proofness when σ is just bidding truthfully since the confirmed bids are always the ones with the highest true values, which maximizes the social welfare. However, it does not satisfy MIC, since the miner is incentivized to inject a fake bid to increase the k-th bid.

Removing the continuous assumption. So far, our Theorem 6.8 relies on the globally optimal strategy σ being a continuous function. We can in fact remove this assumption as shown in the proof of the following corollary.

Corollary 6.9. *No non-trivial, possibly randomized direct-revelation TFM can simultaneously satisfy UIC, MIC, and OCA-proofness when the block size is finite.*

Proof. In Lemma 6.4, we proved that σ strictly monotone. A well-known fact is that any function that is monotone must have only countably many discontinuities within any interval $[x_1, x_2]$ where $x_2 > x_1$; further, all such discontinuities must be jump discontinuities. This means that there must exist two points a^*, b^* such that $b^* > a^* > c^*$ and σ is continuous at a^* and b^*.

Now, we can modify the statement of Lemma 6.6 and require it to hold only on the points $b = a^*$ or $b = b^*$ (rather than for an arbitrary $b > c^*$). Further, we will modify the statement of Lemma 6.7 and require it to hold only on the points $a = a^*$ or $a = b^*$ (rather than for an arbitrary $a > c^*$). With these modifications, the proof of Lemmas 6.6 and 6.7 would hold just like before. Finally, we can redo the proof of Theorem 6.8 except that we choose $a = a^*$ and $b = b^*$. □

7 How to Circumvent the Impossibilities

In this section, we discuss possible ways to circumvent the impossibilities. Recall that in the definition of OCA-proofness, we require all users act independently in the globally optimal strategy σ, and σ should only output a single bid. If we remove any of the two requirements, we can have mechanisms that satisfies UIC, MIC and OCA-proofness, where we present in Sections 7.1 and 7.2. These mechanisms may be somewhat contrived, and may not be practical for the real-world

blockchains. However, the primary point of these mechanisms is to "stress-test" the definitions, and these examples highlight the subtlety of the modeling and help us to have a better understanding of the trade-offs between various notions of collusion-resilience. In Section 7.3, we consider an even weaker definition, called *inclusion-rule-respecting*, which might be the weakest but still meaningful definition that captures the notion of "no way to steal from the protocol." Finally, in Section 7.4, we discuss the use of cryptography in the TFM literature, and point out a future direction by using cryptography and the Bayesian notions of incentive compatibilities.

7.1 Allowing the Globally Optimal Strategy to Coordinate

OCA-proofness requires that all users act independently in the globally optimal strategy σ. However, if we remove this restriction, then the following auctions would simultaneously satisfy UIC, MIC, and OCA-proof (with the aforementioned relaxation).

Posted price auction with random selection and total burning. The mechanism is parametrized with some reserve price $r > 0$ and block size k. Any bid that is at least r is considered eligible. Randomly select up to k bids to include in the block. All included bids are confirmed and they each pay r. All payment is burnt and the miner receives nothing. It is not hard to see that the above mechanism satisfies UIC and MIC. It also satisfies OCA-proofness with the aforementioned relaxation since the global coalition can just have the top k bids bid more than r, and everyone else bid 0.

Vickrey auction with total burning. Suppose we confirm the top k bids and they pay the $(k+1)$-th price, and all payment is burnt. If fewer than k bids exist, then confirm all of them and the all pay 0. The mechanism is obviously UIC and MIC. It also satisfies OCA-proofness with the aforementioned relaxation since the global coalition can just have the top up to k bidders bid their true values, and everyone else bids 0.

7.2 Allowing the Globally Optimal Strategy to Output Multiple Bids

We show that when we allow the globally optimizing strategy $\boldsymbol{\sigma}$ to output multiple bids, then we can actually construct a diret-revelation mechanism that satsifies UIC, MIC, and OCA-proofness. Similar to Section 6.1, we try to signal to the mechanism when everyone is adopting the globally optimal strategy σ. In this mechanism, since σ can output multiple bids, so we can signal through fake bids. We assume the miner and the mechanism can distinguish whether a set of bids come from the same user. In practice, this can be implemented by checking whether these bids are signed by the same public key. Specifically, consider the following mechanism parametrized by $r > 1$ which denotes some reserved price.

- **Globally optimal strategy $\boldsymbol{\sigma}(v)$**: If the user's true value $v \geq r$, $\boldsymbol{\sigma}(v)$ outputs $(r, r/v)$ where $r/v \in (0, 1]$ is a uniquely decodable encoding of the user's true value v. Otherwise, if $v < r$, $\boldsymbol{\sigma}(v)$ simply outputs $\emptyset$, i.e., the user drops its bid.
- **Inclusion rule.**
  - **Case 1**: Check if it is the case that every user $i \in [n]$ submitted a message of the form $(r, r/v_i)$ where $r/v_i \in (0, 1]$ for all $i \in [n]$. If so, decode the true value vector $(v_1, \ldots, v_n)$. Choose the $\min(n, k)$ bids with highest true values, and include their corresponding r bids in the block.

- **Case 2**: Else, if the number of bids is even, henceforth denoted $2n$, check whether there are exactly n bids at r and n number of bids that lie in the range $(0, 1]$. If so, interpret the bid vector as $(r, r/v_1), \ldots, (r, r/v_n)$, as if each pair $(r, r/v_i)$ comes from the i-th user for $i \in [n]$. Now, apply the algorithm of Case 1.
- **Case 3**: Else, if the number of bids is odd, henceforth denoted $2n + 1$, check if there are n bids at r and n bids in the range of $(0, 1]$, and one last bid denoted r'. If $r' > r$, then choose r' to include in the block, and among the remaining n bids at r, randomly choose $\min(k-1, n)$ of them to include in the block; else if $r' \leq r$, randomly choose $\min(k, n)$ bids among all the r-bids to include in the block.
- **Case 4**: In all other cases, randomly choose $\min(k, n)$ bids among all bids that are *strictly larger than* r to include in the block.

- **Confirmation, payment, and miner revenue rules**: All included bids that are at least r are confirmed. Each confirmed bid pays r, and the miner gets nothing.

Claim 7.1. *The above mechanism satisfies UIC, MIC, and a relaxed notion of OCA-proofness where σ is allowed to output multiple bids.*

Proof. We assume $k \geq 1$ in this proof. Otherwise, if $k = 0$, the mechanism can never include any bid, and it is trivial. MIC is obvious since the miner always gets 0 revenue. For OCA-proofness, observe that if the global coalition all take the strategy $\boldsymbol{\sigma}$, then case 1 of the inclusion rule will be triggered, and thus the social welfare is maximized.

Proving UIC is the most complicated part. Fix any user i. Notice that each confirmed bid pays r, so if user i's true value is at most r, it cannot get positive utility regardless its bid. Thus, bidding truthfully is a dominant strategy. Henceforth, we assume user i's true value is strictly larger than r. There are two possibilities.

1. First, before user i submits its bid, the bid vector contains exactly n bids at r and n bids lie in the range $(0, 1]$ for some n. Then, bidding truthfully will lead to case 3, where user i's bid is guaranteed to be included and confirmed, and thus maximizes the utility.

2. Second, before user i submits its bid, the bid vector does not contain exactly n bids at r and n bids lie in the range $(0, 1]$ for some n. Suppose there is no bid strictly larger than r in the bid vector before user i submits its bid. Then, if user i bids truthfully, its bid will be the only bid larger than r, and the inclusion rule goes to Case 4. Since $k \geq 1$, user i's bid is guaranteed to be included and confirmed, and thus maximizes the utility. On the other hand, suppose there are $t \geq 1$ bids strictly larger than r in the bid vector before user i submits its bid. Then, the inclusion can never go to Case 1 or Case 2. If user i bids truthfully, the inclusion rule goes to Case 4, and user i's bid is included with probability $\min(k, t+1)/(t+1)$. However, if user i bids strategically, the inclusion rule may either go to Case 3 or Case 4. For Case 3, it must be user i bids something $\leq r$, and user i has to compete with other r-bid for $k-1$ slots. For Case 4, the inclusion probability cannot be larger than $\min(k, t+1)/(t+1)$ given t bids larger than r are already in the bid vector. Thus, in either case, the utility is better than bidding truthfully.

□

Claim 7.2. *The above mechanism satisfies weak symmetry.*

Proof. To show the weak symmetry, we give an equivalent description as follows. Given a bid vector $\mathbf{b}$, the sorting algorithm check whether $\mathbf{b}$ satisfies the condition of Case 1. If so, the sorting algorithm places the multiple r bids corresponding to the true value vector $(v_1, \ldots, v_n)$ (defined in Case 1 above) from high to low, and sorts the rest in the descending order. Otherwise, if $\mathbf{b}$ does not satisfy the condition of Case 1, the sorting algorithm sorts $\mathbf{b}$ in the descending order and breaks tie arbitrarily.

In the original mechanism, the only case that depends on the extra information (identity, in this case) is Case 1. By applying the sorting algorithm described above, the inclusion rule can implement Case 1 by only depending on the amount of the bids and their relative position in the sorted bid vector.

□

7.3 Inclusion-Rule-Respecting

It is also natural to consider a further relaxation of OCA-proofness henceforth called "inclusion-rule-respecting". In comparison with OCA-proofness, inclusion-rule-respecting only requires that the globally optimal strategy σ not involve altering the inclusion rule, and all other constraints on σ are removed. Inclusion-rule-respecting is strictly weaker than the notions in Section 7.1 and Section 7.2. Therefore, the mechanisms mentioned in Section 7.1 and Section 7.2 simultaneously satisfy UIC, MIC, and inclusion-rule-respecting too.

The "inclusion-rule-respecting" notion has an intuitive interpretation: it discourages miners from altering the authentic Ethereum implementation; in other words, all profiting strategies can be implemented as bidding strategies above the protocol layer. In this sense, "inclusion-rule-respecting" also captures the intuition of "no way to steal from the protocol". One can also view it as follows: global SCP captures "not stealing from the protocol" where the protocol is the union of the miner's inclusion rule as well as users' honest bidding strategies; and inclusion-rule-respecting captures the same notion but where the protocol is only the underlying blockchain protocol. OCA-proofness is somewhere in between.

7.4 Discussions and Open Questions Regarding the Use of Cryptography

Another interesting question is whether we can overcome the impossibilities using cryptography. Shi et al. [SCW23] showed that if the rules of the TFM are enforced through a multi-party computation protocol (henceforth called the MPC-assisted model), then we can design a finite-block TFM that simultaneously satisfies UIC, MIC, and 1-SCP (in the ex-post sense). On the other hand, Shi et al. also showed that simultaneously achieving UIC, MIC, and c-SCP for $c \geq 2$ is impossible in the MPC-assisted model, even for Bayesian notions of equilibrium. Partly this is because even with an MPC protocol enforcing the inclusion rule, a strategic miner or user can still inject fake bids, and the mechanism does not know the number of bids ahead of time (i.e., the mechanism is "permissionless"). It is an interesting open question whether using cryptography and Bayesian notions of equilibrium can help us overcome the impossibilities in this paper. Specifically, Shi et al. [SCW23] suggested that the MPC-assisted model also justifies the relaxed notion of Bayesian equilibrium, since players cannot see others' bids before posting their own.

8 Revelation Principle for Transaction Fee Mechanism

Informally speaking, the *revelation principle* in traditional auction theory says that any mechanism can be simulated by an equivalent direct-revelation mechanism. Whenever the revelation principle

holds, without loss of generality, we may assume that the users' honest bidding strategy is simply truth-telling. TFMs differ from traditional auctions in that it additionally needs to satisfy MIC and collusion resilience, and also the separation of the inclusion rule (executed by the miner) and the confirmation/payment rules (executed by the blockchain). Therefore, one needs to be careful when the revelation principle holds. In this section, we prove that for any fixed c, the revelation principle holds for TFMs that must satisfy UIC, MIC, and c-SCP. As a direct corollary, the revelation principle holds for TFMs that satisfy UIC, MIC, and global SCP. The main subtlety in the proof is that when we bake the user's non-truth-telling bidding rule β into the mechanism itself, not only do we need to have the miner's inclusion rule execute β, the blockchain's confirmation/payment rules must also double-check the correct enforcement of β again. Otherwise, a strategic miner may not honestly enforce β.

Notice that we focus on the mechanisms that satisfy c-SCP instead of OCA-proofness in this section. c-SCP requires that following the honest bidding rule and the honest inclusion rule is a dominant strategy for a coalition consisting of the miner and at most c users. For a non-direct-revelation mechanism with the bidding rule β, β is used by users to satisfy both the UIC and the c-SCP conditions. In Section 8.1, we assume the honest bidding rule β only outputs a single bid. Later in Section 8.2, we generalize the proof so that β can output any non-negative number of bids.

8.1 Revelation Principle: Bidding Rules Output Single Bid

The outcome of a TFM is defined as a tuple $(\mathbf{x}, \mathbf{p}, \mu)$ where $\mathbf{x} \in \{0,1\}^t$ is a bit-vector indicating whether each bid is confirmed or not, $\mathbf{p} \in \mathbb{R}_{\geq 0}^t$ is the vector of payments for all bids, and $\mu \in \mathbb{R}_{\geq 0}$ is the miner's revenue.

Theorem 8.1. *Let c be any natural number. Suppose Π is a non-direct-revelation TFM for block size k that is UIC, MIC, and c-SCP with an individually rational bidding rule β. If β always outputs a single bid, then there exists a direct-revelation TFM Π' for block size k that is UIC, MIC, and c-SCP such that 1) the honest bidding rule is truth-telling, and 2) given any vector of true values, the outcome under an honest execution of Π is identically distributed as the outcome under an honest execution of Π'.*

Proof. Suppose we are given a TFM $\Pi = (\beta, \mathbf{I}, \mathbf{C}, \mathbf{P}, \mu)$ where $\beta : \mathbb{R}_{\geq 0} \to \mathbb{R}$ denotes the user's honest bidding rule, $\mathbf{I}$ denotes the inclusion rule, $\mathbf{C}$ denotes the confirmation rule, $\mathbf{P}$ denotes the payment rule, and μ denotes the miner revenue rule. Given a vector $\mathbf{b} = (b_1, \ldots, b_t)$, let $\beta(\mathbf{b})$ denote the element-wise application of β; that is, $\beta(\mathbf{b}) = (\beta(b_1), \ldots, \beta(b_t))$. We construct a direct-revelation mechanism $\Pi' = (\mathbf{I}', \mathbf{C}', \mathbf{P}', \mu')$ as follows:

- Inclusion rule $\mathbf{I}'$: Given a bid vector $\mathbf{b}$, the miner selects the bids by using $\mathbf{I}$ as if the bid vector is $\beta(\mathbf{b})$. That is, the miner selects the bids from $\mathbf{b}$ if the corresponding bids in $\beta(\mathbf{b})$ are selected by $\mathbf{I}$.
- Confirmation rule $\mathbf{C}'$, payment rule $\mathbf{P}'$ and miner revenue rule μ': Given a created block $\mathbf{B}$, the mechanism applies $\mathbf{C}$ and $\mathbf{P}$ to $\beta(\mathbf{B})$. Then, a bid b in the original block $\mathbf{B}$ is confirmed if and only if its corresponding bid $\beta(b)$ is confirmed when applying $\mathbf{C}$ to $\beta(\mathbf{B})$, and its payment is the same as its corresponding bid when applying $\mathbf{P}$ to $\beta(\mathbf{B})$. The miner revenue is $\mu(\beta(\mathbf{B}))$; that is, applying μ as if the block is $\beta(\mathbf{B})$.

Notice that β is individually rational under Π, so the payment corresponding to the bid $\beta(v)$ never exceeds v. Thus, under the induced mechanism Π', the payment never exceeds the bid, so the individual rationality of the payment rule is respected.

Next, by directly checking the syntax, the user's confirmation probability and expected payment when submitting a bid b under Π' is identically distributed to submitting a bid $\beta(b)$ under Π assuming the miner follows the inclusion rule. Similarly, the miner's revenue when creating a block $\mathbf{B}$ under $\Pi'$is identically distributed to creating a block $\beta(\mathbf{B})$ under Π. Thus, the outcome under an honest execution of Π is identically distributed as the outcome under an honest execution of Π'.

Finally, we show that the induced mechanism Π' satisfies UIC, MIC, and global-SCP. Since submitting a bid b and creating a block $\mathbf{B}$ under Π' is equivalent to submitting a bid $\beta(b)$ and creating a block $\beta(\mathbf{B})$ under Π, respectively, the fact that Π' satisfies UIC and global-SCP directly follows from the fact that Π satisfies UIC and global-SCP under the user's honest bidding rule β.

For proving Π' satisfies MIC, suppose Π' is not MIC for the sake of contradiction. In this case, there exists a bid vector $\mathbf{b}$ and a block $\tilde{\mathbf{B}}$ such that if the miner creates the block $\tilde{\mathbf{B}}$ instead of $\mathbf{I}'(\mathbf{b})$, the miner's utility increases. Then, consider another miner under the mechanism Π, and imagine that the bid vector is $\beta(\mathbf{b})$. Notice that $\mu(\beta(\tilde{\mathbf{B}})) = \mu'(\tilde{\mathbf{B}})$ and $\mu(\mathbf{I}(\beta(\mathbf{b}))) = \mu'(\mathbf{I}'(\mathbf{b}))$. Thus, if the miner creates the block $\beta(\tilde{\mathbf{B}})$ instead of $\mathbf{I}(\beta(\mathbf{b}))$, the miner's utility increases. It violates the fact that Π is MIC. Thus, Π' must satisfy MIC.

□

8.2 Revelation Principle: Allowing Bidding Rule to Output Multiple Bids

In this section, we extend Theorem 8.1 to allow the bidding rule to output multiple bids. The basic idea for proving the revelation principle is still the same — trying to bake the non-truth-telling bidding rule β into the mechanism itself. However, when β may output multiple bids, a user i will submit a vector $\mathbf{b}_i$ of bids instead of a single real number, and the inclusion rule may ask the miner to only select a subset of the bids from $\mathbf{b}_i$. Therefore, the new challenge in this case is how to make the blockchain's confirmation/payment rules also double-check the correct enforcement of β again, given that the blockchain can only see a subset of the bids from $\mathbf{b}_i$.

To handle this difficulty, we need to relax the syntax of the inclusion rule. Earlier in our definitions (Section 2.1), we require that the inclusion rule outputs a subset of the input bid vector. In this section, we slightly relax this syntax requirement, and allow the honest inclusion rule to inject fake bids into the block. The purpose of the fake bids in the honest execution is to encode the auxiliary information for the blockchain's confirmation/payment rules. We can also modify the individual rationality requirement accordingly to additionally require that an honest miner's utility is always non-negative, where the miner's utility is its revenue minus the fees it paid for the fake bids. This relaxation in the syntax is non-essential for the impossibility results in this paper, since all the proofs for our impossibility results (Sections 4, 5 and 6.2) still hold even if the honest inclusion rule can inject fake bids.

Now, we are ready to present the revelation principle. To include the auxiliary information, the induced direct-revelation mechanism requires the block size to be $3k$, given a non-direct-revelation mechanism for block size k.

Theorem 8.2. *Let c be any natural number. Given any non-direct-revelation TFM Π for block size k that is UIC, MIC, and c-SCP with an individually rational bidding rule, there exists a direct-revelation TFM Π' for block size $3k$ that is UIC, MIC, and c-SCP such that 1) the honest bidding rule is truth-telling, and 2) given any vector of true values, the outcome under an honest execution of Π is identically distributed as the outcome under an honest execution of Π'.*

Proof of Theorem 8.2. The rest of this section is dedicated to proving Theorem 8.2. Suppose we are given a TFM $\Pi = (\beta, \mathbf{I}, \mathbf{C}, \mathbf{P}, \mu)$ where $\beta : \mathbb{R}_{\geq 0} \to \mathbb{R}^*$ denotes the user's honest bidding strategy,

$\mathbf{I}$ denotes the inclusion rule, $\mathbf{C}$ denotes the confirmation rule, $\mathbf{P}$ denotes the payment rule, and μ denotes the miner revenue rule. We construct a direct-revelation mechanism $\Pi' = (\mathbf{I}', \mathbf{C}', \mathbf{P}', \mu')$ as follows:

- Inclusion rule $\mathbf{I}'$: given a bid vector $\mathbf{b} = (b_1, \ldots, b_t)$, let $\beta(\mathbf{b}) = (\beta(b_1), \ldots, \beta(b_t))$. Create a block $\mathbf{B}'$ that includes the following:
  - for each $j \in [t]$, if some bid in the vector $\beta(b_j)$ is selected by the original inclusion rule $\mathbf{I}(\beta(\mathbf{b}))$, then include b_j in $\mathbf{B}'$;
  - for each included bid b_j, attach the following extra annotation in $\mathbf{B}'$:

$$\mathsf{info}(b_j) = \text{bids in } \beta(b_j) \text{ selected by } \mathbf{I}(\beta(\mathbf{b}))$$

  A *valid block* $\mathbf{B}$ is one in which the annotation for each $b_j \in \mathbf{B}$ is a subset of the vector $\beta(b_j)$. It is not hard to see that we can encode a valid block using a vector of length at most $3k$.[8]

- The confirmation rule $\mathbf{C}'$, the payment rule $\mathbf{P}'$, and the miner revenue rule μ': If the input block is not valid, then no one is confirmed, and the miner revenue is zero. Else, parse the block as $\{b'_j, \mathbf{s}'_j = \mathsf{info}(b'_j)\}_j$, form an imaginary block $\{\mathbf{s}'_j\}_j$, and run the original confirmation rule $\mathbf{C}$, payment rule $\mathbf{P}$ and miner revenue rule μ on $\{\mathbf{s}'_j\}_j$. A bid b'_j in the input block is considered confirmed if the primary bid in $\beta(b'_j)$ is contained in $\mathbf{s}'_j$ and is confirmed by $\mathbf{C}(\{\mathbf{s}'_j\}_j)$, and its payment is the sum of all payments of $\mathbf{s}'_j$ in $\mathbf{P}(\{\mathbf{s}'_j\}_j)$. The miner is paid $\mu(\{\mathbf{s}'_j\}_j)$.

More intuitively, in the direct-revelation mechanism Π', the miner simulates β by applying β to all bids it has received, resulting in $\beta(\mathbf{b})$. It then simulates the original inclusion rule of the non-direct mechanism, and the result is $\mathbf{I}(\beta(\mathbf{b}))$, indicating which of $\beta(\mathbf{b})$ would have been included by the original $\mathbf{I}$. The miner includes in the block each bid b_j such that at least one of $\beta(b_j)$ would have been included by $\mathbf{I}(\beta(\mathbf{b}))$, and for each included bid b_j, it attaches the extra information which bids among $\beta(b_j)$ would have been included by $\mathbf{I}(\beta(\mathbf{b}))$. This way, the blockchain's confirmation, payment, and miner-revenue rules can double-check the correct enforcement of β again, before simulating the effect of the original confirmation, payment, and miner revenue rules of the non-direct mechanism — formally, the checking is accomplished through a block validity check in our reduction.

Lemma 8.3. *Assume the miner follows the mechanism honestly. Then, the outcome when all users follow the bidding rule β under the mechanism Π is identically distributed as the outcome when all users bid truthfully under the mechanism Π'.*

Proof. Let $(v_1, \ldots, v_t)$ be the true values of all users. Under mechanism Π, if all users follow the bidding rule β, the created block will be $\mathbf{B} = \mathbf{I}(\beta(v_1), \ldots, \beta(v_t))$. For any user i, since the fake bids have no intrinsic values, user i's bid is considered as confirmed if and only if its primary bid in $\beta(v)$ is confirmed. User i's payment is the sum of the payments of all its bids $\beta(v)$. The miner revenue in this case is $\mu(\mathbf{B})$.

Under mechanism Π', if all users bid truthfully, the created block will be $\mathbf{B}'$ parsed as $\{b'_j, \mathsf{info}(b'_j)\}_j$. Notice that $\{\mathsf{info}(b'_j)\}_j$ is identically distributed as $\mathbf{B}$. The bid b'_j under mechanism Π' is considered confirmed if the primary bid in $\beta(b'_j)$ is contained in $\mathsf{info}(b'_j)$ and is confirmed by $\mathbf{C}(\{\mathsf{info}(b'_j)\}_j)$, and its payment is the sum of all payments of $\mathbf{s}'_j$ in $\mathbf{P}(\{\mathsf{info}(b'_j)\}_j)$. The miner revenue in this case is $\mu(\{\mathsf{info}(b'_j)\}_j)$.

[8] For example, we can divide the block into three parts: the first part encodes users' original bids b_j; the second part encodes $\beta(b_j)$; and the third part encodes the mapping between the first part and the second part.

Because $\{\mathsf{info}(b'_j)\}_j$ is identically distributed as $\mathbf{B}$, the outcomes of the honest execution of two mechanisms are also identically distributed by checking all the syntax above.

□

Lemma 8.4. *The following statements hold.*

- *If* Π *is UIC, then* Π' *is UIC.*
- *If* Π *is MIC, then* Π' *is MIC.*
- *For all* c*, if* Π *is* c*-SCP, then* Π' *is* c*-SCP.*

Proof. We will prove three properties individually.

Π' is UIC. For the sake of contradiction, suppose Π' is not UIC. That is, under mechanism Π', there exists a user i with true value v and a bid vector $\mathbf{b}_{-i}$ such that user i's utility increases if it submits a vector $\mathbf{f}$ (possibly includes some fake bids) instead of v when other users' bids are $\mathbf{b}_{-i}$. Denote the above as Scenario 1. Then, consider another Scenario 2, where the mechanism is Π, and other users' bids are $\beta(\mathbf{b}_{-i})$. The strategic user i can submit a vector $\beta(\mathbf{f})$ instead of $\beta(v)$.

By Lemma 8.3, the confirmation probability and the payment of the bids $\mathbf{f}$ (v, resp.) in Scenario 1 are identically distributed as the confirmation probability and the payment of the bids $\beta(\mathbf{f})$ ($\beta(v)$, resp.) in Scenario 2. Thus, the expected utility of user i if it submits $\mathbf{f}$ (v, resp.) in Scenario 1 is the same as the expected utility of user i if it submits $\beta(\mathbf{f})$ ($\beta(v)$, resp.) in Scenario 2. Thus, in Scenario 2, user i's utility increases if it $\beta(\mathbf{f})$ instead of $\beta(v)$. It violates UIC under Π, so Π' must satisfy UIC.

Π' is MIC. For the sake of contradiction, suppose Π' is not MIC. That is, there exists a bid vector $\mathbf{b}$ and a block $\tilde{\mathbf{B}} = \{b'_j, \mathbf{s}'_j = \mathsf{info}(b'_j)\}_j$ such that if the miner creates the block $\tilde{\mathbf{B}}$ instead of $\mathbf{I}'(\mathbf{b})$, the miner's utility increases. Denote the above as Scenario 1. Then, consider another Scenario 2, where the mechanism is Π, and the incoming bid vector is $\beta(\mathbf{b})$. The strategic miner can create a block $\{\mathbf{s}'_j\}_j$ instead of $\mathbf{I}(\beta(\mathbf{b}))$.

Recall the miner's utility is the revenue minuses the cost of injecting the fake bids. The miner revenue of the block $\tilde{\mathbf{B}}$ ($\mathbf{I}'(\mathbf{b})$, resp.) in Scenario 1 is the same as the miner revenue of the block $\{\mathbf{s}'_j\}_j$ ($\mathbf{I}(\beta(\mathbf{b}))$, resp.) in Scenario 2. If $\{\mathbf{s}'_j\}_j$ contains some fake bids, the expected payment of those fake bids in Scenario 2 is also the same as the expected payment of the fake bids when the created block is $\tilde{\mathbf{B}}$ in Scenario 1. Therefore, in Scenario 2, if the miner creates $\{\mathbf{s}'_j\}_j$ instead of $\mathbf{I}(\beta(\mathbf{b}))$, the miner's utility increases. It violates MIC under Π, so Π' must satisfy MIC.

Π' is c-SCP for all c. For the sake of contradiction, suppose Π' is not c-SCP for some c. That is, there exist a coalition C formed by the miner and at most c users, a bid vector $\mathbf{b}_{-C}$, and a block $\tilde{\mathbf{B}}$ such that when all non-colluding users' bids are $\mathbf{b}_{-C}$, C's utility increases if the created block is $\tilde{\mathbf{B}}$ instead of $\mathbf{I}'(\mathbf{b}_{-C}, \mathbf{b}_C)$, where $\mathbf{b}_C$ is the true values of all users in C. Denote the above as Scenario 1. Then, consider another Scenario 2, which is the same as scenario 1 except that the mechanism is Π, and the bid vector of non-colluding user is $\beta(\mathbf{b}_{-C})$. Parse $\tilde{\mathbf{B}} = \{b'_j, \mathbf{s}'_j = \mathsf{info}(b'_j)\}_j$. The coalition C can create a block $\{\mathbf{s}'_j\}_j$ instead of $\mathbf{I}(\beta(\mathbf{b}_{-C}, \mathbf{b}_C))$.

Following the same argument as UIC and MIC, we conclude that the joint utility of C of the block $\tilde{\mathbf{B}}$ ($\mathbf{I}'(\mathbf{b}_{-C}, \mathbf{b}_C)$, resp.) in Scenario 1 is the same as the joint utility of C of the block $\{\mathbf{s}'_j\}_j$ ($\mathbf{I}(\beta(\mathbf{b}_{-C}, \mathbf{b}_C))$, resp.) in Scenario 2. Thus, in Scenario 2, if the coalition creates $\{\mathbf{s}'_j\}_j$ instead of $\mathbf{I}(\beta(\mathbf{b}_{-C}, \mathbf{b}_C))$, the joint utility of C increases. It violates c-SCP under Π, so Π' must satisfy c-SCP. □

The proof of Theorem 8.2 directly follows from Lemma 8.3 and Lemma 8.4.

References

[ACH11] Gilad Asharov, Ran Canetti, and Carmit Hazay. Towards a game theoretic view of secure computation. In *Eurocrypt*, 2011.

[ADGH06] Ittai Abraham, Danny Dolev, Rica Gonen, and Joseph Halpern. Distributed computing meets game theory: Robust mechanisms for rational secret sharing and multiparty computation. In *PODC*, 2006.

[AL11] Gilad Asharov and Yehuda Lindell. Utility dependence in correct and fair rational secret sharing. *Journal of Cryptology*, 24(1), 2011.

[BCD+] Vitalik Buterin, Eric Conner, Rick Dudley, Matthew Slipper, and Ian Norden. Ethereum improvement proposal 1559: Fee market change for eth 1.0 chain. https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1559.md.

[BEOS19] Soumya Basu, David A. Easley, Maureen O'Hara, and Emin Gün Sirer. Towards a functional fee market for cryptocurrencies. *CoRR*, abs/1901.06830, 2019.

[BGR23] Maryam Bahrani, Pranav Garimidi, and Tim Roughgarden. Transaction fee mechanism design with active block producers. *arXiv preprint arXiv:2307.01686*, 2023.

[CCWS21] Kai-Min Chung, T-H. Hubert Chan, Ting Wen, and Elaine Shi. Game-theoretic fairness meets multi-party protocols: The case of leader election. In *CRYPTO*. Springer-Verlag, 2021.

[CGL+18] Kai-Min Chung, Yue Guo, Wei-Kai Lin, Rafael Pass, and Elaine Shi. Game theoretic notions of fairness in multi-party coin toss. In *TCC*, volume 11239, pages 563–596, 2018.

[CMW23] Davide Crapis, Ciamac C Moallemi, and Shouqiao Wang. Optimal dynamic fees for blockchain resources. *arXiv preprint arXiv:2309.12735*, 2023.

[CS23] Hao Chung and Elaine Shi. Foundations of transaction fee mechanism design. In *Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 3856–3899. SIAM, 2023.

[DR07] Yevgeniy Dodis and Tal Rabin. Cryptography and game theory. In *AGT*, 2007.

[EFW22] Meryem Essaidi, Matheus V. X. Ferreira, and S. Matthew Weinberg. Credible, strategyproof, optimal, and bounded expected-round single-item auctions for all distributions. In Mark Braverman, editor, *13th Innovations in Theoretical Computer Science Conference, ITCS 2022, January 31 - February 3, 2022, Berkeley, CA, USA*, volume 215 of *LIPIcs*, pages 66:1–66:19, 2022.

[FMPS21] Matheus V. X. Ferreira, Daniel J. Moroz, David C. Parkes, and Mitchell Stern. Dynamic posted-price mechanisms for the blockchain transaction-fee market. *CoRR*, abs/2103.14144, 2021.

[FW20] Matheus V. X. Ferreira and S. Matthew Weinberg. Credible, truthful, and two-round (optimal) auctions via cryptographic commitments. In Péter Biró, Jason D. Hartline, Michael Ostrovsky, and Ariel D. Procaccia, editors, *EC '20: The 21st ACM Conference on Economics and Computation, Virtual Event, Hungary, July 13-17, 2020*, pages 683–712. ACM, 2020.

[GKM+13] Juan A. Garay, Jonathan Katz, Ueli Maurer, Björn Tackmann, and Vassilis Zikas. Rational protocol design: Cryptography against incentive-driven adversaries. In *FOCS*, 2013.

[GKTZ15] Juan Garay, Jonathan Katz, Björn Tackmann, and Vassilis Zikas. How fair is your protocol? a utility-based approach to protocol optimality. In *PODC*, 2015.

[GLR10] Ronen Gradwohl, Noam Livne, and Alon Rosen. Sequential rationality in cryptographic protocols. In *FOCS*, 2010.

[GTZ15] Juan A. Garay, Björn Tackmann, and Vassilis Zikas. Fair distributed computation of reactive functions. In *DISC*, volume 9363, pages 497–512, 2015.

[GY22] Yotam Gafni and Aviv Yaish. Greedy transaction fee mechanisms for (non-) myopic miners. *arXiv preprint arXiv:2210.07793*, 2022.

[HT04] Joseph Halpern and Vanessa Teague. Rational secret sharing and multiparty computation. In *STOC*, 2004.

[Kat08] Jonathan Katz. Bridging game theory and cryptography: Recent results and future directions. In *Theory of Cryptography Conference*, pages 251–272. Springer, 2008.

[KKLP23] Aggelos Kiayias, Elias Koutsoupias, Philip Lazos, and Giorgos Panagiotakos. Tiered mechanisms for blockchain transaction fees. *arXiv preprint arXiv:2304.06014*, 2023.

[KMSW22] Ilan Komargodski, Shinichiro Matsuo, Elaine Shi, and Ke Wu. log*-round game-theoretically-fair leader election. In *CRYPTO*, 2022.

[KN08] Gillat Kol and Moni Naor. Cryptography and game theory: Designing protocols for exchanging information. In *TCC*, 2008.

[LRMP23] Stefanos Leonardos, Daniël Reijsbergen, Barnabé Monnot, and Georgios Piliouras. Optimality despite chaos in fee markets. In *International Conference on Financial Cryptography and Data Security*, pages 346–362. Springer, 2023.

[LSZ19] Ron Lavi, Or Sattath, and Aviv Zohar. Redesigning bitcoin's fee market. In *The World Wide Web Conference, WWW 2019*, pages 2950–2956, 2019.

[Mye81] Roger B. Myerson. Optimal auction design. *Math. Oper. Res.*, 6(1), 1981.

[Ndi23] Abdoulaye Ndiaye. Blockchain price vs. quantity controls. *Quantity Controls (July 27, 2023)*, 2023.

[OPRV09] Shien Jin Ong, David C. Parkes, Alon Rosen, and Salil P. Vadhan. Fairness with an honest minority and a rational majority. In *TCC*, 2009.

[PS17] Rafael Pass and Elaine Shi. Fruitchains: A fair blockchain. In *PODC*, 2017.

[Rou20] Tim Roughgarden. Transaction fee mechanism design for the Ethereum blockchain: An economic analysis of EIP-1559. Manuscript, https://timroughgarden.org/papers/eip1559.pdf, 2020.

[Rou21] Tim Roughgarden. Transaction fee mechanism design. In *EC*, 2021.

[SCW23] Elaine Shi, Hao Chung, and Ke Wu. What can cryptography do for decentralized mechanism design? In *ITCS*, volume 251 of *LIPIcs*, pages 97:1–97:22. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023.

[TY23] Wenpin Tang and David D Yao. Transaction fee mechanism for proof-of-stake protocol. *arXiv preprint arXiv:2308.13881*, 2023.

[WAS22] Ke Wu, Gilad Asharov, and Elaine Shi. A complete characterization of game-theoretically fair, multi-party coin toss. In *Eurocrypt*, 2022.

[WSC24] Ke Wu, Elaine Shi, and Hao Chung. Maximizing Miner Revenue in Transaction Fee Mechanism Design. In Venkatesan Guruswami, editor, *15th Innovations in Theoretical Computer Science Conference (ITCS 2024)*, 2024.

[XFP23] Matheus Venturyne Xavier Ferreira and David C Parkes. Credible decentralized exchange design via verifiable sequencing rules. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, pages 723–736, 2023.

[Yao] Andrew Chi-Chih Yao. An Incentive Analysis of Some Bitcoin Fee Designs (Invited Talk). In *ICALP 2020*.

[ZCZ22] Zishuo Zhao, Xi Chen, and Yuan Zhou. Bayesian-nash-incentive-compatible mechanism for blockchain transaction fee allocation. https://arxiv.org/abs/2209.13099, 2022.