

# What Can Cryptography Do for Decentralized Mechanism Design?

Elaine Shi ✉🏠

ECE and CSD Department, Carnegie Mellon University, Pittsburgh, PA, USA

Hao Chung ✉🏠

ECE Department, Carnegie Mellon University, Pittsburgh, PA, USA

Ke Wu ✉🏠 

CSD Department, Carnegie Mellon University, Pittsburgh, PA, USA

---

## Abstract

Recent works of Roughgarden (EC'21) and Chung and Shi (SODA'23) initiate the study of a new decentralized mechanism design problem called transaction fee mechanism design (TFM). Unlike the classical mechanism design literature, in the decentralized environment, even the auctioneer (i.e., the miner) can be a strategic player, and it can even collude with a subset of the users facilitated by binding side contracts. Chung and Shi showed two main impossibility results that rule out the existence of a *dream* TFM. First, any TFM that provides incentive compatibility for individual users and miner-user coalitions must always have zero miner revenue, no matter whether the block size is finite or infinite. Second, assuming finite block size, no non-trivial TFM can simultaneously provide incentive compatibility for any individual user and for any miner-user coalition.

In this work, we explore what new models and meaningful relaxations can allow us to circumvent the impossibility results of Chung and Shi. Besides today's model that does not employ cryptography, we introduce a new MPC-assisted model where the TFM is implemented by a joint multi-party computation (MPC) protocol among the miners. We prove several feasibility and infeasibility results for achieving *strict* and *approximate* incentive compatibility, respectively, in the plain model as well as the MPC-assisted model. We show that while cryptography is not a panacea, it indeed allows us to overcome some impossibility results pertaining to the plain model, leading to non-trivial mechanisms with useful guarantees that are otherwise impossible in the plain model. Our work is also the first to characterize the mathematical landscape of transaction fee mechanism design under approximate incentive compatibility, as well as in a cryptography-assisted model.

**2012 ACM Subject Classification** Security and privacy → Cryptography

**Keywords and phrases** Transaction Fee Mechanism Design

**Digital Object Identifier** 10.4230/LIPIcs.ITCS.2023.97

**Related Version** *Full Version:* <https://arxiv.org/abs/2209.14462>

*Full Version:* <https://eprint.iacr.org/2022/1294>

**Funding** Research supported by NSF awards 2212746, 2044679, 1704788, a Packard Fellowship, a generous gift from the late Nikolai Mushegian, a gift from Google, and an ACE center grant from Algorand Foundation.

## 1 Introduction

The widespread adoption of blockchains and cryptocurrencies spurred a new class of *decentralized* mechanism design problems. The recent works of Roughgarden [29, 30] as well as Chung and Shi [7] considered a particularly important decentralized mechanism design problem, that is, *transaction fee mechanism* (TFM) design. In a transaction fee mechanism (TFM), we are auctioning space in the block to users who want their transactions included and confirmed in the block. If the block can contain up to  $k$  transactions, one can equivalently think of selling  $k$  identical products to the bidders.



© Elaine Shi, Hao Chung, and Ke Wu;

licensed under Creative Commons License CC-BY 4.0

14th Innovations in Theoretical Computer Science Conference (ITCS 2023).

Editor: Yael Tauman Kalai; Article No. 97; pp. 97:1–97:22

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Prior works [24, 32, 4, 5, 29, 30, 12] observed that transaction fee mechanism design departs significantly from classical mechanism design [26]. The vast majority of classical auctions assume that the auctioneer honestly implements the prescribed mechanism. In comparison, in a blockchain environment, the auctioneer (i.e., the miner of the block), can be a strategic player in itself: it can deviate from the prescribed mechanism if it increases its expected gain; or it can collude with a subset of the users, and play strategically to improve the coalition’s joint utility. As earlier works pointed out [24, 32, 4, 5, 29, 30], the existence of decentralized smart contracts in blockchain environments make it easy for the miner and users to rendezvous and engage in *binding* side contracts. Such side contracts allow the coalition to split their gains off the table in a binding fashion.

Observing the new challenges that arise in a decentralized environment, earlier works [24, 32, 4, 5, 29, 30] formulated a set of desiderata for a “dream” TFM:

- *User incentive compatibility (UIC)*: a user’s best strategy is to bid truthfully, even when the user has observed others’ bids.
- *Miner incentive compatibility (MIC)*: the miner’s best strategy is to implement the honest mechanism, even when the miner has observed all users’ bids.
- *c-side-contract-proofness (c-SCP)*: playing honestly maximizes the joint utility of a coalition consisting of the miner and at most  $c$  users, even after having observed all others’ bids.

A line of works explored how to get a dream TFM. However, assuming that the block size is *finite*, i.e., there can be more bids than the block size, all known works fall short of achieving all three properties at the same time. The closest we have come to in terms of achieving a dream TFM is in fact Ethereum’s EIP-1559. At a very high-level, when there is congestion, EIP-1559 behaves like a first-price auction which is not UIC. When the block size is infinite (i.e., no congestion), EIP-1559 approximates the following “burning posted price” auction: there is a fixed reserve price  $r$ , every bid that is at least  $r$  gets included and confirmed, and pays the price of  $r$ . All users’ payment is burnt and the miner gets nothing<sup>1</sup>. Roughgarden [29, 30] proved that when the block size is *infinite*, indeed, the burning posted price auction achieves all three properties at the same time!

Subsequently, Chung and Shi [7] further explored the landscape of TFM. They proved two interesting impossibility results:

1. *Zero miner revenue*. Any (possibly randomized) TFM that satisfies both UIC and SCP must always have 0 miner revenue, even when the miner colludes with at most one user, and no matter whether the block size is finite or infinite. This shows that the total burning in EIP-1559 is no accident: it is necessary to achieve all three properties under infinite block size.
2. *Finite-block impossibility*. Suppose that block size is finite, then no non-trivial (possibly randomized) TFM can achieve UIC and SCP at the same time, even when the miner colludes with at most one user. This shows that it is no accident that all prior works fail to achieve the dream TFM for finite block sizes – indeed, there is a mathematical impossibility!

Given the status quo of our understanding, we ask the following natural question:

*Are there meaningful new models or relaxations that allow us to circumvent the impossibility results of Chung and Shi?*

---

<sup>1</sup> In practice, the miner gets a fixed block reward that is irrelevant to our game-theoretic analysis, so we ignore the fixed block reward in our modeling.

Chung and Shi [7] made an initial exploration along this line. They show a relaxation that allows us to circumvent the impossibilities and achieve positive miner revenue under finite block size. In particular, their relaxation requires the additional assumption that offending bids (e.g., overbid or fake transactions) that have been posted to the public cannot be retracted in the future, and thus the offender may have to pay a cost when the offending transaction is confirmed in the future. While this assumption holds for some cryptocurrencies such as Bitcoin, it may not be universally true for all cryptocurrencies. Therefore, an important question is what other models or relaxations allow us to circumvent the impossibilities.

In this paper, we explore two new directions, aiming to understand whether they allow us to circumvent the impossibilities of Chung and Shi [7]: *i)* using an approximate notion of incentive compatibility that allows an  $\epsilon$  additive slack; and *ii)* having the miners jointly run a multi-party computation (MPC) protocol to realize the TFM. Throughout the paper, we refer to the today's model, which does employ cryptography, as the *plain model*, and we refer to the case where the TFM is realized with MPC as the *MPC-assisted model*.

## 1.1 Our Results and Contributions

Our paper makes novel contributions at both *conceptual* and *technical* levels. From a technical perspective, prior to our work, we lacked techniques for characterizing the solution space of approximate incentive compatibility – in particular, classical tools like Myerson's Lemma [25] breaks down when we allow  $\epsilon$  slack in the incentive compatibility, and thus our classical insights often fail. One of our main technical contributions is to develop new techniques for mathematically reasoning about approximate incentive compatibility. On the conceptual front, while an elegant line of work has shown ways in which cryptography and game theory can help each other [19, 22, 1, 27, 3, 2, 15, 14, 16, 21, 10, 18, 9, 31, 8, 28, 23, 13, 11] (see Section 1.2 for more discussions), our work is of a different nature. Our results reveal exciting new connections between cryptography and mechanism design, motivated by a practical problem. The popularity of blockchains and decentralized applications poses many exciting new challenges for decentralized mechanism design, and cryptography-meets-game-theory is a natural and promising paradigm. We thus hope that our new conceptual contributions can provide fodder and inspire new works in this exciting and much explored space.

We give a summary of our main results below.

### 1.1.1 Characterizing Miner Revenue under Approximate Incentive Compatibility

We first focus on the plain model that was studied in earlier works [24, 32, 4, 29, 30, 12, 7]. Recall that assuming infinite block size, it is possible to achieve a dream TFM (e.g., the burning posted price auction), but the miner revenue has to be zero. We ask the following question: *suppose we are willing to relax the incentive compatibility notion and allow an  $\epsilon$  additive slack, can we circumvent the zero miner revenue lower bound? If so, exactly how much miner revenue can we hope for?*

More specifically,  $\epsilon$ -incentive-compatibility (including  $\epsilon$ -UIC,  $\epsilon$ -MIC, and  $\epsilon$ -SCP) requires that any deviation cannot increase the strategic individual or coalition's utility by more than  $\epsilon$ . We show that under  $\epsilon$ -incentive-compatibility, we can achieve linear (in the number of users) miner revenue assuming infinite block size. Moreover, we give matching upper- and lower-bounds that tightly characterize exactly how much miner revenue can be attained.

**Infinite block size**

Consider the simple posted price auction with reserve price  $r \leq \frac{\epsilon}{c}$  where  $c$  is the maximum number of users controlled by the strategic coalition: all bids that bid at least  $r$  are confirmed. Each confirmed bid pays  $r$ . All payment goes to the miner. It is not hard to show that the above auction satisfies strict UIC, strict MIC (for an arbitrarily sized miner-coalition), and  $\epsilon$ -SCP against  $c$ -sized coalitions. Further, the expected total miner revenue is  $\Theta(n \cdot \frac{\epsilon}{c})$  when the users' true values are not too small.

Although the above posted price achieves linear in  $n$  revenue, the drawback is that the miner revenue is unscalable: even as the users' bids scale up (e.g., by some multiplicative factor), the miner revenue does not grow proportionally. We therefore ask if randomization can help achieve scalability in miner revenue. We show that indeed the following randomized TFM achieves scalability in miner revenue:

*Proportional auction* // Let  $r$  be a fixed reserve price.

- Every bid  $b \geq r$  is confirmed with probability 1 and every candidate bid  $b < r$  is confirmed with probability  $b/r$ . Each confirmed bid  $b$  pays  $p = \min\{\frac{b}{2}, \frac{r}{2}\}$ .
- For each confirmed bid, miner gets a pre-determined threshold  $r' = \sqrt{\frac{2r\epsilon}{9c}}$  if  $p \geq r'$ .

For example, suppose all users' bids are sampled independently from some distribution  $\mathcal{D}$ , and let  $m$  be the median of the distribution such that  $\Pr_{x \sim \mathcal{D}}[x \geq m] \geq 1/2$  (or any other constant). Then, if we set  $r = m$ , the expected miner revenue (taken over the randomness of users' bids as well as of the TFM itself) is  $\Omega(n \cdot \min(m, \sqrt{\frac{m\epsilon}{c}}))$ .

Combining the posted price auction and the proportional auction, we have the following theorem:

► **Theorem 1.1.** *Consider the hybrid auction which, given some bid distribution  $\mathcal{D}$  with median  $m$ , runs either the posted price auction with reserve price  $r = \min(\frac{\epsilon}{c}, m)$  or the proportional auction with the reserve price  $r = m$ , depending on which one has higher expected revenue. The hybrid auction is strict UIC, strict MIC (for an arbitrarily sized miner coalition), and  $\epsilon$ -SCP against any miner-user coalition with at most  $c$  users. Further, it achieves  $\Omega(n \cdot (\min(\frac{\epsilon}{c} + \sqrt{\frac{m\epsilon}{c}}, m)))$  expected total miner revenue.*

Next, we prove a matching bound that shows the limitation on how much miner revenue can be attained under approximate incentive compatibility, as stated in the following theorem – this bound holds no matter whether the block size is finite or infinite.

► **Theorem 1.2 (Limit on miner revenue for infinite block size).** *For any possibly randomized TFM (in the plain model) that satisfies  $\epsilon$ -UIC,  $\epsilon$ -MIC, and  $\epsilon$ -SCP for miner-user coalitions with 1 user, the expected total miner revenue over a random bid vector sampled from  $\mathcal{D}^n$  must be upper bounded by*

$$\mathbf{E}_{\mathbf{b} \sim \mathcal{D}^n} [\mu(\mathbf{b})] \leq 6n \cdot (\epsilon + \sqrt{\epsilon} \cdot \mathbf{E}_{x \sim \mathcal{D}}[\sqrt{x}]),$$

where  $\mu(\mathbf{b})$  denotes the total miner revenue under the bid vector  $\mathbf{b}$ ,  $n$  is the number of users,  $\mathcal{D}_i$  denotes the true value distribution of user  $i \in [n]$ .

**Finite block size**

Another natural question is: *can we circumvent the finite-block impossibility under approximate incentive compatibility?* Unfortunately, although it is indeed possible to overcome the finite-block impossibility with approximate incentive compatibility, we prove a new impossibility result that rules out the existence of “useful” mechanisms whose social welfare (i.e., the sum of everyone’s utilities) scales up proportionally w.r.t. the bid distribution:

► **Theorem 1.3** (Scalability barrier for approximate incentive compatibility in the plain model). *Fix any  $\epsilon > 0$ , and suppose that the block size is  $k$ . Any (possibly random) TFM in the plain model that simultaneously satisfies  $\epsilon$ -UIC,  $\epsilon$ -MIC, and  $\epsilon$ -SCP (even when the miner colludes with at most one user) has at most  $\tilde{O}(k^3\epsilon)$  social welfare where  $k$  is the block size and  $\tilde{O}(\cdot)$  hides logarithmic factors.*

### 1.1.2 Can We Circumvent the Finite-Block Impossibility with Cryptography?

Due to the negative result of Theorem 1.3, we want to seek other avenues that allow us to circumvent the finite-block impossibility. Since cryptography is widely deployed in today's blockchains, it is natural to ask whether we can bring cryptography to the design of transaction fee mechanisms, to help us achieve what is otherwise impossible.

#### New model: MPC-assisted TFM

Consider a scenario henceforth called the MPC-assisted model, where a set of miners jointly run a multi-party computation (MPC) protocol to implement the TFM. Although in practice, lighter-weight cryptography would be desirable, as an initial theoretical exploration of the feasibility/infeasibility landscape, it makes sense to start with a generic abstraction like MPC. One may think of the MPC protocol as providing the following ideal functionality  $\mathcal{F}_{\text{TFM}}$ :

- Each player (either user or miner) may act as any number of identities (including 0), and on behalf of each identity, submit a bid to  $\mathcal{F}_{\text{TFM}}$ .
- The ideal functionality  $\mathcal{F}_{\text{TFM}}$  executes the prescribed *allocation rule* of the TFM to decide which transactions to include and confirm in the block; it executes the *payment rule* and *miner revenue rule* of the TFM to decide how much each confirmed bid pays and the total miner revenue.  $\mathcal{F}_{\text{TFM}}$  then sends to all players the set of bids that are confirmed, what price each confirmed bid pays, and the total miner revenue.

We require that the total miner revenue does not exceed the total payment, and that the total miner revenue is split among the miners.

We assume that there is a separate process to decide the set of miners whose job is to jointly run the MPC protocol. For example, this decision can be made through either proof-of-work or proof-of-stake. In the former case, the total miner revenue is effectively split among the miners proportional to their mining power. In the latter case, the total miner revenue is effectively split among the miners proportional to their stake.

We assume that the majority of the miners are honest and that the MPC provides guaranteed output (i.e., the strategic miners cannot cause the MPC protocol to abort without producing outcome). Note that if we can indeed design an incentive compatible protocol in the MPC-assisted model, then, no miner would be incentivized to deviate from the honest protocol, and this reinforces the honest majority assumption.

Intuitively, an MPC-assisted TFM restricts the strategy space for players in comparison with the plain model:

- R1** A strategic individual or coalition must decide its strategy without having seen honest users' bids (*c.f.* in the plain model, a strategic individual or coalition can decide their strategy after seeing other players' bids).
- R2** Once the set of bids are committed to, the allocation rule must be implemented honestly (*c.f.* in the plain model, the winning miner or block proposer can strategically choose which transactions to include in the block).

Exactly because of the MPC-assisted model imposes the above restrictions on the strategy space, we are hopeful that it may allow us to circumvent impossibilities. Before we explain our results, we first discuss how to define incentive compatibility in the MPC-assisted model.

### Ex post vs. Bayesian notions of incentive compatibility

In the plain model, because a strategic individual or coalition can decide their bids after seeing others' bids, prior works [30, 7] considered an *ex post* notion of incentive compatibility. In the new MPC-assisted model, since players must submit their bids to  $\mathcal{F}_{\text{TFM}}$  without seeing others' bids, it also makes sense to consider a *Bayesian* notion of equilibrium.

Informally, we say that an MPC-assisted TFM satisfies *Bayesian Nash Equilibrium (BNE)* for a strategic coalition (or individual)  $\mathcal{C}$ , following the honest strategy allows  $\mathcal{C}$  to maximize its expected gain, assuming that the bids of users not in  $\mathcal{C}$  are drawn independently from some known distribution. If the coalition  $\mathcal{C}$  consists of an individual user, we say that the scheme satisfies *Bayesian UIC*. When  $\mathcal{C}$  consists of at most  $\rho$  fraction of the miners, we say that the scheme satisfies *Bayesian MIC* against a  $\rho$ -sized miner-coalition. Finally, when the coalition  $\mathcal{C}$  consists of at most  $\rho$  fraction of miners as well as at least 1 and at most  $c$  users, we say that the scheme satisfies *Bayesian SCP* against a  $(\rho, c)$ -sized coalition.

Jumping ahead, for the MPC-assisted model, all our mechanism designs achieve incentive compatibility even in the *ex post* setting – in other words, the incentive compatibility guarantees hold even if  $\mathcal{F}_{\text{TFM}}$  leaks other players' bids to the strategic players before they decide their own strategy. On the other hand, all of our impossibilities hold even for the Bayesian setting. This makes both our upper- and lower-bounds stronger.

### MPC-assisted TFM under strict incentive compatibility

Unfortunately, as we show in the full version, the MPC-assisted model does not help us circumvent the zero miner revenue lower bound, even for Bayesian notions of equilibrium. Instead, the main question we care about here is *whether the MPC-assisted model allows us to circumvent the finite-block impossibility*. It turns out that the answer is not a simple binary one.

First, we show that absent user-user collusion, we can indeed circumvent the strong finite-block impossibility of Chung and Shi [7]. Specifically, we can indeed construct a TFM that simultaneously achieves UIC, MIC, and  $(\rho, c = 1)$ -SCP for any  $\rho$ . In particular, consider the following *finite-block posted price auction* – recall that to specify an MPC-assisted TFM, we only need to specify the allocation rule, the payment and miner revenue rules.

*MPC-assisted, finite-block posted price auction*

Let  $r$  be a fixed reserve price. Any bid that is at least  $r$  is considered as a candidate. Randomly choose up to block size  $k$  candidates to confirm. Any confirmed bid pays  $r$ . All payment is burnt and the miner revenue is 0.

► **Theorem 1.4** (MPC-assisted, finite-block posted price auction). *The above MPC-assisted, finite-block posted price auction satisfies UIC, MIC, and  $(\rho, 1)$ -SCP in the ex post setting for an arbitrary  $\rho \in [0, 1]$ .*

Since Theorem 1.4 holds even in the ex post setting, another interpretation is that the enforcement of the allocation rule (i.e., restriction R2, and not R1) is what allows us to circumvent the finite-block impossibility when  $c = 1$ .



■ **Table 1 Mathematical landscape of TFM.** Results in gray background are shown in this paper.  $\times$  means impossible and  $\checkmark$  means possible.  $\Theta(\cdot)$  means that we show matching upper and lower bounds – here  $m$  is a term that depends on the scale of the bid distribution, and we ignore terms related to  $c$  for simplicity. Unless otherwise noted, the impossibilities hold even for  $c = 1$ .

		plain model	MPC-assisted model
Infinite block	strict	0 miner rev [7]	0 miner rev
	approximate	$\Theta(n \cdot (\epsilon + \sqrt{m\epsilon}))$ miner rev	$\Theta(n \cdot (\epsilon + \sqrt{m\epsilon}))$ miner rev
Finite block	strict	$\times$ [7]	$\checkmark$ : $c = 1$ , $\times$ : $c \geq 2$
	approximate	scalability $\times$ (ignoring log terms)	scalability $\checkmark$

The above finite-block posted price auction works for  $c = 1$ , i.e. no user-user collusion; however, it fails when the coalition may contain  $c \geq 2$  users. Imagine that the number of users  $n = k + 1$ , and the coalition consists of two users and any fraction of miners. Now, suppose one of the colluding users has true value  $v \gg r$ , and the other has true value  $v' = r$ . In this case, the user with true value  $v' = r$  should simply drop out and not submit a bid. This guarantees that the friend with large true value will be confirmed, and thus the coalition’s joint utility increases.

It turns out that this is no accident. We prove that for  $c \geq 2$ , no MPC-assisted TFM can achieve UIC, MIC, and SCP for  $(\rho, c)$ -sized coalitions at the same time for any choice of  $\rho$ . Further, the impossibility holds even assuming Bayesian notions of incentive compatibility.

► **Theorem 1.5** (Finite-block impossibility in the MPC-assisted model for  $c \geq 2$ ). *Let  $c \geq 2$  and let  $\rho \in [0, 1]$ . No (possibly randomized) MPC-assisted TFM with non-trivial utility can simultaneously achieve Bayesian UIC, Bayesian MIC, and Bayesian SCP for  $(\rho, c)$ -sized coalitions, assuming finite block size.*

### MPC-assisted TFM under approximate incentive compatibility

Recall that in the plain model, even with approximate incentive compatibility, we cannot have scalable TFMs whose social welfare scales w.r.t. the bid distribution (Theorem 1.3). We show that if we consider approximate incentive compatibility in the MPC-assisted model, we can overcome this scalability barrier. Specifically, we construct an MPC-assisted TFM called the “diluted posted price auction” that can achieve up to  $\Theta(M \cdot k)$  social welfare when many people’s bids are large enough, where  $M$  is an upper bound on users’ bid.

#### MPC-assisted, diluted posted price auction

- Let  $r$  be a fixed reserve price, let  $M$  be the maximum possible value of the bid, and let  $k$  be the block size.
- Remove all bids that are less than  $r$ , and suppose that there are  $\ell$  bids left – these bids form the candidate pool.
- Let  $N = \max\{c \cdot \sqrt{\frac{kM}{2c}}, k\}$ . If  $\ell < N$ , pad the candidate pool with fake 0 bids such that its size is  $N$ .
- Choose  $k$  bids at random from the candidate pool. All real bids chosen are confirmed and pay the reserve price  $r$ .
- The miner gets  $\frac{2\epsilon}{c}$  for each confirmed bid.

In the above mechanism, suppose we set the reserve price  $r \leq M/2$ , and further, imagine that  $n \gg k$  people bid  $M$ . In this case, we will achieve  $\Theta(M \cdot k)$  social welfare with high probability.

► **Theorem 1.6** (MPC-assisted, diluted posted price auction). *The above MPC-assisted, diluted posted price auction satisfies strict UIC, strict MIC, and  $\epsilon$ -SCP for  $(\rho, c)$ -sized coalitions in the ex post setting, for any choice of  $\rho$  and  $c$ . Further, the mechanism is scalable, i.e., it can achieve  $\Theta(M \cdot k)$  expected social welfare under some bid configurations.*

### Summary of landscape

Summarizing our understanding so far, we present the mathematical landscape of TFM in Table 1. Our results show that cryptography can help us circumvent fundamental impossibilities of the plain model under finite block size. First, for strict incentive compatibility, cryptography allows us to overcome the finite-block impossibility for  $c = 1$  (Theorem 1.4). Second, with approximate incentive compatibility, cryptography allows us to overcome the scalability barrier for finite block size in the plain model.

On the other hand, cryptography is also not a panacea. For example, it does not fundamentally help us improve miner revenue in the infinite block size setting.

## 1.2 Additional Related Work

We review some additional related works besides the most closely related works on transaction mechanism design [24, 32, 4, 5, 29, 30, 12, 7] mentioned earlier.

Earlier, an elegant line of work [19, 22, 1, 27, 3, 2, 15, 14, 16, 21, 10, 18, 9, 31, 8, 28, 23, 13, 11] revealed ways in which cryptography and game theory can help each other. Among them, some works [10] showed how to rely on cryptography to remove the trusted mediator assumption in certain game theoretic notions such as correlated equilibrium. Some [19, 1, 20, 27, 9, 31] showed that adopting game theoretic notions of fairness rather than the more stringent cryptographic notions of fairness can allow us to circumvent well-known lower bounds. Recently, Ferreira et al. [13] and Essaidi et al. [11] showed that using cryptographic commitments can help us circumvent lower bounds pertaining to credible auctions. As Chung and Shi [7] explained, credible auction is of a different nature from transaction fee mechanism design. Transaction fee mechanism is a new type of decentralized mechanism design problem, and the new connections between cryptography and mechanism design revealed in our paper differ in nature from the settings in prior works.

## 2 Model and Definitions

### Notation

We use bold letters to denote vectors. For a vector  $\mathbf{b} = (b_1, \dots, b_N)$ , we use  $b_i$  to represent the  $i$ -th entry of vector  $\mathbf{b}$ . The notation  $\mathbf{b}_{-i} = (b_1, b_2, \dots, b_{i-1}, b_{i+1}, \dots, b_N)$  represents all except the  $i$ -th entry. We often use  $(\mathbf{b}_{-i}, b_i)$  and  $\mathbf{b}$  interchangeably. Throughout the paper, we use  $n$  to denote the number of users, and  $N$  to denote the number of bids.  $N$  is equal to  $n$  if everyone behaves truthfully. However, strategic users may post zero or multiple bids – in this case  $N$  may not be equal to  $n$ . Given a distribution  $\mathcal{D}$ , we use the notation  $\text{Supp}(\mathcal{D})$  to denote its support. We use  $\mathbb{R}^{\geq 0}$  to denote non-negative real numbers.



## 2.1 Transaction Fee Mechanism in the Plain Model

We first define transaction fee mechanism (TFM) in the plain model. Henceforth, we use  $\mathcal{C}$  to denote a coalition of strategic players (or a strategic individual). In particular,  $\mathcal{C}$  can be a user, the miner of the present block, or a coalition of the miner and one or more users.

### Plain model

In the plain model, a transaction fee mechanism (TFM) describes the following game:

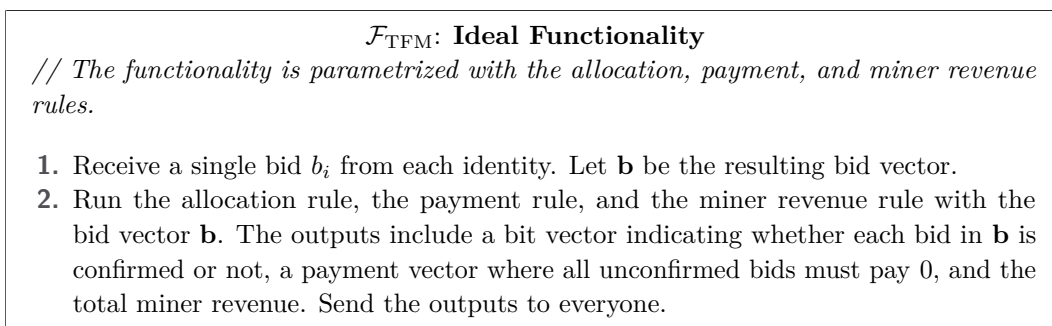
1. Users not in  $\mathcal{C}$  submit their bids where each bid is represented by a single real value – let  $\mathbf{b}_{-\mathcal{C}}$  denote the resulting bid vector.
2. The coalition  $\mathcal{C}$  sees  $\mathbf{b}_{-\mathcal{C}}$ , and then users in  $\mathcal{C}$  submit their bids.
3. The miner of the present block, possibly a member of  $\mathcal{C}$ , chooses up to  $k$  bids to include in the block, where  $k$  denotes the maximum block size.
4. Among the at most  $k$  bids included in the block, the trusted blockchain decides 1) which of them are confirmed, 2) how much each confirmed bid pays, and 3) how much revenue is paid to the miner.

Therefore, to specify a transaction fee mechanism (TFM) in the plain model, it suffices to specify the following rules which are *possibly randomized* functions:

- *Inclusion rule*: given a bid vector  $\mathbf{b}$ , the inclusion rule chooses up to  $k$  bids to include in the block;
- *Confirmation and payment rules*: Given the at most  $k$  bids included in the block, the confirmation rule decides which ones to confirm, and the payment rule decides how much each confirmed user pays.
- *Miner revenue rule*: Given the at most  $k$  bids included in the block, the miner revenue rule decides how much the miner earns.

In particular, the inclusion rule is implemented by the miner, and if the miner is strategic, it may not follow the prescribed inclusion rule but instead choose an arbitrary set of bids to include. By contrast, the confirmation, payment, and miner revenue rules are implemented by the blockchain, and honest implementation is guaranteed.

We assume that the (honest) TFM is *symmetric* in the following sense: if we apply any permutation  $\pi$  to an input bid vector  $\mathbf{b} = (b_1, \dots, b_N)$ , it does not change the distribution of the *random variable* represented by the set  $\{(b_i, x_i, p_i)\}_{i \in [N]}$  where  $x_i$  and  $p_i$  are random variables denoting the probability that bid  $i$  is confirmed, and its payment, respectively. An equivalent, more operational view of the above condition is the following. We may assume that the honest 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 this 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 or identity. At this point, 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. Note that our symmetry requirement is natural and quite general – it captures all the mechanisms we know so far [24, 32, 4, 5, 29, 30, 12]. In particular, due to possible tie-breaking in the sorting step, our symmetry condition does *not* require two bids of the same amount to receive the same treatment, i.e., the distribution of their outcomes can be different.



■ **Figure 1** Ideal functionality realized by the MPC protocol.

### Strategy space

A user's truthful behavior is submit a single bid representing its true value. However, strategic users may choose to submit zero to multiple bids, and the bids need not reflect their true value.

An honest miner does not submit any bids and honestly implements the prescribed inclusion rule. A strategic miner, on the other hand, may not honestly implement the prescribed inclusion rule – it can pick an arbitrary set of up to  $k$  bids of its choice to include. A strategic miner can also post fake bids. A coalition  $\mathcal{C}$ 's strategy space is defined in the most natural manner, i.e., it includes any strategic behavior of its members.

Notably, any strategic player in  $\mathcal{C}$  can decide its actions *after* having observed the bids of the remaining users not in  $\mathcal{C}$ .

## 2.2 Transaction Fee Mechanism in the MPC-Assisted Model

Imagine that all miners jointly run an multi-party computation (MPC) protocol that implements the TFM. Figure 1 depicts the natural ideal functionality (denoted  $\mathcal{F}_{\text{TFM}}$ ) realized by the MPC protocol. Further, the MPC protocol can achieve full security with guaranteed output as long as the majority of the miners are honest. Therefore, following the modular composition [6] paradigm in the standard cryptography literature, we can simply assume that a trusted party  $\mathcal{F}_{\text{TFM}}$  exists – this is often referred to as the  $\mathcal{F}_{\text{TFM}}$ -hybrid model. The instantiation of  $\mathcal{F}_{\text{TFM}}$  is available in the full version.

### MPC-assisted model

A transaction fee mechanism (TFM) in the MPC-assisted model describes the following game:

1. Every player (i.e., user or user) can take on *zero to multiple* identities, and every identity submits a bid represented by a single real value to  $\mathcal{F}_{\text{TFM}}$  defined in Figure 1.
2.  $\mathcal{F}_{\text{TFM}}$  decides which bids to confirm, how much each confirmed bid pays, and the total miner revenue. The total miner revenue is split among the miners.

Therefore, to specify a TFM in the MPC-assisted model, we need to specify the allocation rule, the payment rule, and the miner revenue rule – we assume that these rules are *possibly randomized*, polynomial-time algorithms, and the syntax of the rules are evident from  $\mathcal{F}_{\text{TFM}}$  in Figure 1. In comparison with the plain model, here the *inclusion* rule and the *confirmation* rule are combined into a single *allocation* rule, since both inclusion and confirmation decisions are made by  $\mathcal{F}_{\text{TFM}}$ . Just like in the plain model, we assume that the (honest) TFM is symmetric.

### Strategy space

A user's honest behavior is to take on a *single* identity, submit a single bid which reflects its true value. However, as mentioned above, any strategic user can take on zero or multiple identities, submit zero or multiple bids that need not be its true value.

An honest miner does not take on any identities or submit any bids. However, a strategic miner can take on one or more identities and submit fake bids. Unlike the plain model, here, a strategic miner can no longer choose which bids to include in the block – the allocation rule (i.e., the counterpart of the inclusion + confirmation rules of the plain model) is enforced by  $\mathcal{F}_{\text{TFM}}$ .

One technicality is whether the distribution of users' identities matter, and whether choosing identities strategically should be part of the strategy space. Jumping ahead, all of our mechanisms are proven to be incentive compatible even when the strategic individual or coalition can arbitrarily choose their identities as long as they cannot impersonate honest users' identities. On the other hand, all of our impossibility results hold even when the strategic individual or coalition is forced to choose their identities from some a-priori known distribution. This makes both our feasibility and infeasibility results stronger.

## 2.3 Defining Incentive Compatibility

### Utility

Every user  $i \in [n]$  has a true value  $v_i \in \mathbb{R}^{\geq 0}$  if its transaction is confirmed. If user  $i$ 's transaction is confirmed and the user pays  $p_i$ , then its utility is defined as  $v_i - p_i$ . A miner's utility is simply its revenue.

The utility of any strategic coalition  $\mathcal{C}$  is the sum of the utilities of all members of  $\mathcal{C}$ . Considering the joint utility of the coalition is appropriate since we assume that the coalition has a *binding* mechanism (e.g., decentralized smart contracts) to split off their gains off the table.

### Ex post incentive compatibility

We first define ex post incentive compatibility for both the plain model and the MPC-assisted model. Roughly speaking, ex post incentive compatibility requires that a strategic player or coalition's best response is always to behave honestly, even after observing the remaining users' bids. Similarly, ex post  $\epsilon$ -incentive compatibility requires that no strategy can increase a strategic player or coalition's expected utility by more than  $\epsilon$  in comparison with the honest strategy, and this should hold even if the coalition can decide its strategy *after* having observed the remaining users' bids.

Below in our formal definitions, we define the *approximate* case that allows  $\epsilon$  slack. When  $\epsilon = 0$ , we get *strict* incentive compatibility – in this case, we can omit writing the  $\epsilon$ .

- **Definition 2.1** (Ex post incentive compatibility). *We say that a mechanism satisfies ex post  $\epsilon$ -incentive compatibility for a set of players  $\mathcal{C}$  (possibly an individual), iff for any bid vector  $\mathbf{b}_{-\mathcal{C}}$  posted by users not in  $\mathcal{C}$ , for any vector of true values  $\mathbf{v}_{\mathcal{C}}$  of users in  $\mathcal{C}$ , no strategy can increase  $\mathcal{C}$ 's expected utility by more than  $\epsilon$  in comparison with honest behavior. Specifically,*
- *UIC. We say that a TFM (in either the plain or MPC-assisted model) satisfies ex post  $\epsilon$ -user incentive compatibility (UIC), iff for any  $n$ , for any  $i \in [n]$ , for any bid vector  $\mathbf{b}_{-i}$  of all users other than  $i$ , for any true value  $v_i$  of user  $i$ , no strategy can increase  $i$ 's expected utility by more than  $\epsilon$  in comparison with truthful bidding.*

## 97:12 What Can Cryptography Do for Decentralized Mechanism Design?

- *MIC.* In the plain model, we focus on the miner of the present block when defining miner incentive compatibility. We say a TFM in the plain model satisfies *ex post*  $\epsilon$ -miner incentive compatibility MIC, iff for any bid vector  $\mathbf{b}$ , no strategy can increase the miner's expected utility by more than  $\epsilon$  in comparison with honest behavior. Recall that here, the miner's honest behavior is to honestly implement the inclusion rule and not inject any fake bids.

In the MPC-assisted model, we want MIC to hold for any coalition controlling at most  $\rho$  fraction of the miners. Therefore, we say that an MPC-assisted TFM satisfies *ex post*  $\epsilon$ -MIC against  $\rho$ -sized coalitions, iff for any coalition controlling at most  $\rho$  fraction of the miners, for any bid vector  $\mathbf{b}$ , no strategy can increase the miner's expected utility by more than  $\epsilon$  in comparison with honest behavior. In the  $\mathcal{F}_{\text{TFM}}$ -hybrid world, the miner's honest behavior is simply not to take on any identities and inject any fake bids.

- *SCP.* In the plain model, we want side-contract-proofness to hold for any miner-user coalition that involves the miner of the present block, and up to  $c$  users. We say that a TFM in the plain model satisfies *ex post*  $\epsilon$ -side-contract-proofness (SCP) for  $c$ -sized coalitions, iff for any miner-user coalition consisting of the miner and up to  $c$  users, for any bid vector  $\mathbf{b}_{-C}$  posted by users not in  $C$ , no strategy can increase  $C$ 's expected utility by more than  $\epsilon$  in comparison with honest behavior.

In the MPC-assisted model, we want SCP to hold for any miner-user coalition that involves up to  $\rho$  fraction of the miners and up to  $c$  users. We say that an MPC-assisted TFM satisfies *ex post*  $\epsilon$ -SCP for  $(\rho, c)$ -sized coalitions, iff for any miner-user coalition<sup>2</sup> consisting of at most  $\rho$  fraction of the miners and up to  $c$  users, for any bid vector  $\mathbf{b}_{-C}$  posted by users not in  $C$ , no strategy can increase the coalition's utility by more than  $\epsilon$  in comparison with honest behavior.

### Bayesian incentive compatibility

For the MPC-assisted model, it also makes sense to consider a Bayesian notion of incentive compatibility. In particular, the MPC-assisted model requires that the strategic player or coalition decides its strategy without having seen the remaining users' bids. We may assume that the strategic player or coalition has some a-prior belief of each honest user's true value distribution. We assume that all honest users' true values are independently and identically distributed (i.i.d.) and sampled from some distribution  $\mathcal{D}$ . In Bayesian incentive compatibility, we imagine that a strategic individual or coalition cares about maximizing its expected utility where the expectation is taken over not just the random coins of the mechanism, but also the remaining honest users' bids.

Henceforth, given a set  $\mathcal{S}$  of players, we use the notation  $\mathcal{D}_{\mathcal{S}}$  to denote  $\mathcal{D}^u$  where  $u$  is the number of users in  $\mathcal{S}$ . Similarly,  $\mathcal{D}_{-i} := \mathcal{D}^{n-1}$ . Again, we define  $\epsilon$ -incentive compatibility for the Bayesian setting below, where the corresponding strict incentive compatibility notions can be obtained by setting  $\epsilon = 0$ .

► **Definition 2.2** (Bayesian incentive compatibility). *We say that an MPC-assisted TFM satisfies Bayesian  $\epsilon$ -incentive compatibility for a coalition or individual  $C$ , iff for any  $\mathbf{v}_C$  denoting the true values of users in  $C$ , sample  $\mathbf{b}_{-C} \sim \mathcal{D}_{-C}$ , then, no strategy can increase  $C$ 's expected utility by more than  $\epsilon$  in comparison with honest behavior, where the expectation is taken over randomness of the honest users bids  $\mathbf{b}_{-C}$ , as well as random coins consumed by the TFM. Specifically,*

<sup>2</sup> We require the miner-user coalition to consist of a non-zero fraction the miners and at least one user – otherwise the definition would degenerate to UIC or MIC.

- *UIC.* We say that an MPC-assisted TFM satisfies Bayesian  $\epsilon$ -UIC, iff for any  $n$ , for any user  $i \in [n]$ , for any true value  $v_i \in \mathbb{R}^{\geq 0}$  of user  $i$ , for any strategic bid vector  $\mathbf{b}_i$  from user  $i$  which could be empty or consist of multiple bids,

$$\mathbf{E}_{\mathbf{b}_{-i} \sim \mathcal{D}_{-i}} [\text{util}^i(\mathbf{b}_{-i}, v_i)] \geq \mathbf{E}_{\mathbf{b}_{-i} \sim \mathcal{D}_{-i}} [\text{util}^i(\mathbf{b}_{-i}, \mathbf{b}_i)] - \epsilon$$

where  $\text{util}^i(\mathbf{b})$  denotes the expected utility (taken over the random coins of the TFM) of user  $i$  when the bid vector is  $\mathbf{b}$ .

- *MIC.* We say that an MPC-assisted TFM satisfies Bayesian  $\epsilon$ -MIC for  $\rho$ -sized coalitions, iff for any miner coalition  $\mathcal{C}$  controlling at most  $\rho$  fraction of the miners, for any strategic bid vector  $\mathbf{b}'$  injected by the miner,

$$\mathbf{E}_{\mathbf{b}_{-\mathcal{C}} \sim \mathcal{D}_{-\mathcal{C}}} [\text{util}^{\mathcal{C}}(\mathbf{b}_{-\mathcal{C}})] \geq \mathbf{E}_{\mathbf{b}_{-\mathcal{C}} \sim \mathcal{D}_{-\mathcal{C}}} [\text{util}^{\mathcal{C}}(\mathbf{b}_{-\mathcal{C}}, \mathbf{b}')] - \epsilon$$

where  $\text{util}^{\mathcal{C}}(\mathbf{b})$  denotes the expected utility (taken over the random coins of the TFM) of the coalition  $\mathcal{C}$  when the input bid vector is  $\mathbf{b}$ .

- *SCP.* We say that an MPC-assisted TFM satisfies Bayesian  $\epsilon$ -SCP for  $(\rho, c)$ -sized coalitions, iff for any miner-user coalition consisting of at most  $\rho$  fraction of the miners and at most  $c$  users, for any true value vector  $\mathbf{v}_{\mathcal{C}}$  of users in  $\mathcal{C}$ , for any strategic bid vector  $\mathbf{b}_{\mathcal{C}}$  of the coalition (whose length may not be equal to the number of users in  $\mathcal{C}$ ),

$$\mathbf{E}_{\mathbf{b}_{-\mathcal{C}} \sim \mathcal{D}_{-\mathcal{C}}} [\text{util}^{\mathcal{C}}(\mathbf{b}_{-\mathcal{C}}, \mathbf{v}_{\mathcal{C}})] \geq \mathbf{E}_{\mathbf{b}_{-\mathcal{C}} \sim \mathcal{D}_{-\mathcal{C}}} [\text{util}^{\mathcal{C}}(\mathbf{b}_{-\mathcal{C}}, \mathbf{b}_{\mathcal{C}})] - \epsilon$$

Note that the Bayesian notions of incentive compatibility do not make sense in the plain model, since in the plain model, the strategic individual or coalition can decide its move *after* having observed the remaining honest users' bids. This is why we adopt only the ex post notion in the plain model. Formally, it is easy to show that any mechanism that satisfies Bayesian incentive compatibility in the plain model also satisfies ex post incentive compatibility.

In the MPC-assisted model, both notions make sense, and the ex post notions are strictly stronger than the Bayesian counterparts. Jumping ahead, all of our impossibility results for the MPC-assisted model work even for the Bayesian notions, and all of our mechanism designs in the MPC-assisted model work even for the ex post notions. This makes both our lower- and upper-bounds stronger.

### 3 Approximate Incentive Compatibility for Infinite Block Size

In the plain model, no UIC and SCP mechanism (even for  $c = 1$  and infinite block size) can achieve positive miner revenue [7]. In our full version, we show that the same zero miner revenue lower bound holds even in the MPC-assisted model. Therefore, we consider how to get meaningful miner revenue using the relaxed notion of approximate incentive compatibility. In this section, we give a tight characterization of approximate incentive compatibility for infinite block size. This tight characterization applies to both the MPC-assisted model and the plain model.

#### 3.1 Bounds on Miner Revenue

We first prove a limit on miner revenue in the MPC-assisted model, which holds even for in the Bayesian setting. The same limit applies to the plain model for the ex post setting – to see this, observe that the strategy space is strictly larger in the plain model, and moreover, for the plain model, we only care about  $\rho = 1$ .

## 97:14 What Can Cryptography Do for Decentralized Mechanism Design?

We now show an MPC-assisted mechanism simultaneously satisfies  $\epsilon$ -UIC,  $\epsilon$ -MIC and  $\epsilon$ -SCP even for the Bayesian setting and even for  $c = 1$  and an arbitrary choice  $\rho \in (0, 1]$ , then the miner can gain at most  $O(n \cdot (\epsilon + \sqrt{m^* \cdot \epsilon}))$ -miner revenue, where  $n$  is the number of users, and  $m^*$  is a term that depends on the “scale” of the bid distribution.

To prove the limit on the miner revenue, we care only about the probability of each bid being confirmed, the expected payment of each bid, and the miner revenue. Therefore, we introduce the following notations to denote the outputs of the allocation, payment, and miner revenue rules – we assume that each user’s true value is drawn i.i.d. from some distribution  $\mathcal{D}$  since we are considering the Bayesian setting:

- **Allocation rule:** given a bid vector  $\mathbf{b} = (b_1, \dots, b_N)$ , the allocation rule outputs a vector  $\mathbf{x}(\mathbf{b}) := (x_1, \dots, x_N) \in [0, 1]^N$ , where each  $x_i$  denotes the probability of  $b_i$  being confirmed.
- **Payment rule:** given a bid vector  $\mathbf{b} = (b_1, \dots, b_N)$ , the payment rule outputs a vector  $\mathbf{p}(\mathbf{b}) := (p_1, \dots, p_N) \in \mathbb{R}^N$ , where each  $p_i$  denotes the expected payment of  $b_i$ .
- **Miner revenue rule:** given a bid vector  $\mathbf{b} = (b_1, \dots, b_N)$ , the miner revenue rule outputs  $\mu(\mathbf{b}) \in \mathbb{R}$ , denoting the amount paid to the miner.

We also define  $\mathcal{D}_{-i} := \mathcal{D}^{N-1}$ , and for the  $i$ -th user, we define

$$\bar{x}_i(\cdot) = \mathbf{E}_{\mathbf{b}_{-i} \sim \mathcal{D}_{-i}} [\mathbf{x}_i(\mathbf{b}_{-i}, \cdot)], \quad \bar{p}_i(\cdot) = \mathbf{E}_{\mathbf{b}_{-i} \sim \mathcal{D}_{-i}} [\mathbf{p}_i(\mathbf{b}_{-i}, \cdot)], \quad \bar{\mu}_i(\cdot) = \mathbf{E}_{\mathbf{b}_{-i} \sim \mathcal{D}_{-i}} [\mu(\mathbf{b}_{-i}, \cdot)].$$

Henceforth, we often use  $(\mathbf{x}, \mathbf{p}, \mu)$  to denote a TFM in the MPC-assisted model. The crux of our proof is to characterize how miner revenue changes when we lower one user’s bid to 0. We then apply this argument  $n$  times, and lower each user’s bid one by one to 0 to get the desired bound. To make the second step work, we need to use approximate MIC to remove a user’s bid from consideration once we have lowered it to zero – this ensures that in any step of our inductive argument, the non-strategic users’ bids are always i.i.d. sampled from  $\mathcal{D}$ .

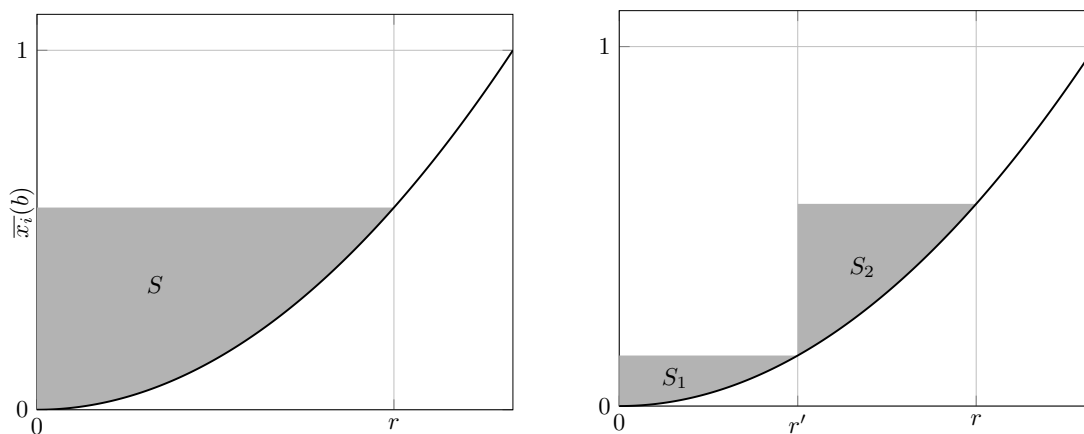
### Warmup

To understand how much the miner revenue changes when one user lowers its bid to 0, we start from a simplified case where a TFM  $(\mathbf{x}, \mathbf{p}, \mu)$  is Bayesian *strict*-UIC and Bayesian  $\epsilon$ -SCP for  $c = 1$  and some  $\rho \in (0, 1]$ . By Myerson’s Lemma [25], strict-UIC implies that, for any user  $i$ , the allocation rule  $x_i(\cdot)$  must be non-decreasing. Moreover, the expected payment when bidding  $b$  is specified as

$$\bar{p}_i(b) = b \cdot \bar{x}_i(b) - \int_0^b \bar{x}_i(t) dt.$$

We care about how much the miner revenue can increase when user  $i$  bids  $r$  instead of 0. One trivial upper bound can be obtained as follows. Imagine that user  $i$ ’s true value is 0, but it bids  $r$  instead. In this case, the user’s loss in utility (in comparison with truthful bidding) is represented by the area of the gray triangle  $S$  in Figure 2a. Due to  $\epsilon$ -SCP, the miner revenue increase when user  $i$  bids  $r$  instead of 0 must be upper bounded by  $S + \epsilon$ . This bound, however, is not tight. To make it tighter, we consider bounding it in two steps by introducing a mid-point  $r' \in (0, r)$ . If user  $i$ ’s true value is 0, but it bids  $r'$  instead, its utility loss is the area  $S_1$  of Figure 2b. By  $\epsilon$ -SCP, we conclude that  $\bar{\mu}_i(r') - \bar{\mu}_i(0) \geq S_1 + \epsilon$ . Now, imagine user  $i$ ’s true value is  $r'$  but it bids  $r$  instead. Using a similar argument, we conclude that  $\bar{\mu}_i(r) - \bar{\mu}_i(r') \geq S_2 + \epsilon$  (see Figure 2b). Summarizing the above, we have that  $\bar{\mu}_i(r) - \bar{\mu}_i(0) \geq S_1 + S_2 + 2\epsilon$ .





(a) When user  $i$  changes its bid from 0 to  $r$ , it loses utility  $S$ . Therefore, miner revenue changes by no more than  $S + \epsilon$ .

(b) When user  $i$  changes its bid from 0 to  $r'$ , it loses utility  $S_1$ . Then when it changes its bid from  $r'$  to  $r$ , it loses utility  $S_2$ .

■ **Figure 2** User's utility change.

To get a tight bound, the key is how to choose the optimal number of steps  $L$  we use in the above argument. Taking more steps makes the total area of the gray triangles smaller; however, every step incurs an extra  $\epsilon$ . Given the number of steps  $L$ , the sum of the  $L$  triangles is upper bounded by  $r/L$ , and since each step incurs an additive  $\epsilon$  term, our goal is to minimize the expression  $r/L + \epsilon L$ . Picking  $L = \sqrt{\frac{r}{\epsilon}}$  minimizes the expression and thus we have that  $\bar{\mu}_i(r) - \bar{\mu}_i(0) \leq 2\sqrt{r\epsilon}$ .

**Full proof.** The above warmup argument works for strict-UIC and  $\epsilon$ -SCP. We want to prove a limitation on miner revenue for Bayesian  $\epsilon$ -UIC and  $\epsilon$ -SCP. The challenge is that for  $\epsilon$ -UIC, Myerson's lemma no longer holds – in particular, the allocation rule may not even be monotone any more. The key idea our proof is to give a generalization of Myerson's lemma to account for the  $\epsilon$  slack in incentive compatibility. The full proof is available in the full version.

### 3.2 Achieving Optimal Revenue: Proportional Auction

We now show that the limit on miner revenue in Theorem 1.2 is asymptotically tight, i.e., we can indeed design a TFM, even in the plain model, whose miner revenue asymptotically matches that in Theorem 1.2 for some natural bid distribution.

#### Proportional Auction (plain model)

**Parameters:** the slack  $\epsilon$ , the reserved price  $r$  where  $r \geq 2\epsilon$ .

**Input:** a bid vector  $\mathbf{b} = (b_1, \dots, b_N)$ .

**Mechanism:**

- *Inclusion rule.* Include all bids in  $\mathbf{b}$ .
- *Confirmation rule.* For each bid  $b$ , if  $b < r$ , it is confirmed with the probability  $b/r$ ; otherwise, if  $b \geq r$ , it is confirmed with probability 1.
- *Payment rule.* For each confirmed bid  $b$ , if  $b < r$ , it pays  $b/2$ ; otherwise, it pays  $r/2$ .
- *Miner revenue rule.* For each confirmed bid  $b$ , if  $b \geq \sqrt{2r\epsilon^a}$ , then miner is paid  $\frac{\sqrt{2r\epsilon}}{2}$ .

<sup>a</sup> This guarantees that the miner revenue does not exceed the total payment.

## 97:16 What Can Cryptography Do for Decentralized Mechanism Design?

The above mechanism is called the proportional mechanism since the user's confirmation probability is proportional to the bid in the region  $[0, r]$ , and any bid that is at least  $r$  is confirmed with probability 1.

► **Theorem 3.1.** *The above proportional auction in the plain model is UIC, MIC and  $\frac{5}{4}c\epsilon$ -SCP against  $c$ -sized coalitions for arbitrary  $c \geq 1$ .*

### Proof intuition

We provide the proof intuition here, the full proof is available in the full version. First, UIC and MIC are easy to prove. Observe that the allocation rule (i.e., the union of the inclusion and confirmation rules) is monotone, and by design, the payment rule is the unique one that satisfies Myerson's Lemma. Therefore, the mechanism satisfies UIC. It is easy to see that injecting a bid does not help the miner, since each bid's contribution to the miner revenue is independent and limited by the payment amount.

Proving that the mechanism satisfies  $\frac{5}{4}c\epsilon$ -SCP is more technical. Here we give an illustrative explanation to show that the joint utility of each user and the miner can increase by at most  $\frac{5}{4}\epsilon$ . Since underbidding does not increase the user's utility or the miner's revenue, we focus on overbidding. Note that overbidding does not increase the joint utility for a user whose true value is  $v \geq r$ . Therefore, we focus in the case where the colluding user has true value  $v < r$  and overbids.

If  $v \geq \sqrt{2r\epsilon}$ , the user's utility loss when overbidding to  $v'$  is represented by the gray triangle in Figure 3a. Meanwhile, the miner's expected revenue increases by  $\frac{\sqrt{2r\epsilon}}{2}(\frac{v'}{r} - \frac{v}{r})$ , which is the area of the dashed rectangle in Figure 3a. Therefore, when the user overbids by  $v' - v = \frac{\sqrt{2r\epsilon}}{2}$ , the coalition's utility increase is maximized and equals to  $\frac{\epsilon}{4}$ .

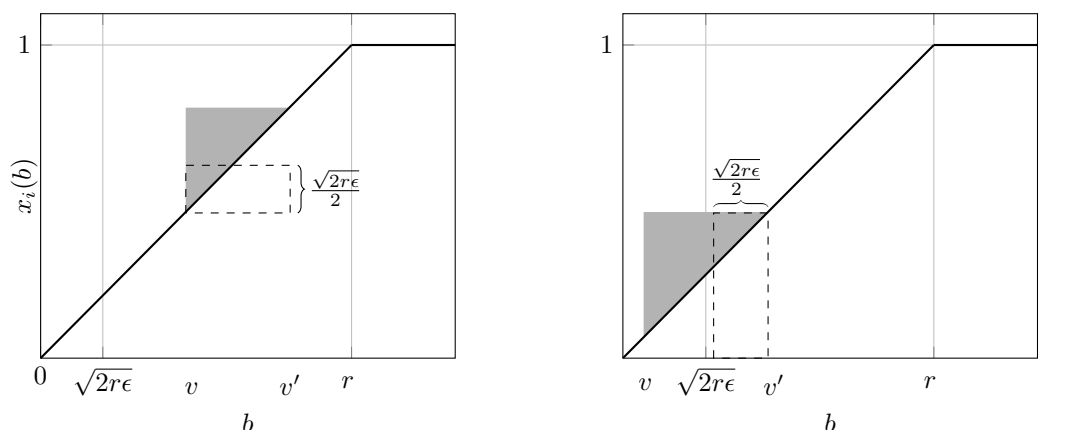
If  $v < \sqrt{2r\epsilon}$  and the colluding user overbids to  $v' \geq \sqrt{2r\epsilon}$ , then the user's utility loss when overbidding to  $v'$  is represented by the area of the gray triangle in Figure 3b. The miner's revenue now increases by  $\frac{v'}{r} \cdot \frac{\sqrt{2r\epsilon}}{2}$ , because the user's utility would be 0 if the user behaves honestly. The increase in the miner's revenue is represented by the dashed rectangle in Figure 3b. The increase in the joint utility of the coalition is maximized when  $v$  is arbitrarily close to  $\sqrt{2r\epsilon}$  and the user overbids by  $v' - v = \frac{\sqrt{2r\epsilon}}{2}$ . In this case, the joint utility of the coalition increases by  $\frac{5}{4}\epsilon$ .

## 4 Characterization of Finite Block Size in the Plain Model

In real-world blockchains, we do not have an infinite block size. Chung and Shi [7] showed that no non-trivial plain-model TFM can achieve strict UIC and strict SCP (even when  $c = 1$ ) for finite block size. In this section, we show that although approximate incentive compatibility can help us overcome this impossibility, nonetheless we cannot get useful mechanisms whose social welfare scales with the bid distribution (ignoring logarithmic terms).

► **Theorem 4.1.** *Suppose the block size is upper bounded by  $k$ . Fix any  $\epsilon > 0$ . Given any TFM in the plain model that satisfies  $\epsilon$ -UIC,  $\epsilon$ -MIC and  $\epsilon$ -SCP when the miner can collude with at most  $c = 1$  user, and given any bid vector  $\mathbf{b}$ , let  $M = \max(\mathbf{b})$  be the maximum bid of any user, it must be that*

- *the miner's expected revenue is upper bounded by  $12k^2\epsilon \log(\frac{M}{\epsilon} + 1) + 2k\epsilon$ ;*
- *every user's expected utility is upper bounded by  $12k^2\epsilon \log(\frac{M}{\epsilon} + 1) + (2k + 1)\epsilon$  conditioned on the bid being included in the block, and assuming the bid reflects its true value;*
- *the expected social welfare is upper bounded by  $O(k^3\epsilon \log(\frac{M}{\epsilon} + 1) + k^2\epsilon)$ .*



(a) An illustrative example of the coalition's joint utility change when the user's true value  $v \geq \sqrt{2r\epsilon}$ .

(b) An illustrative example of the coalition's joint utility change when the user's true value  $v < \sqrt{2r\epsilon}$ .

■ **Figure 3** Coalition's joint utility change when the miner colluding with one user.

A direct corollary of Theorem 4.1 is that there is no non-trivial mechanism that satisfies approximate incentive compatibility if the user's true value is unbounded. This implies that there is no universal mechanism that works for all bid distributions. Formally,

► **Corollary 4.2.** *Suppose the block size is upper bounded by  $k$ . Fix any  $\epsilon > 0$ . If users' true values are unbounded, then no (possibly randomized) non-trivial TFM in the plain model can simultaneously satisfy  $\epsilon$ -UIC and  $\epsilon$ -SCP, even if the miner colludes with only one user.*

**Proof.** For the sake of contradiction, assume that there exists an  $\epsilon > 0$ , such that there exists a non-trivial TFM satisfying  $\epsilon$ -UIC and  $\epsilon$ -SCP. Recall that  $x_i(\mathbf{b})$  denotes the probability of user  $i$ 's bid being confirmed given that the world consists of the bid vector  $\mathbf{b}$  (assuming the mechanism is honestly implemented). We define  $\tilde{x}_i(\mathbf{b}')$  to be the probability of user  $i$ 's bid being confirmed conditioned on its bid being included in the block configuration  $\mathbf{b}'$ . According to the assumption that the mechanism is non-trivial, there must exist an  $i \in [k]$  and a block configuration  $\mathbf{b}' = (b^*, \mathbf{b}_{-i})$  such that  $b^*$  has a positive probability  $\tilde{x}_i(\mathbf{b}')$  of being confirmed.

Now imagine the world consists of the bid vector  $\mathbf{b}$  where

$$\mathbf{b} = (b_1, b_2, \dots, b_{k-1}, \underbrace{M, M, \dots, M}_T),$$

where  $T \geq \frac{2k}{\tilde{x}_i(\mathbf{b}')}$  and  $M$  is some large number (larger than  $\max\{b_1, \dots, b_k\}$ ) that we will specify later.

Since the block size is bounded by  $k$ , there must exist a user  $j$  whose true value is  $M$  yet its probability of being confirmed is no more than  $\frac{k}{T} \leq \frac{1}{2}\tilde{x}_i(\mathbf{b}')$  by our choice of  $T$ . Therefore, user  $j$ 's utility (assuming the mechanism is honestly implemented) is at most  $M \cdot \frac{1}{2}\tilde{x}_i(\mathbf{b}')$ . Now consider the coalition of the miner and user  $j$ . By Theorem 4.1, their joint utility when behaving honestly is at most

$$M \cdot \frac{1}{2}\tilde{x}_i(\mathbf{b}')$$

## 97:18 What Can Cryptography Do for Decentralized Mechanism Design?

However, the miner can ask user  $j$  to bid  $b^*$  instead of its true value  $M$  and include  $(b_1, \dots, b_{k-1}, b^*)$  into the block, where the bid  $b^*$  comes from user  $j$ . Since the payment cannot exceed the bid, now the utility of user  $j$  is at least

$$M \cdot \tilde{x}_i(\mathbf{b}') - b^*.$$

As long as  $M$  is large enough such that

$$M \cdot \tilde{x}_i(\mathbf{b}') - b^* \geq M \cdot \frac{1}{2} \tilde{x}_i(\mathbf{b}') + 12k^2\epsilon \log\left(\frac{M}{\epsilon} + 1\right) + 2k\epsilon + \epsilon,$$

the coalition gains  $\epsilon$  more joint utility comparing to honest strategy. This contradicts  $\epsilon$ -SCP. Note that since user's true value can be unbounded, such  $M$  must exist. Therefore, there does not exist a non-trivial mechanism that satisfies  $\epsilon$ -UIC and  $\epsilon$ -SCP simultaneously. ◀

### Proof Roadmap

We first explain the blueprint. To prove that the total social welfare is small, we first show that the miner revenue must be  $\tilde{O}(k^2\epsilon)$  for any bid configuration. If we can show this, then given that the block size is finite, we can show that every user  $i$ 's utility conditioned on being included is small, which then allows us to bound the total social welfare. Suppose this is not the case, i.e., suppose that under some bid configuration  $\mathbf{b} := (b_1, \dots, b_N)$ , there is a user  $i$  with expected utility (conditioned on being included) significantly larger than the maximum possible expected miner revenue (which is upper bounded by  $\tilde{O}(k^2\epsilon)$ ). Then, imagine a world consisting of  $\mathbf{b}$  and additionally (infinitely) many users whose true value is the same as  $b_i$ . In this case, there must be one such user  $j$  whose expected utility is almost 0. Thus, if  $j$  is the miner's colluding friend, the miner would be willing to sacrifice all of its revenue, pretend that the world consists of  $\mathbf{b}$  where the  $i$ -th coordinate is replaced with  $j$ 's bid, and run the honest mechanism subject to  $j$  being included. In this case, the coalition can increase its expected joint utility since user  $j$  would be doing much better than the honest case.

The crux of our proof, therefore, is to show that the expected miner revenue must be bounded for any bid vector. To show this, we take two main steps. First, we show that if the world consists of only bids of value  $M$ , the expected miner revenue must be small. Using the above as base case, we then go through an inductive argument to show that in fact, for any bid vector where users do not necessarily bid  $M$ , the miner revenue must be small too. Note that showing the first step itself relies on another inductive argument that inducts on the length of the bid vector. The full proof is available in the full version.

## 5 Characterization for Finite Block Size in the MPC-Assisted Model

### 5.1 Characterization for Strict Incentive Compatibility

In this section, we give a characterization of strict incentive compatibility in the MPC-assisted model for finite block size. We show that cryptography helps us overcome the finite-block impossibility [7] for  $c = 1$ , but for  $c \geq 2$ , the impossibility still holds.

#### 5.1.1 Feasibility for $c = 1$

In the MPC-assisted model, we indeed can have a mechanism that achieves UIC, MIC, and  $(\rho, 1)$ -SCP against a coalition controlling  $\rho \in (0, 1]$  fraction of the miners and  $c = 1$  user.

**MPC-assisted, finite-block posted price auction**

**Parameters:** the reserved price  $r$ , and a block size  $k$ .

**Input:** a bid vector  $\mathbf{b} = (b_1, \dots, b_N)$ .

**Mechanism:**

- *Allocation rule.* Any bid that is at least  $r$  is considered as a candidate. Randomly select  $k$  bids from the candidates to confirm.
- *Payment rule.* Each confirmed bid pays  $r$ .
- *Miner revenue rule.* Miner gets 0 revenue.

In the above mechanism, the miner gains zero revenue. This is inevitable as we show in our full version. Even in the MPC-assisted model, the miner must have zero revenue if we insist on strict incentive compatibility (even under Bayesian notions of equilibrium).

► **Theorem 5.1.** *Assuming a finite block size  $k$ . The above MPC-assisted, finite-block posted price auction in the MPC-assisted model satisfies UIC, MIC, and  $(\rho, 1)$ -SCP (in the ex post setting) for arbitrary  $\rho \in (0, 1]$ .*

**Proof.** We will prove the three incentive compatibility properties separately.

**UIC.** Let  $v_i$  denote the true value of user  $i$ . First, refusing to bid cannot increase its utility. Moreover, injecting bids does not help either. To see this, assume that user  $i$  bids its true value  $v_i$  and injects a bid  $b'$ . If  $b' < r$ , then it does not influence user  $i$ 's utility. If  $b' \geq r$ , it either decreases the probability of user  $i$  being confirmed if  $v_i \geq r$ , or it brings user  $i$  negative expected utility if  $v_i < r$ .

Thus, we only need to argue that overbidding or underbidding does not increase the user's utility. If user  $i$ 's true value  $v_i < r$ , then its utility when overbidding  $b \geq r$  is  $q \cdot (v_i - r) < 0$ , where  $q$  is the probability of  $b$  being confirmed. If user  $i$ 's true value  $v_i \geq r$ , then underbidding  $b < r$  brings it 0-utility, whereas the honest utility  $q(v_i - r)$  is positive. Therefore, no matter how user  $i$  deviates from the protocol, its utility does not increase.

**MIC.** Since the total miner revenue is always 0, injecting fake bids does not increase the colluding miner's utility. The miner cannot increase its utility by deviating from the protocol.

**SCP.** No matter how the coalition deviates, the colluding miner's revenue is always 0. Therefore, the joint utility of the coalition is at most the utility of the colluding user. By strict UIC, the joint utility does not increase. ◀

Note that the above mechanism does not work for  $c = 2$ . Imagine that the miner colludes with two users  $i$  and  $j$ , where user  $i$  has true value exactly  $r$  and user  $j$  has a sufficiently large true value. User  $i$  may choose not to bid to increase the probability of user  $j$  being confirmed. This brings the coalition strictly more utility than behaving honestly.

### 5.1.2 Impossibility for $c \geq 2$

Unfortunately, even in the MPC-assisted model, no mechanism with non-trivial utility can achieve UIC, MIC, and  $(\rho, 2)$ -SCP, even for Bayesian notions of incentive compatibility. To see this, observe that under the strict incentive compatible notion,  $(\rho, c)$ -SCP implies that any coalition of  $\leq c$  users cannot benefit from any deviation<sup>3</sup>, since the miner revenue has to be 0. Similar to the proof in Goldberg and Hartline [17], we show that any mechanism that

<sup>3</sup> We credit Bahrani, Garimidi, Roughgarden, Shi, and Weinberg for making this observation.

is Bayesian UIC and Bayesian SCP against a  $(\rho, 2)$ -sized coalition (for an arbitrary  $\rho \in (0, 1]$ ) must satisfy the following condition: no matter how a user  $j$  changes its bid, user  $i$ 's utility should not change, and thus derive the impossibility result. Formally,

► **Theorem 5.2.** *Suppose the block size is  $k$ . No MPC-assisted mechanism with non-trivial utility simultaneously achieves Bayesian UIC, Bayesian MIC and Bayesian SCP against  $(\rho, 2)$ -sized coalitions.*

The full proof is available in the full version.

## 5.2 Feasibility of Approximate Incentive Compatibility

Although strict (even Bayesian) incentive compatibility is impossible to achieve for  $c \geq 2$  in the MPC-assisted model, we have meaningful feasibility results if we allow  $\epsilon$  additive slack. Still, we use  $k$  to denote the finite block size and  $M$  to denote the upper bound of the true values. Specifically, we can achieve  $\Theta(kM)$  social welfare as long as many people place high enough bids, which is asymptotically the best possible social welfare one can hope for.

### MPC-assisted, Diluted Posted Price Auction

**Parameters:** the block size  $k$ , an upper bound  $c$  of the number of users colluding with the miner, an upper bound  $M$  of users' true values, a slack  $\epsilon \geq 0$ , and a posted-price  $r$  such that  $r \geq \frac{\epsilon}{2c}$ .

**Input:** a bid vector  $\mathbf{b} = (b_1, \dots, b_N)$ .

**Mechanism:**

1. *Allocation rule.*

- Given a bid vector  $\mathbf{b} = (b_1, \dots, b_N)$ , remove all bids which are smaller than  $r$ . Let  $\tilde{\mathbf{b}} = (\tilde{b}_1, \dots, \tilde{b}_\ell)$  denote the resulting vector.
- Let  $T = \max\left(2c\sqrt{\frac{kM}{\epsilon}}, k\right)$ . If  $\ell \geq T$ , let  $\mathbf{d} = \tilde{\mathbf{b}}$ . Else, let  $\mathbf{d} = (\tilde{b}_1, \dots, \tilde{b}_\ell, 0, \dots, 0)$  such that  $|\mathbf{d}| = T$ . In other words,  $\mathbf{d}$  is  $\tilde{\mathbf{b}}$  appended with  $T - \ell$  zeros.
- Randomly choose a set  $S$  of size  $k$  from  $\mathbf{d}$ , and every non-zero bid in  $S$  is confirmed.

2. *Payment rule.* For each confirmed bid  $b$ , it pays  $r$ .

3. *Miner revenue rule.* For each confirmed bid  $b$ , the miner is paid  $\frac{\epsilon}{2c}$ .

► **Theorem 5.3.** *Suppose there exists an upper bound  $M$  on users' true values. The above MPC-assisted, diluted posted price auction satisfies UIC, MIC, and  $\epsilon$ -SCP (in the ex post setting) against  $(\rho, c)$ -sized coalitions for arbitrary  $\rho \in (0, 1]$  and  $c \geq 1$ .*

The proof is available in the full version.

---

## References

- 1 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.
- 2 Gilad Asharov, Ran Canetti, and Carmit Hazay. Towards a game theoretic view of secure computation. In *Eurocrypt*, 2011.
- 3 Gilad Asharov and Yehuda Lindell. Utility dependence in correct and fair rational secret sharing. *Journal of Cryptology*, 24(1), 2011.
- 4 Soumya Basu, David A. Easley, Maureen O'Hara, and Emin Gün Sirer. Towards a functional fee market for cryptocurrencies. *CoRR*, abs/1901.06830, 2019. [arXiv:1901.06830](https://arxiv.org/abs/1901.06830).



- 5 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>.
- 6 Ran Canetti. Security and composition of multiparty cryptographic protocols. *Journal of Cryptology*, 2000.
- 7 Hao Chung and Elaine Shi. Foundations of transaction fee mechanism design. *arXiv preprint*, 2021. [arXiv:2111.03151](https://arxiv.org/abs/2111.03151).
- 8 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.
- 9 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.
- 10 Yevgeniy Dodis and Tal Rabin. Cryptography and game theory. In *AGT*, 2007.
- 11 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.
- 12 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. [arXiv:2103.14144](https://arxiv.org/abs/2103.14144).
- 13 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.
- 14 Juan Garay, Jonathan Katz, Björn Tackmann, and Vassilis Zikas. How fair is your protocol? a utility-based approach to protocol optimality. In *PODC*, 2015.
- 15 Juan A. Garay, Jonathan Katz, Ueli Maurer, Björn Tackmann, and Vassilis Zikas. Rational protocol design: Cryptography against incentive-driven adversaries. In *FOCS*, 2013.
- 16 Juan A. Garay, Björn Tackmann, and Vassilis Zikas. Fair distributed computation of reactive functions. In *DISC*, volume 9363, pages 497–512, 2015.
- 17 Andrew V. Goldberg and Jason D. Hartline. Collusion-resistant mechanisms for single-parameter agents. In *SODA 2005*, pages 620–629, 2005.
- 18 Ronen Gradwohl, Noam Livne, and Alon Rosen. Sequential rationality in cryptographic protocols. In *FOCS*, 2010.
- 19 Joseph Halpern and Vanessa Teague. Rational secret sharing and multiparty computation. In *STOC*, 2004.
- 20 Sergei Izmalkov, Silvio Micali, and Matt Lepinski. Rational secure computation and ideal mechanism design. In *FOCS*, 2005.
- 21 Jonathan Katz. Bridging game theory and cryptography: Recent results and future directions. In *TCC*, 2008.
- 22 Gillat Kol and Moni Naor. Cryptography and game theory: Designing protocols for exchanging information. In *TCC*, 2008.
- 23 Ilan Komargodski, Shin'ichiro Matsuo, Elaine Shi, and Ke Wu.  $\log^*$ -round game-theoretically-fair leader election. In *CRYPTO*, 2022.
- 24 Ron Lavi, Or Sattath, and Aviv Zohar. Redesigning bitcoin's fee market. In *The World Wide Web Conference, WWW 2019*, pages 2950–2956, 2019.
- 25 Roger B. Myerson. Optimal auction design. *Math. Oper. Res.*, 6(1), 1981.
- 26 Noam Nisan, Tim Roughgarden, Eva Tardos, and Vijay V. Vazirani. *Algorithmic Game Theory*. Cambridge University Press, USA, 2007.
- 27 Shien Jin Ong, David C. Parkes, Alon Rosen, and Salil P. Vadhan. Fairness with an honest minority and a rational majority. In *TCC*, 2009.
- 28 Rafael Pass and Elaine Shi. Fruitchains: A fair blockchain. In *PODC*, 2017.

## 97:22 What Can Cryptography Do for Decentralized Mechanism Design?

- 29 Tim Roughgarden. Transaction fee mechanism design for the Ethereum blockchain: An economic analysis of EIP-1559. Manuscript, <https://timroughgarden.org/papers/eip1559.pdf>, 2020.
- 30 Tim Roughgarden. Transaction fee mechanism design. In *EC*, 2021.
- 31 Ke Wu, Gilad Asharov, and Elaine Shi. A complete characterization of game-theoretically fair, multi-party coin toss. In *Eurocrypt*, 2022.
- 32 Andrew Chi-Chih Yao. An Incentive Analysis of Some Bitcoin Fee Designs (Invited Talk). In *ICALP 2020*, 2020. doi:10.4230/LIPIcs.ICALP.2020.1.