Beyond Incentive Compatibility: Rational Harm-Proof Transaction Fee Mechanisms*

Forest Zhang Elain Park Ke Wu

University of Michigan, Ann Arbor, MI, USA

{forestz,elainpk,kewucse}@umich.edu

Abstract

On a blockchain, users compete for scarce block space in an auction run by the miner to get their transactions confirmed in the block. This auction is called *transaction fee mechanism* (TFM). Recent work [Rou21, CS23, SCW23] has been focused on *incentive compatibility* (IC), requiring that honest behavior maximizes the payoff for each type of strategic player: users, the miner, or miner–user coalitions. In this work, we introduce *rational-harm proofness (RHP)*, which rules out deviations that harm honest parties without also reducing the deviator's own utility relative to the honest baseline. RHP closes a gap left by IC: IC does not forbid utility neutral yet externally harmful deviations. For example, in a second-price auction, the second-highest bidder can increase the winner's payment without affecting their own payoff. Such deviation is eliminated by RHP.

We characterize TFMs satisfying RHP alongside incentive compatibility for users (UIC) and miners (MIC). For finite block size, we develop a *complete characterization* in two models:

- In the *plain model*—where a single miner unilaterally implements the auction—we prove a *tetrilemma* (3-out-of-4 impossibility): among the four desired properties {positive miner revenue, UIC, MIC, RHP against miner–user coalitions}, no mechanism achieves all four simultaneously. This trade-off is tight: any three are jointly achievable in the plain model.
- In the *MPC-assisted model*—where a committee of miners jointly implement the auction via multi-party computation (MPC)—we construct a randomized TFM with a positive miner revenue that achieves UIC, MIC, and RHP against all three types of strategic players. We further show that randomness is necessary: any deterministic TFM satisfying UIC and RHP in this model must confirm no transactions when the number of users exceeds the block size.

Finally, we show that IC and RHP are *incomparable*: for each strategic role, there are mechanisms satisfying one but not the other in both models. Our results broaden the design objectives for TFMs: beyond incentive compatibility, mechanisms should also preclude costless harm to honest participants.

*Author order is randomized.

Contents

1 Introduction **3**
- 1.1 Our Results . . . 4
- 1.2 Design Implications and Rationale . . . 8
- 1.3 Additional Related Work . . . 10

2 Technical Overview **11**
- 2.1 Impossibility of UIC+MIC+CRHP in the Plain Model . . . 12
- 2.2 Impossibility under Weak-CRHP . . . 15
- 2.3 Feasibility in the MPC-Assisted Model . . . 17
- 2.4 Impossibility of UIC+URHP for Deterministic MPC-assisted TFMs . . . 18

3 Model and Preliminaries **18**
- 3.1 Notation . . . 18
- 3.2 Transaction Fee Mechanism . . . 18
- 3.3 Game Induced by TFM . . . 19
  - 3.3.1 TFM Game in the Plain Model. . . . 19
  - 3.3.2 MPC-Assisted Model . . . 20
- 3.4 Utility and Incentive Compatibility . . . 21
- 3.5 Myerson's Lemma . . . 22

4 Characterization in the Plain Model **23**
- 4.1 Feasibility Results . . . 23
- 4.2 Impossibilities in the Plain Model . . . 26
  - 4.2.1 Proof of the plain-model induction lemma . . . 30
- 4.3 Impossibility Under Weak-CRHP . . . 33

5 Characterizations in the MPC-Assisted Model **40**
- 5.1 Feasibility in the MPC-assisted Model . . . 40
- 5.2 Characterization of Deterministic Mechanisms . . . 43
  - 5.2.1 Deterministic Feasibility in the MPC-Assisted Model . . . 43
  - 5.2.2 Deterministic Impossibility in the MPC-Assisted Model . . . 44

6 IC and RHP are Incomparable **46**
- 6.1 Comparison in the Plain Model . . . 46
  - 6.1.1 UIC vs. URHP in the Plain Model . . . 46
  - 6.1.2 MIC vs. MRHP in the Plain Model . . . 47
  - 6.1.3 1-SCP vs. 1-CRHP in the Plain Model . . . 48
- 6.2 Comparison in the MPC-Assisted Model . . . 48
  - 6.2.1 UIC vs. URHP in the MPC-Assisted Model . . . 48
  - 6.2.2 MIC vs. MRHP in the MPC-Assisted Model . . . 48
  - 6.2.3 1-SCP vs. 1-CRHP in the MPC-Assisted Model . . . 50

References **51**

1 Introduction

Block space on a blockchain is a scarce resource, so users compete with each other to get their transactions confirmed in a block. This process can essentially be viewed as an auction where the block producer, also called the miner, sells the limited k number of block slots. Each user bids to get one slot for its transaction, and a *transaction fee mechanism* (TFM) decides which transactions are confirmed, how much each confirmd transaction pays, and how much revenue the miner receives.

Recent progress [LSZ19, Yao20, BEOS19, BCD+19, Rou21, FMPS21] observed that, due to the decentralized environment of blockchain, TFM design departs significantly from classical auction design. For example, classical auctions typically assume a trusted auctioneer and focus on the strategies of individual users. In contrast, on a blockchain, the auctioneer is a strategic miner who may deviate from the prescribed protocol to gain more revenue. Additionally, smart contracts make it easy for miners and users to enter binding side contracts and split their joint gains off-chain. A growing body of work therefore explores *incentive compatibility* (IC) properties of TFM so that the honest behavior is provably best for all participants. Ideally, a "dream" TFM should satisfy 1.) *user incentive compatibility* (UIC): bidding one's true valuation is optimal for each individual user; 2.) *miner incentive compatibility* (MIC): the miner is incentivized to execute the mechanism honestly; and 3.) *side-contract proofness* (SCP): no miner-user coalition can deviate to jointly profit.

However, incentive compatibility alone does not protect honest participants. There are deviations that leave a strategic player's utility unchanged compared to honest behavior, yet strictly harm others. Standard incentive compatibility notions do not rule out such utility-neutral but externally harmful actions. For example, the gold-standard second-price auction [Vic61] is known to be incentive compatible for individual users: the highest bidder wins and pays the second-highest price. However, the second-highest bidder can raise their bid slightly without changing their own utility (the bidder still loses and pays nothing) but increase the winner's payment. Such manipulations are costless for the deviator but impose real externalities on others.

Concern about such harm is well established in blockchain protocol design. For example, Herlihy's atomic-swap [Her18] formulation separately requires that coalition deviations not leave conforming parties worse off in addition to IC. Subsequent work [XH21] studies attacks that impose losses on honest participants in cross-chain transactions. More broadly, griefing-style attacks [But18], in which a participant can impose disproportionate harm on others at relatively low cost, have been studied in blockchain protocols including hashed timelock contracts [TYME21] and payment channels [AMSKM23]. These works motivate treating harm to other participants as a design concern separate from whether a deviation is profitable under the mechanism's modeled utility. In particular, when several strategies yield the same utility as honest behavior, protecting honest participants should not rely on the deviator choosing a benign strategy. This motivates us to ask

Can we design TFMs that achieve desired incentive compatibilities while also protecting honest participants from being harmed by rational deviations?

Related concepts have been studied in classical mechanism design under non-bossiness and robustness to secondary goals [SS81, Tho16, LSZ23, DPTM24, Car19, JM06, LRS21]. Thus, the underlying concern is not unique to TFMs. However, those notions apply to individual agents and do not capture the decentralized setting of TFMs with strategic miners and miner-user coalitions. In this work, we initiate a systematic study of the above question in the context of TFMs where the mechanism implementer is strategic and can collude with the users. We formalize the requirement that no strategic players (whether a user, miner, or miner-user coalition) can harm any honest participants unless they also harm the deviator themselves as a property called **rational-harm proofness**

(RHP). We then characterize when TFMs can achieve RHP alongside the standard incentive guarantees. For practical viability, we also target *positive miner revenue* so that participation is profitable for miners.

Our results apply to two settings: (1) the **plain model**, where a single miner unilaterally determines the block contents, capturing today's mainstream blockchain architecture; and (2) the **MPC-assisted model** [SCW23], where a committee of M miners jointly execute a cryptographic primitive, called the multi-party computation (MPC), to implement the TFM. We assume $M \geq 3$ in this model. The detailed results are summarized below.

1.1 Our Results

Model at a Glance. We begin with a high-level model of TFM to contextualize our results. Formal definitions appear in Section 3. We focus on a single block of finite size k. One can view the mechanism as selling k identical block slots. Each user i has a private true value v_i indicating the maximum they are willing to pay for a block slot. Users submit bids for inclusion, and a miner proposes a block of up to k bids. A TFM specifies, upon a received bid vector, 1.) up to k bids to include from the input bids; 2.) the set of confirmed bids and the payment charge to each confirmed bid; 3.) the miner's revenue. Once the set of up to k bids to include are fixed[1], the confirmation, payment, and miner revenue rules are honestly executed on-chain. Importantly, a TFM must work for *any* number of input bids due to the open and permissionless environment of blockchain. Moreover, on blockchain, not all payments need to go to the miner: some or even all payments can be *burned*.

In the *plain model*, a single miner unilaterally determines which bids to include. In the *MPC-assisted model*, a committee of M miners jointly execute the mechanism via an MPC, as if a trusted party were running the mechanism honestly on all bids delivered to the committee. We assume that less than half of the miners are corrupted, and the MPC provides guaranteed output delivery of the outcome prescribed by the protocol[2].

We require the mechanism to satisfy three basic properties: 1.) *Individual rationality*: no bid pays more than its value; 2.) *Budget feasibility*: the miner's revenue does not exceed the total payments paid by users, i.e., the mechanism does not create money.[3]; 3.) *Weak symmetry*: metadata such as the identity or timestamp of a bid is used only for tie-breaking; otherwise, outcomes depend only on bid values. For later reference, we note that all of our impossibility results hold assuming only weak symmetry, but our posted-price feasibility constructions are strongly symmetric, meaning that all bids with the same value have identical outcome distributions, without a tie-breaking based on metadata.

Strategy Space. We focus on direct-revelation mechanisms, in which honest users submit a single bid equal to their true values. An honest miner includes up to k bids as prescribed in the mechanism, without censoring honest bids or injecting fake ones.

Strategic players may deviate to increase their utility. We consider three types of strategic players: 1.) A single user. A strategic user can bid an arbitrary value for its transaction, refuse to bid, and/or inject any number of *fake bids* since pseudonyms are easy to register on-chain. 2.) Strategic miner(s). In the plain model, the single miner can inject fake bids, drop honest users'

[1]There is a subtle distinction between a bid being included in a block versus being confirmed. A bid must be included to have a chance of confirmation, but depending on the mechanism, not all included bids are necessarily confirmed; see Section 3 for detailed explanation.

[2]When instantiating with real-world cryptography, there is a negligible probability of breaking cryptography, but our results are stated in the ideal world assuming an ideal functionality.

[3]The miner gets a fixed block reward independent from the transaction fees, so we do not model the block reward.

bids, and select any set of up to k bids for the block. In the MPC-assisted model, a coalition of $m < M/2$ miners can inject fake bids, but they cannot selectively censor honest users' bids or change the outcome, and the MPC provides guaranteed output delivery. 3.) A miner-user coalition, containing the miner and some users in the plain model, or $m < M/2$ miners together with some users. A coalition's strategy is a combination of its members' strategies.

Utility. A user with true value v for a transaction gets utility $v-p$ if that transaction is confirmed and pays p, and 0 if not confirmed. A miner's utility is its revenue minus any cost it pays for its own fake bids. A coalition's utility is the sum of its members' utilities.

Conceptual Contribution: Defining RHP Our first contribution is conceptual: we elevate the principle of "no costless harm" to a first-class requirement for TFM design. As illustrated by the earlier second-price auction example, a user may raise the winner's payment and thereby reduce a rival's utility without affecting its own payoff.

We formalize *rational-harm proofness (RHP)* as the requirement that rational players cannot make any honest participant strictly worse off unless the deviators also make themselves worse off, compared to the honest behavior. We define RHP as a property of the mechanism and take the honest profile as its baseline rather than tying the notion to equilibrium outcomes of the induced TFM game. An equilibrium-based formulation would depend on equilibrium existence and selection choices, whereas our goal is a notion that is well-defined for *every* TFM instance independently of such choices.

We adopt *ex-post* notions because they capture the *public-mempool* reality of many blockchains: bids are broadcast and observable by strategic participants, in particular by the miner before deciding what to include, and often by other users who can react via last move. Ex-post definitions ensure robustness in such environments where a strategic players can make their decisions based on the honest users' bids, rather than relying on bid secrecy.

Formally, for any strategic player $\mathcal{C}$, whether an individual user, miner, or miner-user coalition, let $H_{\mathcal{C}}$ denote $\mathcal{C}$'s honest strategy. For any true value profile $\mathbf{v} = (v_1, ..., v_n)$ of all the users, let $\mathsf{util}_i(\mathbf{v}; S_{\mathcal{C}})$ and $\mathsf{util}_{\mathcal{C}}(\mathbf{v}; S_{\mathcal{C}})$ denote the expected utility of a player i and the coalition $\mathcal{C}$, respectively, in the randomized experiment where players in $\mathcal{C}$ adopts some (possibly randomized) strategy $S_{\mathcal{C}}$ and players outside $\mathcal{C}$ behaves honestly.

Definition 1.1 (Rational-harm proofness)**.** Fix a coalition of strategic players $\mathcal{C}$ and a protected set of honest players $\mathcal{H}$ such that $\mathcal{C} \cap \mathcal{H} = \emptyset$. We say that a TFM satisfies rational-harm proofness (RHP) against $\mathcal{C}$ for protecting $\mathcal{H}$ if, for any true value vector $\mathbf{v}$ of users and any strategy $S_{\mathcal{C}}$ for coalition $\mathcal{C}$ such that

$$\mathsf{util}_{\mathcal{C}}(\mathbf{v}; S_{\mathcal{C}}) \geq \mathsf{util}_{\mathcal{C}}(\mathbf{v}; H_{\mathcal{C}}),$$

it holds that

$$\mathsf{util}_i(\mathbf{v}; S_{\mathcal{C}}) \geq \mathsf{util}_i(\mathbf{v}; H_{\mathcal{C}})$$

for every protected honest player $i \in \mathcal{H}$. Here util_a and $\mathsf{util}_{\mathcal{C}}$ denote expected utilities in the randomized experiment where the users' true value vector is $\mathbf{v}$, players in $\mathcal{C}$ adopt $S_{\mathcal{C}}$, players outside $\mathcal{C}$ behave honestly, and $H_{\mathcal{C}}$ denotes the honest strategy of coalition $\mathcal{C}$.

To help understand RHP, let us take the first-price auction in the plain model as an example. Here, the k highest bidder gets confirmed and pays their own bid. Under honest behavior, every confirmed user bids its true value and therefore obtains utility zero, while every unconfirmed user also obtains utility zero. Thus, first-price auction satisfies RHP in the sense that no user can be harmed compared to honest case. Intuitively, although strategic players may change the allocation or payments, they cannot make an honest user worse off than its zero-utility honest baseline.

This example also illustrates what RHP does *not* guarantee. The first-price auction is not UIC: a winning user may lower its bid to make it barely enough to be the top k bids. This strictly increases its utility. Thus, RHP protects honest participants relative to the prescribed honest baseline, but does not by itself ensure that the honest baselline is incentive compatible. Conversely, as illustrated by the earlier second-price example, IC does not prevent utility-neutral deviations that harm others.

The first-price and second-price examples together demonstrate necessity of requiring both RHP and IC: They are complementary requirements. IC makes the prescribed honest behavior optimal for the strategic player, while RHP protects honest participants against the external effects of rational deviations.

RHP for different strategic roles. TFMs have three natural classes of strategic players already reflected in the IC notions defined in prior works: an individual user, the miner, and a miner-user coalition. We take the same distinction for RHP and instantiate Definition 1.1 for these three strategic roles. These are not separate underlying notions, but three instantiations of the same RHP definition with different deviating strategy spaces and protected participants. Distinguishing them lets us separate precisely which sources of rational harm a mechanism protects against, and whether these protections can be achieved simultaneously:

- *User rational-harm proofness (URHP)* iff Definition 1.1 holds for any $\mathcal{C} = \{i\}$ containing an individual user i and $\mathcal{H}$ contains all users except i. URHP protects honest users from an individual deviating user.
- *Miner rational-harm proofness (MRHP)* iff Definition 1.1 holds for the single miner in the plain model, with $\mathcal{H}$ equal to all users, and for any nonempty coalition of $m < M/2$ miners in the MPC-assisted model, with $\mathcal{H}$ equal to all users and all miners outside the coalition.
- *d-coalition rational-harm proofness (d-CRHP)* iff Definition 1.1 holds for coalitions containing the miner and at least one but at most d users in the plain model, or a nonempty coalition of $m < M/2$ miners and at least one but at most d users in the MPC-assisted model, protecting all players outside the coalition.

Our URHP notion focuses only on protecting honest users from rival-user: we do not require an individual user deviation to preserve miner revenue. A user may reduce miner revenue simply by choosing not to participate, which we view as ordinary demand response rather than harm to be protected against. In contrast, MRHP and CRHP concern deviations involving miners and therefore also protect non-colluding honest miners in the MPC-assisted model.

Our design target. Ideally, a TFM would satisfy all of the standard incentive guarantees (UIC, MIC, and SCP) together with all RHP guarantees (URHP, MRHP, CRHP), as well as positive miner revenue. However, for finite block size, prior work [CS23, SCW23] implies that UIC and d-SCP, for $d \geq 2$, can coexist in either model only if every user and miner has zero expected utility under honest behavior on every valuation profile. Since UIC is tightly coupled to user experience, we therefore prioritize UIC and aim to achieve UIC, MIC, all three RHP guarantees, and positive miner revenue.

In this case, UIC and MIC ensures that the honest protocol forms an equilibrium, and RHP then provides protections of honest participants compared to this honest baseline. Now CRHP becomes especially useful when SCP is impossible: Even when we cannot prevent a coalition from benefiting, CRHP ensures that the coalition not obtain such a benefit at the expense of honest participants.

This full collection of desired properties—**UIC, MIC, URHP, MRHP, CRHP, and positive miner revenue**—is our common design target in both the plain model and the MPC-assisted model. Our impossibility results are stated under smaller subsets of these properties because they identify stronger obstructions. We state only the assumptions needed for each impossibility.

We also define a weaker notion called *weak RHP*, which only requires that any *strictly profitable* deviation for $\mathcal{C}$ does not harm honest participants. This is weaker than RHP and weaker than IC, since IC rule out the existence of any strictly profitable deviations.

Landscape in the Plain Model. We first consider the plain model, where a single miner determines which bids to include. This setting reflects the architecture of most mainstream blockchains. The game proceeds as follows: honest users submit their bids truthfully; any strategic players then choose their strategies after observing the honest bids; the miner selects up to k bids for the block. The blockchain protocol then honestly confirms some of these bids and determines payments and miner revenue according to the mechanism's rules.

Unfortunately, it is impossible to achieve all desired properties in the plain model. In fact, the impossibility already follows from only four of them: UIC, MIC, 1-CRHP, and positive miner revenue. Any TFM satisfying all four must be *degenerate*, meaning that it confirms bids only when there are no more than k bids. Formally,

Theorem 1.2 (Impossibility in the plain model)**.** *Let k be the finite block size. In the plain model, any UIC, MIC, and 1-CRHP TFM must be degenerate: it confirms no bids when there are more than k bids. Moreover, miner revenue must always be zero.*

In fact, even if we relax 1-CRHP to weak 1-CRHP, the miner revenue still must always be zero.

Theorem 1.3 (Impossibility under weak-CRHP)**.** *The miner revenue in any UIC, MIC, and weak 1-CRHP TFM in the plain model must always be zero.*

Corollary 1.4. *Only trivial TFMs, where no bids are ever confirmed, satisfy UIC, MIC, MRHP, and (weak) 1-CRHP in the plain model.*

On the other hand, Theorem 1.2 is tight: any three of the four desired properties can be achieved simultaneously. We present these witness mechanisms in Section 4.1.

Theorem 1.5. *Any three of the four properties of UIC, MIC, 1-CRHP, and positive miner revenue can simultaneously be achieved.*

Landscape in the MPC-assisted Model. In the MPC-assisted model, M miners jointly execute the TFM and share the total revenue. Strategic miners can still inject fake bids, but the MPC prevents them from altering the computed outcome once all bids are submitted. It is convenient to think of an ideal functionality $\mathcal{F}$ that honestly implements the mechanism as follows:

Fix an arbitrary strategic player $\mathcal{C}$, which in the MPC-assisted model could be an individual user, a coalition of $m < M/2$ miners, or a miner-user coalition of $m < M/2$ miners and some users. Honest users submit their bids to $\mathcal{F}$. After seeing these honest bids, the strategic coalition $\mathcal{C}$ decides what bids to submit. Then $\mathcal{F}$ computes the TFM outcome (which bids are confirmed, payments, miner revenue) based on all submitted bids and sends the outcome to all players. This ideal functionality can be instantiated by real-world protocols [GMW87, Can01] with guaranteed output delivery when $m < M/2$ miners are colluding.

In the MPC-assisted model, we can simultaneously achieve all the desire properties, UIC, MIC, all three RHP variants, as well as positive miner revenue.

Mechanism 1.6 (Posted-price with random selection)**.** *Let* $\mathsf{res} > 0$ *be the reserve and* $0 < \epsilon \leq \mathsf{res}$ *be the revenue parameter. Let* E *be the set of bids at least* res*. Randomly choose* $\min\{k, |E|\}$ *bids from* E *to include and confirm. Each confirmed bid pays the reserve price* res*. The miner gets total revenue* ϵ *if at least one bid is confirmed, and zero otherwise.*

Theorem 1.7 (Feasibility in the MPC-assisted model)**.** *Mechanism 1.6 (posted-price with random selection) achieves UIC, MIC, URHP, MRHP, d-CRHP for any* $d \leq k$*, and positive miner revenue in the MPC-assisted model.*

We stress that practical realization of Mechanism 1.6 remains simple. It requires a censorship resistance inclusion list and an independent non-biasable randomness beacon. We discuss this further in Section 1.2.

A natural question is whether the use of randomness is necessary for the above result. Can we achieve all properties with a deterministic mechanism? Interestingly, there is a deterministic degenerated mechanism that achieves all properties in the MPC-assisted model. In fact, this is unavoidable for any deterministic mechanism:

Theorem 1.8 (Characterization of deterministic mechanism in the MPC-assisted model)**.** *Let* k *denote the block size. Any deterministic UIC and URHP TFM in the MPC-assisted model must be degenerate: no bid can be confirmed whenever the number of bids exceeds* k*.*

IC and RHP are Incomparable. The previous first-price and second-price examples already show that UIC and URHP are incomparable. More generally, this incomparability holds for each of the three strategic roles:

Theorem 1.9 (IC and RHP are incomparable)**.** *In both the plain and the MPC-assisted model, IC and RHP are incomparable. For each strategic role* X *(user, miner, or miner–user coalition), there exist mechanisms that are* X*-IC but not* X*-RHP, and vice versa.*

The mechanisms demonstrating this incomparability are given in Section 6, where we summarize the results in Table 1 for the plain model and Table 2 for the MPC-assisted model.

Organization. We give an overview of the techniques used in our impossibility results in Section 2. The detailed model and preliminaries are given in Section 3. Characterizations in the plain model and the MPC-assisted model are given in Section 4 and Section 5, respectively. We present the comparison between IC and RHP in Section 6. Our design rationale and additional related work appear in Sections 1.2 and 1.3.

1.2 Design Implications and Rationale

Implications for protocol design. Our results identify a concrete design tradeoffs for TFMs. In today's mainstream plain model, if congestion can occur (i.e., the number of pending transactions exceed the block capacity k), then no mechanism can simultaneously satisfy all four desiderata—UIC, MIC, CRHP, and positive miner revenue. Thus, designers must either provision the system so that the capacity constraint is effectively non-binding (e.g., operating in an "always non-congested" regime), or accept an explicit compromise among these properties during congestion.

Technically, the main driving force behind our plain-model impossibilities is the miner's ability to *censor* honest bids without reducing its own payoff. This reveals a practical route around the

barrier in the MPC-assisted model. Because bids are public, realizing Mechanism 1.6 does not require private computation. Under the honest-majority assumption, it suffices to have 1.) a censorship-resistant inclusion mechanism that establishes the set of submitted bids, and 2.) an independent non-biasable randomness beacon sampled after the submitted bids are fixed. Once the bid set and randomness are fixed, the prescribed random selection is publicly computable and verifiable, while the honest-majority committee ensures that the resulting outcome is executed and delivered. Thus, the mechanism remains lightweight and does not inherently require a generic MPC implementation. Committee-based inclusion proposals such as FOCIL [TDM+24] and public-verfiable randomness [Eth26] already provide natural building blocks toward such a realization.

Prioritize UIC over coalition-IC. For finite block size, prior work [CS23, SCW23] implies that UIC and d-SCP (incentive compatibility against miner-user coalitions with up to d users), for $d \geq 2$, can coexist in either the plain or the MPC-assisted model only if every user and miner has zero expected utility under honest behavior on every valuation profile. Moreover, other collusion-resistance goals such as *off-chain agreement proofness* (OCA-proofness [Rou21]) remain impossible with UIC and MIC during congestion [CRS24]. Given this tension between UIC and coalition resistance, we prioritize UIC and ask what protection can still be provided against miner–user coalitions. From a practical perspective, UIC avoids the bid guessing in mechanisms like first-price auctions, which leads to poor user experience [Lop17]; Ethereum's move to the posted-price structure in EIP-1559 was motivated in part by simplifying fee estimation for users [BCD+19]. CRHP provides a complementary residual guarantee: even if a miner–user coalition can profit from deviating, it cannot obtain this benefit at the expense of protected honest participants.

Comparing CRHP with other coalition-resistant notions. In addition to SCP and OCA-proofness, a broad TFM literature studies alternative notions of coalition-resistance and their compatibility with UIC. As we already shown in Theorem 1.9, CRHP is incomparable to SCP. OCA-proofness is primarily concerned with preventing the miner and *all* users from "stealing from the protocol", but it does not in general rule out deviations by a miner colluding with a subset of users that harm non-colluding users. To capture such off-chain coordination more directly, [GTW25, GTW24] study *off-chain influence-proofness* (OffC-IP), which rules out deviations where the miner shifts price discovery or bidding off-chain to extract additional profit via influence/threat channels. A different weakening is *(IC+IR)-collusion resilience* [FGR24], which restricts attention to off-chain agreements implementable by side mechanisms that remain incentive-compatible and individually rational for the colluding players. In contrast to these notions, CRHP approaches coalition-resistance from a different angle: it does not attempt to preclude profitable collusion, but rather, rules out coalitions imposing *costless harm* on non-colluding users.

Scope of the posted-price with random selection. Mechanism 1.6 satisfies UIC, MIC, and all variants of RHP while achieving positive revenue in the MPC-assisted model, but it does *not* satisfy SCP. To see this, suppose no honest user has value at least res, and consider a coalition containing $m < M/2$ miners and one user with value $v \in (\mathsf{res} - m\epsilon/M, \mathsf{res})$.

Under honest behavior, no bid is eligible, so no transaction is confirmed and the coalition obtains utility zero. If the colluding user instead bids res, its transaction is confirmed and pays res, while the colluding miners receive a total revenue share of $m\epsilon/M$. The coalition's utility becomes $v - \mathsf{res} + \frac{m\epsilon}{M} > 0$. Thus, the deviation is strictly profitable and the mechanism is not SCP.

Importantly, this deviation does not harm any protected participant: all honest users remain unconfirmed with utility zero, while miners outside the coalition gain positive revenue. This illustrates the distinction between SCP and CRHP. CRHP does not rule out every profitable coalition deviation; rather, it ensures that a rational coalition cannot profit at the expense of protected honest participants.

1.3 Additional Related Work

Transaction fee mechanisms. There is a rich line of literature of TFM focusing on different models considered in this work. In response to the UIC + SCP impossibility results, [WSC24, GTW25, CSLZZ25] relax ex-post incentive compatibilities and instead study Bayesian notions of incentive compatibility.

Conversely, [SCW23] studies approximate-IC as another way to circumvent impossibility results for exact incentive compatibility. Approximate IC and RHP constrain different aspects of deviations. An ϵ-IC guarantees that strategic players gain at most ϵ more utility compared to honest behavior by deviating. But approximate-IC does not bound the harm that such a deviation may impose on honest participants. RHP instead constrains this external harm whenever the deviation is rational, while allowing the deviator's utility gain itself to be arbitrarily large as long as protected participants are not harmed. Thus, neither notion substitutes for the other.

Prior work also shows limitations of approximate IC under finite block size. In the plain model, [SCW23] proves a scalability barrier for mechanisms satisfying ϵ-UIC, ϵ-MIC, and ϵ-SCP. In the MPC-assisted model, the diluted posted-price mechanism of [SCW23] satisfies exact UIC and MIC together with ϵ-SCP. It pads the candidate pool with dummy bids before random selection and may therefore leave block capacity unused even when at least k eligible real bids are present. Our randomized posted-price mechanism also achieves exact UIC and MIC, but provides d-CRHP for $1 \leq d \leq k$ as its coalition-side guarantee. It confirms exactly $\min\{k, \ell\}$ eligible submitted bids when there are ℓ such bids, without padding the candidate pool.

Randomness in the plain model. Our plain model follows the strategy space of [CS23, CRS24]: a strategic miner controls which bids enter the block and may choose arbitrary randomness and deviate from any prescribed randomized inclusion rule. A public randomness beacon alone does not enforce that the miner applies the prescribed random selection to the intended set of candidate bids. An alternative model, as in [GY24], allows the miner to omit bids and inject fake bids but evaluates deviations under the prescribed randomized allocation rule on the resulting bid vector. Unlike our plain model, it does not give the miner direct control over the realized allocation randomness. Characterizing RHP under this alternative strategy space is an interesting direction for future work.

TFM for other consensus. Many papers also study TFM for other types of consensus protocols. [GHR25] and [SMT25] consider blockchain models in which multiple block producers participate in block construction such as DAG-based consensus (see survey [RPM24]) and FOCIL [TDM+24]. Another line of work extends the classical single-resource TFM model to settings in which transactions consume multiple scarce blockchain resources. In these multidimensional fee markets, distinct resources (e.g., computation, data availability, or storage) are priced separately, and transactions may require varying quantities of each. [DECA23] proposes formal multidimensional fee mechanisms, while [ADM24, LNPR25] analyze their efficiency and optimality properties. Empirical analyses of Ethereum's EIP-4844 (blob) fee market appear in [HM25].

Robustness to secondary goals, non-bossiness, and bounded maximin fairness. There is a rich literature on making mechanisms robust to *secondary goals* beyond direct payoff [Car19, JM06, LRS21, LSZ23]. For example, [JM06] studies auctions with externalities where bidders' utilities depend on others' allocations or information, and recent work formalizes robustness to hidden secondary goals via non-bossy mechanisms [LSZ23]. We refer the reader to Carroll's survey [Car19].

RHP is also related to the classical notion of *non-bossiness* [SS81, Tho16, DPTM24], which restricts an agent from changing others' outcomes without changing its own. Most formulations focus on allocations, while TFMs involve both allocation and payments. Utility-based variants have also been studied [Kla01, SSY07, Rit83, LSZ23], but they typically concern individual agents, restrict

deviations that leave the deviator's own outcome unchanged, and do not distinguish whether the induced change to others is harmful or beneficial. In contrast, RHP operates directly on utility, applies to both individual and coalitional deviations, and specifically protects honest participants against harmful deviations that are no worse for the deviator.

Recently, [CMST25] introduced the notion of *bounded-maximin fairness* in the context of atomic swaps. This notion ensures honest parties have non-negative utility from any polynomial-time profitable strategy performed by any coalition with arbitrary, but bounded external incentives, such as locked collateral, outside the mechanism's allocations. In contrast, our notion uses the honest outcome as a baseline for honest parties and does not depend on external incentives.

Griefing and griefing factors. RHP is closely related to the blockchain literature on *griefing*, where a participant takes an action that harms other participants even when doing so may also impose a cost on the attacker. Buterin introduced *griefing factors* as a way to quantify the harm inflicted on others relative to the attacker's own loss [But17,But18]. This perspective has subsequently been studied in blockchain settings including mining games [LSCP23], payment channels [MBS+23], and cross-chain transactions [XH21]; see also the broader analysis in [Geo23].

RHP addresses a complementary boundary of this concern. Griefing-factor analyses ask how much harm can be imposed relative to the attacker's cost, including attacks for which the attacker is willing to incur a positive utility loss. RHP does not rule out all such costly griefing attacks. Instead, it requires that whenever a deviation is no worse for the deviator according to the modeled utility, including both utility-neutral and strictly profitable deviations, the deviation cannot make a protected honest participant worse off. Thus, RHP focuses on the particularly conservative case in which harming others requires no sacrifice in the deviator's modeled utility.

Miner deviations and credible auctions. Akbarpour and Li [AL20] introduce *credible auctions*, requiring that the auctioneer (miner) has no incentive to *safely* deviate from the prescribed mechanism, where a deviation is *safe* if it admits a plausible explanation to all users. Credibility is related to, but distinct from, MIC. As shown in [CS23], a TFM can be MIC yet fail credibility. Moreover, [AL20] proves a trilemma: a revenue-optimal auction cannot be simultaneously *credible*, *strategy-proof*, and *static*. By comparison, our impossibility results target a different scope: we do not impose revenue optimality as an objective. Subsequent work [FW20, EFW22] demonstrates that cryptographic techniques can circumvent the trilemma impossibility, but these constructions do not ensure harm-prevention as provided by RHP or explicitly address the miner-user coalition in TFMs.

2 Technical Overview

This section highlights the core ideas behind our results. The main technical challenge in analyzing RHP is that we must track not only how a deviation changes the deviator's own utility, but also its effect on every honest participant's utility. This is different from the analysis of incentive compatibility, which considers only the deviator's payoff. We outline below the key idea under our impossibility theorems and main feasibility in the MPC-assisted model.

Notation. For a bid vector $\mathbf{b} = (b_1, ..., b_n)$, we use $\max(\mathbf{b})$ to denote $\max_{i\in[n]}(b_i)$. We use $\mathbf{b}_{-i}$ to denote $(b_1, \ldots, b_{i-1}, b_{i+1} \ldots, b_n)$, and we use $(\mathbf{b}_{-i}, b_i)$ and $\mathbf{b}$ interchangeably. For any $i \in [n]$, we use $x_i(\mathbf{b})$, $p_i(\mathbf{b})$, and $\mathsf{util}_i(\mathbf{b})$ to denote the confirmation probability, expected payment, and expected utility, respectively, of user i's true value b_i, when everyone behaves honestly with an input bid vector $\mathbf{b}$. We use $\mu(\mathbf{b})$ to denote the expected miner revenue in the honest case.

We focus on bids with *unique* values since we only require weak symmetry for the mechanisms for the impossibility. We call a bid b_i *unique in* $\mathbf{b}$ if $b_j \neq b_i$ for all $j \neq i$. For a bid vector $\mathbf{b}$ and

a unique value z in $\mathbf{b}$, let $\mathrm{idx}_{\mathbf{b}}(z)$ be the index i such that $b_i = z$. We write $\widetilde{x}_z(\mathbf{b}) := x_{\mathrm{idx}_{\mathbf{b}}(z)}(\mathbf{b})$, $\widetilde{p}_z(\mathbf{b}) := p_{\mathrm{idx}_{\mathbf{b}}(z)}(\mathbf{b})$, and $\widetilde{\mathsf{util}}_z(\mathbf{b}) := \mathsf{util}_{\mathrm{idx}_{\mathbf{b}}(z)}(\mathbf{b})$. These value-indexed quantities are used only when z is unique in $\mathbf{b}$. For two sets S and T, we use $S \prec T$ to show that $\sup S < \inf T$.

2.1 Impossibility of UIC+MIC+CRHP in the Plain Model

We start by sketching the proof of Theorem 1.2 that any TFM satisfying UIC, MIC, and 1-CRHP in the plain model cannot confirm any bids when the input bid vector $|\mathbf{b}| > k$. We first explain the proof for deterministic TFMs to illustrate the main idea, and then discuss how to generalize it to randomized TFMs.

Impossibility for Deterministic TFM. The proof uses an induction on a carefully constructed sequence of bid vectors. We use a simple *toy example* to illustrate the key idea behind this sequence.

Toy Example: Consider a 1-CRHP TFM. Consider two users with true values $\mathbf{b} = (b_1, b_2)$. We assume that $b_1 < b_2$, making them unique in $\mathbf{b}$. Furthermore, to isolate the core idea behind the proofs, we assume that in the honest execution user 2's bid is confirmed ($x_2(\mathbf{b}) = 1$) and pays $p_2(\mathbf{b}) < b_1$, so user 2 gets a positive utility. Under these conditions, user 1 must also be confirmed in the honest execution. If not, consider a coalition of the miner and user 1. In the honest outcome, their joint utility is just the miner's revenue $\mu(\mathbf{b})$. Now the coalition performs this **censor-then-replace** attack: the miner ignores user 2's bid b_2, and user 1 changes its own bid to b_2 while also injecting a fake bid of value b_1. The resulting bid vector is still $\mathbf{b}$ but now both b_1 and b_2 come from user 1. By weak symmetry, the bid of value b_2 (now coming from user 1) would still be confirmed and charged $p_2(\mathbf{b})$, while the bid of value b_1 is not confirmed. Under this strategy, the coalition's joint utility strictly increases: the miner's revenue is unchanged, and user 1 now gets utility $b_1 - p_2(\mathbf{b}) > 0$, while the honest user 2 is harmed. This contradicts 1-CRHP. Thus b_1 must be confirmed in the honest execution.

The above toy example can be generalized to a useful "above-payment-guarantee" lemma: *In an honest execution of a (weak) 1-CRHP TFM, if some unique bid b_i earns positive utility, then* any *unique bid in b that is higher than $p_i(\mathbf{b})$ must also be confirmed.* Intuitively, if a higher bid is not confirmed, then it can collude with the miner and perform the censor-then-replace attack on b_i, which contradicts 1-CRHP. Here, we require uniqueness of the bid to get rid of the potential tie breaking that can depend on the metadata.

Induction. Next, we show how to prove Theorem 1.2 for deterministic TFM. Assume for sake of contradiction that there exists a deterministic TFM satisfying UIC, MIC, and 1-CRHP in which some bid v_{i^*} is confirmed when the input bid vector is $\mathbf{v}$ with $|\mathbf{v}| > k$. We will construct a sequence of bid vectors $\mathbf{v}^{(m)}$ for $m = 1, 2, ...$, and prove by induction that m bids must be confirmed in $\mathbf{v}^{(m)}$. This directly contradicts the block size k when $m = k + 1$. The sequence is constructed as follows:

$$b_1 = \max(\mathbf{v}) + 1, \qquad \mathbf{v}^{(1)} = (\mathbf{v}_{-i^*}, b_1),$$
$$b_m = \frac{1}{2}(\max(\mathbf{v}) + b_{m-1}), \qquad \mathbf{v}^{(m)} = \left(\mathbf{v}^{(m-1)}, b_m\right) \quad \text{for } m > 1.$$

The inductive invariant states that

$$b_m \text{ must be confirmed in } \mathbf{v}^{(m)} \text{ and its payment } \widetilde{p}_{b_m}(\mathbf{v}^{(m)}) \le \max(\mathbf{v}).$$

Effectively, in each step, we add a bid b_m that lies between the payment $\widetilde{p}_{b_{m-1}}\left(\mathbf{v}^{(m-1)}\right) \le \max(\mathbf{v})$ and b_{m-1} to $\mathbf{v}^{(m-1)}$. By the inductive statement, b_m gets a positive utility in $\mathbf{v}^{(m)}$, and all b_z for $z \in [m]$ is higher than b_m's payment. Thus, by the above-payment-guarantee lemma, all b_z for $z \in [m]$ must be confirmed.

The induction proof uses Myerson's lemma (Lemma 3.5). Roughly speaking, for a deterministic UIC TFM, for any fixed other users' bids $\mathbf{b}_{-i}$, there exists a critical value v^* such that any $b_i > v^*$ gets confirmed and pays v^*, i.e., $x_i(b_i, \mathbf{b}_{-i}) = 1$ and $p_i(b_i, \mathbf{b}_{-i}) = v^*$ for any $b_i > v^*$.

Base case: The base case follows directly from UIC and the Myerson's lemma: Raising user i^*'s bid in $\mathbf{v}$ to $\max(\mathbf{v}) + 1$ must maintain its confirmation probability and payment. Thus, $\widetilde{x}_{b_1}(\mathbf{v}^{(1)}) = 1$ and $\widetilde{p}_{b_1}(\mathbf{v}^{(1)}) = p_{i^*}(\mathbf{v}) \le \max(\mathbf{v})$ where the inequality follows from individual rationality.

Inductive step: Now assume we have $\mathbf{v}^{(m-1)}$ where b_{m-1} is confirmed and pays no more than $\max(\mathbf{v})$. By Myerson's Lemma, it suffices to show that for any b such that $\max(\mathbf{v}) < b < b_{m-1}$, bid b must be confirmed in $(\mathbf{v}^{(m-1)}, b)$. This implies that $\widetilde{x}_{b_m}(\mathbf{v}^{(m)}) = 1$ and $\widetilde{p}_{b_m}(\mathbf{v}^{(m)}) \le \max(\mathbf{v})$.

For the sake of contradiction, assume that there exists some $\max(\mathbf{v}) < b^* < b_{m-1}$ such that b^* is not confirmed in $(\mathbf{v}^{(m-1)}, b^*)$. Imagine a world where $\mathbf{v}^{(m-1)}$ is the honest bid vector. Since $|\mathbf{v}^{(m-1)}| \ge |\mathbf{v}| > k$, some user j must be unconfirmed in the honest case. Consider a coalition consisting of the miner and user j who injects a fake bid b^*. Since b^* is unconfirmed, the miner revenue must remain unchanged by MIC: $\mu(\mathbf{v}^{(m-1)}) = \mu(\mathbf{v}^{(m-1)}, b^*)$. Therefore, this strategy does not decrease the coalition's utility compared to the honest case, since user j's original bid still gives nonnegative utility by individual rationality.[4] That said, by 1-CRHP, this strategy should harm no honest bid in $\mathbf{v}^{(m-1)}$, including b_{m-1}. Therefore, b_{m-1} should still get a positive utility in $(\mathbf{v}^{(m-1)}, b^*)$ and pays no more than $\max(\mathbf{v})$. However, by the above-payment-guarantee, since b^* is greater that the payment of b_{m-1} in $(\mathbf{v}^{(m-1)}, b^*)$, we know that b^* must be confirmed, which contradicts our assumption. This completes the induction proof.

Generalizing to Randomized TFMs. The above proof idea needs significant adaptation for randomized mechanisms. If the TFM uses randomness, then having more than k bids, each with a positive *confirmation probability* is no longer an immediate contradiction. In a randomized TFM, different random outcomes might confirm different sets of at most k bids. Therefore, we derive a stronger condition called the *k-winners lemma*: If a TFM is MIC and (weak) 1-CRHP, then it must be that

$$|W(\mathbf{b})| \le k, \text{ where } W(\mathbf{b}) := \{i \colon \mathsf{util}_i(\mathbf{b}) > 0\}. \tag{1}$$

Here, $W(\mathbf{b})$ denotes the set of *winners* who have positive expected utility in the honest case when the input bid vector is $\mathbf{b}$. Note that positive *utility* is a strictly stronger requirement than positive *confirmation probability*. We prove this lemma formally in Section 4.2. For the overview, we assume it is true and show how to prove Theorem 1.2.

For possibly randomized TFMs, the "above-payment-guarantee" can be generalized to "above-ratio-guarantee": *In a 1-CRHP TFM , if a unique bid b_i has positive expected utility in $\mathbf{b}$, then any unique bid in $\mathbf{b}$ above the ratio $p_i(\mathbf{b})/x_i(\mathbf{b})$ must have a positive confirmation probability.* In the deterministic case, this ratio $p_i(\mathbf{b})/x_i(\mathbf{b})$ is simply the payment itself. We define, for any bid b_i such that $x_i(\mathbf{b}) > 0$, the *ratio* as

$$r_i(\mathbf{b}) := p_i(\mathbf{b})/x_i(\mathbf{b}), \qquad \text{and if } b_i \text{ unique, } \widetilde{r}_{b_i}(\mathbf{b}) := \widetilde{p}_{b_i}(\mathbf{b})/\widetilde{x}_{b_i}(\mathbf{b}).$$

If a unique bid $b > \widetilde{r}_b(\mathbf{b})$, then b gets a positive utility in $\mathbf{b}$.

To prove Theorem 1.2, suppose for the sake of contradiction, that for some UIC, MIC, and 1-CRHP TFM, there exists some $\mathbf{v}$ where $|\mathbf{v}| = n > k$ and $x_{i^*}(\mathbf{v}) > 0$ for some $i^* \in [n]$. As in the deterministic case, we will construct a sequence of bid vectors $\mathbf{v}^{(m)} = (\mathbf{v}^{(m-1)}, b_m)$, each adding a new bid b_m to $\mathbf{v}^{(m-1)}$, where $\widetilde{r}_{b_{m-1}}(\mathbf{v}^{(m-1)}) < b_m < b_{m-1}$. We then prove that $|W(\mathbf{v}^{(m)})| \ge m$ by induction, which leads to a contradiction of the k-winner lemma for $m > k$.

[4] This is why this proof does not work for the impossibility w.r.t. weak 1-CRHP.

Challenges. However, simply adding one bid in each step is **not** enough. Using the above-ratio-guarantee, we can argue similarly as the deterministic case that b_m gets a positive confirmation probability in $(\mathbf{v}^{(m-1)}, b_m)$. Then raising b_m to some b'_m ends up with a positive *utility* for b'_m in $(\mathbf{v}^{(m-1)}, b'_m)$ by a corollary of Myerson's lemma.

The challenge is that raising b_m to b'_m can alter payments for others: this naive approach might make earlier winners $b_1, ..., b_{m-1}$ lose their utility, breaking the inductive invariant. Note that 1-CRHP does not rule out such strategies since raising b_m to b'_m may harm the coalition themselves in a randomized TFMs. We overcome this by carefully choosing a set S_m of two possible values $\alpha^{(m)} < \beta^{(m)}$ that the new bid b_m can take. Effectively, we build a sequence of *sets* of bid vectors $V^{(m)} = \{\mathbf{v}_{-i^*}\} \times S_1 \times \cdots \times S_m = \{(\mathbf{v}_{-i^*}, b_1, ..., b_m) : b_j \in S_j \text{ for } j \in [m]\}$. The induction will show that for each m, we have some $\mathbf{b} \in V^{(m)}$ such that $|W(\mathbf{b})| \geq m$.

Base case: Pick $\max(\mathbf{v}) < \alpha^{(1)} < \beta^{(1)}$ to be two values large enough such that b_1 has a positive utility in $(\mathbf{v}_{-i^*}, b_1)$ for any $b_1 \in S_1 = \{\alpha^{(1)}, \beta^{(1)}\}$. Such values must exist since $x_{i^*}(\mathbf{v}) > 0$. Specifically, choose $v^* > \max(\mathbf{v})$, put $\tau = \widetilde{r}_{v^*}(\mathbf{v}_{-i^*}, v^*) < v^*$, and choose $\max\{\max(\mathbf{v}), \tau\} < \alpha^{(1)} < \beta^{(1)} < v^*$. Monotonicity of the ratio then gives the bound $\widetilde{r}_{b_1}(\mathbf{v}_{-i^*}, b_1) \leq \tau < \alpha^{(1)}$. Let $V^{(1)} = \{\mathbf{v}_{-i^*}\} \times S_1$. Then for any $\mathbf{b} \in V^{(1)}$, we have $|W(\mathbf{b})| \geq 1$.

Inductive step: We demonstrate the main idea with $m = 2$, and summarize the general construction afterwards. Let $r^{(1)} := \max_{\mathbf{v}^{(1)} \in V^{(1)}} r_{n+1}(\mathbf{v}^{(1)},\ \alpha^{(1)})$ and $\alpha^{(2)}$ and $\beta^{(2)}$ be such that $\max\{\max(\mathbf{v}), r^{(1)}\} < \alpha^{(2)} < \beta^{(2)} < \alpha^{(1)}$. By a similar argument as in the deterministic case, $\alpha^{(1)}$ must have a positive confirmation probability in $(\mathbf{v}^{(1)}, \alpha^{(1)})$ for any $\mathbf{v}^{(1)} \in V^{(1)}$, and therefore, $r^{(1)}$ is well-defined. More precisely, the censor-then-replace argument gives positive confirmation probability to every newly appended bid $t \in (\alpha^{(1)} - \epsilon, \alpha^{(1)})$ for sufficiently small $\epsilon > 0$, independent of the choice $\mathbf{v}^{(1)} \in V^{(1)}$ (Claim 4.15). Raising this bid to $\alpha^{(1)}$ at the fixed index $n + 1$ gives strictly positive utility, even when it ties the existing bid b_1. Thus each ratio $r_{n+1}(\mathbf{v}^{(1)},\ \alpha^{(1)})$ for $\mathbf{v}^{(1)} \in V^{(1)}$ is strictly below $\alpha^{(1)}$, so $r^{(1)} < \alpha^{(1)}$. The value $r^{(1)}$ is an upper bound for the ratio $\widetilde{r}_b(\mathbf{v}^{(1)}, b)$ for any bid $b < \alpha^{(1)}$ with a positive confirmation probability. This maximum guarantees that the new bid $b_2 \in S_2 = \{\alpha^{(2)}, \beta^{(2)}\}$ *always* lies between $b_1 \geq \alpha^{(1)}$ and its corresponding ratio, no matter which value b_1 takes on. Let $V^{(2)} = \{\mathbf{v}_{-i^*}\} \times S_1 \times S_2$. We show that

$$\text{for any } \mathbf{v}^{(2)} = (\mathbf{v}_{-i^*}, b_1, b_2) \in V^{(2)},\ \widetilde{\mathsf{util}}_{b_2}(\mathbf{v}^{(2)}) > 0 \text{ for any } b_2 \in S_2; \tag{2}$$

$$\text{for any } i \in [2],\ \widetilde{\mathsf{util}}_{\beta^{(i)}}\left(\mathbf{v}_{-i^*}, \beta^{(1)}, \beta^{(2)}\right) > 0, \tag{3}$$

which completes the induction proof for $m = 2$ since $|W(\mathbf{v}_{-i^*}, \beta^{(1)}, \beta^{(2)})| \geq 2$.

Property (2) directly follows from UIC, since any bid $b > r^{(1)}$ must have a positive utility in $(\mathbf{v}^{(1)}, b)$ for any $\mathbf{v}^{(1)} \in V^{(1)}$. Otherwise, when the honest bid vector is $(\mathbf{v}^{(1)}, b)$, the user with true value b is incentivized to overbid to $\alpha^{(1)}$ to gain a positive utility.

To see why (3) is true, consider $\mathbf{b}' = (\mathbf{v}_{-i^*}, \alpha^{(1)}, \beta^{(2)})$. Since $\beta^{(2)}$ has a positive utility in $\mathbf{b}'$ by (2), and $\alpha^{(1)} > \beta^{(2)} > r^{(1)} \geq \widetilde{r}_{\beta^{(2)}}(\mathbf{b}')$, we know $\alpha^{(1)}$ must have a positive confirmation probability in $\mathbf{b}'$by the above-ratio-guarantee. Therefore, raising $\alpha^{(1)}$ to $\beta^{(1)}$ gives $\beta^{(1)}$ a positive utility. This completes the proof for $m = 2$.

In general, at each step m, we define $r^{(m-1)} = \max_{\mathbf{v}^{(m-1)} \in V^{(m-1)}} r_{n+m-1}\left(\mathbf{v}^{(m-1)}, \alpha^{(m-1)}\right)$ as an upper bound, over all possible $\mathbf{v}^{(m-1)} \in V^{(m-1)}$, of the ratio that a new bid smaller than $\alpha^{(m-1)}$ could have if it gets a positive confirmation probability. For every $\mathbf{v}^{(m-1)} \in V^{(m-1)}$, the newly appended bidder has strictly positive utility when bidding $\alpha^{(m-1)}$, and hence

$$r_{n+m-1}\left(\mathbf{v}^{(m-1)}, \alpha^{(m-1)}\right) < \alpha^{(m-1)}.$$

Since $V^{(m-1)}$ is finite, it follows that $r^{(m-1)} < \alpha^{(m-1)}$. We then pick $\max\{\max(\mathbf{v}), r^{(m-1)}\} < \alpha^{(m)} < \beta^{(m)} < \alpha^{(m-1)}$ and define $S_m = \{\alpha^{(m)}, \beta^{(m)}\}$ and $V^{(m)} = V^{(m-1)} \times S_m$. Roughly speaking, in the m-th step, for any $(b_1, ..., b_m) \in S_1 \times \cdots \times S_m$, the new bid b_m must get a positive utility in $(\mathbf{v}_{-i^*}, b_1, ..., b_m)$. Now consider specifically $\mathbf{b}' = (\mathbf{v}_{-i^*}, \beta^{(1)}, ..., \beta^{(m)})$. Using the above-ratio-guarantee and our choice of the sets S_j, we can conclude that for any $n \le j \le n+m-1$, we have $x_j(\mathbf{b}'_{-j}, \alpha^{(j-n+1)}) > 0$. Therefore, $\mathsf{util}_j(\mathbf{b}') > 0$ for each $n \le j \le n+m-1$. When $m = k+1$, this directly contradicts the k-winners lemma. This completes the impossibility proof for randomized TFMs in the plain model. We omit the details of the inductive reasoning here. See Section 4.2 for the complete proof.

2.2 Impossibility under Weak-CRHP

We first give a high-level overview of the proof techniques as this proof is quite involved. Recall that weak 1-CRHP means that strictly profitable deviations must not harm honest players, but it does not rule out utility-neutral deviations that are harmful to others.

This relaxation complicates the proof as mentioned in Footnote 4. In the 1-CRHP setting, each step of the induction used a contradiction argument to show that a newly added bid b_m must receive a positive confirmation probability: if b_m were not confirmed, a miner–user coalition could instead inject b_m without changing joint utility, and under 1-CRHP such a deviation cannot harm any honest player. Under only weak 1-CRHP, however, this utility-neutral strategy can harm honest players, so the earlier argument breaks down.

To overcome this, we adopt a slightly different approach. The key observation is that by MIC, if we start with some bid vector $\mathbf{v}$ with a positive miner revenue, then adding any set of additional bids $\mathbf{b}$ will still produce $\mu(\mathbf{v}, \mathbf{b}) > 0$. By budget feasibility, this implies that some bid must have a positive confirmation probability in $(\mathbf{v}, \mathbf{b})$. We use the following lemma to argue that this confirmed bid must be one of the newly added bids.

Lemma 2.1 (no-persistent-old-winner, informal)**.** *Fix a TFM in the plain model satisfying UIC, MIC, and weak 1-CRHP. Suppose $\mathbf{v} = (v_1, \ldots, v_n)$ and a sequence of sets $S_1, ..., S_k \subset \mathbb{R}_{\ge 0}$ such that each $|S_j| \ge 2$, and that $\{\max(\mathbf{v})\} \prec S_1 \prec \cdots \prec S_k$. Then there is no $i \in [n]$ such that $x_i(\mathbf{v}, \mathbf{b}) > 0$ for all $\mathbf{b} = (b_1, \ldots, b_k) \in S_1 \times \cdots \times S_k$.*

Suppose, for the sake of contradiction, that there exists a UIC, MIC, weak 1-CRHP TFM and an initial bid vector $\mathbf{v}$ with $\mu(\mathbf{v}) > 0$. We inductively construct a sequence of bid-vector sets $V^{(m)}$ by adding k new sets, instead of one set, at each step, then pruning the old sets and fixing $k-1$ fresh coordinates in a background vector $\mathbf{v}^{(m)}$. Thus $V^{(m)} = \{\mathbf{v}^{(m)}\} \times S_1^{(m)} \times \cdots \times S_m^{(m)}$, where $|\mathbf{v}^{(m)}| = n + (k-1)m$ and $\mathbf{v} \subseteq \mathbf{v}^{(1)} \subseteq \cdots \subseteq \mathbf{v}^{(m)}$. We show by induction that for each m there exists some $\mathbf{b} \in V^{(m)}$, such that $\mu(\mathbf{b}) > 0$ and $|W(\mathbf{b})| \ge m$. For $m = k+1$ this yields a contradiction to the k-winner lemma (which remains valid under weak 1-CRHP). In the induction proof, we will make use of the following dense Cartesian product lemma of Erdős:

Lemma 2.2 ([Erd64, Corollary, p. 188])**.** *For all positive integers p, a and $\xi \in (0, 1]$, there exists N such that, if $T \subseteq A_1 \times \cdots \times A_p$, each $|A_i| = N$ for $i \in [p]$, and $|T| \ge \xi \cdot N^p$, then there exist subsets $B_i \subseteq A_i$ with $|B_i| \ge a$ such that*

$$B_1 \times \cdots \times B_p \subseteq T.$$

Looking ahead, in the induction, each newly added set $A_j^{(m)}$ in the m-th step has size N_m. The invariant maintains $\{\max(\mathbf{v}^{(m)})\} \prec S_m^{(m)} \prec \cdots \prec S_1^{(m)}$ and a bound $r^{(m)} < \min S_m^{(m)}$ on every

ratio $\widetilde{r}_{b_\ell}(\mathbf{v}^{(\ell)}, b_1, \ldots, b_\ell)$, for all $\ell \le m$ and $(b_1, \ldots, b_\ell) \in S_1^{(m)} \times \cdots \times S_\ell^{(m)}$; all these ratios have positive denominators. In particular, b_m has positive utility, so the above-ratio-guarantee gives every larger b_i positive confirmation probability. The sequence of N_m is defined backwards starting from $N_{k+2} = 2$, such that at the end of the m-th step, there exist m sets $S_1^{(m)}, ..., S_m^{(m)}$, each with size N_{m+1}, such that any b_i in $\mathbf{b} = (b_1, ..., b_m) \in S_1^{(m)} \times ... \times S_m^{(m)}$ must have a positive confirmation probability in $(\mathbf{v}^{(m)}, \mathbf{b})$. Therefore, b_i must have a positive utility in all possible $(\mathbf{v}^{(m)}, \mathbf{b})$ as long as $b_i > \min S_i^{(m)}$. We show how to choose N_m given N_{m+1} in the base case and inductive step below.

Base case: Let $\{\max(\mathbf{v})\} \prec A_1^{(1)} \prec ... \prec A_k^{(1)}$ be k sets, each of size N_1, where N_1 is the N in Lemma 2.2 with $p = k$, $\xi = \frac{1}{n+k}$, and $a = N_2$. By MIC, $\mu(\mathbf{v}, \mathbf{b}) > 0$ for any $\mathbf{b} \in A_1^{(1)} \times \cdots \times A_k^{(1)}$. Therefore, some bid must have a positive confirmation probability in each $(\mathbf{v}, \mathbf{b})$. For any bid vector $\widehat{\mathbf{b}}$ with at least one bid of positive confirmation probability, let $\phi(\widehat{\mathbf{b}})$ denote the index of a lowest-valued bid among those with positive confirmation probability, breaking ties by index. The $n + k$ possible values of $\phi(\mathbf{v}, \mathbf{b})$ give a natural partition of $A_1^{(1)} \times \cdots \times A_k^{(1)}$:

$$T_i = \{\mathbf{b} \in A_1^{(1)} \times \cdots \times A_k^{(1)} : \phi(\mathbf{v}, \mathbf{b}) = i\} \text{ for } i \in [n + k].$$

At least one of these sets $|T_{i^*}| \ge \frac{1}{n+k} \cdot N_1^k$ for some $i^* \in [n + k]$. By Lemma 2.2, there exists $B_j^{(1)} \subseteq A_j^{(1)}$ for all $1 \le j \le k$ such that for each such set, $|B_j^{(1)}| \ge N_2$, such that $B_1^{(1)} \times \cdots \times B_k^{(1)} \subseteq T_{i^*}$, i.e., the i^*-th bid has positive confirmation probability in $(\mathbf{v}, \mathbf{b})$ for any $\mathbf{b} \in B_1^{(1)} \times \cdots \times B_k^{(1)}$. By Lemma 2.1, i^* cannot be one of the old bids from $\mathbf{v}$, i.e., $i^* > n$. Let $\ell = i^* - n$.

Pick an arbitrary $\mathbf{b}^* \in B_1^{(1)} \times \cdots \times B_k^{(1)} \subseteq T_{i^*}$, and let $\mathbf{v}^{(1)} = (\mathbf{v}, \mathbf{b}^*_{-\ell})$. Choose $v^* > \max A_k^{(1)}$. Raising the selected bid to v^* gives positive utility by Myerson's lemma, so $\tau := \widetilde{r}_{v^*}(\mathbf{v}^{(1)}, v^*) < v^*$. Let $S_1^{(1)}$ be a set with N_2 values such that $\{\max\{\max A_k^{(1)}, \tau\}\} \prec S_1^{(1)} \prec \{v^*\}$, and the ratio $r^{(1)}$ (defined analogously as in Section 2.1) $r^{(1)} = \widetilde{r}_{\max S_1^{(1)}}(\mathbf{v}^{(1)}, \max S_1^{(1)})$. By Myerson's lemma, $\widetilde{x}_{b_1}(\mathbf{v}^{(1)}, b_1) > 0$ for any $b_1 \in S_1^{(1)}$. By monotonicity of the payment-to-confirmation ratio (Lemma 4.6), $r^{(1)} \le \max\{\max A_k^{(1)}, \tau\} < \min S_1^{(1)}$.

Inductive step: Pick k sets $A_1^{(2)}, ..., A_k^{(2)}$ such that $\{r^{(1)}, \max(\mathbf{v}^{(1)})\} \prec A_1^{(2)} \prec \cdots \prec A_k^{(2)} \prec S_1^{(1)}$ and each $|A_j^{(2)}| = N_2$. This sequence of sets exist because $\{r^{(1)}, \max(\mathbf{v}^{(1)})\} \prec S_1^{(1)}$ by construction. Here, N_2 is the N in Lemma 2.2 with $p = k + 1$, $\xi = \frac{1}{n+2k}$, and $a = N_3$. Still, by MIC, $\mu(\mathbf{v}^{(1)}, \mathbf{b}, b_1) > 0$ for any $(\mathbf{b}, b_1) \in A_1^{(2)} \times \cdots \times A_k^{(2)} \times S_1^{(1)}$, meaning that some bid must have a positive confirmation probability. The $n+2k$ possible values of $\phi(\mathbf{v}^{(1)}, \mathbf{b}, b_1)$ give a natural partition of $A_1^{(2)} \times \cdots \times A_k^{(2)} \times S_1^{(1)}$ for $i \in [n + 2k]$:

$$T_i = \left\{(\mathbf{b}, b_1) \in A_1^{(2)} \times \cdots \times A_k^{(2)} \times S_1^{(1)} : \phi(\mathbf{v}^{(1)}, \mathbf{b}, b_1) = i\right\}.$$

By a similar reasoning as in the base case, there must exist an $i^* \in [n + 2k]$, such that there exists $B_j^{(2)} \subseteq A_j^{(2)}$ and $S_1^{(2)} \subseteq S_1^{(1)}$, each of size N_3, such that $B_1^{(2)} \times \cdots \times B_k^{(2)} \times S_1^{(2)} \subseteq T_{i^*}$, i.e., the i^*'th bid has a positive confirmation probability in $(\mathbf{v}^{(1)}, \mathbf{b}, b_1)$ for all $(\mathbf{b}, b_1) \in B_1^{(2)} \times \cdots \times B_k^{(2)} \times S_1^{(2)}$. The set-to-winners argument underlying Lemma 2.1, with b_1 held fixed, shows that i^* cannot be smaller than $n + k$. On the other hand, because ϕ selects a lowest-valued bid with positive confirmation probability, the censor-then-replace argument shows that $i^* < n + 2k$. That is, i^* must represent one of the new bids from $B_1^{(2)} \times \cdots \times B_k^{(2)}$. Let $\ell = i^* - |\mathbf{v}^{(1)}|$.

Pick an arbitrary $(\mathbf{b}^*, b_1) \in B_1^{(2)} \times \cdots \times B_k^{(2)} \times S_1^{(2)} \subseteq T_{i^*}$, and let $\mathbf{v}^{(2)} = (\mathbf{v}^{(1)}, \mathbf{b}^*_{-\ell})$. Put $\gamma := \min S_1^{(1)}$ and $J := |\mathbf{v}^{(2)}| + 1$. For each $b_1 \in S_1^{(2)}$, reinsert the selected fresh bid at index J; weak

symmetry preserves its positive confirmation probability. Raising it to γ at this fixed index gives positive utility by Myerson's lemma, even if $\gamma = b_1$. Since $S_1^{(2)}$ is finite, $\tau_2 := \max_{b_1 \in S_1^{(2)}} r_J(\mathbf{v}^{(2)}, \gamma, b_1) < \gamma$. Let $S_2^{(2)}$ be a set with N_3 values such that $\{\max\{\max A_k^{(2)}, r^{(1)}, \tau_2\}\} \prec S_2^{(2)} \prec \{\gamma\}$, and set $r^{(2)} := \max\{\max A_k^{(2)}, r^{(1)}, \tau_2\}$. Ratio monotonicity preserves the invariant, so b_2 has positive utility and the above-ratio-guarantee applies to b_1. Then b_1 and b_2 must have a positive confirmation probability in $(\mathbf{v}^{(2)}, b_1, b_2)$ for any $(b_1, b_2) \in S_1^{(2)} \times S_2^{(2)}$.

In general, for all $m \geq 2$, the inductive step proceeds analogously. Define N_i backward as follows: set $N_{k+2} := 2$, and for each $i = k+1, k, \ldots, 1$, let N_i be the number N given by Lemma 2.2 with parameters $p = k+i-1$, $\xi = \frac{1}{n+ki}$, and $a = N_{i+1}$. This choice ensures that at the end of the $(k+1)$-th step we obtain sets $S_1^{(k+1)}, \ldots, S_{k+1}^{(k+1)}$, each of size two, such that for every $\mathbf{b} = (b_1, \ldots, b_{k+1}) \in S_1^{(k+1)} \times \cdots \times S_{k+1}^{(k+1)}$, each coordinate b_i has a positive confirmation probability in $(\mathbf{v}^{(k+1)}, \mathbf{b})$. Consequently, taking $b_i^* := \max S_i^{(k+1)}$ for all $i \in [k+1]$ yields a bid vector $(\mathbf{v}^{(k+1)}, b_1^*, \ldots, b_{k+1}^*)$ in which all b_i^* enjoy positive utility, by a similar reasoning in Section 2.1, which contradicts the k-winner lemma.

2.3 Feasibility in the MPC-Assisted Model

We next explain why Mechanism 1.6 simultaneously achieves all desired properties once inclusion and correct output delivery are enforced by the MPC. For $N > 0$ eligible bids, let $q(N) := \min\{1, k/N\}$ denote the confirmation probability of each eligible bid. Set $q(0) := 0$. Every confirmed bid pays the fixed reserve res, while the total miner revenue is the fixed amount ϵ whenever the block is nonempty. UIC and MIC follows from prior work, so we focus on explaining why it achieves d-CRHP.

Fix a coalition containing $1 \leq m < M/2$ miners and at most $d \leq k$ users. Let h be the number of eligible honest users outside the coalition and t be the number of eligible colluding users. Let the sum of these eligible colluding users' utility had they be confirmed be s. Then under any deviation, besides the miner revenue, the total utility contribution from colluding bids is at most s.

In the honest case, as long as $h + t > 0$, colluding miners gets revenue $m\epsilon/M$. Each eligible user gets confirmed with probability $q(h+t)$, so colluding users' expected utility is $q(h+t)s$. Let N be the resulting number of eligible bids under deviation. Then $N \geq h$, and the colluding users' utility is at most $\mathbb{E}[q(N)]s$.

There are two possible cases. If $h > 0$, the block is always non-empty under every deviation, so the revenue of honest miners is always the same. If the coalition wants to harm an eligible honest user, the coalition has to decrease its expected confirmation probability, i.e., make $\mathbb{E}[q(N)] < q(h+t)$. If $s > 0$, the bound $\mathbb{E}[q(N)]s$ then makes the coalition strictly worse off. If $s = 0$, every colluding user has value at most res; a deviation that does not lower coalition utility must therefore use no eligible fake bids or below-reserve users' eligible bids. Hence $N \leq h + t$ almost surely, so no honest user is harmed. If $h = 0$, i.e., there is no honest eligible user. Then only honest miners need to be protected. If $t = 0$, their honest revenue is zero and cannot decrease, so assume $t > 0$. This is where we need $d \leq k$. In the honest case, since $t \leq d \leq k$, all eligible colluding users are already confirmed in the honest case. Therefore, any rational deviation must keep the block nonempty with probability one: each nonempty outcome gives conditional coalition utility at most $m\epsilon/M + s$, its honest utility, while an empty outcome gives zero and $m\epsilon/M > 0$. This guarantees honest miners' revenue. The condition $d \leq k$ ensures that all eligible colluding users already fit in the block in the honest case, so the coalition cannot profit by dropping some colluding users to increase the confirmation probability of the others.

2.4 Impossibility of UIC+URHP for Deterministic MPC-assisted TFMs

The proof of Theorem 1.8 is very similar to the deterministic impossibility in the plain model. However, we cannot directly use the above-payment-guarantee lemma because it utilizes a censor-then-replace attack, which cannot be performed in the MPC-assisted model. Instead we prove the above-payment-guarantee for deterministic UIC and URHP mechanisms in the MPC-assisted model. The crux of the proof is to start with a slightly weaker claim: *for a deterministic TFM that satisfies UIC and URHP, if b_i gets a positive utility in $\mathbf{b}$, then any unique bid higher than b_i must also be confirmed.* Then we only need to show that any unique b_j between $p_i(\mathbf{b})$ and b_i must be confirmed to get the above-payment-guarantee lemma.

Suppose for the sake of contradiction that, in some deterministic UIC and URHP TFM in the MPC-assisted model, a unique bid $b_j > p_i(\mathbf{b})$ is not confirmed even though user i has positive utility in $\mathbf{b}$. First let user j lower its bid to some $b'_j \in (p_i(\mathbf{b}), b_j) \setminus \{b_\ell : \ell \in [n]\}$. By UIC, user j still has zero utility under this deviation, so URHP implies that user i remains unharmed and therefore still has positive utility. Now choose $v \in (p_i(\mathbf{b}), b'_j)$ and consider the honest profile $(\mathbf{b}_{-i}, v)$. Using the weaker claim above and Myerson's lemma, user j has positive utility in this profile. However, user i can deviate from the truthful bid v to its original bid b_i without changing its own utility, while the resulting bid vector is $\mathbf{b}$, where user j has zero utility. This contradicts URHP. This proves the above-payment-guarantee for UIC and URHP TFMs in the MPC-assisted model. The rest of the proof follows by a similar reasoning of the deterministic case in Section 2.1. Here an unconfirmed user alone injects the unconfirmed fake bid, without decreasing its utility by individual rationality. The above-payment-guarantee forces the previous winner either to lose confirmation or to pay at least the fake bid, which exceeds its old payment; this harms that winner and contradicts URHP. The proof of this impossibility is given in Section 5.2.2.

3 Model and Preliminaries

3.1 Notation

Let $\mathbb{N}$ denote the set of natural numbers and $\mathbb{R}_{\geq 0}$ denote the non-negative real numbers. Given a bid vector $\mathbf{b} = (b_1, \ldots, b_n)$ and any $i \in [n]$, we use $\mathbf{b}_{-i}$ to denote $(b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_n)$. We use $(\mathbf{b}_{-i}, b'_i)$ to denote the vector obtained by replacing b_i with b'_i in $\mathbf{b}$, and treat this as equivalent to $(b_1, \ldots, b_{i-1}, b'_i, b_{i+1}, \ldots, b_n)$. For vectors $\mathbf{a}$ and $\mathbf{b}$, we write $\mathbf{a} \subseteq \mathbf{b}$ if every entry of $\mathbf{a}$ appears in $\mathbf{b}$. We use $|\mathbf{b}|$ to denote the number of elements in vector $\mathbf{b}$. For any vector $\mathbf{v} = (v_1, v_2, \ldots, v_n)$, we define $\max(\mathbf{v}) \coloneqq \max_{i \in [n]} v_i$. For a vector $\mathbf{v}$ and $S \subseteq [n]$, let $\mathbf{v}_S := (v_i)_{i \in S}$. For a bid vector $\mathbf{b}$ and a value z that appears exactly once in $\mathbf{b}$, let $\mathrm{idx}_{\mathbf{b}}(z)$ be the unique index i such that $b_i = z$. We write $\widetilde{x}_z(\mathbf{b}) := x_{\mathrm{idx}_{\mathbf{b}}(z)}(\mathbf{b})$, $\widetilde{p}_z(\mathbf{b}) := p_{\mathrm{idx}_{\mathbf{b}}(z)}(\mathbf{b})$, and $\widetilde{\mathsf{util}}_z(\mathbf{b}) := \mathsf{util}_{\mathrm{idx}_{\mathbf{b}}(z)}(\mathbf{b})$. These value-indexed quantities are used only when z is unique in $\mathbf{b}$. For two sets S and T, we use $S \prec T$ to show that $\sup S < \inf T$.

3.2 Transaction Fee Mechanism

We consider a transaction fee mechanism (TFM) where each block has a finite capacity of k transactions. Assume each user has a true value of $v_i \in \mathbb{R}_{\geq 0}$ that measures the maximum amount a user is willing to pay to get its transaction confirmed in the block. Each user i submits their transaction together with a *bid* b_i. We assume each transaction takes one slot in the block. In this paper, "bid" and "transaction" are used interchangeably. A TFM with capacity k is defined as a tuple $(\mathbf{I}, \mathbf{C}, \mathbf{P}, \mathbf{R})$ where:

- **Inclusion rule $\mathbf{I}(\cdot)$**: takes a bid vector $\mathbf{b}$ as input, and outputs a *block* $B \subseteq \mathbf{b}$ of at most k bids to include.
- **Confirmation rule $\mathbf{C}(\cdot)$**: takes as input a block B of the included bids and chooses a subset of included bids to confirm. Specifically, $\mathbf{C}(B)$ outputs a vector $(x_1, ..., x_{|B|}) \in \{0,1\}^{|B|}$, indicating whether each bid is confirmed.
- **Payment rule $\mathbf{P}(\cdot)$**: takes a block B as input and outputs a vector of $(p_1, ..., p_{|B|}) \in \mathbb{R}_{\geq 0}^{|B|}$, indicating the price paid by each transaction in B.
- **Revenue rule $\mathbf{R}(\cdot)$**: takes a block B as input, and outputs the miner's revenue $\mu \in \mathbb{R}_{\geq 0}$.

A feasible TFM $(\mathbf{I}, \mathbf{C}, \mathbf{P}, \mathbf{R})$ should satisfy the following properties:

- *Space feasibility:* the size of the block $|B| \leq k$.
- *Individual rationality:* a user's payment shall not exceed the bid amount, i.e., for any $b_i \in B$, its payment $p_i \leq b_i$. Unconfirmed bids pay zero.
- *budget feasibility*: the miner's revenue cannot exceed the total payment collected from all confirmed bids, i.e., $\mu \leq \sum_{i=1}^{|B|} p_i$. When the miner's revenue is strictly less than the total payments, we say that the difference is *burnt*.

Among the four rules, the confirmation rule, payment rule, and revenue rule are all executed by the blockchain based on the block, and we treat these three rules as always correctly implemented based on the input block B. The inclusion rule is either implemented by the miner in the plain model or implemented by an MPC in the MPC-assisted model.

Weak Symmetry. Given a bid $\mathbf{b} = (b_1, ..., b_n)$, let x_i and p_i denote the random variable representing the probability of bid b_i getting confirmed and the payment it needs to pay in an honest execution. We say that a TFM satisfies *weak symmetry* iff the joint distribution of $(\{(b_i, x_i, p_i)\}_{i \in [n]}, \mu)$ is the same for input bid vector $\pi(\mathbf{b})$ for any permutation π on $\mathbf{b}$.

An operational view of weak symmetry assumes the following: Given a bid vector $\mathbf{b}$ where each bid may carry some metadata such as identity, public keys of the user, or timestamp. The honest mechanism first sorts the bids based on the amount, and can perform arbitrary tie-breaking rule based on the metadata if multiple bids have the same amount. After the sorting step, all the four rules $(\mathbf{I}, \mathbf{C}, \mathbf{P}, \mathbf{R})$ depend only on bid amounts and positions in the sorted vector. Weak symmetry is a natural requirement in practice and does not require two bids of the same amount to always receive the same treatment.

3.3 Game Induced by TFM

Henceforth, let $\mathcal{C}$ denotes the strategic players. Specifically, $\mathcal{C}$ can be a strategic user, strategic miner(s) in control of the current block, or a coalition of the miner(s) and one or more users.

3.3.1 TFM Game in the Plain Model.

In the plain model, the TFM game is defined as follows:

1. Each honest users not in $\mathcal{C}$ submits their bid represented by a single real-value bid. Let $\mathbf{b}_{-\mathcal{C}}$ denote the bids from these honest users.

2. The coalition $\mathcal{C}$ decides their bids $\mathbf{b}_{\mathcal{C}}$ according to $\mathbf{b}_{-\mathcal{C}}$.

3. The miner selects up to k bids from $(\mathbf{b}_{\mathcal{C}}, \mathbf{b}_{-\mathcal{C}})$ to form a block B.

4. The blockchain protocol executes the confirmation rule $\mathbf{C}$, payment rule $\mathbf{P}$, and miner revenue rule $\mathbf{R}$ to the block B created by the miner.

Strategy Space. In this paper, we focus on direct-revelation mechanism, i.e., for an user i with true value v_i, the honest strategy $H_i(v_i) = v_i$ is to submit a single bid representing its true value. A strategic user may choose to submit a bid vector $\mathbf{b}_i^*$ that contains zero to multiple bids which do not necessarily reflect their true value. We call all the additional bids that the user injects as *fake* bids.

A miner's honest behavior $H_{\mathcal{M}}$ is to implement the prescribed inclusion rule on the input bid vector $\mathbf{b}$ without submitting any fake bids, i.e., if users' honest bid vector is $\mathbf{b}$, honest miner strategy $H_{\mathcal{M}}(\mathbf{b})$ outputs a block $\mathbf{I}(\mathbf{b})$. In the plain model, a strategic miner may choose to deviate from the prescribed inclusion rule arbitrarily by dropping bids, injecting fake bids, and arbitrarily choosing the randomness used in the inclusion rule, i.e., the strategy $S_{\mathcal{M}}(\mathbf{b})$ outputs an arbitrary block B^* of size at most k. Players can adopt mixed strategies. A strategic coalition can adopt a combination of the strategies of its members.

3.3.2 MPC-Assisted Model

In the MPC-assisted model, M miners jointly run a multi-party computation (MPC) to realize an ideal functionality that honestly implements the inclusion rule, and the M miners share the total revenue. We assume that the strategic coalition contains $m < M/2$ miners and that the MPC provides guaranteed output delivery. Concretely, there is an ideal functionality $\mathcal{F}_{\text{TFM}}$ that, on input $\mathbf{b}$, implements the honest inclusion, confirmation, payment and revenue rule on $\mathbf{b}$. In this paper, we analyze incentives in the "ideal" world with $\mathcal{F}_{\text{TFM}}$. The real-world MPC-assisted model can be instantiated under standard cryptographic assumptions. In the MPC-assisted model, the game runs as follows:

1. Users not in $\mathcal{C}$ submit bids represented by a single real value to $\mathcal{F}_{\text{TFM}}$. Let $\mathbf{b}_{-\mathcal{C}}$ denote the bids from users outside $\mathcal{C}$.

2. $\mathcal{F}_{\text{TFM}}$ sends $\mathbf{b}_{-\mathcal{C}}$ to $\mathcal{C}$ and receives a bid vector $\mathbf{b}_{\mathcal{C}}$ from the coalition.

3. $\mathcal{F}_{\text{TFM}}$ implements the inclusion, confirmation, payment, and revenue rule on $(\mathbf{b}_{-\mathcal{C}}, \mathbf{b}_{\mathcal{C}})$. The outputs include a vector indicating whether each bid is confirmed or not, a payment vector of every bid's payment, and the total miner revenue.

4. Send the outcome to every player.

Strategy Space. User's strategy space is the same as in the plain model. An honest miner does not submit any bids, whereas strategic miner(s) may inject one or more fake bids. Unlike in the plain model, now strategic miner(s) can no longer drop honest users' bids or arbitrarily choose which subset of bids to include since now the inclusion rule is implemented by the ideal functionality $\mathcal{F}_{\text{TFM}}$. A strategic coalition can adopt a combination of the strategies of its members.

3.4 Utility and Incentive Compatibility

Utility. Each user i has a true value $v_i \in \mathbb{R}_{\geq 0}$ if its primary bid representing its transaction gets confirmed. All the fake bids have true value 0. Let p_i denote the total payment user i needs to pay. Then user i's utility is $v_i - p_i$ if its primary bid gets confirmed and $-p_i$ otherwise. A miner's utility is its revenue $\mu - p_{\mathcal{M}}$, where $p_{\mathcal{M}}$ denotes the total payment from the miner if they inject any fake bids. A coalition's joint utility is the sum of all coalition members' utilities.

Below, for a strategic player or coalition, denoted as $\mathcal{C}$, we use $H_{\mathcal{C}}$ to denote $\mathcal{C}$'s honest strategy of $\mathcal{C}$. Let $\mathbf{v}$ represent the vector of true values of all users. We use $\mathsf{util}_i(\mathbf{v}; S_{\mathcal{C}})$ to denote the expected utility of user i in the following randomized experiment:

- In the mechanism, players in $\mathcal{C}$ adopts (possibly randomized) strategy S, while all other players act honestly, where all users' true values are represented by $\mathbf{v}$.
- Output utility of player i.

A miner j's expected utility $\mathsf{mutil}_j(\mathbf{v}; S_{\mathcal{C}})$ and coalition's joint utility $\mathsf{util}_{\mathcal{C}}(\mathbf{v}; S_{\mathcal{C}})$ are defined analogously w.r.t the above randomized experiment.

Definition 3.1 (Incentive compatibility)**.** Given a TFM $(\mathbf{I}, \mathbf{C}, \mathbf{P}, \mathbf{R})$, we say that the TFM satisfies incentive compatibility (IC) w.r.t. a strategic player or coalition, denoted as $\mathcal{C}$, iff for any true value vector $\mathbf{v}$ of users, for any strategy $S_{\mathcal{C}}$ of coalition $\mathcal{C}$, we have

$$\mathsf{util}_{\mathcal{C}}(\mathbf{v}; S_{\mathcal{C}}) \leq \mathsf{util}_{\mathcal{C}}(\mathbf{v}; H_{\mathcal{C}}).$$

Specifically, we say that a TFM satisfies

- *User incentive compatibility (UIC)* if the above holds when $\mathcal{C}$ contains an individual user, and the miner acts honestly.
- *Miner incentive compatibility (MIC)* in the plain model if the above holds when $\mathcal{C}$ only contains the miner.

  In the MPC-assisted model, we say that a TFM satisfies MIC if the above holds when $\mathcal{C}$ contains $m < M/2$ miners jointly running the MPC implementing $\mathcal{F}_{\text{TFM}}$.
- *d-side-contract-proofness (d-SCP)* in the plain model for some integer $d \geq 1$ if the above holds when $\mathcal{C}$ contains the miner and at least one but no more than d number of users.

  In the MPC-assisted model, we say that a TFM satisfies d-SCP for some integer $d \geq 1$ if the above holds when $\mathcal{C}$ contains $m < M/2$ miners running the MPC and at least one but no more than d number of users.

In this work, we introduce a new notion which requires that a rational strategic player cannot harm other honest players without harming themselves. We formalize this as *Rational-Harm Proofness* (RHP).

Definition 3.2 (Restatement of Definition 1.1)**.** Fix a coalition of strategic players $\mathcal{C}$ and a protected set of honest players $\mathcal{H}$ such that $\mathcal{C} \cap \mathcal{H} = \emptyset$. We say that a TFM satisfies rational-harm proofness (RHP) against $\mathcal{C}$ for protecting $\mathcal{H}$ if, for any true value vector $\mathbf{v}$ of users and any strategy $S_{\mathcal{C}}$ for coalition $\mathcal{C}$ such that

$$\mathsf{util}_{\mathcal{C}}(\mathbf{v}; S_{\mathcal{C}}) \geq \mathsf{util}_{\mathcal{C}}(\mathbf{v}; H_{\mathcal{C}}),$$

it holds that

$$\mathsf{util}_i(\mathbf{v}; S_{\mathcal{C}}) \geq \mathsf{util}_i(\mathbf{v}; H_{\mathcal{C}})$$

for every protected honest player $i \in \mathcal{H}$. Here util_a and $\mathsf{util}_{\mathcal{C}}$ denote expected utilities in the randomized experiment where the users' true value vector is $\mathbf{v}$, players in $\mathcal{C}$ adopt $S_{\mathcal{C}}$, players outside $\mathcal{C}$ behave honestly, and $H_{\mathcal{C}}$ denotes the honest strategy of coalition $\mathcal{C}$.

Based on the three types of strategic players, we say that a TFM satisfies

- *User rational-harm proofness (URHP)* iff Definition 1.1 holds for any $\mathcal{C} = \{i\}$ containing an individual user i and $\mathcal{H}$ contains all users except i. URHP protects honest users from an individual deviating user; it does not protect the miner.
- *Miner rational-harm proofness (MRHP)* iff Definition 1.1 holds for the single miner in the plain model, with $\mathcal{H}$ equal to all users, and for any nonempty coalition of $m < M/2$ miners in the MPC-assisted model, with $\mathcal{H}$ equal to all users and all miners outside the coalition.
- *d-coalition rational-harm proofness (d-CRHP)* iff Definition 1.1 holds for coalitions containing the miner and at least one but at most d users in the plain model, protecting all users outside the coalition, and for coalitions containing a nonempty coalition of $m < M/2$ miners and at least one but at most d users in the MPC-assisted model, protecting all users outside the coalition and all miners outside the coalition. User-only deviations are covered by URHP.

We also define a weaker notion called *weak RHP*: any strategy that *strictly* benefits the coalition must not harm any players outside the coalition.

Definition 3.3 (Weak RHP)**.** A TFM is *weakly RHP* w.r.t. $\mathcal{C}$ if Definition 3.2 holds with the strict inequality $u_{\mathcal{C}}(\mathbf{v}; S_{\mathcal{C}}) > u_{\mathcal{C}}(\mathbf{v}; H_{\mathcal{C}})$ in place of $\geq$. Equivalently, every strictly profitable deviation for $\mathcal{C}$ must weakly preserve the utility of every protected honest player.

Fact 3.4. *If a TFM is incentive compatible w.r.t. some $\mathcal{C}$, then it is weak RHP w.r.t. $\mathcal{C}$.*

Proof. Since incentive compatibility rule out the existence of any strictly profitable strategies of $\mathcal{C}$ compared to honest behavior, it automatically achieves weak RHP w.r.t. $\mathcal{C}$. □

3.5 Myerson's Lemma

Our impossibility will rely on the famous Myerson's Lemma. Below, we use $x_i(\mathbf{b})$ and $p_i(\mathbf{b})$ to denote user i's probability of getting confirmed and its expected payment under input bid vector $\mathbf{b}$ when everyone behaves honestly. We define $\mathsf{util}_i(\mathbf{b}) := b_i \cdot x_i(\mathbf{b}) - p_i(\mathbf{b})$ as the honest expected utility when $\mathbf{b}$ is also the true value vector.

Lemma 3.5 (Myerson's Lemma [Mye81])**.** *If a TFM satisfies UIC, then*

- **Monotone allocation***: For any user i, any other users' bids $\mathbf{b}_{-i}$, any $b_i' > b_i$, it must be $x_i(\mathbf{b}_{-i}, b_i') \geq x_i(\mathbf{b}_{-i}, b_i)$.*
- **Unique payment***: For any user i, any other users' bids $\mathbf{b}_{-i}$, and bid b_i from user i, user i's expected payment can be uniquely determined as*

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

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

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

4 Characterization in the Plain Model

4.1 Feasibility Results

In this section, we present the mechanisms referenced in Theorem 1.5 and show how each mechanism achieves any three of the four target properties: UIC, MIC, CRHP, and positive miner revenue. For completeness, we restate each mechanism with respect to the four rules for defining a TFM.

UIC + MIC + CRHP

Singleton posted-price //Reserve price $\mathsf{res} \geq 0$.

- **Inclusion & Confirmation**: If there is only one bid, and it is at least res, include and confirm that bid. Otherwise, include and confirm no bids.
- **Payment & Revenue:** The confirmed bid pays the reserve res, and the miner gets nothing.

Lemma 4.1. *The above singleton posted-price satisfies UIC, MIC, URHP, and d-CRHP for any $d \geq 1$ in the plain model.*

Proof. For UIC, fix a user. If there are no other bids, bidding at least reserve gives utility $v_i - \mathsf{res}$ and bidding below reserve gives zero; this is exactly the posted-price threshold rule. If there is at least one other bid, the user cannot get its own transaction confirmed by adding bids because the honest inclusion rule confirms a bid only when the submitted vector contains exactly one bid, which is eligible. Fake bids only create additional bids and cannot improve the user's utility. Thus truthful bidding with no fake bids is optimal.

MIC: Miner revenue is always zero. Fake bids can only create payment costs for the miner and cannot increase revenue, so honest behavior is weakly optimal.

URHP: A deviating user can harm another user only if that other user has positive honest utility and becomes unconfirmed or pays more. Payments are fixed at reserve. An honest user can have positive utility in the singleton mechanism only when it is the only submitted bid and its value is above reserve. If another strategic user is present, this cannot be the honest baseline. Hence no rational user deviation can harm a protected user.

***d*-CRHP:** A protected honest user can have positive honest utility only when it is the unique submitted bid. But a d-CRHP coalition contains at least one user in addition to the miner, so under honest play there is more than one submitted bid and no protected user is confirmed. More generally, any deviation that creates a singleton confirmed bid can only benefit coalition users and cannot make an outside user worse off relative to the honest baseline. □

Not 1-SCP: If there are multiple users and a colluding user has value above reserve, the miner can include only the colluding user's bid, giving the colluding user positive utility while miner revenue remains zero.

Not MRHP: If there is a single honest user with value above reserve, the miner can censor the bid, keep revenue zero, and reduce that user's utility to zero.

UIC + CRPH + Positive Revenue

All-or-nothing posted-price //Reserve price $\mathsf{res} \geq 0$.
//Revenue parameter $0 < \epsilon \leq \mathsf{res}$.

- **Inclusion & Confirmation**: If there are no more than k bids and all bids are strictly greater than res, include and confirm all bids. Otherwise, include and confirm no bids. The strict inequality is intentional and avoids zero-utility reserve-boundary deviations in the URHP proof.
- **Payment & Revenue:** Each confirmed bid pays the reserve price res, and the miner receives a revenue share of ϵ per confirmed bid.

Lemma 4.2. *The above all-or-nothing posted-price satisfies UIC, d-CRHP for any $d \geq 1$ and positive revenue in the plain model. Additionally, it satisfies URHP and MRHP.*

Proof. UIC follows from the same posted-price threshold argument as in Lemma 4.1: a bid strictly above reserve is needed for confirmation, confirmed bids pay the reserve, and fake bids either preserve the all-or-nothing success condition while adding nonpositive fake-bid surplus or make the condition fail. Positive revenue is immediate whenever the mechanism confirms at least one bid.

URHP: Because strict eligibility implies any honestly confirmed strategic user has strictly positive utility, any user-only deviation that makes the all-or-nothing condition fail and harms another confirmed user also makes the deviating user lose strictly positive utility. Fake bids that remain confirmed create non-positive fake-bid surplus and cannot help.

MRHP: In the honest baseline, if any protected honest user has positive utility, then all submitted bids are above reserve, there are at most k bids, all users are confirmed, and miner revenue is ϵ times the number of confirmed bids. Any miner deviation that makes a protected honest user unconfirmed must either make the all-or-nothing test fail or omit that user. In either case the total number of confirmed real honest bids falls, so the miner's revenue falls by at least ϵ for each omitted protected confirmed user. Fake bids cannot compensate because each confirmed fake bid costs the miner res and increases miner revenue by at most $\epsilon \leq \mathsf{res}$.

***d*-CRHP:** The same revenue-loss argument applies to miner-user coalitions. Colluding users who were honestly confirmed have strictly positive utility because their values are strictly above reserve. Confirmed fake bids have nonpositive net contribution because they cost res and increase miner revenue by at most $\epsilon \leq \mathsf{res}$. Therefore a deviation that harms a protected honest user strictly lowers the coalition's joint utility. These arguments also cover mixed deviations: when any protected user has positive honest utility, every pure deviation weakly lowers the strategic party's utility, and every pure deviation that harms a protected user lowers it strictly. Thus a mixture that preserves the strategic party's expected utility cannot harm a protected user. □

Not MIC or 1-SCP: Let S be the honest bid vector. If $|S| > k$ and every bid is above res, the miner gets 0 revenue. By ignoring $|S| - k$ bids from S, the miner can include exactly k bids and earn $k\epsilon > 0$ revenue. The above mechanism does not achieve 1-SCP for the same reason as the miner can collude with any of the included players for the same effect.

UIC + MIC + Positive Revenue

Posted-price with random selection //Reserve price $\mathsf{res} > 0$.
//Revenue parameter $0 < \epsilon \leq \mathsf{res}$.

- **Inclusion & Confirmation**: Let S be the set of bids at least the reserve price res. If $|S| \leq k$, include and confirm all bids in S. Otherwise, uniformly at random choose k bids in S to include and confirm.
- **Payment & Revenue**: Each confirmed bid pays the reserve price res. The miner receives total revenue ϵ if at least one bid is confirmed, and zero otherwise.

Lemma 4.3. *The above posted-price with random selection TFM satisfies UIC, MIC, and positive revenue in the plain model. Additionally, it achieves URHP.*

Proof. **UIC:** The allocation and payment rule satisfies Myerson's lemma: for a fixed user and fixed other bids, the allocation probability is zero below reserve and equals the uniform-selection probability at or above reserve, while the expected payment is the reserve times that probability. To also rule out fake bids, let h be the number of eligible outside bids. A user of value v submitting an eligible primary bid and f eligible fake bids has utility $q(v - \mathsf{res} - f\mathsf{res})$, where $q = \min\{1, k/(h + 1 + f)\}$. For $v \geq \mathsf{res}$, this is at most the truthful utility $q_0(v - \mathsf{res})$, where $q_0 = \min\{1, k/(h + 1)\}$: the bound is immediate if the former utility is negative, and otherwise follows from $q \leq q_0$. For $v < \mathsf{res}$ it is nonpositive. With no eligible primary bid the utility is also nonpositive, and ineligible bids have no effect. These bounds establish UIC, including for mixed deviations.

MIC: If there is at least one eligible real bid, honest miner revenue is already ϵ, the maximum possible revenue. Censoring some eligible bids while leaving at least one eligible bid can keep revenue at ϵ but cannot increase it. Censoring all eligible bids gives zero revenue unless the miner injects a fake eligible bid; an injected fake bid costs at least res and yields at most ϵ, so it is not profitable since $\epsilon \leq \mathsf{res}$. If there are no eligible real bids, injecting fake eligible bids yields revenue at most ϵ but costs at least res per confirmed fake bid, so it cannot strictly improve miner utility.

URHP: A user-only deviation can harm another user only by reducing that user's confirmation probability. Under random selection this requires adding eligible competition, either by overbidding with an ineligible real bid or injecting eligible fake bids. Turning a real bid with value below reserve into an eligible bid gives non-positive expected surplus and is strictly negative if it is ever confirmed. Injected fake eligible bids have true value zero and impose expected payment costs. A user with value exactly reserve is already eligible under truthful bidding and has zero surplus, so changing the real bid within the eligible range does not add competition; fake bids still cost money. Therefore any user-harming deviation lowers the deviating user's utility. Since UIC bounds every pure deviation by truthful utility, a mixed deviation cannot offset such a strict loss with a gain from another pure deviation. Hence the argument also covers mixed deviations. □

Not 1-SCP: The miner can choose the random seed or inclusion subset to favor a colluding eligible user, increasing the coalition's utility while keeping miner revenue unchanged.

Not MRHP: The plain miner can manipulate inclusion or randomness, or censor eligible honest users, while keeping fixed revenue ϵ as long as at least one eligible bid remains.

Not 1-CRHP: The same deviation, with a colluding eligible user kept confirmed or favored by the miner, harms an outside eligible user while preserving the coalition's utility.

MIC + CRHP + Positive Revenue

First-price auction

- **Inclusion & Confirmation:** Include and confirm the top k bids, breaking ties arbitrarily.
- **Payment & Revenue:** All confirmed bids pay their bid price and all payments go to the miner.

Lemma 4.4. *The above first-price auction satisfies URHP, MIC, MRHP, d-CRHP for any $d \geq 1$, d-SCP for any $d \geq 1$, and has positive miner revenue in the plain model.*

Proof. **MIC:** The miner receives all payments, so they would have to increase payments from users to increase their utility. In the honest inclusion rule, the top bids are confirmed and paid, and there is no way to have payments higher than the bids.

URHP, d-CRHP & MRHP: Under truthful bidding in a first-price auction, every confirmed user pays its value and every unconfirmed user gets zero, so every user's honest utility is zero. No deviation can make an honest user's utility strictly below zero because individual rationality and non-confirmation both give utility at least zero. Hence URHP, MRHP, and d-CRHP hold.

d-SCP: In the honest case, because all payments go to the miner, the joint utility of the miner and any set of users is equal to the summation of the top $\min\{k, n\}$ valuations. Under any deviation, a confirmed colluding user's payment cancels within the coalition, leaving its true value; a confirmed outside user contributes its truthful bid, also its true value; and a confirmed fake bid contributes zero after its payment cancels. Thus coalition utility is the sum of the true values of at most k confirmed real users, outcome by outcome and hence also in expectation under mixed deviations. It is impossible to gain more utility than this for any coalition due to the block size limit, budget feasibility, and individual rationality (See Section 3.2). □

Not UIC: Since users pay their own bid, a confirmed user may profit by underbidding while still remaining confirmed. This deviation harms miner revenue, not a protected user under URHP.

4.2 Impossibilities in the Plain Model

We first introduce the following useful lemmas in our impossibility proofs. Recall that, for a bid vector $\mathbf{b} = (b_1, \ldots, b_n)$, for $i \in [n]$, $x_i(\mathbf{b})$, $p_i(\mathbf{b})$ and $\mathsf{util}_i(\mathbf{b})$ denote the confirmation probability, expected payment, and expected utility for bid b_i in $\mathbf{b}$ when the honest inclusion rule is followed. For unique bid values we use the value-indexed convention from Section 3: $x_z(\mathbf{b})$, $p_z(\mathbf{b})$, and $\mathsf{util}_z(\mathbf{b})$ denote the allocation probability, expected payment, and expected utility of the unique bid with value z. We keep the decorated notation $\widetilde{x}_z$, $\widetilde{p}_z$, and $\widetilde{\mathsf{util}}_z$ only as typographic reminders of this value-indexed convention.

Lemma 4.5. *For any TFM that satisfies UIC, given any $\mathbf{b}_{-i}$, let $b^* = \inf\{b : x_i(\mathbf{b}_{-i}, b) > 0\} < +\infty$. Then for any $v^* > v \geq b^*$, we have $\mathsf{util}_i(\mathbf{b}_{-i}, v^*) > \mathsf{util}_i(\mathbf{b}_{-i}, v)$.*

Proof. Suppose that for some $\mathbf{b}_{-i}$ and v, we have $x_i(\mathbf{b}_{-i}, v) > 0$. Then for any $v^* > v$,

$$\begin{aligned}
\mathsf{util}_i(\mathbf{b}_{-i}, v^*) &= v^* \cdot x_i(\mathbf{b}_{-i}, v^*) - p_i(\mathbf{b}_{-i}, v^*) \\
&= \int_0^{v^*} x_i(\mathbf{b}_{-i}, t)dt && \text{by Myerson's Lemma (Lemma 3.5).} \\
&> \int_0^{v} x_i(\mathbf{b}_{-i}, t)dt = \mathsf{util}_i(\mathbf{b}_{-i}, v)
\end{aligned}$$

The only remaining case is $v = b^*$ with $x_i(\mathbf{b}_{-i}, v) = 0$. Choose $w \in (v, v^*)$. By the definition of b^* and monotonicity, $x_i(\mathbf{b}_{-i}, w) > 0$. Myerson's payment identity gives

$$\mathsf{util}_i(\mathbf{b}_{-i}, v^*) - \mathsf{util}_i(\mathbf{b}_{-i}, v) = \int_v^{v^*} x_i(\mathbf{b}_{-i}, t)\, dt \geq (v^* - w) x_i(\mathbf{b}_{-i}, w) > 0.$$

□

Lemma 4.6. *For any TFM that satisfies UIC, given any $\mathbf{b}_{-i}$, let $b^* = \inf\{b : x_i(\mathbf{b}_{-i}, b) > 0\} < +\infty$. Then for any $v^* \geq v > b^*$, the ratio $\frac{p_i(\mathbf{b}_{-i}, v^*)}{x_i(\mathbf{b}_{-i}, v^*)} \geq \frac{p_i(\mathbf{b}_{-i}, v)}{x_i(\mathbf{b}_{-i}, v)}$.*

Proof. For this proof, abbreviate $x(t) := x_i(\mathbf{b}_{-i}, t)$ and $p(t) := p_i(\mathbf{b}_{-i}, t)$. By Myerson's Lemma,

$$\frac{p(v)}{x(v)} = v - \frac{\int_0^v x(t)\, dt}{x(v)}.$$

Therefore,

$$\frac{p(v^*)}{x(v^*)} - \frac{p(v)}{x(v)} = \left(\frac{1}{x(v)} - \frac{1}{x(v^*)}\right) \int_0^v x(t)\, dt + (v^* - v) - \frac{1}{x(v^*)} \int_v^{v^*} x(t)\, dt.$$

Both terms are nonnegative. The first is nonnegative because $x(v^*) \geq x(v) > 0$ by monotonicity. For the second, monotonicity gives $x(t) \leq x(v^*)$ for every $t \in [v, v^*]$, and hence

$$\int_v^{v^*} x(t)\, dt \leq (v^* - v) x(v^*).$$

Thus,

$$\frac{p(v^*)}{x(v^*)} \geq \frac{p(v)}{x(v)}.$$

□

Lemma 4.7. *Suppose a TFM $(\mathbf{I}, \mathbf{C}, \mathbf{P}, \mathbf{R})$ satisfies MIC in the plain model. For any $\mathbf{b} \subseteq \mathbf{b}'$, it must be that $\mu(\mathbf{b}') \geq \mu(\mathbf{b})$.*

Proof. For the sake of contradiction, suppose this was not the case, so $\mu(\mathbf{b}') < \mu(\mathbf{b})$. Then, when the miner sees the honest bid vector $\mathbf{b}'$, they censor the bids not in $\mathbf{b}$ perform the honest inclusion rule as if the input bid vector is $\mathbf{b}$ to gain more revenue. This contradicts MIC. □

Lemma 4.8. *Suppose a TFM $(\mathbf{I}, \mathbf{C}, \mathbf{P}, \mathbf{R})$ satisfies MIC in the plain model. Then for any bid vectors $\mathbf{b}, \mathbf{b}', \mathbf{v}$, we have $\mu(\mathbf{b}, \mathbf{v}) \geq \mu(\mathbf{b}', \mathbf{v}) - \sum_{i=1}^{|\mathbf{b}'|} p_i(\mathbf{b}', \mathbf{v})$.*

Proof. For the sake of contradiction, suppose $\mu(\mathbf{b}, \mathbf{v}) < \mu(\mathbf{b}', \mathbf{v}) - \sum_{i=1}^{|\mathbf{b}'|} p_i(\mathbf{b}', \mathbf{v})$. Consider the world where $(\mathbf{b}, \mathbf{v})$ is the honest bid vector. The miner's honest utility is $\mu(\mathbf{b}, \mathbf{v})$. Consider the following miner strategy: it deviates from the honest inclusion rule by ignoring the bids in $\mathbf{b}$ and submitting the fake bids in $\mathbf{b}'$ to achieve the bid vector $(\mathbf{b}', \mathbf{v})$. Inserting the fake bids costs the miner $\sum_{i=1}^{|\mathbf{b}'|} p_i(\mathbf{b}', \mathbf{v})$ so the miner's utility is

$$\mu(\mathbf{b}', \mathbf{v}) - \sum_{i=1}^{|\mathbf{b}'|} p_i(\mathbf{b}', \mathbf{v}) > \mu(\mathbf{b}, \mathbf{v}), \qquad \text{by assumption}$$

which contradicts MIC. □

Recall that, for a bid vector $\mathbf{b} = (b_1, \ldots, b_n)$, for $i \in [n]$, $x_i(\mathbf{b})$, $p_i(\mathbf{b})$ and $\mathsf{util}_i(\mathbf{b})$ denote the confirmation probability, expected payment, and expected utility for bid b_i in $\mathbf{b}$ when the honest inclusion rule is followed. Also, $\widetilde{x}_{b_i}(\mathbf{b})$, $\widetilde{p}_{b_i}(\mathbf{b})$, and $\widetilde{\mathsf{util}}_{b_i}(\mathbf{b})$ are defined analogously for a unique bid b_i in bid vector $\mathbf{b}$.

In a (possibly randomized) mechanism, the inclusion rule, confirmation rule, payment rule and miner revenue rule can be randomized. However, the randomness used in the inclusion rule is freely chosen by the miner, whereas the randomness used in other rules come from the blockchain. Let Ω and $\mathcal{D}$ be the sample space and distribution of the randomness specified by the honest inclusion rule. For each $r \in \Omega$, define $x_i(\mathbf{b} \mid r)$, $p_i(\mathbf{b} \mid r)$, and $\mu(\mathbf{b} \mid r)$ as the expected confirmation probability of bid b_i, the expected payment of bid b_i, and the expected miner revenue, respectively, conditioned on the randomness used in the inclusion rule being r. The expectation in each case is now taken over the randomness used in the confirmation, payment, and miner revenue rules, respectively.

By definition,

$$x_i(\mathbf{b}) = \mathop{\mathbb{E}}_{r \leftarrow \mathcal{D}}[x_i(\mathbf{b} \mid r)], \qquad p_i(\mathbf{b}) = \mathop{\mathbb{E}}_{r \leftarrow \mathcal{D}}[p_i(\mathbf{b} \mid r)], \qquad \mu(\mathbf{b}) = \mathop{\mathbb{E}}_{r \leftarrow \mathcal{D}}[\mu(\mathbf{b} \mid r)].$$

We define $\mathsf{util}_i(\mathbf{b} \mid r)$ analogously as user i's honest expected utility conditioned on randomness r used in the inclusion rule when the input bid vector is $\mathbf{b}$. Value-indexed utilities such as $\widetilde{\mathsf{util}}_v(\mathbf{b})$ are used only when v is unique in $\mathbf{b}$. Let

$$W(\mathbf{b}) \colon = \{i \in [n] : \mathsf{util}_i(\mathbf{b}) > 0\}$$

to be the set of users whose honest expected utility is strictly positive under the bid vector $\mathbf{b}$.

Lemma 4.9. *Suppose a TFM $(\mathbf{I}, \mathbf{C}, \mathbf{P}, \mathbf{R})$ satisfies weak 1-CRHP in the plain model. For any bid vector $\mathbf{b} = (b_1, \ldots, b_n)$ where there exists a unique b_i in $\mathbf{b}$ such that $\mathsf{util}_i(\mathbf{b}) > 0$, for all unique b_j in $\mathbf{b}$ where $b_j > \frac{p_i(\mathbf{b})}{x_i(\mathbf{b})}$, we have $x_j(\mathbf{b}) > 0$.*

In words, if there is a unique bid b_i in $\mathbf{b}$ with positive utility, all unique bids greater than the ratio $p_i(\mathbf{b})/x_i(\mathbf{b})$ must have positive confirmation probability as well.

Proof. Seeking contradiction, suppose there exists a bid vector $\mathbf{b} = (b_1, \ldots, b_n)$ where b_i is a unique bid in $\mathbf{b}$ and $\mathsf{util}_i(\mathbf{b}) > 0$, but $x_j(\mathbf{b}) = 0$ for some unique $b_j > \frac{p_i(\mathbf{b})}{x_i(\mathbf{b})}$ in $\mathbf{b}$.

Consider a world where $\mathbf{b}$ is the honest bid vector. Consider a coalition consisting of user j with true value b_j and the miner, whose joint expected utility in the honest case equals $\mu(\mathbf{b})$. The coalition can perform the following strategy:

- The miner ignores the bid b_i from user i;
- User j changes its bid to b_i and injects a fake bid of value b_j under an arbitrary fake identity.
- The miner performs the honest inclusion rule on the remaining bids.

Because the bids b_i and b_j are unique, by weak symmetry, the fake bid at b_j will not be confirmed, while user j's real bid at b_i will have positive confirmation probability with expected payment $p_i(\mathbf{b})$. Under the deviation, the coalition's joint utility equals

$$\mu(\mathbf{b}) + b_j \cdot x_i(\mathbf{b}) - p_i(\mathbf{b}) > \mu(\mathbf{b}) + \frac{p_i(\mathbf{b})}{x_i(\mathbf{b})} \cdot x_i(\mathbf{b}) - p_i(\mathbf{b}) = \mu(\mathbf{b}),$$

where the rightmost expression is the coalition's expected joint utility in the honest case. However, user i in the honest case has positive utility, but is now unconfirmed. Thus, this strategy increases the coalition's joint utility while harming the honest user i, contradicting weak 1-CRHP. □

Lemma 4.10. *Suppose a TFM* $(\mathbf{I}, \mathbf{C}, \mathbf{P}, \mathbf{R})$ *satisfies MIC in the plain model. Then, for any* $\mathbf{b}$*, we have* $\mu(\mathbf{b} \mid r) = \mu(\mathbf{b})$ *almost surely:*

$$\Pr_{r \leftarrow \mathcal{D}}[\mu(\mathbf{b} \mid r) = \mu(\mathbf{b})] = 1.$$

Proof. By MIC, it must be that $\mu(\mathbf{b} \mid r) \leq \mu(\mathbf{b})$ for any $r \in \Omega$. Otherwise, the miner can fix r as the randomness used in the inclusion rule instead of sampling the randomness from $\mathcal{D}$ and strictly increases its expected revenue. Since $\mu(\mathbf{b}) = \mathop{\mathbb{E}}_{r \leftarrow \mathcal{D}}[\mu(\mathbf{b} \mid r)]$, we have $\Pr_{r \leftarrow \mathcal{D}}[\mu(\mathbf{b} \mid r) = \mu(\mathbf{b})] = 1$. □

Lemma 4.11. *Suppose a TFM* $(\mathbf{I}, \mathbf{C}, \mathbf{P}, \mathbf{R})$ *satisfies MIC and weak* 1*-CRHP, and the block size is bounded by* k *in the plain model. Then, for every bid vector* $\mathbf{b} = (b_1, \ldots, b_n)$*,*

$$|W(\mathbf{b})| \leq k,$$

i.e., at most k *users can have positive expected utility under the honest mechanism.*

Proof. Assume, for the sake of contradiction, that there exists a bid vector $\mathbf{b}$ where $|W(\mathbf{b})| \geq k+1$. Since the block size is at most k, the inclusion rule cannot include more than k bids for any randomness $r \in \Omega$. Therefore, there must exists some $i \in W(\mathbf{b})$ and a set $\Omega_i := \{r \in \Omega : x_i(\mathbf{b} \mid r) = 0\}$ such that $\Pr_{r \leftarrow \mathcal{D}}[\Omega_i] > 0$, this implies that

$$\Pr_{r \leftarrow \mathcal{D}}[\mathsf{util}_i(\mathbf{b} \mid r) = 0] > 0 \tag{4}$$

Recall that by definition, $\mathsf{util}_i(\mathbf{b}) = \mathbb{E}_{r \leftarrow \mathcal{D}}[\mathsf{util}_i(\mathbf{b} \mid r)] > 0$. Together with Equation (4), this means that $\Pr_{r \leftarrow \mathcal{D}}[\Omega_i'] > 0$, where $\Omega_i' = \{r \in \Omega : \mathsf{util}_i(\mathbf{b} \mid r) > \mathsf{util}_i(\mathbf{b})\}$.

For every fixed randomness, at most k bids can be included. Thus, for each $r \in \Omega_i'$, there exists some $j \in W(\mathbf{b})$ such that $x_j(\mathbf{b} \mid r) = 0$. By the pigeonhole principle, there exists some $j^* \in W(\mathbf{b})$ such that

$$\Pr_{r \leftarrow \mathcal{D}}[\mathsf{util}_i(\mathbf{b} \mid r) > \mathsf{util}_i(\mathbf{b}) \text{ and } x_{j^*}(\mathbf{b} \mid r) = 0] > 0.$$

Define set $\Omega^* := \{r \in \Omega : \mathsf{util}_i(\mathbf{b} \mid r) > \mathsf{util}_i(\mathbf{b}) \text{ and } x_{j^*}(\mathbf{b} \mid r) = 0 \text{ and } \mu(\mathbf{b} \mid r) = \mu(\mathbf{b})\}$. By Lemma 4.10, we have $\Pr_{r \leftarrow \mathcal{D}}[\Omega^*] > 0$.

Consider the following strategy by a coalition of the miner and user i as follows: the miner picks an arbitrary randomness $r^* \in \Omega^*$ in the inclusion rule. By the choice of Ω^*, the coalition's expected joint utility becomes:

$$\mu(\mathbf{b} \mid r^*) + \mathsf{util}_i(\mathbf{b} \mid r^*) = \mu(\mathbf{b}) + \mathsf{util}_i(\mathbf{b} \mid r^*) > \mu(\mathbf{b}) + \mathsf{util}_i(\mathbf{b}),$$

which strictly improves the coalition's expected joint utility. Meanwhile, user j^*, who, in the honest case, has positive expected utility, is now excluded and receives zero utility, violating weak 1-CRHP. □

Throughout the proof, we will rely on bids having strictly positive utility. Therefore, in our argument, we often need to remove the infimum value from a set, which might have zero utility. For this purpose, we define an operator $\mathsf{rmInf}(\cdot)$. For any nonempty set $S \subseteq \mathbb{R}_{\geq 0}$, $\mathsf{rmInf}(S) = S \setminus \{\inf S\}$. Recall that for two sets S and S', we say $S \prec S'$ if $\sup S < \inf S'$.

Lemma 4.12. *Let* $(\mathbf{I}, \mathbf{C}, \mathbf{P}, \mathbf{R})$ *be a TFM that satisfies UIC, MIC, and weak* 1*-CRHP. Suppose there exists a bid vector* $\mathbf{v} = (v_1, \ldots, v_n)$ *and a sequence of sets* $S_1, \ldots, S_m \subseteq \mathbb{R}_{\geq 0}$ *such that, for every* $\mathbf{b} = (b_1, \ldots, b_m) \in S_1 \times \cdots \times S_m$*, each* b_ℓ *is unique in* $(\mathbf{v}, \mathbf{b})$ *and* $x_{b_1}(\mathbf{v}, \mathbf{b}) > 0$*. If* $|S_\ell| \geq 2$ *for all* ℓ *and* $S_1 \prec \cdots \prec S_m$*, then there exists a bid vector* $\mathbf{b}^*$ *with* $|W(\mathbf{b}^*)| \geq m$*.*

Proof. Pick an arbitrary $\mathbf{b} = (b_1, \ldots, b_m) \in \mathsf{rmInf}(S_1) \times \cdots \times \mathsf{rmInf}(S_m)$ and set $\mathbf{b}^* = (\mathbf{v}, \mathbf{b})$.

First consider b_1. Choose $\widehat{b}_1 \in S_1$ with $\widehat{b}_1 < b_1$. By assumption,

$$x_{\widehat{b}_1}(\mathbf{v}, \widehat{b}_1, b_2, \ldots, b_m) > 0.$$

Hence, by Lemma 4.5, $\mathsf{util}_{b_1}(\mathbf{b}^*) > 0$.

Now fix any $\ell > 1$, and choose $\widehat{b}_\ell \in S_\ell$ with $\widehat{b}_\ell < b_\ell$. Let $\widehat{\mathbf{b}}$ be obtained from $\mathbf{b}^*$ by replacing b_ℓ with $\widehat{b}_\ell$. Choose $\widehat{b}_1 \in S_1$ with $\widehat{b}_1 < b_1$. By assumption, the bid $\widehat{b}_1$ has positive confirmation probability when the first and ℓ-th coordinates are $\widehat{b}_1$ and $\widehat{b}_\ell$, respectively. Raising $\widehat{b}_1$ to b_1 and applying Lemma 4.5 shows that b_1 has positive utility in $\widehat{\mathbf{b}}$.

Since $S_1 \prec S_\ell$, we have

$$\widehat{b}_\ell > b_1 > \frac{p_{b_1}(\widehat{\mathbf{b}})}{x_{b_1}(\widehat{\mathbf{b}})}.$$

Thus, by Lemma 4.9, $\widehat{b}_\ell$ has positive confirmation probability in $\widehat{\mathbf{b}}$. Raising $\widehat{b}_\ell$ to b_ℓ and applying Lemma 4.5 gives $\mathsf{util}_{b_\ell}(\mathbf{b}^*) > 0$.

Therefore all $b_1, \ldots, b_m$ have positive utility in $\mathbf{b}^*$, so $|W(\mathbf{b}^*)| \geq m$. □

Our impossibility relies on the following key technical lemma.

Lemma 4.13. *Suppose a TFM $(\mathbf{I}, \mathbf{C}, \mathbf{P}, \mathbf{R})$ with block size k satisfies UIC, MIC, and 1-CRHP, and let $\mathbf{v}$ be a bid vector such that $|\mathbf{v}| \geq k+1$ and index i^* where $x_{i^*}(\mathbf{v}) > 0$. Then there exists a bid vector $\mathbf{b}^*$ such that*

$$|W(\mathbf{b}^*)| \geq k+1.$$

Combining Lemma 4.13 and Lemma 4.11, we immediately get the following impossibility result:

Theorem 4.14. *Let k denote the block size. If a TFM $(\mathbf{I}, \mathbf{C}, \mathbf{P}, \mu)$ satisfies UIC, MIC, and 1-CRHP, then it must be degenerate.*

Proof. By Lemma 4.13 and Lemma 4.11. □

4.2.1 Proof of Lemma 4.13

Suppose, for the sake of contradiction, that there exists $\mathbf{v}$ where $|\mathbf{v}| \geq k+1$ and $x_i(\mathbf{v}) > 0$ for an index $i \in [n]$. Here $n = |\mathbf{v}|$. We will prove a stronger result using induction to construct $\mathbf{b}^*$ such that $|W(\mathbf{b}^*)| \geq k+1$.

For any $m \in [k+1]$, our induction constructs a sequence of positive real numbers $\epsilon^{(1)}, ..., \epsilon^{(m)}$, a sequence of sets $S^{(1)}, \ldots, S^{(m)} \subset \mathbb{R}_{\geq 0}$ such that properties (Prop′-1)-(Prop′-3) below hold.

(Prop′-1) Each $S^{(\ell)}$ contains two values: $S^{(\ell)} = \{\alpha^{(\ell)}, \beta^{(\ell)}\}$ with $\alpha^{(\ell)} < \beta^{(\ell)}$.

(Prop′-2) $\max(\mathbf{v}) + \epsilon^{(m)} < \alpha^{(m)} < \beta^{(m)} < \alpha^{(m-1)} < \beta^{(m-1)} < \cdots < \alpha^{(1)} < \beta^{(1)}$.
This implies that $\left\{\max(\mathbf{v}) + \epsilon^{(m)}\right\} \prec S^{(m)} \prec \cdots \prec S^{(1)}$

(Prop′-3) For all $\mathbf{b} = (b_1, \ldots, b_m) \in S^{(1)} \times \cdots \times S^{(m)}$, b_m is unique in $(\mathbf{v}_{-i}, \mathbf{b})$. Moreover,

$$\widetilde{x}_{b_m}(\mathbf{v}_{-i}, \mathbf{b}) > 0 \quad \text{and} \quad \frac{\widetilde{p}_{b_m}(\mathbf{v}_{-i}, \mathbf{b})}{\widetilde{x}_{b_m}(\mathbf{v}_{-i}, \mathbf{b})} \leq \alpha^{(m)} - \epsilon^{(m)}.$$

As an implication, $\widetilde{\mathsf{util}}_{b_m}(\mathbf{v}_{-i}, \mathbf{b}) > 0$.

We first show how the lemma follows assuming that the above properties holds for any $m \in [k+1]$ and give the induction proof afterwards. Let $m = k+1$. Consider $\mathbf{v}_{-i}$ and the sequence of sets $S^{(1)}, ..., S^{(k+1)}$. By (Prop′-1), $|S^{(\ell)}| \geq 2$ for all $\ell \in [k+1]$. From (Prop′-2), we also know that $S^{(k+1)} \prec \cdots \prec S^{(1)}$, and that for $\mathbf{b} = (b_1, \ldots, b_m) \in S^{(1)} \times \cdots \times S^{(m)}$, each b_ℓ is unique in $(\mathbf{v}_{-i}, \mathbf{b})$. Furthermore, $\widetilde{x}_{b_m}(\mathbf{v}_{-i}, \mathbf{b}) > 0$ by (Prop′-3). Thus, the assumptions of Lemma 4.12 hold for $\mathbf{v}_{-i}$ and the sets $S^{(k+1)}, ..., S^{(1)}$, which means that some $\mathbf{b}^*$ exists where $|W(\mathbf{b}^*)| \geq k+1$.

Induction Proof. In the rest of the proof, we focus on the induction for proving properties (Prop′-1) - (Prop′-3). For clarity, in our induction, we use superscripts to refer to the propositions for a particular $m \in [k+1]$, i.e. $\text{(Prop′-1)}^{(m)}$ represents property (Prop′-1) for m.

Base Case: $m = 1$. Let $v^* = \max(\mathbf{v}) + 1$. Consider a bid vector $\mathbf{v}' = (\mathbf{v}_{-i}, v^*)$. Since $x_i(\mathbf{v}) > 0$, by Lemma 4.5, we know that $\mathsf{util}_i(\mathbf{v}_{-i}, v^*) > \mathsf{util}_i(\mathbf{v}) \geq 0$, and thus $\tau := \frac{p_i(\mathbf{v}')}{x_i(\mathbf{v}')} < v^*$. Define

$$\epsilon^{(1)} := \frac{1}{3}(v^* - \max(\mathbf{v}, \tau)) > 0 \quad \text{and} \quad S^{(1)} := \left\{\alpha^{(1)} = v^* - \epsilon^{(1)}, \beta^{(1)} = v^* - \frac{1}{2}\epsilon^{(1)}\right\}.$$

We now prove the properties:

- $\text{(Prop′-1)}^{(1)}$ and $\text{(Prop′-2)}^{(1)}$ are true by construction. In particular, $\alpha^{(1)} - \epsilon^{(1)} = \max(\mathbf{v}, \tau) + \epsilon^{(1)} > \max(\mathbf{v})$.
- Pick an arbitrary $b_1 \in S^{(1)}$. By Myerson's Lemma (Lemma 3.5), $\widetilde{x}_{b_1}(\mathbf{v}_{-i}, b_1) \geq x_i(\mathbf{v}) > 0$. Furthermore, we have

$$\begin{aligned} \frac{\widetilde{p}_{b_1}(\mathbf{v}_{-i}, b_1)}{\widetilde{x}_{b_1}(\mathbf{v}_{-i}, b_1)} &\leq \frac{p_i(\mathbf{v}')}{x_i(\mathbf{v}')} && \text{by Lemma 4.6} \\ &= \tau \leq \max(\mathbf{v}, \tau) \leq \alpha^{(1)} - \epsilon^{(1)}. \end{aligned}$$

  Thus, $\text{(Prop′-3)}^{(1)}$ is satisfied.

Inductive Steps: $1 < m \leq k+1$. Suppose $S^{(1)}, \ldots, S^{(m-1)}$ and $\epsilon^{(m-1)}$ are the sequence of sets and the real number respectively that satisfy $\text{(Prop′-1)}^{(m-1)}$-$\text{(Prop′-3)}^{(m-1)}$. We now construct $S^{(m)}$ and $\epsilon^{(m)}$. Recall that $\alpha^{(m-1)} = \min S^{(m-1)}$.

Claim 4.15. *For all $\mathbf{b} = (b_1, \ldots, b_{m-1}) \in S^{(1)} \times \cdots \times S^{(m-1)}$ and any $\tau \in (\alpha^{(m-1)} - \epsilon^{(m-1)}, \alpha^{(m-1)})$, let $\mathbf{b}_\tau = (\mathbf{v}_{-i}, \mathbf{b}, \tau)$. Then τ is a unique bid in $\mathbf{b}_\tau$ and $\widetilde{x}_\tau(\mathbf{b}_\tau) > 0$.*

Proof. By $\text{(Prop′-2)}^{(m-1)}$, τ and b_{m-1} are both unique bids in $\mathbf{b}_\tau$. In the rest of this proof, we focus on proving that $\widetilde{x}_\tau(\mathbf{b}_\tau) > 0$. Suppose for the sake of contradiction that $\widetilde{x}_\tau(\mathbf{b}_\tau) = 0$. We first show that

$$\widetilde{\mathsf{util}}_{b_{m-1}}(\mathbf{b}_\tau) \geq \widetilde{\mathsf{util}}_{b_{m-1}}(\mathbf{v}_{-i}, \mathbf{b}). \tag{5}$$

Suppose for the sake of contradiction that $\widetilde{\mathsf{util}}_{b_{m-1}}(\mathbf{b}_\tau) < \widetilde{\mathsf{util}}_{b_{m-1}}(\mathbf{v}_{-i}, \mathbf{b})$. Consider a world where $(\mathbf{v}_{-i}, \mathbf{b})$ is the honest input bid vector. Since $|(\mathbf{v}_{-i}, \mathbf{b})| = n + m - 2 \geq n > k$, by Lemma 4.11, there must exist some user j whose expected utility is 0 in the honest case. By $\text{(Prop′-3)}^{(m-1)}$, this user is distinct from the user bidding b_{m-1}. Now consider a coalition made up of the miner and user j that performs the following strategy: they inject a fake bid at τ, faking a world with input bid vector $\mathbf{b}_\tau$, and performs the honest mechanism on $\mathbf{b}_\tau$. The fake bid τ must be unconfirmed by assumption. In the honest case, their expected joint utility is just the expected miner revenue $\mu(\mathbf{v}_{-i}, \mathbf{b})$. The coalition's strategic utility is $\mu(\mathbf{b}_\tau) + \mathsf{util}_j(\mathbf{b}_\tau) \geq \mu(\mathbf{v}_{-i}, \mathbf{b})$ by Lemma 4.7 and individual rationality.

However, the user bidding b_{m-1} is harmed by the assumption that $\widetilde{\mathsf{util}}_{b_{m-1}}(\mathbf{b}_\tau) < \widetilde{\mathsf{util}}_{b_{m-1}}(\mathbf{v}_{-i}, \mathbf{b})$, which contradicts 1-CRHP.

Now we are ready to prove the claim statement. Consider a world where $\mathbf{b}_\tau$ is the honest bid vector. Let u denote the user whose true value is b_{m-1} and let u' denote the user who's valuation is τ. Then user u's expected utility in the honest case is

$$\widetilde{\mathsf{util}}_{b_{m-1}}(\mathbf{b}_\tau) \geq \widetilde{\mathsf{util}}_{b_{m-1}}(\mathbf{v}_{-i}, \mathbf{b}) \qquad \text{by Equation (5)} > 0 \qquad \text{by (Prop′-3)}^{(m-1)}$$

Consider a coalition made of the user u' and the miner. Since $\widetilde{x}_\tau(\mathbf{b}_\tau) = 0$ by the assumption, the coalition's expected joint utility in the honest case is simply the expected miner revenue $\mu(\mathbf{b}_\tau)$. Consider the following strategy of the coalition:

- The miner ignores the bid b_{m-1} from user u;
- User u' raises its bid to b_{m-1}. The miner then performs the honest inclusion rule on $(\mathbf{v}_{-i}, \mathbf{b})$ where the bid at b_{m-1} now comes from the coalition.

Under this strategy, the coalition's expected joint utility becomes

$$\begin{aligned}
&\mu(\mathbf{v}_{-i}, \mathbf{b}) + \left(\tau \cdot \widetilde{x}_{b_{m-1}}(\mathbf{v}_{-i}, \mathbf{b}) - \widetilde{p}_{b_{m-1}}(\mathbf{v}_{-i}, \mathbf{b})\right) \\
&> \mu(\mathbf{v}_{-i}, \mathbf{b}) + \left(\alpha^{(m-1)} - \epsilon^{(m-1)}\right) \cdot \widetilde{x}_{b_{m-1}}(\mathbf{v}_{-i}, \mathbf{b}) - \widetilde{p}_{b_{m-1}}(\mathbf{v}_{-i}, \mathbf{b}) && \text{by choice of } \tau \\
&\geq \mu(\mathbf{v}_{-i}, \mathbf{b}) + \left(\frac{\widetilde{p}_{b_{m-1}}(\mathbf{v}_{-i}, \mathbf{b})}{\widetilde{x}_{b_{m-1}}(\mathbf{v}_{-i}, \mathbf{b})}\right) \cdot \widetilde{x}_{b_{m-1}}(\mathbf{v}_{-i}, \mathbf{b}) - \widetilde{p}_{b_{m-1}}(\mathbf{v}_{-i}, \mathbf{b}) && \text{by (Prop′-3)}^{(m-1)} \\
&= \mu(\mathbf{v}_{-i}, \mathbf{b}) \geq \mu(\mathbf{b}_\tau) && \text{by Lemma 4.8}
\end{aligned}$$

The last step comes from the assumption that $\widetilde{x}_\tau(\mathbf{b}_\tau) = 0$. This strategy strictly benefits the coalition while harming honest user u, which contradicts 1-CRHP. □

Let $q = n+m-1$ denote the final bidder in the concatenated vector $(\mathbf{v}_{-i}, \mathbf{b}, t)$; keep this bidder's identity fixed as its bid t varies. Consider the value

$$\delta := \min_{\mathbf{b} \in S^{(1)} \times \cdots \times S^{(m-1)}} \left(\alpha^{(m-1)} - \frac{p_q(\mathbf{v}_{-i}, \mathbf{b}, \alpha^{(m-1)})}{x_q(\mathbf{v}_{-i}, \mathbf{b}, \alpha^{(m-1)})}\right). \tag{6}$$

By claim 4.15 and Lemma 4.5, $\frac{p_q(\mathbf{v}_{-i}, \mathbf{b}, \alpha^{(m-1)})}{x_q(\mathbf{v}_{-i}, \mathbf{b}, \alpha^{(m-1)})} < \alpha^{(m-1)}$ for all $\mathbf{b} \in S^{(1)} \times \cdots \times S^{(m-1)}$. Indeed, raising this bidder's bid from any $t \in (\alpha^{(m-1)} - \epsilon^{(m-1)}, \alpha^{(m-1)})$ to $\alpha^{(m-1)}$ strictly increases its nonnegative utility. This uses the fixed index q even when $\alpha^{(m-1)} = b_{m-1}$, so it does not assume equal treatment of tied bids. Since there is only a finite number of possible $\mathbf{b}$ by $\text{(Prop′-1)}^{(m-1)}$, we have $\delta > 0$. Define

$$\epsilon^{(m)} := \frac{1}{2}\min\left(\delta, \epsilon^{(m-1)}\right) \quad \text{and} \quad S^{(m)} := \left\{\alpha^{(m)} = \alpha^{(m-1)} - \epsilon^{(m)}, \beta^{(m)} = \alpha^{(m-1)} - \frac{1}{2}\epsilon^{(m)}\right\}$$

- $\text{(Prop′-1)}^{(m)}$ follows by construction.
- By construction, $\beta^{(m)} < \alpha^{(m-1)}$. Moreover,

$$\begin{aligned}
\alpha^{(m)} = \alpha^{(m-1)} - \epsilon^{(m)} &> \max(\mathbf{v}) + \epsilon^{(m-1)} - \epsilon^{(m)} && \text{by (Prop′-2)}^{(m-1)} \\
&\geq \max(\mathbf{v}) + \epsilon^{(m)}. && \text{by choice of } \epsilon^{(m)}
\end{aligned}$$

  $\text{(Prop′-2)}^{(m)}$ thus follows by combining $\max(\mathbf{v}) + \epsilon^{(m)} < \alpha^{(m)} < \beta^{(m)} < \alpha^{(m-1)}$ and $\text{(Prop′-2)}^{(m-1)}$.

- Let $\mathbf{b} = (b_1, \ldots, b_m) \in S^{(1)} \times \cdots \times S^{(m)}$. By claim 4.15, $\widetilde{x}_{b_m}(\mathbf{v}_{-i}, \mathbf{b}) > 0$. Furthermore, we have

$$\begin{aligned}
\frac{\widetilde{p}_{b_m}(\mathbf{v}_{-i}, \mathbf{b})}{\widetilde{x}_{b_m}(\mathbf{v}_{-i}, \mathbf{b})} &\leq \frac{p_q(\mathbf{v}_{-i}, \mathbf{b}_{-m}, \alpha^{(m-1)})}{x_q(\mathbf{v}_{-i}, \mathbf{b}_{-m}, \alpha^{(m-1)})} && \text{by Lemma 4.6} \\
&\leq \alpha^{(m-1)} - \delta && \text{by Equation (6)} \\
&\leq \alpha^{(m-1)} - 2\epsilon^{(m)} = \alpha^{(m)} - \epsilon^{(m)}. && \text{by choice of } \epsilon^{(m)}
\end{aligned}$$

  Thus, (Prop′-3)$^{(m)}$ is satisfied.

Corollary 4.16. *Let k denote the block size. If a TFM $(\mathbf{I}, \mathbf{C}, \mathbf{P}, \mu)$ satisfies UIC, MIC, and 1-CRHP, then the miner revenue must be zero, i.e., $\mu(\mathbf{b}) = 0$ for any $\mathbf{b}$.*

Proof. Seeking contradiction, suppose that there was a transaction fee mechanism $(\mathbf{I}, \mathbf{C}, \mathbf{P}, \mathbf{R})$ that satisfies UIC, MIC, and 1-CRHP, and has finite block size k, and for a bid vector $\mathbf{b}$, $\mu(\mathbf{b}) > 0$. Now consider $\mathbf{b}' = (\mathbf{b}, \underbrace{0, \ldots, 0}_{k+1}) = (b'_1, \ldots, b'_n)$. By Lemma 4.7, $\mu(\mathbf{b}') \geq \mu(\mathbf{b}) > 0$. Thus, by budget feasibility (see Section 3.2), there exists $i \in [n]$ where $x_i(\mathbf{b}') > 0$. Additionally, $n > k$, so by Theorem 4.14, this is impossible, leading to a contradiction. □

4.3 Impossibility Under Weak-CRHP

In this section, we present the proof of the stronger impossibility result under weak-CRHP. The proof relies on the following technical lemma.

Lemma 4.17. *Suppose a TFM $(\mathbf{I}, \mathbf{C}, \mathbf{P}, \mathbf{R})$ satisfies UIC, MIC, and weak 1-CRHP, and let $\mathbf{v}$ be a bid vector such that $\mu(\mathbf{v}) > 0$. Then, there exists a bid vector $\mathbf{b}^*$ such that*

$$|W(\mathbf{b}^*)| > k.$$

Combining Lemma 4.17 and Lemma 4.11, we immediately get the following impossibility result:

Theorem 4.18 (Restatement of Theorem 1.3)**.** *Let k denote the block size. If a TFM $(\mathbf{I}, \mathbf{C}, \mathbf{P}, \mathbf{R})$ satisfies UIC, MIC, and weak 1-CRHP, then miner revenue must be zero, i.e. $\mu(\mathbf{b}) = 0$ for any $\mathbf{b}$.*

Proof. Note that Lemma 4.11 holds for weak 1-CRHP TFMs. The theorem thus follows from Lemma 4.17 and Lemma 4.11. □

Proof of Lemma 4.17 As with previous proofs, we start with a bid vector $\mathbf{v} = (v_1, \ldots, v_n)$ such that $\mu(\mathbf{v}) > 0$ and construct inductively a sequence of sets of vectors, such that in the m-th step, we can obtain a vector $\mathbf{b}^{(m)}$ such that $|W(\mathbf{b}^{(m)})| \geq m$. Then when $m = k + 1$, this contradicts Lemma 4.11. To aide in our proof, we utilize the following implication of Erdős's corollary [Erd64, Corollary, p. 188] to determine the size of our sets.

Lemma 4.19. *(from [Erd64, Corollary, p. 188]) For all positive integers p, a and all $\xi \in (0, 1]$ there exists N such that, if $G \subseteq A_1 \times \cdots \times A_p$, $|A_i| = N$ for each i, and if $|G| \geq \xi N^p$, then there exist subsets $B_i \subseteq A_i$ with $|B_i| \geq a$ such that*

$$B_1 \times \cdots \times B_p \subseteq G.$$

Like in the proof of Lemma 4.13, in each inductive step, we build a sequence of sets $S_1^{(m)}, ..., S_m^{(m)}$, each of size at least two. To ensure that we can pick sets of size at least two in step $k+1$, we define the following sequence N_m for $m \in [k+2]$ backwards:

$$\begin{aligned} &N_{k+2} := 2, \\ &N_m := N \text{ in Lemma 4.19 with } (p = k+m-1,\ \xi = \tfrac{1}{n+m\cdot k},\ a = N_{m+1}),\ \text{for } 1 \le m \le k+1. \end{aligned} \tag{7}$$

Specifically, for any $m \in [k+1]$, we construct a sequences of sets $S_1^{(m)}, \ldots, S_m^{(m)}$, bid vectors $\mathbf{v}^{(m)}$, and real numbers $\epsilon^{(m)}$ such that they satisfy the properties listed in (Prop*-1)–(Prop*-5) below.

(Prop*-1) For all $\ell \in [m]$, $|S_\ell^{(m)}| = N_{m+1}$.

(Prop*-2) $\mathbf{v} \subseteq \mathbf{v}^{(1)} \subseteq \cdots \subseteq \mathbf{v}^{(m)}$, and $|\mathbf{v}^{(m)}| = n + (k-1)m$.

(Prop*-3) For $m \ge 2$ and $\ell \in [m-1]$,

$$S_\ell^{(m)} \subseteq S_\ell^{(m-1)} \subseteq ... \subseteq S_\ell^{(\ell)}.$$

(Prop*-4) $S_m^{(m)} \prec \cdots \prec S_1^{(m)}$. Furthermore,

$$\max(\mathbf{v}^{(m)}) \le \min S_m^{(m)} - \epsilon^{(m)}$$

(Prop*-5) Fix any $\ell \in [m]$ and let $\mathbf{b} = (b_1, \ldots, b_\ell) \in S_1^{(m)} \times \cdots \times S_\ell^{(m)}$. Then, the following hold:

$$\widetilde{x}_{b_\ell}\left(\mathbf{v}^{(\ell)}, \mathbf{b}\right) > 0, \quad \text{and} \quad \frac{\widetilde{p}_{b_\ell}\left(\mathbf{v}^{(\ell)}, \mathbf{b}\right)}{\widetilde{x}_{b_\ell}\left(\mathbf{v}^{(\ell)}, \mathbf{b}\right)} \le \min S_m^{(m)} - \epsilon^{(m)}.$$

We first show how the lemma follows assuming that the above properties holds for any $m \in [k+1]$ and give the induction proof afterwards. Let $m = k+1$. Consider $\mathbf{v}^{(k+1)}$ and the sequence of sets $S_1^{(k+1)}, ..., S_{k+1}^{(k+1)}$. By (Prop*-1) and Equation (7), $|S_\ell^{(k+1)}| \ge 2$ for all $\ell \in [k+1]$. From (Prop*-4), we also know that $S_{k+1}^{(k+1)} \prec \cdots \prec S_1^{(k+1)}$, and that for $\mathbf{b} = (b_1, \ldots, b_m) \in S_1^{(k+1)} \times \cdots \times S_{k+1}^{(k+1)}$, each b_ℓ is unique in $(\mathbf{v}^{(k+1)}, \mathbf{b})$. Furthermore, $\widetilde{x}_{b_m}(\mathbf{v}^{(k+1)}, \mathbf{b}) > 0$ by (Prop*-5) with $\ell = m = k+1$. By weak symmetry, we may reorder these unique bids in increasing order of their sets. Thus, the assumptions of Lemma 4.12 hold for $\mathbf{v}^{(k+1)}$ and the sets $S_{k+1}^{(k+1)}, ..., S_1^{(k+1)}$, which means that some $\mathbf{b}^*$ exists where $|W(\mathbf{b}^*)| \ge k+1$.

Induction Proof. In the rest of the proof, we focus on the induction for proving properties (Prop*-1) - (Prop*-5). For clarity, in our induction, we use superscripts to refer to the propositions for a particular $m \in [k+1]$, i.e. (Prop*-1)$^{(m)}$ represents property (Prop*-1) for m.

Base Case: $m = 1$. Define a sequence of sets A_z for $z \in [k]$ such that

$$\{\max(\mathbf{v}) + z + 1\} \prec A_z \prec \{\max(\mathbf{v}) + z + 2\}$$

and $|A_z| = N_1$ for all $z \in [k]$. By construction $A_1 \prec \cdots \prec A_k$. We define $\phi(\cdot)$ to select a lowest-valued bid among those with positive confirmation probability, breaking ties by the index:

$$\phi\left(\widehat{\mathbf{b}}\right) := \min\left\{ i : x_i(\widehat{\mathbf{b}}) > 0 \text{ and } \widehat{b}_i = \min_{j : x_j(\widehat{\mathbf{b}}) > 0} \widehat{b}_j \right\}. \tag{8}$$

Consider the bid vector $(\mathbf{v}, \mathbf{v}')$ for $\mathbf{v}' \in A_1 \times \cdots \times A_k$. By Lemma 4.7, $\mu(\mathbf{v}, \mathbf{v}') \geq \mu(\mathbf{v}) > 0$, and therefore, by budget feasibility, there exists an index i such that $x_i(\mathbf{v}, \mathbf{v}') > 0$. Thus, $\phi(\mathbf{v}, \mathbf{v}')$ is well defined. The $n+k$ possible values of $\phi(\mathbf{v}, \mathbf{v}')$ naturally give the following partition of $A_1 \times \cdots \times A_k$:

$$T_i := \left\{\mathbf{v}' \in A_1 \times \cdots \times A_k : \phi(\mathbf{v}, \mathbf{v}') = i\right\}$$

for $i \in [n+k]$.

Since this is a partition of k sets $A_1, \ldots, A_k$ all of size N_1, there must exist a smallest index i^* such that $|T_{i^*}| \geq \frac{1}{n+k} \cdot N_1^k$. By Lemma 4.19 and the definition of N_1 and N_2, we know that there exists subsets $B_z \subseteq A_z$ for all $z \in [k]$ with $|B_z| = N_2$ such that $B_1 \times \cdots \times B_k \subseteq T_{i^*}$.

Claim 4.20. $i^* > n$.

Proof. Suppose for the sake of contradiction that $i^* \leq n$. Choose a two-element set $V \subset (v_{i^*}, \min B_1) \setminus \{v_1, \ldots, v_n\}$. This is possible because $\min B_1 > \max(\mathbf{v})$, and gives $V \prec B_1$. From Myerson's Lemma (Lemma 3.5), for $\mathbf{v}' \in B_1 \times \cdots \times B_k$ and $v^* \in V$, $x_{i^*}((\mathbf{v}_{-i^*}, v^*), \mathbf{v}') \geq x_{i^*}(\mathbf{v}, \mathbf{v}') > 0$ where the last step comes from the definition of i^*. Thus, by construction, the hypothesis of Lemma 4.12 is satisfied with respect to $\mathbf{v}_{-i^*}$ and the sets $V, B_1, \ldots, B_k$, and we can conclude that there exists $\mathbf{b}^*$ such that $|W(\mathbf{b}^*)| \geq k+1$, which contradicts Lemma 4.11. □

Thus, we know that for every bid vector $(\mathbf{v}, \widehat{\mathbf{v}})$ where $\widehat{\mathbf{v}} \in B_1 \times \cdots \times B_k \subseteq T_{i^*}$, we have $x_{i^*}(\mathbf{v}, \widehat{\mathbf{v}}) > 0$, so the bid falls in $B_{i^*-n} \subseteq A_{i^*-n}$ has a positive confirmation probability. Pick an arbitrary $\widehat{\mathbf{v}} \in B_1 \times \cdots \times B_k \subseteq T_{i^*}$. Let $v^* = \max(\mathbf{v}) + k + 3 > \widehat{v}_{i^*-n}$. Consider a bid vector $\mathbf{v}^* = ((\mathbf{v}, \widehat{\mathbf{v}})_{-i^*}, v^*)$. Since $x_{i^*}(\mathbf{v}, \widehat{\mathbf{v}}) > 0$, by Lemma 4.5, we know that $\mathsf{util}_{i^*}(\mathbf{v}^*) > \mathsf{util}_{i^*}(\mathbf{v}, \widehat{\mathbf{v}}) \geq 0$, and thus $\tau := \frac{p_{i^*}(\mathbf{v}^*)}{x_{i^*}(\mathbf{v}^*)} < v^*$. We define the following:

- $\mathbf{v}^{(1)} := (\mathbf{v}, \widehat{\mathbf{v}})_{-i^*}$;
- $\epsilon^{(1)} := \frac{1}{2}(v^* - \max\{\max A_k, \tau\}) > 0$;
- $S_1^{(1)}$ s.t. $\left\{v^* - \epsilon^{(1)}\right\} \prec S_1^{(1)} \prec \{v^*\}$ and $|S_1^{(1)}| = N_2$.

We now prove the properties:

- (Prop*-1)$^{(1)}$ and (Prop*-2)$^{(1)}$ follow by construction.
- (Prop*-3)$^{(1)}$ is trivially satisfied.
- (Prop*-4)$^{(1)}$ follows from construction and the fact that

$$\begin{aligned} \min S_1^{(1)} - \epsilon^{(1)} &> v^* - 2\epsilon^{(1)} \\ &= \max\{\max A_k, \tau\} \\ &\geq \max(\mathbf{v}^{(1)}). \end{aligned}$$

- (Prop*-5)$^{(1)}$, note that for any $b_1 \in S_1^{(1)}$, and $b' \in B_{i^*-n}$, we know that $b_1 > v^* - \epsilon^{(1)} > \max A_k \geq b'$. Reinserting b' into $\mathbf{v}^{(1)}$ gives, up to a permutation, a vector in $\{\mathbf{v}\} \times B_1 \times \cdots \times B_k$, so weak symmetry and the definition of T_{i^*} imply that this bid has positive confirmation probability. Thus,

$$\begin{aligned} \widetilde{x}_{b_1}(\mathbf{v}^{(1)}, b_1) &\geq \widetilde{x}_{b'}(\mathbf{v}^{(1)}, b') && \text{by Myerson's Lemma (Lemma 3.5)} \\ &> 0. && \text{by definition of } i^* \end{aligned}$$

Furthermore,

$$\begin{aligned}\frac{\widetilde{p}_{b_1}(\mathbf{v}^{(1)}, b_1)}{\widetilde{x}_{b_1}(\mathbf{v}^{(1)}, b_1)} &\leq \frac{\widetilde{p}_{v^*}(\mathbf{v}^{(1)}, v^*)}{\widetilde{x}_{v^*}(\mathbf{v}^{(1)}, v^*)} && \text{by Lemma 4.6}\\ &= \tau \\ &\leq \max\{\max A_k, \tau\} \\ &\leq \min S_1^{(1)} - \epsilon^{(1)}.\end{aligned}$$

Thus, (Prop*-5)$^{(1)}$ is satisfied.

Inductive Step: $m > 1$. Suppose $S_1^{(m-1)}, \ldots, S_{m-1}^{(m-1)}$, $\mathbf{v}^{(1)}, \ldots, \mathbf{v}^{(m-1)}$, and $\epsilon^{(m-1)}$ are the sequences of sets, bid vectors, and the real number respectively that satisfy (Prop*-1)$^{(m-1)}$-(Prop*-5)$^{(m-1)}$. For simplicity, let $\gamma := \min S_{m-1}^{(m-1)}$, and

$$\alpha := \gamma - \epsilon^{(m-1)}, \quad \Delta := \frac{\epsilon^{(m-1)}}{k+2}. \tag{9}$$

Then for $z \in [k]$, redefine A_z such that

$$\{\alpha + z \cdot \Delta\} \prec A_z \prec \{\alpha + (z+1) \cdot \Delta\} \tag{10}$$

and $|A_z| = N_m$ for $z \in [k]$. By construction, we have $A_1 \prec \cdots \prec A_k$.

Consider the bid vector $\mathbf{v}^* = (\mathbf{v}^{(m-1)}, \mathbf{v}')$ where $\mathbf{v}' \in \left(\prod_{z=1}^k A_z\right) \times \left(\prod_{\ell=1}^{m-1} S_\ell^{(m-1)}\right)$. Then $|\mathbf{v}^*| = n + k \cdot m$. Recall the definition of $\phi(\cdot)$ from Equation (8). Again, by Lemma 4.7 and (Prop*-2)$^{(m-1)}$, $\mu(\mathbf{v}^*) \geq \mu(\mathbf{v}) > 0$. Therefore, by budget feasibility, there exists $i \in [n + k \cdot m]$ such that $x_i(\mathbf{v}^*) > 0$, and thus, $\phi(\mathbf{v}^*)$ is well defined. The $n + m \cdot k$ possible values of $\phi(\mathbf{v}^*)$ naturally give the following partition of $\left(\prod_{z=1}^k A_z\right) \times \left(\prod_{\ell=1}^{m-1} S_\ell^{(m-1)}\right)$.

$$T_i := \left\{\mathbf{v}' \in \left(\prod_{z=1}^{k} A_z\right) \times \left(\prod_{\ell=1}^{m-1} S_\ell^{(m-1)}\right) : \phi(\mathbf{v}^{(m-1)}, \mathbf{v}') = i\right\}$$

for $i \in [n + k \cdot m]$. The sequence $\{T_i\}_{i \in [n+k\cdot m]}$ is a partition of the product of $k + m - 1$ sets $A_1, \ldots, A_k, S_1, \ldots S_{m-1}$, each of size N_m by (Prop*-1)$^{(m-1)}$. Thus, by the pigeon hole principle, let i^* be the smallest index such that $|T_{i^*}| \geq \frac{1}{n+m\cdot k} \cdot N_m^{k+m-1}$. By Lemma 4.19 and the definitions of N_m and N_{m+1}, there exist subsets

$$B_z \subseteq A_z \text{ for all } z \in [k], \quad \text{and} \quad B_z \subseteq S_{z-k}^{(m-1)} \text{ for all } z \in \{k+1, \ldots, k+m-1\},$$

each satisfying $|B_z| = N_{m+1}$, such that

$$B_1 \times \cdots \times B_{k+m-1} \subseteq T_{i^*}.$$

Note that in any vector $\mathbf{v}^* = (\mathbf{v}^{(m-1)}, \mathbf{v}')$ where $\mathbf{v}' \in \left(\prod_{z=1}^k A_z\right) \times \left(\prod_{\ell=1}^{m-1} S_\ell^{(m-1)}\right)$, the indices can be understood as follows:

- The bids $\mathbf{v}_i^*$ for $1 \leq i \leq n + (k-1)(m-1)$ come from $\mathbf{v}^{(m-1)}$: $\mathbf{v}_i^* = \mathbf{v}_i^{(m-1)}$.
- The bids $\mathbf{v}_i^*$ for $n + (k-1) \cdot (m-1) + 1 \leq i \leq n + (k-1) \cdot (m-1) + k$ come from $A_1 \times \cdots \times A_k$: $\mathbf{v}_i^* \in A_{i-n-(k-1)(m-1)}$.

- The bids $\mathbf{v}_i^*$ for $n + (k-1)\cdot(m-1) + k + 1 \le i \le n + k \cdot m$ come from $S_1^{(m-1)} \times \cdots \times S_{m-1}^{(m-1)}$: $\mathbf{v}_i^* \in S_{i-n-(k-1)(m-1)-k}^{(m-1)}$.

Let $L := n + (k-1)\cdot(m-1)$ and $R := n + (k-1)\cdot(m-1) + k$ be the left and right boundary indices of bids that come from A_1 through A_k.

Claim 4.21. $L < i^*$.

Proof. Suppose for the sake of contradiction that $i^* \le L$. Let $\mathbf{b} = (b_1, \ldots, b_{m-1}) \in B_{k+1} \times \cdots \times B_{k+m-1}$, and choose a two-element set $V \subset (\mathbf{v}_{i^*}^{(m-1)}, \min B_1) \setminus \{\mathbf{v}_1^{(m-1)}, \ldots, \mathbf{v}_L^{(m-1)}, b_1, \ldots, b_{m-1}\}$. This is possible because $\min B_1 > \max(\mathbf{v}^{(m-1)})$, and gives $V \prec B_1$. Raising bid i^* to any value in V preserves its positive confirmation probability by Myerson's Lemma. Similarly to the base case, by construction, the hypothesis of Lemma 4.12 is satisfied w.r.t $(\mathbf{v}_{-i^*}^{(m-1)}, b_1, \ldots, b_{m-1})$ and the sets $V, B_1, \ldots, B_k$. Thus, we can conclude that there exists $\mathbf{b}^*$ such that $|W(\mathbf{b}^*)| > k$, which contradicts Lemma 4.11. □

Claim 4.22. $i^* \le R$.

Proof. Suppose, for the sake of contradiction, that $i^* > R$. Let $j^* := i^* - R$, so the bid selected by $\phi(\cdot)$ comes from $S_{j^*}^{(m-1)}$. Pick

$$\mathbf{v}' = (a_1, \ldots, a_k, b_1, \ldots, b_{m-1}) \in \prod_{z=1}^{k+m-1} \mathsf{rmInf}(B_z).$$

In particular, $b_{j^*} \in \mathsf{rmInf}(B_{k+j^*})$. Since $B_1 \times \cdots \times B_{k+m-1} \subseteq T_{i^*}$, the bid b_{j^*} has positive confirmation probability for every choice of the coordinates from the corresponding B_z's. If we replace b_{j^*} by $\min B_{k+j^*}$ while keeping all other bids fixed, the resulting bid vector is still in T_{i^*}, so this lower bid also has positive confirmation probability. Therefore, by Lemma 4.5, user i^* has strictly positive utility at bid b_{j^*}.

Consider the world where $(\mathbf{v}^{(m-1)}, \mathbf{v}')$ is the honest bid vector. Let u be the user with bid a_k. By Equation (10) and (Prop*-4)$^{(m-1)}$, we have $a_k < b_{j^*}$.

Since $\phi(\mathbf{v}^{(m-1)}, \mathbf{v}') = i^*$ selects a lowest-valued bid with positive confirmation probability, user u must have zero confirmation probability in the honest execution. Thus, the coalition consisting of the miner and user u has honest joint utility

$$\mu(\mathbf{v}^{(m-1)}, \mathbf{v}').$$

Now consider the following deviation. The miner censors:

- the bid b_{j^*} from user i^*;
- the bids $a_1, \ldots, a_{k-1}$;
- all bids in $\mathbf{v}^{(m-1)}$ that are not in $\mathbf{v}^{(j^*)}$;
- all bids b_ℓ for $\ell \in \{j^*+1, \ldots, m-1\}$.

User u changes its bid from a_k to b_{j^*}, and the miner then performs the honest inclusion rule on the resulting bid vector

$$\mathbf{v}^* = (\mathbf{v}^{(j^*)}, b_1, \ldots, b_{j^*}).$$

We first compare miner revenue. Except for the bid b_{j^*}, which is replaced by user u's bid of the same amount, every bid removed by the deviation has value strictly smaller than b_{j^*}. For the bids $a_1, \ldots, a_{k-1}$ this follows from Equation (10); for $b_{j^*+1}, \ldots, b_{m-1}$ it follows from (Prop*-4)$^{(m-1)}$; and for the bids in $\mathbf{v}^{(m-1)} \setminus \mathbf{v}^{(j^*)}$ it follows from (Prop*-2) and (Prop*-4) applied to the subsequent inductive steps.

Since $\phi(\mathbf{v}^{(m-1)}, \mathbf{v}') = i^*$ selects a lowest-valued bid with positive confirmation probability, all these strictly lower bids have zero confirmation probability, and hence zero payment. Replacing the original bid b_{j^*} by user u's bid of the same amount does not change the mechanism outcome by weak symmetry. Therefore, by Lemma 4.8,

$$\mu(\mathbf{v}^*) \geq \mu(\mathbf{v}^{(m-1)}, \mathbf{v}').$$

Conversely, $\mathbf{v}^*$ is a subvector of $(\mathbf{v}^{(m-1)}, \mathbf{v}')$ in bid amounts, so Lemma 4.7 gives

$$\mu(\mathbf{v}^*) \leq \mu(\mathbf{v}^{(m-1)}, \mathbf{v}').$$

Hence $\mu(\mathbf{v}^*) = \mu(\mathbf{v}^{(m-1)}, \mathbf{v}')$.

It remains to consider user u's utility. Since $(b_1, \ldots, b_{j^*}) \in S_1^{(m-1)} \times \cdots \times S_{j^*}^{(m-1)}$, (Prop*-5)$^{(m-1)}$ gives

$$\frac{\widetilde{p}_{b_{j^*}}(\mathbf{v}^*)}{\widetilde{x}_{b_{j^*}}(\mathbf{v}^*)} \leq \gamma - \epsilon^{(m-1)}.$$

Moreover, by Equation (10), we have $a_k > \gamma - \epsilon^{(m-1)}$. Therefore,

$$a_k \widetilde{x}_{b_{j^*}}(\mathbf{v}^*) - \widetilde{p}_{b_{j^*}}(\mathbf{v}^*) > (\gamma - \epsilon^{(m-1)})\widetilde{x}_{b_{j^*}}(\mathbf{v}^*) - \widetilde{p}_{b_{j^*}}(\mathbf{v}^*) \geq 0.$$

Thus user u obtains strictly positive utility under the deviation, while the miner revenue is unchanged. The coalition therefore strictly increases its joint utility.

At the same time, user i^* had strictly positive utility in the honest execution and its bid is censored by the deviation. This contradicts weak 1-CRHP. □

By claim 4.21 and claim 4.22, for every $(\mathbf{v}^{(m-1)}, \mathbf{v}')$ where $\mathbf{v}' \in B_1 \times \cdots \times B_{k+m-1} \subseteq T_{i^*}$, we know that a bid with positive confirmation probability exists within the set $B_{i^*-L} \subseteq A_{i^*-L}$. Pick an arbitrary $\widehat{\mathbf{v}} \in B_1 \times \cdots \times B_k$, and define $\mathbf{v}^{(m)} = \left(\mathbf{v}^{(m-1)}, \widehat{\mathbf{v}}\right)_{-i^*}$.

Recall that $\gamma := \min S_{m-1}^{(m-1)}$. Consider the value

$$\delta := \min_{\mathbf{b} \in B_{k+1} \times \cdots \times B_{k+m-1}} \left(\gamma - \frac{p_R(\mathbf{v}^{(m)}, \gamma, \mathbf{b})}{x_R(\mathbf{v}^{(m)}, \gamma, \mathbf{b})} \right). \tag{11}$$

We show that $\delta > 0$. Fix any $\mathbf{b} \in B_{k+1} \times \cdots \times B_{k+m-1}$. Choose γ' such that $\max A_k < \gamma' < \gamma$. Since $B_1 \times \cdots \times B_{k+m-1} \subseteq T_{i^*}$, the bid at index i^* has positive confirmation probability in $(\mathbf{v}^{(m-1)}, \widehat{\mathbf{v}}, \mathbf{b})$. This bid comes from one of $A_1, \ldots, A_k$, so its value is smaller than γ'. By Lemma 4.5, raising this bid to γ' gives it strictly positive utility. The resulting bid vector is a permutation of $(\mathbf{v}^{(m)}, \gamma', \mathbf{b})$, so by weak symmetry, the bid γ' at index R has strictly positive utility in $(\mathbf{v}^{(m)}, \gamma', \mathbf{b})$.

Since $\gamma > \gamma'$, Lemma 4.5 further implies that the bid γ at index R has strictly positive utility in $(\mathbf{v}^{(m)}, \gamma, \mathbf{b})$. Therefore,

$$\frac{p_R(\mathbf{v}^{(m)}, \gamma, \mathbf{b})}{x_R(\mathbf{v}^{(m)}, \gamma, \mathbf{b})} < \gamma.$$

This holds for every $\mathbf{b} \in B_{k+1} \times \cdots \times B_{k+m-1}$. Since this set is finite, we have $\delta > 0$. Thus, we can define the following:

- $\mathbf{v}^{(m)} = \left(\mathbf{v}^{(m-1)}, \widehat{\mathbf{v}}\right)_{-i^*}$;
- $S_1^{(m)}, \ldots, S_{m-1}^{(m)} = B_{k+1}, \ldots, B_{k+m-1}$;
- $\epsilon^{(m)} := \frac{1}{2}\min(\delta, \Delta)$;
- $S_m^{(m)}$ s.t. $\{\gamma - \epsilon^{(m)}\} \prec S_m^{(m)} \prec \{\gamma\}$ and $|S_m^{(m)}| = N_{m+1}$.

We now prove the properties:

- (Prop*-1)$^{(m)}$, (Prop*-2)$^{(m)}$, and (Prop*-3)$^{(m)}$ are satisfied by construction.
- (Prop*-4)$^{(m)}$ follows from construction. Since $S_\ell^{(m)} = B_{k+\ell} \subseteq S_\ell^{(m-1)}$ for every $\ell \in [m-1]$ and $S_m^{(m)} \prec \{\gamma\} \preceq S_{m-1}^{(m)}$, we have $S_m^{(m)} \prec \cdots \prec S_1^{(m)}$. Moreover, by (Prop*-4)$^{(m-1)}$ and Equation (10),

  $$\max(\mathbf{v}^{(m)}) \leq \max A_k < \gamma - \Delta.$$

  Since $2\epsilon^{(m)} \leq \Delta$ and $\min S_m^{(m)} > \gamma - \epsilon^{(m)}$, we have

  $$\max(\mathbf{v}^{(m)}) < \gamma - \Delta \leq \gamma - 2\epsilon^{(m)} < \min S_m^{(m)} - \epsilon^{(m)}.$$

  Thus, (Prop*-4)$^{(m)}$ holds.
- We first consider $\ell \in [m-1]$. Since $S_z^{(m)} \subseteq S_z^{(m-1)}$ for every $z \in [m-1]$, the positive-confirmation guarantee in (Prop*-5)$^{(m-1)}$ continues to hold. Moreover,

  $$\min S_m^{(m)} - \epsilon^{(m)} > \gamma - 2\epsilon^{(m)} \geq \gamma - \Delta > \gamma - \epsilon^{(m-1)} = \min S_{m-1}^{(m-1)} - \epsilon^{(m-1)}.$$

  Therefore, the payment-ratio bound in (Prop*-5)$^{(m-1)}$ also implies the required bound in (Prop*-5)$^{(m)}$ for every $\ell \in [m-1]$.

  It remains to prove (Prop*-5)$^{(m)}$ for $\ell = m$. Let $\mathbf{b} = (b_1, \ldots, b_m) \in S_1^{(m)} \times \cdots \times S_m^{(m)}$ and let $\ell^* := i^* - L$. By construction,

  $$(b_1, \ldots, b_{m-1}) \in B_{k+1} \times \cdots \times B_{k+m-1}.$$

  Fix any $b' \in B_{\ell^*}$. Together with the fixed bids in $\mathbf{v}^{(m)}$ and $(b_1, \ldots, b_{m-1})$, reinserting b' gives, up to a permutation, a bid vector whose coordinates outside $\mathbf{v}^{(m-1)}$ lie in $B_1 \times \cdots \times B_{k+m-1} \subseteq T_{i^*}$. Hence, by weak symmetry and the definition of T_{i^*},

  $$\widetilde{x}_{b'}(\mathbf{v}^{(m)}, \mathbf{b}_{-m}, b') > 0.$$

  On the other hand, by Equation (10) and the choice of $\epsilon^{(m)}$,

  $$b_m > \gamma - \epsilon^{(m)} > \gamma - \Delta > \max A_k \geq b'.$$

  Therefore, Myerson's Lemma gives

  $$\widetilde{x}_{b_m}(\mathbf{v}^{(m)}, \mathbf{b}) > 0.$$

  It remains to prove the payment-ratio bound. Since $|\mathbf{v}^{(m)}| = R - 1$ and b_m is unique, weak symmetry gives

  $$\frac{\widetilde{p}_{b_m}(\mathbf{v}^{(m)}, \mathbf{b})}{\widetilde{x}_{b_m}(\mathbf{v}^{(m)}, \mathbf{b})} = \frac{p_R(\mathbf{v}^{(m)}, b_m, \mathbf{b}_{-m})}{x_R(\mathbf{v}^{(m)}, b_m, \mathbf{b}_{-m})}.$$

Since $b_m < \gamma$, Lemma 4.6 and the definition of δ imply

$$\begin{aligned}\frac{\widetilde{p}_{b_m}(\mathbf{v}^{(m)}, \mathbf{b})}{\widetilde{x}_{b_m}(\mathbf{v}^{(m)}, \mathbf{b})} &\leq \frac{p_R(\mathbf{v}^{(m)}, \gamma, \mathbf{b}_{-m})}{x_R(\mathbf{v}^{(m)}, \gamma, \mathbf{b}_{-m})} \\ &\leq \gamma - \delta \\ &\leq \gamma - 2\epsilon^{(m)} \\ &< \min S_m^{(m)} - \epsilon^{(m)}.\end{aligned}$$

Thus, (Prop*-5)$^{(m)}$ holds.

Corollary 4.23. *Only trivial TFMs, where no bids are ever confirmed, satisfy UIC, MIC, MRHP, and weak* 1*-CRHP in the plain model.*

Proof. By Theorem 4.18, a TFM that satisfies UIC, MIC, and weak 1-CRHP in the plain model must have zero miner revenue. Suppose for the sake of contradiction that for some bid vector $\mathbf{b}$, $x_i(\mathbf{b}) > 0$. By Lemma 4.5, this implies a bid vector $\mathbf{b}'$ exists where $\mathsf{util}_i(\mathbf{b}') > \mathsf{util}_i(\mathbf{b}) \geq 0$. Since the miner revenue is always 0, in a world where $\mathbf{b}'$ is the honest bid vector, the miner can ignore all bids to harm user i at no cost, contradicting MRHP. □

5 Characterizations in the MPC-Assisted Model

In this section, we present the feasibility and impossibility results in the MPC-assisted model. Recall that in the MPC-assisted model, a committee of M miners jointly run a multi-party computation (MPC) to implement the TFM.

5.1 Feasibility in the MPC-assisted Model

In this section, we present a mechanism that achieves all desired properties, UIC, MIC, all RHP variants, and positive revenue in the MPC-assisted model.

MPC-assisted, posted price with random selection

//Reserve price $\mathsf{res} > 0$, revenue parameter $0 < \epsilon \leq \mathsf{res}$.

- **Inclusion & Confirmation**: Let E be the set of bids at least the reserve price res. If $|E| \leq k$, include and confirm all bids in E. Otherwise, uniformly at random choose k bids in E to include and confirm.
- **Payment & Revenue**: Each confirmed bid pays the reserve price res. If at least one bid is confirmed, the total miner revenue is ϵ, which is divided equally among the M miners; otherwise, the total miner revenue is zero.

Theorem 5.1. *In the MPC-assisted model, posted price with uniform random selection satisfies UIC, MIC, URHP, MRHP, and* d*-CRHP for every* $1 \leq d \leq k$*. Total miner revenue is positive when* $|E| \geq 1$*.*

Proof. Let E be the set of eligible submitted bids at least reserve, and let $N = |E|$. If $N = 0$, no bid is confirmed and total miner revenue is zero. If $N > 0$, each eligible bid is confirmed with probability $q(N) := \min\{1, k/N\}$ under uniform random selection, pays res conditional on confirmation, and the total miner revenue is ϵ.

UIC: For a single real bid and fixed other bids, the user's allocation probability is zero below reserve and equal to a constant q at or above reserve; the expected payment is $\mathsf{res} \cdot q$. This is the Myerson threshold payment. Fake bids cannot help: every eligible fake bid has true value zero and, whenever confirmed, pays reserve; it also weakly lowers the real bid's confirmation probability. If the user's true value is below reserve, every strategy gives nonpositive utility. Otherwise, fake eligible bids cannot increase the confirmation probability of its real bid. Omitting the real bid also gives nonpositive utility. Therefore truthful bidding with no fake bids is optimal.

MIC: A miner coalition of size $m < M/2$ can inject fake bids. It cannot censor honest bids or alter the random selection, and the MPC provides guaranteed output delivery. If $N > 0$, honest total miner revenue is already ϵ, the maximum possible. Fake bids cannot increase it and may require fake payments. If $N = 0$, fake eligible bids can create revenue ϵ, but the coalition receives only $m\epsilon/M$ while paying at least res for each confirmed fake bid. Since $m < M/2$ and $\epsilon \leq \mathsf{res}$, this is not profitable. Thus MIC holds.

URHP: A user-only deviation can harm another user only by reducing that user's confirmation probability. This requires adding eligible competition. Adding eligible fake bids imposes strictly positive expected reserve payments on fake bids and weakly lowers the deviator's own real-bid confirmation probability. Turning a below-reserve real bid into an eligible bid gives strictly negative expected surplus. Changing an already eligible real bid has no effect on the allocation except through fake bids. Therefore any user-harming deterministic bidding strategy strictly lowers the deviating user's expected utility. By UIC, no deterministic bidding strategy improves on the deviating user's honest expected utility. Thus a randomized deviation that does not lower the deviator's expected utility uses deterministic bidding strategies that preserve this expected utility with probability one, and each such strategy weakly preserves every honest user's expected utility. Hence URHP holds.

MRHP: A miner-only coalition can harm an honest user only by adding eligible fake bids that dilute the user's confirmation probability. Adding eligible fake bids cannot increase the total miner revenue beyond the fixed ϵ and imposes payments whenever a fake bid is confirmed. If there is an eligible honest bid, the block remains nonempty and every honest miner outside the coalition continues to receive ϵ/M; if there is no eligible honest bid, every honest miner's baseline revenue is zero. Hence any deterministic bidding strategy that harms a protected honest user makes the deviating miner coalition strictly worse off, while honest miners outside the coalition cannot be harmed. By MIC, no deterministic strategy improves on honest utility. Thus a randomized deviation that does not lower expected utility uses utility-neutral deterministic strategies with probability one, each preserving every protected user's and miner's utility.

d-CRHP: Let $\mathcal{C}$ be a coalition containing $1 \leq m < M/2$ miners and a set $\mathcal{U}$ of at most $d \leq k$ users. We show that any deviation that does not decrease the coalition's expected utility cannot harm any user or miner outside $\mathcal{C}$.

Let h be the number of eligible honest users outside $\mathcal{C}$ and t be the number of users in $\mathcal{U}$ whose true values are at least res, and define

$$s := \sum_{i \in \mathcal{U}} \max\{v_i - \mathsf{res}, 0\} \text{ and } a := \frac{m\epsilon}{M}.$$

Recall that $q(N) := \min\{1, k/N\}$ for $N > 0$, and set $q(0) := 0$. Under honest behavior, there are $h + t$ eligible bids, so the coalition's expected utility is

$$\mathsf{util}_{\mathcal{C}}(\mathbf{v}; H_{\mathcal{C}}) = a \cdot \mathbf{1}_{\{h+t>0\}} + q(h+t) \cdot s.$$

Now consider an arbitrary (possibly randomized) strategy $S_{\mathcal{C}}$ by $\mathcal{C}$. Let $T \subseteq \mathcal{U}$ be the set of colluding users whose primary bids are eligible under $S_{\mathcal{C}}$, and let f be the number of eligible fake

bids. Then under strategy $S_{\mathcal{C}}$, we have $N = h + |T| + f$. Let $z = \sum_{i \in T}(v_i - \mathsf{res}) - f \cdot \mathsf{res}$. Then $z \leq s$.

Conditioned on an arbitrary realization of input bid vector under $S_{\mathcal{C}}$, every eligible bid is confirmed with probability $q(N)$. Hence the coalition's expected utility, conditioned on this realization of bid vector, is $a \cdot \mathbf{1}_{\{N>0\}} + q(N) \cdot z$. We split into two cases.

Case 1: $h > 0$ Then $N > 0$ under every deviation, so every honest miner outside $\mathcal{C}$ continues to receive revenue ϵ/M. An eligible honest user $j \notin \mathcal{C}$ has expected utility $(v_j - \mathsf{res})\mathbb{E}[q(N)]$ under the deviation, where the expectation is taken over randomness used in $S_{\mathcal{C}}$. Compared with j's utility $(v_j - \mathsf{res})q(h+t)$ under honest behavior, it can be harmed only if

$$\mathbb{E}[q(N)] < q(h+t).$$

Suppose first that $s > 0$. If an honest user is harmed, the coalition's expected utility under the deviation satisfies

$$\mathsf{util}_{\mathcal{C}}(\mathbf{v}; S_{\mathcal{C}}) = a + \mathbb{E}[q(N)z] \leq a + s\mathbb{E}[q(N)] < a + s \cdot q(h+t) = \mathsf{util}_{\mathcal{C}}(\mathbf{v}; H_{\mathcal{C}}).$$

Therefore, the coalition must also be harmed.

It remains to consider $s = 0$. In this case, $z \leq 0$ for every realized bidding strategy, while the coalition's honest utility is a. Since $q(N) > 0$ when $h > 0$, a deviation with expected utility at least a must satisfy $z = 0$ with probability one. Therefore, it must be that $f = 0$ and for every $i \in T$, we have $v_i = \mathsf{res}$. Thus under the strategy $S_{\mathcal{C}}$, every eligible bid from the coalition must come from one of the t users whose true value is exactly res. Hence, $N \leq h + t$ with probability one. Thus $q(N) \geq q(h+t)$ with probability one, so no honest user is harmed.

Case 2: $h = 0$**.** All honest users outside $\mathcal{C}$ are below the reserve and therefore have utility zero under both honest behavior and any deviation, so only honest miners outside $\mathcal{C}$ need to be considered. If $t = 0$, the honest total miner revenue is zero, so no honest miner outside $\mathcal{C}$ can be harmed. Therefore, we focus on the case where $t > 0$. Since $t \leq |\mathcal{U}| \leq d \leq k$, all t honestly eligible colluding users are confirmed under honest behavior, and

$$\mathsf{util}_{\mathcal{C}}(\mathbf{v}; H_{\mathcal{C}}) = a + s.$$

For every realized bid vector where $N > 0$, $q(N)z \leq s$, because $z \leq s$ and $q(N) \leq 1$. Hence conditioned on any realized bid vector such that $N > 0$, coalition's conditional utility is at most $a + s$; while under any bid vector such that $N = 0$, coalition's utility is zero. If $\rho := \Pr[N = 0]$, then

$$\mathsf{util}_{\mathcal{C}}(\mathbf{v}; S_{\mathcal{C}}) \leq (1 - \rho)(a + s).$$

Since $a > 0$, any deviation satisfying

$$\mathsf{util}_{\mathcal{C}}(\mathbf{v}; S_{\mathcal{C}}) \geq \mathsf{util}_{\mathcal{C}}(\mathbf{v}; H_{\mathcal{C}}) = a + s$$

must have $\rho = 0$. Therefore the block remains nonempty with probability one, and every honest miner outside $\mathcal{C}$ continues to receive ϵ/M.

Thus every deviation that weakly increases the coalition's expected utility weakly preserves the utility of every honest user and miner outside the coalition. The mechanism therefore satisfies d-CRHP for every $1 \leq d \leq k$. □

Not 1-SCP: Assume $M \geq 3$ and choose $1 \leq m < M/2$. Suppose no honest bid is eligible and a colluding user has true value $v \in (\mathsf{res} - m\epsilon/M, \mathsf{res})$, where m is the number of colluding miners. If the user bids at least reserve, it is confirmed, pays reserve, and the miner coalition obtains revenue share $m\epsilon/M$. The coalition's gain is $m\epsilon/M - (\mathsf{res} - v) > 0$. This deviation does not harm any honest user, consistent with CRHP.

5.2 Characterization of Deterministic Mechanisms

5.2.1 Deterministic Feasibility in the MPC-Assisted Model

While the previous mechanism achieves all desired properties, it relies on randomness to choose the set of k bids to confirm. In this section, we show that the all-or-nothing posted price is a deterministic mechanism satisfies all desired properties in the MPC-assisted model.

MPC-assisted, all or nothing posted price auction.
//Reserve price $\mathsf{res} > 0$, revenue parameter $0 < \epsilon \leq \mathsf{res}$.
Mechanism:

- **Inclusion Rule & Confirmation Rule:** If there are $\leq k$ bids and each bid is strictly greater than res, include and confirm all bids. Otherwise, include and confirm no bids. The strict threshold is intentional for the URHP boundary case.
- **Payment Rule & Miner Revenue Rule:** Each confirmed bid pays the reserve price res. The total miner revenue is ϵ per confirmed bid and is divided equally among the M miners.

Lemma 5.2. *The above TFM satisfies UIC, MIC, URHP, MRHP, d-CRHP for any $d \geq 1$, and has positive miner revenue in the MPC-assisted model.*

Proof. The strict-threshold all-or-nothing argument from Lemma 4.2 gives UIC and URHP, and proves the user-protection requirements of MRHP and d-CRHP. In the MPC-assisted model, MRHP and d-CRHP additionally protect honest miners outside the strategic coalition. We verify this additional requirement and MIC below.

MIC: A miner coalition of size $1 \leq m < M/2$ cannot censor honest bids and can only inject fake bids. The MPC provides guaranteed output delivery. An input bid vector fails only if it contains more than k bids or a bid at or below reserve; injecting fake bids cannot fix either condition. Since $m < M/2$ and $\epsilon \leq \mathsf{res}$, let $a := m\epsilon/M < \mathsf{res}$ denote the coalition's share of the miner revenue generated by each confirmed bid. Suppose first that the honest bid vector contains $N \leq k$ bids, all strictly above res, so that all N bids are confirmed and the coalition's honest utility is Na. If the coalition injects f fake bids and the resulting bid vector still satisfies the confirmation condition, its utility becomes

$$(N + f)a - f\mathsf{res} = Na + f(a - \mathsf{res}) \leq Na.$$

If instead the injection causes the mechanism to confirm no bids, the coalition obtains utility $0 \leq Na$. Thus injecting fake bids cannot increase the coalition's utility. Therefore MIC holds, including for randomized strategies by averaging.

It remains to prove that honest miners outside the coalition are protected against miner coalition or miner-user coalition. Fix a coalition $\mathcal{C}$ containing $1 \leq m < M/2$ miners and possibly some users.

If the honest execution confirms no bid, then every honest miner outside $\mathcal{C}$ receives zero revenue and therefore cannot be harmed. Suppose instead that the honest execution confirms $N > 0$ bids. Then $N \leq k$, every bid is strictly greater than res, and every miner receives revenue $N\epsilon/M$.

Fix an arbitrary strategy of $\mathcal{C}$. If the deviation ends up with no bid being confirmed, then the coalition loses its positive honest miner revenue, so the deviation strictly decreases the coalition's utility.

It remains to consider a deviation under which the mechanism confirms a positive number of bids. Changing a colluding user's bid while keeping it strictly above res does not affect either the allocation or payment. Dropping a colluding user's bid with value $v_i > \mathsf{res}$ decreases the coalition's

utility by $(v_i - \mathsf{res}) + \frac{m\epsilon}{M} > 0$, because the coalition loses both the user's utility and its share of the miner revenue generated by this bid. Similarly, adding a fake bid decreases the coalition's utility by $\mathsf{res} - \frac{m\epsilon}{M} > 0$, because the fake bid pays res, while the colluding miners receives only an m/M fraction of the additional revenue ϵ.

Therefore, every deviation that either drops a colluding user's bid or adds a fake bid strictly decreases the coalition's utility. Any deviation that does not decrease the coalition's utility must therefore preserve the same number of confirmed bids as under honest behavior. Hence every honest miner outside $\mathcal{C}$ continues to receive revenue $N\epsilon/M$.

The same argument applies to randomized strategies, since every realization gives the coalition utility at most its honest utility, a randomized deviation can have expected utility at least the honest utility only if the realized bidding strategy preserves the same number of confirmed bids and miner revenue with probability one. Thus MRHP and d-CRHP also protect honest miners outside the coalition.

□

Not 1-SCP: Assume $M \geq 3$, so a coalition with one miner is allowed. Imagine a world with k users, where $k-1$ of them have true value above res, but one has a true value $(\mathsf{res} - \frac{\epsilon}{2M})$. Consider the coalition consisting of one miner and this user with true value below res. In the honest case, no one gets confirmed, so this coalition gets a joint utility of 0. However, if the user raises their bid to $\mathsf{res} + 1$, the joint utility now becomes $k \cdot \frac{\epsilon}{M} + (\mathsf{res} - \frac{\epsilon}{2M}) - \mathsf{res} > 0$.

5.2.2 Deterministic Impossibility in the MPC-Assisted Model

The above all-or-nothing posted price is degenerate in the sense that it confirms no bid when there are more than k users. Unfortunately, this is necessary for deterministic mechanisms, even in the MPC-assisted model.

Lemma 5.3. *Suppose a deterministic TFM $(\mathbf{I}, \mathbf{C}, \mathbf{P}, \mathbf{R})$ satisfies UIC and URHP in the MPC-assisted model. For any bid vector $\mathbf{b} = (b_1, \ldots, b_n)$, if there exists some $b_i \in \mathbf{b}$ such that $\mathsf{util}_i(\mathbf{b}) > 0$, then for every j where b_j is unique in $\mathbf{b}$ and $b_j > b_i$, it must hold that $x_j(\mathbf{b}) = 1$.*

Proof. For the sake of contradiction, suppose that there exists $\mathbf{b}$ where $\mathsf{util}_i(\mathbf{b}) > 0$ and $x_j(\mathbf{b}) = 0$ for some unique $b_j > b_i$. Consider the bid vector $\mathbf{b}'$ where the user i and user j swap bid values: $b'_i = b_j$, $b'_j = b_i$, and $b'_\ell = b_\ell$ for $\ell \notin \{i, j\}$. By weak symmetry, the bid at b_j must now be unconfirmed, i.e. $x_i(\mathbf{b}') = 0$, since $\mathbf{b}'$ and $\mathbf{b}$ only differ by metadata and the bid at b_j is unique.

However, consider the world where $\mathbf{b}$ is the honest bid vector and the intermediate bid vector $\mathbf{b}^* = (\mathbf{b}_{-j}, b_i)$ is achieved by the strategy where user j underbids to b_i. By Myerson's Lemma (Lemma 3.5), the confirmation function $x_j(\mathbf{b}_{-j}, v)$ is weakly increasing in v, and thus $0 \leq x_j(\mathbf{b}_{-j}, b_i) \leq x_j(\mathbf{b}_{-j}, b_j) = 0$. Thus, the underbidding strategy cannot harm user j. Consequently, by URHP, $\mathsf{util}_i(\mathbf{b}^*) \geq \mathsf{util}_i(\mathbf{b}) > 0$ which implies $x_i(\mathbf{b}^*) = 1$ in a deterministic TFM. Now, by Myerson's Lemma (Lemma 3.5), when user i raises their bid to b_j to transform $\mathbf{b}^*$ into $\mathbf{b}'$, $x_i(\mathbf{b}') = 1$, which is a contradiction. □

Lemma 5.4. *Suppose a deterministic TFM $(\mathbf{I}, \mathbf{C}, \mathbf{P}, \mathbf{R})$ satisfies UIC and URHP in the MPC-assisted model. For any bid vector $\mathbf{b} = (b_1, \ldots, b_n)$, if there exists some $b_i \in \mathbf{b}$ such that $\mathsf{util}_i(\mathbf{b}) > 0$, then for every j where b_j is unique and $b_j > p_i(\mathbf{b})$, it must hold that $x_j(\mathbf{b}) = 1$.*

Proof. For the sake of contradiction, suppose that there exists $\mathbf{b}$ where $\mathsf{util}_i(\mathbf{b}) > 0$ and $x_j(\mathbf{b}) = 0$ for some unique $b_j > p_i(\mathbf{b})$. We then define $\mathbf{b}' = (\mathbf{b}_{-j}, b'_j)$ where $b'_j \in (p_i(\mathbf{b}), b_j) \setminus \{b_z : z \in [n]\}$. Note that b'_j is unique in $\mathbf{b}'$. By Myerson's Lemma (Lemma 3.5), the confirmation function $x_j(\mathbf{b}_{-j}, v)$ is

weakly increasing in v, and thus $0 \le x_j(\mathbf{b}_{-j}, b'_j) \le x_j(\mathbf{b}_{-j}, b_j) = 0$. This means the expected utility of user j is still 0 under the underbidding strategy. In a world where $\mathbf{b}$ is the honest bid vector, user j can adopt the strategy to underbid to b'_j to achieve the realized bid vector $\mathbf{b}'$. Thus, by URHP, $\mathsf{util}_i(\mathbf{b}') \ge \mathsf{util}_i(\mathbf{b}) > 0$ which implies $p_i(\mathbf{b}') \le p_i(\mathbf{b})$ in a deterministic TFM.

Claim 5.5. *For $v \in (p_i(\mathbf{b}), b'_j)$, $\mathsf{util}_j(\mathbf{b}_{-i}, v) > 0$.*

Proof. It is sufficient to prove that $x_j(\mathbf{b}'_{-i}, v) = 1$ as Lemma 4.5 would imply that $\mathsf{util}_j(\mathbf{b}_{-i}, v) > \mathsf{util}_j(\mathbf{b}'_{-i}, v) \ge 0$. By Myerson's Lemma (Lemma 3.5), $x_i(\mathbf{b}'_{-i}, v) = 1$ since $v > p_i(\mathbf{b}) \ge p_i(\mathbf{b}')$. Furthermore, $v < b'_j$, so by Lemma 5.3, $x_j(\mathbf{b}'_{-i}, v) = 1$. □

Consider any $v \in (p_i(\mathbf{b}), b'_j)$ and the true-value profile $\widehat{\mathbf{v}} := (\mathbf{b}_{-i}, v)$. By the above claim, user j has strictly positive utility when everyone behaves honestly under $\widehat{\mathbf{v}}$.

Now consider the deviation in which user i reports b_i, producing the submitted bid vector $\mathbf{b}$. Since $\mathsf{util}_i(\mathbf{b}) > 0$, user i is confirmed when bidding b_i, and in a deterministic UIC mechanism $p_i(\mathbf{b})$ is the threshold payment for user i when the other bids are fixed to $\mathbf{b}_{-i}$. Because $v > p_i(\mathbf{b})$, honest bid v is also confirmed and pays the same threshold $p_i(\mathbf{b})$. Therefore, with user i's true value fixed to v, both truthful reporting and the deviation to report b_i give user i utility $v - p_i(\mathbf{b}) > 0$. Thus,

$$\mathsf{util}_i(\widehat{\mathbf{v}}; S_i) = \mathsf{util}_i(\widehat{\mathbf{v}}; H_i),$$

where S_i denotes the strategy that reports b_i.

Under this deviation, the resulting bid vector is $\mathbf{b}$, where $\mathsf{util}_j(\mathbf{b}) = 0$ by assumption. Hence user i has a utility-neutral deviation that reduces user j's utility from a strictly positive value to zero, contradicting URHP. □

Theorem 5.6. *Let k denote the block size. If a deterministic TFM $(\mathbf{I}, \mathbf{C}, \mathbf{P}, \mathbf{R})$ satisfies UIC and URHP in the MPC-assisted model, then no bid can be confirmed whenever the number of bids exceeds k.*

Proof. Suppose, for the sake of contradiction, that there is a bid vector $\mathbf{v} = (v_1, \ldots, v_n)$ with $n > k$ and some confirmed bid. Choose a confirmed bid i^* and define $b_1 = \max(\mathbf{v})+1$ and $\mathbf{v}^{(1)} = (\mathbf{v}_{-i^*}, b_1)$. For $m > 1$, choose $b_m = \frac{1}{2}(b_{m-1} + \max(\mathbf{v}))$ and set $\mathbf{v}^{(m)} = (\mathbf{v}^{(m-1)}, b_m)$.

We use the following claim, proved below by induction:

$$\widetilde{x}_{b_m}(\mathbf{v}^{(m)}) = 1 \qquad \text{and} \qquad \widetilde{p}_{b_m}(\mathbf{v}^{(m)}) \le \max(\mathbf{v}) \quad \text{for every } m \ge 1. \tag{12}$$

Applying to $m = k + 1$, the bid b_{k+1} is confirmed and pays at most $\max(\mathbf{v})$, so it has strictly positive utility. Since $b_1 > \cdots > b_{k+1} > \max(\mathbf{v})$ and all these bids are unique, Lemma 5.3 implies that $b_1, \ldots, b_k$ are also confirmed in $\mathbf{v}^{(k+1)}$. Hence $\mathbf{v}^{(k+1)}$ contains $k+1$ confirmed bids, contradicting block capacity k. □

of Claim 12. The proof is by induction. The base case follows from UIC and Myerson's threshold-payment formula because b_1 replaces a confirmed bid by a higher value, so $\widetilde{x}_{b_1}(\mathbf{v}^{(1)}) = 1$ and $\widetilde{p}_{b_1}(\mathbf{v}^{(1)}) \le \max(\mathbf{v})$. For the inductive step, fix $b' \in (\max(\mathbf{v}), b_{m-1})$, keeping the appended bid's index and metadata fixed as its amount varies. If the unique fake bid b' were unconfirmed in $(\mathbf{v}^{(m-1)}, b')$, an unconfirmed user (which exists since $|\mathbf{v}^{(m-1)}| > k$) could inject that unconfirmed fake bid without lowering its zero honest utility: the fake bid pays zero, and individual rationality gives nonnegative utility from its unchanged truthful primary bid. By Lemma 5.4, the bid b_{m-1} must then become unconfirmed or pay at least b': if it remained confirmed and paid less than $b' < b_{m-1}$, it would have positive utility and the lemma would force b' to be confirmed. Since

Table 1: Mechanisms for the incomparability of IC and RHP in the plain model.

Strategic Player	Mechanism	IC	RHP
User	Burning first-price auction (Section 6.1.1)	✗ UIC	✓ URHP
	Second price auction (Section 6.1.1)	✓ UIC	✗ URHP
Miner	All-or-nothing posted price (Section 4.1)	✗ MIC	✓ MRHP
	2-winner second-price (Section 6.1.2)	✓ MIC	✗ MRHP
Miner-user coalition	All-or-nothing posted price (Section 4.1)	✗ 1-SCP	✓ 1-CRHP
	2-winner second-price (Section 6.1.2)	✓ 1-SCP	✗ 1-CRHP

$b' > \max(\mathbf{v}) \geq \widetilde{p}_{b_{m-1}}(\mathbf{v}^{(m-1)})$, in either case the utility of the bid b_{m-1} would be strictly lower than in the original vector $\mathbf{v}^{(m-1)}$, violating URHP. Hence every $b' \in (\max(\mathbf{v}), b_{m-1})$ is confirmed. Myerson's lemma then gives the payment bound for b_m: its threshold is at most the infimum of this interval, namely $\max(\mathbf{v})$, and the induction follows. □

6 IC and RHP are Incomparable

This section presents the mechanisms witness to show that IC and RHP are incomparable with respect to all three types of strategic players and in both the plain and the MPC-assisted models. We summarize the mechanisms in Table 1 for the plain model and Table 2 for the MPC-assisted model.

6.1 Comparison in the Plain Model

6.1.1 UIC vs. URHP in the Plain Model

Second-price auction

- **Inclusion & Confirmation:** Include highest two bids, and confirm the top bid. Break ties arbitrarily.
- **Payment & Revenue:** All confirmed bids pay the price of the lowest included bid (if only one bid is included, is pays 0) and all payments go to the miner.

Lemma 6.1 (UIC does not imply URHP in the plain model)**.** *The above second-price auction satisfies UIC but not URHP in the plain model.*

Proof. **UIC:** For deviations without fake bids, UIC follows from the fact that for any fixed user i, for fixed other users' bids $\mathbf{b}_{-i}$, user i's allocation is monotone and the price is exactly as defined in Lemma 3.5. To include fake bids, let r be the highest outside bid, or zero if none exists. Truthful utility is $\max\{v_i - r, 0\}$. Under any deviation, a confirmed primary bid pays at least r, while confirmed fake bids only add payment costs; without a confirmed primary bid, utility is nonpositive. Thus every deviation is bounded by truthful utility, also after averaging over mixed strategies.
Not URHP: Suppose the honest bid vector was $(0, v_2)$ where $0 < v_2$. Then, in the honest case, user 1 has utility 0 and user 2 has utility v_2. When user 1 raises their bid to $\frac{v_2}{2}$, their utility remains the same. However, user 2's payment rises, resulting in half the utility $v_2 - \frac{v_2}{2} = \frac{v_2}{2}$. □

Burning first-price auction

- **Inclusion & Confirmation:** Include and confirm the top k bids, breaking ties arbitrarily.
- **Payment & Revenue:** All confirmed bid price pay their bids, and all payments are burned.

Lemma 6.2 (URHP does not imply UIC in the plain model)**.** *The above burning first-price auction satisfies URHP but not UIC in the plain model.*

Proof. **URHP:** Every protected honest user has utility exactly 0 under every deviation: a confirmed truthful bid pays its value, and an unconfirmed bid pays nothing. Therefore no deviation, including a mixed strategy, can harm an honest user. URHP does not protect miner revenue.

Not UIC: There is an incentive for strategic underbidding, where a user can bid below their true valuation to increase utility while still being confirmed. □

6.1.2 MIC vs. MRHP in the Plain Model

2-winner second-price auction //Block size $k \geq 2$.

- **Inclusion Rule & Confirmation Rule:** The honest inclusion rule includes the two highest bids, or all bids if there is only one submitted bid. The confirmation rule confirms the top two included bids, or the single bid if only one is included. Break ties deterministically based on metadata.
- **Payment Rule:** If two bids are confirmed, both pay the lower confirmed bid. If only one bid is confirmed, it pays 0.
- **Miner Revenue Rule:** The miner receives the common payment of the confirmed bids as revenue, while the remaining payments are burned.

Lemma 6.3 (MIC does not imply MRHP in the plain model)**.** *The above 2-winner second price auction is MIC but not MRHP.*

MIC: Let h_2 denote the second-highest honest bid, taking $h_2 = 0$ if fewer than two honest bids are submitted. Under honest behavior, the miner's utility is h_2.

Consider any miner deviation. If fewer than two bids are confirmed, the miner revenue is 0. Suppose two bids are confirmed and let p be the lower confirmed bid, so the miner revenue is p. If both confirmed bids are real user bids, then $p \leq h_2$. If at least one confirmed bid is fake bid from the miner, then every confirmed fake bid pays p, while the miner receives total revenue only p; hence the miner's utility is at most $0 \leq h_2$. Thus no deviation gives the miner utility greater than the honest utility, and MIC holds.

Not MRHP: Consider the honest bid vector $(1, 1, 3)$. The lowest confirmed bid is 1, so the miner revenue is 1 and user 3 has utility 2. The miner can censor bid 3. The two remaining bids are $(1, 1)$, so the miner revenue remains 1, while user 3 becomes unconfirmed and its utility falls to 0. Hence MRHP fails.

Lemma 6.4 (MRHP does not imply MIC in the plain model)**.** *All-or-nothing posted-price auction (Section 4.1) with $\epsilon > 0$ is MRHP but not MIC.*

Proof. By Lemma 4.2. □

6.1.3 1-SCP vs. 1-CRHP in the Plain Model

Lemma 6.5 (1-SCP does not imply 1-CRHP in the plain model)**.** *The* 2*-winner second-price auction is* 1*-SCP but not* 1*-CRHP in the plain model.*

Proof. **1-SCP:** Suppose, for the sake of contradiction, that $\mathbf{v}$ is the true value vector and there exists a coalition $\mathcal{C}$ consisting of the miner and a user i with valuation v_i, and a joint strategy $S_{\mathcal{C}}$ such that $\mathsf{util}_{\mathcal{C}}(\mathbf{v}; S_{\mathcal{C}}) > \mathsf{util}_{\mathcal{C}}(\mathbf{v}; H_{\mathcal{C}})$. Let p denote the payment associated with each confirmed bid under $S_{\mathcal{C}}$ and let p_H denote the payment associated with each confirmed bid in the honest outcome. We bound utility for each realized deviation; averaging these bounds then covers mixed strategies.

Case 1: i is confirmed under $S_{\mathcal{C}}$. Here, $\mathcal{C}$'s joint utility is at most the user's valuation minus the payment, plus the payment received by the miner:

$$v_i - p + p = v_i.$$

The coalition's utility could be strictly less than v_i if the deviation involves fake bids that incur additional payments. If i were also confirmed under the honest strategy, the coalition's total utility would again be v_i; thus the deviation yields no gain. Therefore, we can assume that i is unconfirmed under the honest strategy. The joint utility in the honest case comes solely from the miner revenue which equals p_H. Since i is unconfirmed, we know $v_i \leq p_H$. This shows $S_{\mathcal{C}}$ does not benefit the coalition.

Case 2: i is unconfirmed under $S_{\mathcal{C}}$. Here, $\mathcal{C}$'s joint utility comes solely from the miner revenue, p, but could be lower due to confirmed fake bids. In the honest case, the joint utility is at least p_H, the miner revenue. If $p \leq p_H$, the deviation does not benefit $\mathcal{C}$. If $p > p_H$, then there must be at least one confirmed fake bid injected at or above p, meaning the coalition's joint utility under $S_{\mathcal{C}}$ would be at most $0 \leq p_H$.

In both cases, $S_{\mathcal{C}}$ does not produce a joint utility higher than the honest joint utility for the coalition. This is a contradiction.

Not 1-CRHP: Consider the honest value vector $(1, 2)$ and the coalition $\mathcal{C}$ consisting of the miner and user 1. Under the honest strategies, $\mathcal{C}$'s joint utility is 1 while user 2's utility is 1. However, if the miner censors user 2, $\mathcal{C}$'s joint utility is still 1 while user 2's utility is 0. Thus, this strategy harms user 2 without harming the coalition. □

Lemma 6.6 (1-CRHP does not imply 1-SCP in the plain model)**.** *All-or-nothing posted-price auction (Section 4.1) with $\epsilon > 0$ is d-CRHP for any $d \geq 1$ but not* 1*-SCP.*

Proof. By Lemma 4.2. □

6.2 Comparison in the MPC-Assisted Model

6.2.1 UIC vs. URHP in the MPC-Assisted Model

Lemma 6.1 and Lemma 6.2 still hold in the MPC-assisted model.

6.2.2 MIC vs. MRHP in the MPC-Assisted Model

Table 2: Mechanisms for the incomparability of IC and RHP in the MPC-assisted model.

Strategic Player	Mechanism	IC	RHP
User	Burning first-price auction (Section 6.1.1)	✗ UIC	✓ URHP
	Second price auction (Section 6.1.1)	✓ UIC	✗ URHP
Miner	Revenue-capped first-price (Section 6.2.2)	✗ MIC	✓ MRHP
	Trigger-posted-price (Section 6.2.2)	✓ MIC	✗ MRHP
Miner-user coalition	Burning first-price (Section 6.1.1)	✗ 1-SCP	✓ 1-CRHP
	Trigger-posted-price (Section 6.2.2)	✓ 1-SCP	✗ 1-CRHP

MPC-assisted, trigger-posted-price auction //Reserve price $\mathsf{res} > 0$.

- **Inclusion Rule & Confirmation Rule:** If there is exactly one bid strictly above reserve, include and confirm that bid. Otherwise, no bids are included or confirmed.
- **Payment & Miner Revenue Rule:** All confirmed bids pay the reserve price, and all payments are burned.

Lemma 6.7 (MIC does not imply MRHP in the MPC-assisted model.)**.** *The above MPC assisted, trigger posted price auction satisfies MIC but not MRHP.*

Proof. All confirmed bids pay the same amount, so we will only be referring to the confirmation probability in the proof below.
MIC: The miner receives no revenue so MIC, is trivially satisfied.
Not MRHP: Consider when there is an unconfirmed user 1 and a confirmed user 2 with positive utility in the honest case. Then the miner coalition has expected honest utility 0, and user 2 has positive expected honest utility. If the miner coalition injects two bids above reserve, its expected utility is still 0 while user 2's bid is now unconfirmed, leading to zero utility. This witnesses failure of MRHP without relying on a user-only deviation. □

Revenue-capped first-price auction //Block size $k \geq 2$

- **Inclusion Rule & Confirmation Rule:** Include the top 2 bids but confirm only the highest bid, breaking ties arbitrarily.
- **Payment Rule:** The confirmed bid pays its bid.
- **Miner Revenue Rule:** The total miner revenue is the highest non-confirmed included bid, or 0 if there is no non-confirmed included bid. Total revenue is divided equally among the M miners.

Lemma 6.8 (MRHP does not imply MIC in the MPC-assisted model)**.** *The above mechanism satisfies MRHP but not MIC in the MPC-assisted model.*

Proof. **MRHP:** Fix a coalition $\mathcal{C}$ of $1 \leq m < M/2$ miners. Every honest user always has utility 0: if confirmed, the user pays its truthful bid, and if unconfirmed, it pays nothing. Hence a miner deviation cannot harm an honest user.

Let R_H denote the total miner revenue under honest behavior and let R' denote the expected total miner revenue under an arbitrary, possibly randomized, deviation. Let $F \geq 0$ denote the expected total payment incurred by confirmed fake bids injected by $\mathcal{C}$. Since revenue is divided equally, the coalition's honest utility is $\frac{m}{M}R_H$, while its expected utility under the deviation is

$$\frac{m}{M}R' - F.$$

Therefore, if the deviation does not decrease the coalition's utility, then

$$\frac{m}{M}R' - F \geq \frac{m}{M}R_H,$$

which implies $R' \geq R_H$. Hence every honest miner outside $\mathcal{C}$ receives expected revenue at least R_H/M, so no honest miner is harmed. Thus the mechanism satisfies MRHP.

Not MIC: Consider the honest bid vector $(1, 0)$. The honest total miner revenue is 0. A nonempty coalition of $m < M/2$ miners can inject a fake bid of value $1/2$. The real bid 1 remains the unique confirmed bid, while the fake bid $1/2$ is the highest non-confirmed bid and therefore raises the total miner revenue to $1/2$. The fake bid is unconfirmed and pays nothing, so the coalition's utility increases by $m/(2M) > 0$. Hence MIC fails. □

6.2.3 1-SCP vs. 1-CRHP in the MPC-Assisted Model

Lemma 6.9 (1-SCP does not imply 1-CRHP in the MPC-assisted model)**.** *The trigger-posted-price satisfies* 1*-SCP but not* 1*-CRHP in the MPC-assisted model.*

Proof. 1**-SCP:** Fix a coalition $\mathcal{C}$ consisting of $1 \leq m < M/2$ miners and one user i. The miners revenue is always zero. Moreover, injecting an eligible fake bid cannot help user i: a confirmed fake bid incurs a payment of res, while an additional eligible fake bid can only change an instance with exactly one eligible bid into an instance with at least two eligible bids, in which no bid is confirmed.

It therefore suffices to consider deviations of user i without eligible fake bids. If there is no eligible honest bid outside $\mathcal{C}$, then user i faces a posted price res: bidding above reserve gives utility $v_i - \mathsf{res}$, while bidding at or below reserve gives utility 0, so truthful bidding is optimal. If there is an eligible honest bid outside $\mathcal{C}$, the coalition cannot censor it, and user i cannot make its own bid the unique eligible bid. Hence the coalition has no strictly profitable deviation, and the mechanism is 1-SCP.

Not 1**-CRHP:** Consider a coalition consisting of $1 \leq m < M/2$ miners and a user with value 0, together with an honest user of value $2\mathsf{res}$. Under honest behavior, the honest user is the unique eligible bidder and obtains utility res, while the coalition has utility 0. The miner coalition can inject one fake bid strictly above res. There are then at least two eligible bids, so no bid is confirmed. The fake bid is unconfirmed and pays nothing, so the coalition's utility remains 0, while the honest user's utility falls from res to 0. Thus 1-CRHP fails. □

Lemma 6.10 (1-CRHP does not imply 1-SCP in the MPC-assisted model)**.** *The burning first-price auction satisfies d-CRHP for every* $d \geq 1$ *but not* 1*-SCP in the MPC-assisted model.*

Proof. d**-CRHP:** Every honest user always has utility 0: if confirmed, the user pays its truthful bid, and if unconfirmed, it pays nothing. Moreover, all payments are burned, so every miner receives zero revenue under every outcome. Consequently, no deviation by a miner-user coalition can make any protected honest user or honest miner strictly worse off. Thus the mechanism satisfies d-CRHP for every $d \geq 1$.

Not 1-SCP: Consider a single user with value $v > 0$ together with any nonempty allowed miner coalition. Under truthful bidding, the user is confirmed, pays v, and obtains utility 0. If the user instead bids some $b \in (0, v)$ while the miners follow the prescribed mechanism, the user remains confirmed and obtains utility $v - b > 0$. Since miner revenue remains zero, this strictly increases the coalition's joint utility. Hence the mechanism is not 1-SCP. □

Acknowledgements. This work is supported by the 2024 Stellar Academic Research Grant.

References

[ADM24] Guillermo Angeris, Theo Diamandis, and Ciamac Moallemi. Multidimensional blockchain fees are (essentially) optimal. *arXiv preprint arXiv:2402.08661*, 2024.

[AL20] Mohammad Akbarpour and Shengwu Li. Credible auctions: A trilemma. *Econometrica, Econometric Society*, 2020.

[AMSKM23] Lukas Aumayr, Pedro Moreno-Sanchez, Aniket Kate, and Matteo Maffei. Breaking and fixing virtual channels: Domino attack and donner. In *Network and Distributed System Security Symposium (NDSS)*, pages 1–18. The Internet Society, 2023.

[BCD+19] Vitalik Buterin, Eric Conner, Rick Dudley, Matthew Slipper, Ian Norden, and Abdelhamid Bakhta. EIP-1559: Fee market change for ETH 1.0 chain. Ethereum Improvement Proposals, no. 1559, `https://eips.ethereum.org/EIPS/eip-1559`, April 2019.

[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.

[But17] Vitalik Buterin. The triangle of harm. `https://vitalik.ca/general/2017/07/16/triangle_of_harm.html`, 2017.

[But18] Vitalik Buterin. A griefing factor analysis model. `https://ethresear.ch/t/a-griefing-factor-analysis-model/2338`, 2018.

[Can01] R. Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *FOCS*, 2001.

[Car19] Gabriel Carroll. Robustness in mechanism design and contracting. *Annual Review of Economics*, 11(1):139–166, 2019.

[CMST25] Hao Chung, Elisaweta Masserova, Elaine Shi, and Sri AravindaKrishnan Thyagarajan. Fairness in the wild: Secure atomic swap with external incentives. Cryptology ePrint Archive, Paper 2025/1086, 2025.

[CRS24] Hao Chung, Tim Roughgarden, and Elaine Shi. Collusion-resilience in transaction fee mechanism design. In *Proceedings of the 25th ACM Conference on Economics and Computation*, pages 1045–1073, 2024.

[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.

[CSLZZ25] Xi Chen, David Simchi-Levi, Zishuo Zhao, and Yuan Zhou. Bayesian mechanism design for blockchain transaction fee allocation. *Operations Research*, 2025.

[DECA23] Theo Diamandis, Alex Evans, Tarun Chitra, and Guillermo Angeris. Designing multidimensional blockchain fee markets. In *5th Conference on Advances in Financial Technologies (AFT 2023)*, volume 282 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 4:1–4:23. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2023.

[DPTM24] Eduardo Duque, Juan Pereyra, and Juan Pablo Torres-Martínez. *Local Non-Bossiness and Preferences Over Colleagues*. Universidad de Chile, Departamento de Economía, 2024.

[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.

[Erd64] P. Erdős. On extremal problems of graphs and generalized graphs. *Israel Journal of Mathematics*, 2(3):183–190, 1964.

[Eth26] Ethereum.org. Block proposal. `https://ethereum.org/developers/docs/consensus-mechanisms/pos/block-proposal/`, 2026. Ethereum documentation, accessed March 29, 2026.

[FGR24] Matheus VX Ferreira, Yotam Gafni, and Max Resnick. Incentive-compatible collusion-resistance via posted prices. *arXiv preprint arXiv:2412.20853*, 2024.

[FMPS21] Matheus VX Ferreira, Daniel J Moroz, David C Parkes, and Mitchell Stern. Dynamic posted-price mechanisms for the blockchain transaction-fee market. In *Proceedings of the 3rd ACM Conference on Advances in Financial Technologies*, pages 86–99, 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.

[Geo23] William George. An analysis of griefs and griefing factors. *Frontiers in Blockchain*, 6:1137155, 2023.

[GHR25] Pranav Garimidi, Lioba Heimbach, and Tim Roughgarden. Transaction fee mechanism design for leaderless blockchain protocols. In *International Conference on Financial Cryptography and Data Security*, pages 20–35. Springer, 2025.

[GMW87] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game. In *ACM symposium on Theory of computing (STOC)*, 1987.

[GTW24] Aadityan Ganesh, Clayton Thomas, and S. Matthew Weinberg. Revisiting the primitives of transaction fee mechanism design. In *Proceedings of the 25th ACM Conference on Economics and Computation (EC)*, 2024.

[GTW25] Aadityan Ganesh, Clayton Thomas, and S Matthew Weinberg. Characterizing off-chain influence proof transaction fee mechanisms. *arXiv preprint arXiv:2512.02354*, 2025.

[GY24] Yotam Gafni and Aviv Yaish. Barriers to collusion-resistant transaction fee mechanisms. In *Proceedings of the 25th ACM Conference on Economics and Computation*, pages 1074–1096, 2024.

[Her18] Maurice Herlihy. Atomic cross-chain swaps. In *PODC*, pages 245–254. ACM, 2018.

[HM25] Lioba Heimbach and Jason Milionis. The early days of the ethereum blob fee market and lessons learnt. In *International Conference on Financial Cryptography and Data Security*, pages 53–71. Springer, 2025.

[JM06] Philippe Jehiel and Benny Moldovanu. Allocative and informational externalities in auctions and related mechanisms. In Richard Blundell, Whitney K. Newey, and Torsten Persson, editors, *Advances in Economics and Econometrics: Theory and Applications, Ninth World Congress*, volume 1, chapter 3, pages 102–135. Cambridge University Press, 2006.

[Kla01] Bettina Klaus. Coalitional strategy-proofness in economies with single-dipped preferences and the assignment of an indivisible object. *Games and Economic Behavior*, 34(1):64–82, 2001.

[LNPR25] Nir Lavee, Noam Nisan, Mallesh Pai, and Max Resnick. Does your blockchain need multidimensional transaction fees? *arXiv preprint arXiv:2504.15438*, 2025.

[Lop17] Jameson Lopp. The challenges of Bitcoin transaction fee estimation. BitGo blog post, May 2017. Accessed: 2026-02-08.

[LRS21] Giuseppe Lopomo, Luca Rigotti, and Chris Shannon. Uncertainty in mechanism design. *arXiv preprint arXiv:2108.12633*, 2021.

[LSCP23] Stefanos Leonardos, Shyam Sridhar, Yun Kuen Cheung, and Georgios Piliouras. Griefing factors and evolutionary in-stabilities in blockchain mining games. In Panos M. Pardalos, Ilias S. Kotsireas, Yike Guo, and William J. Knottenbelt, editors, *Mathematical Research for Blockchain Economy*, pages 75–94. 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.

[LSZ23] Renato Paes Leme, Jon Schneider, and Hanrui Zhang. Nonbossy mechanisms: Mechanism design robust to secondary goals. *arXiv preprint arXiv:2307.11967*, 2023.

[MBS+23] Subhra Mazumdar, Prabal Banerjee, Abhinandan Sinha, Sushmita Ruj, and Bimal Kumar Roy. Strategic analysis of griefing attack in lightning network. *IEEE Transactions on Network and Service Management*, 20(2):1790–1803, 2023.

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

[Rit83] Zvi Ritz. Restricted domains, arrow-social welfare functions and noncorruptible and non-manipulable social choice correspondences: the case of private alternatives. *Mathematical Social Sciences*, 4(2):155–179, 1983.

[Rou21] Tim Roughgarden. Transaction fee mechanism design. *ACM SIGecom Exchanges*, 19(1):52–55, 2021.

[RPM24] Mayank Raikwar, Nikita Polyanskii, and Sebastian Müller. Sok: Dag-based consensus protocols. In *2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 1–18. IEEE, 2024.

[SCW23] Elaine Shi, Hao Chung, and Ke Wu. What Can Cryptography Do for Decentralized Mechanism Design? In Yael Tauman Kalai, editor, *ITCS 2023*, volume 251 of *LIPIcs*, pages 97:1–97:22, Dagstuhl, Germany, 2023. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[SMT25] Aikaterini-Panagiota Stouka, Julian Ma, and Thomas Thiery. Multiple proposer transaction fee mechanism design: Robust incentives against censorship and bribery. *arXiv preprint arXiv:2505.13751*, 2025.

[SS81] Mark A Satterthwaite and Hugo Sonnenschein. Strategy-proof allocation mechanisms at differentiable points. *The Review of Economic Studies*, 48(4):587–597, 1981.

[SSY07] Tatsuyoshi Saijo, Tomas Sjostrom, and Takehiko Yamato. Secure implementation. *Theoretical Economics*, 2(3):203–229, 2007.

[TDM+24] Thomas Thiery, Francesco D'Amato, Julian Ma, Barnabé Monnot, Terence Tsao, Jacob Kaufmann, and Jihoon Song. EIP-7805: Fork-choice enforced inclusion lists (focil). Ethereum Improvement Proposals, November 2024. Created: 2024-11-01. Accessed: 2026-02-08.

[Tho16] William Thomson. Non-bossiness. *Social Choice and Welfare*, 47(3):665–696, 2016.

[TYME21] Itay Tsabary, Matan Yechieli, Alex Manuskin, and Ittay Eyal. MAD-HTLC: Because HTLC is crazy-cheap to attack. In *2021 IEEE Symposium on Security and Privacy (S&P)*, pages 1230–1248. IEEE, 2021.

[Vic61] William Vickrey. Counterspeculation, auctions, and competitive sealed tenders. *The Journal of finance*, 16(1):8–37, 1961.

[WSC24] Ke Wu, Elaine Shi, and Hao Chung. Maximizing Miner Revenue in Transaction Fee Mechanism Design. In Venkatesan Guruswami, editor, *ITCS 2024*, volume 287 of *LIPIcs*, pages 98:1–98:23, Dagstuhl, Germany, 2024. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[XH21] Yingjie Xue and Maurice Herlihy. Hedging against sore loser attacks in cross-chain transactions. In *PODC*, pages 155–164. ACM, 2021.

[Yao20] Andrew Chi-Chih Yao. An Incentive Analysis of Some Bitcoin Fee Designs (Invited Talk). In *47th International Colloquium on Automata, Languages, and Programming (ICALP 2020)*, volume 168 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 1:1–1:12. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2020.