Multiple Proposer Transaction Fee Mechanism Design: Robust Incentives Against Censorship and Bribery

Aikaterini-Panagiota Stouka
Nethermind Research
aikaterini-panagiota@nethermind.io

Julian Ma
Ethereum Foundation
julian@ethereum.org

Thomas Thiery
Ethereum Foundation
thomas@ethereum.org

March 2025

Abstract

Censorship resistance is one of the core value proposition of blockchains. A recurring design pattern aimed at providing censorship resistance is enabling multiple proposers to contribute inputs into block construction. Notably, Fork-Choice Enforced Inclusion Lists (FOCIL) is proposed to be included in Ethereum. However, the current proposal relies on altruistic behavior, without a Transaction Fee Mechanism (TFM). This study aims to address this gap by exploring how multiple proposers should be rewarded to incentivize censorship resistance. The main contribution of this work is the identification of TFMs that ensure censorship resistance under bribery attacks, while also satisfying the incentive compatibility properties of EIP-1559. We provide a concrete payment mechanism for FOCIL, along with generalizable contributions to the literature by analyzing 1) incentive compatibility of TFMs in the presence of a bribing adversary, 2) TFMs in protocols with multiple phases of transaction inclusion, and 3) TFMs of protocols in which parties are uncertain about the behavior and the possible bribe of others.

1 Introduction

Censorship resistance is an essential value of blockchains. Most blockchains elect a single party in each slot, called the proposer[1], who constructs a block. The proposer can decide to censor transactions and may even be incentivized to do so if they can then extract more Maximal Extractable Value (MEV) [4]. Studies such as [6] and [17] provide empirical evidence demonstrating that proposers on Ethereum engage in censorship in practice. Blockchain designers have developed mechanisms to elect multiple proposers in each slot to address the issue. Inclusion Lists ([9] and [15]) is a line of research that explores multiple proposers who only provide input into block construction, leaving one block producer with the ability to order transactions. Multiple Concurrent Block Producers [10] is a different research area that investigates multiple proposers whose input is ordered by a predetermined ordering rule.

However, the question of how transaction fees should be split among multiple proposers remains underexplored. In particular, appropriately allocating transaction fees between multiple proposers to incentivize censorship resistance could improve multiple proposer mechanisms. In this paper, we develop a versatile game-theoretic model to evaluate several payment mechanisms. We examine whether transaction fee mechanisms in multiple proposer protocols maintain the

---

[1]In this paper, we use Ethereum's terminology to reference consensus actors. Other blockchains may use different terminology for similar roles.

incentive compatibility properties of EIP-1559 [11], even in the presence of a bribing adversary and congestion.

The main contribution of this paper is a concrete transaction fee mechanism (TFM) for Fork-Choice Enforced Inclusion Lists (FOCIL) [15], the leading inclusion list mechanism proposed to be included in Ethereum. Although this paper's focus is on FOCIL, the modelling techniques are of independent interest:

- We generalize Roughgarden's canonical model [12] to incorporate censorship resistance under bribing attacks. This generalization is also valuable for single proposer blockchain protocols.

- We provide a general model to evaluate TFMs in blockchain protocols with multiple proposers or multiple phases within a slot.

- We define new properties relevant to blockchain designers related to evaluating censorship resistance under congestion.

1.1 Model

Our starting point is the model of [12] in which users send transactions to a block producer and have private valuations for their transaction inclusion. The block producer picks an allocation rule that determines which transactions are included. The block producer is paid for all transactions they include by a payment rule. A burning rule determines the fee payment to the blockchain protocol. We provide a detailed overview of [12] in Appendix A.

We extend [12] in three main ways. First, we introduce a new phase where multiple proposers each pick an allocation rule. The payment rule now specifies how transaction fees are split among the multiple proposers. The goal is to understand whether the incentive compatibility properties related to EIP-1559 hold in this setting [11]. Second, we introduce an adversary who bribes proposers. The adversary is exogenously motivated to censor a transaction. We analyze both the case in which all proposers are rational and the case in which at least one proposer does not accept bribes but is rational otherwise. Finally, proposers in our model have incomplete information. They may not be certain about the bribe functions of other proposers and they may not be certain they will be a proposer when transactions must be submitted, which has a similar effect as γ-strict utility in [2]. We adjust the incentive compatibility notions of [11] from Nash to Bayesian Nash equilibria accordingly.

We consider three types of transaction fee mechanisms that could be used for FOCIL [15] and find one that is unsuitable. All these TFMs adhere to the EIP-1559 burning rule. In the first TFM, denoted by *Double TFM*, the user specifies two fees: one that is given to the *committee*, composed of proposers who only input transactions, and another given to the *block producer*, the proposer who inputs and orders all transactions. In the second TFM, called *Single TFM*, the user specifies one, total fee and the system (i.e., the blockchain protocol) determines how the fee is split between the committee and the block producer. Finally, in the third TFM, referred to as *Single Prioritized TFM*, the user also sets a single fee and the system determines how the fee is split, with priority given to the committee.

1.2 Results

The main contribution of this paper is to find TFMs that could be used in Ethereum when FOCIL gets implemented [15]. We do so by assessing multiple TFMs along the following axes:

- Is it incentive compatible for users and Bayesian-Nash incentive compatible for committee members and the block producer to follow the TFM's allocation rule?

- What level of censorship resistance does the TFM provide? In other words, under which (i) bribes and (ii) beliefs about the bribes of other parties does a party refrain from censoring at a Bayesian Nash equilibrium?

- Does the TFM satisfy fair-under-congestion, a property that, at a high level, determines whether there exists a fee a user can set to ensure both types of proposers will include their transaction in a Bayesian Nash equilibrium, even under congestion?

We adjust Incentive-Compatibility for Myopic Miners (MMIC) from [12] to accommodate our setting of multiple proposers and incomplete information, leading to Myopic Committee Bayesian-Nash Incentive Compatible (MCBN) and Myopic Block Producer Bayesian-Nash Incentive Compatible (MBBN), which we formally introduce in Section 3.

We prove that the Double TFM and Single TFM exhibit similar incentive properties to Ethereum's current TFM, and enhance censorship resistance even under congestion. In contrast, we prove that the third TFM is not fair-under-congestion. Notably, our model is sufficiently descriptive to allow us to quantify the level of censorship resistance. Moreover, our results hold for various implementations of FOCIL, which we describe in detail later. Although both Double TFM and Single TFM satisfy the same incentive properties, they differ in the following ways: (i) In Double TFM, the splitting of the fee between the committee and the block producer is done by the user, whereas in Single TFM, this split is determined by the system. In Single TFM, we have shown that the level of censorship resistance depends on the fraction of the fee awarded to the committee, and that the fraction which maximizes censorship resistance is influenced by the base fee and the transaction bid (cf. Appendix C.5). This implies that there is no fixed split that maximizes censorship resistance for every possible transaction. As a result, Double TFM can achieve better censorship resistance if the user selects the appropriate fee. The results are summarized in Table 1.

	Double TFM	Single TFM	Single Prioritized TFM
"usually" DSIC	x	x	n/a
MCBN	x	x	n/a
MBBN	x	x	n/a
Universal Censorship Resistance	x	-	n/a
Simple User Experience	-	x	n/a
Fair-under-congestion	x	x	-

Table 1: Overview of results. Properties that are satisfied are denoted by x; those that are not by -; n/a means we do not provide proofs. "Usually" DSIC is the same term as the one [12] uses for when the base fee is not excessively low and users cannot overbid. "Simple User Experience" means that the user does not need to set an extra fee compared to the current Ethereum TFM. "Universal Censorship Resistance" means that it can offer the same level of censorship resistance for every transaction if the user selects an appropriate fee

.

Censorship resistance of Double TFM and Single TFM In Section 4.1 we provide the bribe functions under which the properties of Table 1 are satisfied. At a high level, when there is no congestion, the minimum bribe an external briber needs to censor a transaction t_0, is roughly the fee of this transaction that corresponds to the block producer (denoted by *block producer fee*) plus block producer's cost to perform the following deviation: to add "fake" transactions to the mempool, making the committee members prefer these transactions over t_0, only to later invalidate them with another "fake transaction" in their block. If there is a positive probability γ that the block producer is not the block creator of the current slot (thereby successfully invalidating the fake transactions they added to the mempool) then: the higher the fee of

the transaction t_0 that corresponds to the committee, the more costly the latter deviation is. When there is congestion, the minimum bribe is approximately the difference between the block producer fee of t_0 and the next highest fee of the available transactions.

1.3 Literature Review

Our work builds on the transaction fee mechanism design literature. We start with Roughgarden's canonical model [12] and extend it to multiple proposers, the incomplete information setting, and bribing attacks. We analyze whether the proposed TFMs are compatible with the properties of EIP-1559 as defined in [11] to make implementation in Ethereum practical. Agents in our model may not be sure they will be a proposer in the next slot, meaning their benefit from submitting fake transactions is uncertain. This is based on the γ-strict utility of [2]. Our work is perhaps closest to [3] who extend Roughgarden's model to multiple concurrent proposers. We differentiate our work by adhering to the EIP-1559 burning rule, by focusing on a censorship resistant allocation rule even with a bribing adversary, and by generalizing to multiple proposers, who may not concurrently propose blocks but instead fulfill different roles sequentially, capturing FOCIL [15].

We use modeling techniques from the literature studying censorship resistance. [7] studies bribing attacks on consensus protocols. Bribes may depend not only on the strategies of individuals but also on the strategies of others. We adopt this functionality. [16] propose AUCIL, an inclusion list design, and quantify its censorship resistance. Instead, we analyze whether inclusion lists affect Ethereum's existing TFM. Moreover, our modeling techniques differ since we use an incomplete information setting and do not assume a coordination device, used in [16] to obtain a correlated Nash equilibrium. [1] assume multiple proposers to quantify the robustness of economic censorship games in fraud proofs. Our work aims to increase the robustness of multiple proposer blockchain protocols. Finally, [5] study censorship resistance of blockchain applications under a bribing adversary and suggest a payment rule for multiple concurrent proposers to improve the cost of censorship. We incorporate a more sophisticated malicious adversary who makes conditional bribes and formalize incentive compatibility properties for multiple proposer blockchain protocols.

2 Overview of Fork-Choice Enforced Inclusion Lists (FOCIL) [15]

FOCIL is an inclusion list design that allows each member of a committee of proposers, known as the inclusion list committee, to create a list of transactions that must be included in another proposer's block. We refer to the latter proposer as the block producer and to the inclusion list committee members as includers (cf.[14]).

Includers choose which transactions they include in their inclusion list. They could also include their own transactions in their lists. Transactions included in the block producer's block via inclusion lists must pay the base fee, a protocol-computed reserve price determined by the burning rule of EIP-1559 [11]. Includers send their inclusion lists to the block producer and the attesters.

The block producer includes transactions in their block and may also include transactions originated from themselves. All transactions in the block, whether included via inclusion lists or not, pay the base fee. Moreover, the block proposer may add transactions to the mempool, from which includers select transactions for their inclusion list. The same holds also for the includers. Following Roughgarden's terminology [12], all the transactions in the mempool, inclusion lists and the block originated from the includers and the block producer are called "fake". The block producer must include as many transactions from the inclusion lists as possible in the block. If the block is full, transactions from inclusion lists do not have to be added. Attesters verify the

block producer's actions. A block that does not adhere to the inclusion list rules is disregarded.

[15] explains FOCIL in more detail, especially how consensus attacks are mitigated. [8] explores the design rationale behind FOCIL, specifically why the block producer is still given monopoly ordering rights. Figure 1 provides a detailed overview of the FOCIL mechanism as proposed to be included in Ethereum.

For the purpose of this paper, we assume that includers create their inclusion list without seeing the inclusion lists of other includers and we assume that includers are randomly assigned an order. Since FOCIL has not yet been implemented and its specifications may change slightly, we analyze not only FOCIL as described above but also two different implementations.

- Unconditional FOCIL. Inclusion list transactions must be in the block even if the block is full.

- Unique Senders FOCIL. Each includer may only include one transaction per sender in their list. This prevents the block producer from filling the inclusion list with fake transactions from one sender and draining the sender's balance with one transaction, thereby invalidating all other transactions from this sender.
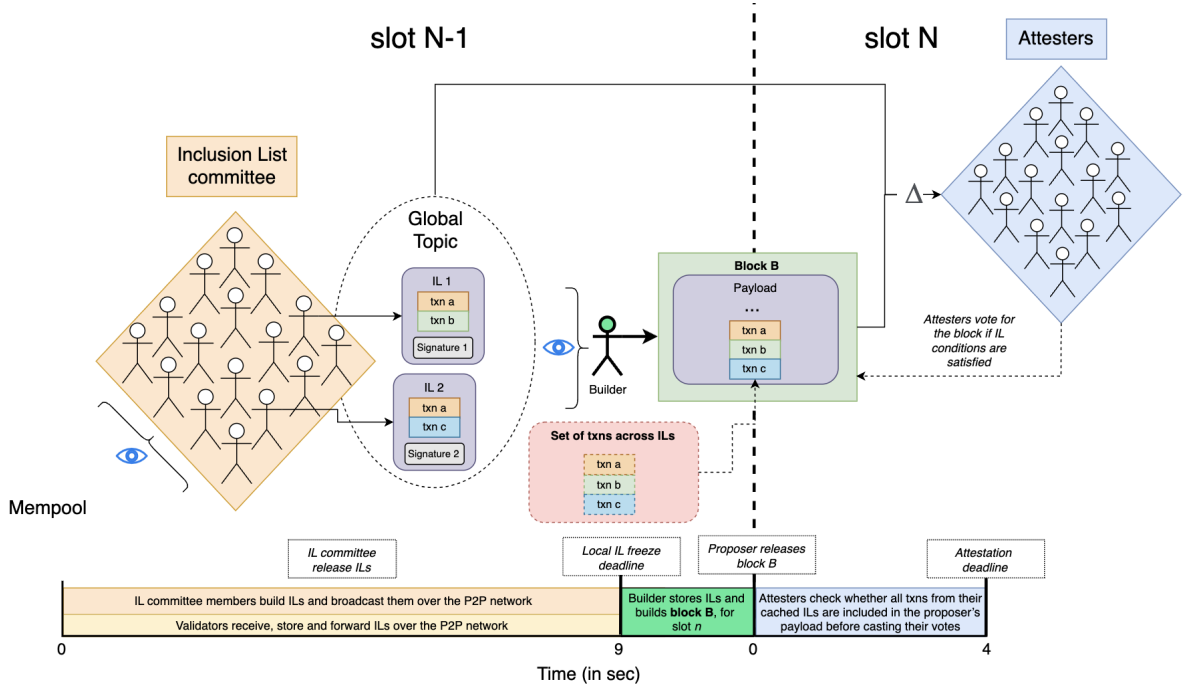

Figure 1: Overview of the FOCIL mechanism. [15]

3   Multiple Proposer Transaction Fee Mechanism Design

This section introduces the paper's model. We start with a high-level description and the rest of the section formally introduces each part of the model.

We consider an *interim stage Bayesian game*, where the parties involved in the game are: n users who send transactions to the mempool, m includers, and the block producer. Moreover, we consider an external malicious briber who wants to censor a transaction t_0 and is committed to reward the includers and the block producer contingent upon their decision to censor a particular transaction. A bribe function determines the final reward every proposer receives from the briber. This function considers several factors such as the transaction characteristics,

the proposer's strategy, and the strategy of the other proposers. Importantly, proposers know their bribe function but are uncertain about the bribe functions of the other parties, holding beliefs about them. The users are of various types based on the characteristics of the transactions they want to send. The includers and the block producer are of different types determined by their bribe function. The external briber is not part of the game; their role is abstracted via the bribe function. Finally, we assume that any block that does not comply with the inclusion list rules will be rejected by the attesters. As a result, users will not incur any fees, and neither the includers nor the block producer will receive any payments.

- Let H be the sequence of the preceding blocks $B_1, \ldots, B_{k-1}$. The new block is denoted by B_k.

- Let M be the mempool with all the available transactions the includers and the block producer can include in their inclusion lists and their block respectively. Following [13], we assume that all the parties have the same view on M.

- Let M_0 be the mempool that consists only of the transactions of the users (not the fake transactions originated from the includers and the block producer).

- Let C_{Block} be the maximum size for B_k.

- Let C_{Incl} be the maximum size for an inclusion list.

3.1 Types and Beliefs of the Parties

Types of the user   Every user is of a specific type determined by the characteristics of the transaction they want to send. Every transaction has the following characteristics:

- A *size* s_t.

- A *value* v_t per unit of size.

- The *public information* p_t.

The value v_t reflects the maximum amount per unit of size the user is willing to pay for the transaction to be included in the block. We follow [12] and assume that the value is not affected by the position of the transaction in the block. The value is known only by the user.

The public information p_t is metadata of the transaction, such as its sender. This characteristic is provided as input to the bribe function to account for situations where the briber intends to censor transactions originating from a specific user.

Beliefs of the user   Every user i has a belief about (i) which is the type of every other user denoted by $\text{Belief}_{\text{User}_i \to \text{Users}}$, and (ii) which is the type of every includer and the block producer denoted by $\text{Belief}_{\text{User}_i \to CM,BP}$.

Types of the includer   Every includer j has a type determined by the bribe they receive to exclude transaction t at the end of the game from the malicious briber based on their strategy and the strategy of the other parties. This bribe is determined by a function $\mu_{CM_j}^{Bribe}(s_t, b_t, p_t, \vec{\alpha}_t, H, M_0)$ which belongs to a set Bribe^{CM}. This set includes all the bribe functions of the includers that we want to consider.

- b_t is the bid per unit of size associated with transaction t.

- $\vec{\alpha}_t \in \{0,1\}^{m+1}$ is the *inclusion vector* which denotes 1 for each includer and block producer that includes the transaction and 0 otherwise.

Beliefs of the includer   Every includer has a belief about the type of the other includers and the block producer, denoted by Belief_{CM}. We assume all the includers have the same beliefs.

Types of the block producer   The block producer has a type determined by the bribe they receive for transaction t at the end of the game from the malicious briber. This bribe is determined by a function $\mu_{BP}^{Bribe}(s_t, b_t, p_t, \vec{\alpha}_t, H, M_0)$ which belongs to a set Bribe^{BP}. This set includes all the bribe functions of the block producer that we want to consider. This function has the same inputs as the bribe function of the includers.

Prior Knowledge   All parties know their type and the sets $\text{Bribe}^{CM}, \text{Bribe}^{BP}$. The block producer knows the type of every includer. This assumption simplifies the model without weakening its implications, because the types of the includers affect the utility of the block producer only via the inclusion lists they create, which the block producer learns immediately.

3.2   Phases and Allocation Rules

Phase 1   In the first phase, users, includers, and the block producer may send transactions to the mempool. The strategies of the parties for this phase are as follows:

- User: the bid b_t per unit of size for transaction t.

- Includer: The set of fake transactions, $F^{Init}_{j, \mu_{CM_j}^{Bribe}}$ they send to the mempool. $\mu_{CM_j}^{Bribe}$ is the type of the includer j.

- Block producer: The set of fake transactions $F^{Init}_{\mu_{BP}^{Bribe}}$ it sends to the mempool. μ_{BP}^{Bribe} is the type of the block producer.

When the type of the includer and the block producer is implied by the context we write F^{Init}_j and F^{Init}_{BP} .

Phase 2   During this phase, every includer j creates at most one inclusion list denoted by $\text{IL}_{j, \mu_{CM_j}^{Bribe}}$, where $\mu_{CM_j}^{Bribe}$ is the type of the includer. When the type of the includer is denoted by the context we write IL_j. In this list, they can include transactions from M and fake transactions created by themselves in this phase. The set of these fake transactions is denoted by $F_{j, \mu_{CM_j}^{Bribe}}$ (when the type of the includer is implied by the context, the set is denoted by F_j). The includers send their inclusion lists to the block producer.

The strategy of includer j of type $\mu_{CM_j}^{Bribe}$ consists of $F_{j, \mu_{CM_j}^{Bribe}}$ and the following allocation rule that determines which transactions from M are included in $\text{IL}_{j, \mu_{CM_j}^{Bribe}}$.

Definition 1. *__Allocation rule for a includer__ j __of type__ $\mu_{CM_j}^{Bribe}$ is a vector-value function $x^{j, \mu_{CM_j}^{Bribe}}$ that takes as input H and M and outputs $x_t^{j, \mu_{CM_j}^{Bribe}}(H, M) \in \{0, 1\}$ for every transaction $t \in M$. When the type of the includer j is implied by the context, we write x^j and x_t^j. $x_t^j(H, M) = 1$ indicates that includer j has included t in their inclusion list, and $x_t^j(H, M) = 0$ the opposite.*

Phase 3 In this phase the block producer receives the list of inclusion lists $\mathsf{IL} = \{\mathsf{IL_1}, \ldots, \mathsf{IL_d}\}$ where $d \leq m$ and creates a block B_k with transactions from M and/or fake transactions issued by themselves in this phase. The set of these fake transactions is denoted by $F_{\mu_{BP}^{Bribe}}$, where μ_{BP}^{Bribe} is the type of the block producer. If the type of the block producer is implied by the context we write F_{BP}.

They may want to include fake transactions in their block: (i) to capture space and exclude transactions that were in the inclusion lists while adhering to the conditions the inclusion lists put on the block; (ii) to affect their payments; or (iii) to make a transaction $t \in F_{BP}^{Init} \cap \mathsf{IL}$ invalid and ensure it can be omitted (thereby avoiding the base fee and the fee for the includers) without risking the block being ignored by the attesters. We assume that the block producer can invalidate all the transactions in $F_{BP}^{Init} \cap \mathsf{IL}$ originating from the same sender with a single fake transaction included in B_k.

The strategy of a block producer of type μ_{BP}^{Bribe} consists of $F_{\mu_{BP}^{Bribe}}$ and the following allocation rule that determines which transactions from M will be included in B_k.

Definition 2. *__Allocation rule for the block producer of type μ_{BP}^{Bribe}__ is a vector-value function $x^{BP,\mu_{BP}^{Bribe}}$ that takes as input H, M and inclusion lists IL, and outputs $x_t^{BP,\mu_{BP}^{Bribe}}(H, M, \mathsf{IL}) \in \{0, 1\}$ for every transaction $t \in M \cup \mathsf{IL}$. When the type of the block producer is implied by the context, we write x^{BP} and x_t^{BP}. $x_t^{BP}(H, M, \mathsf{IL}) = 1$ indicates that the block producer has included t in their block, and $x_t^{BP}(H, M, \mathsf{IL}) = 0$ the opposite.*

Definition 3. *__Feasible allocation rules and set of transactions__.*

- *An allocation rule x^j is inclusion list-feasible if for every H, M it holds:*

$$\sum_{t \in M} x_t^j(H, M) \cdot s_t \leq C_{Incl}$$

- *An allocation rule x_t^{BP} is block-feasible if for every H, M, IL it holds:*

$$\sum_{t \in M} x_t^{BP}(H, M, \mathsf{IL}) \cdot s_t \leq C_{Block}$$

- *A set of transactions T is inclusion list-feasible if $\sum_{t \in T} s_t \leq C_{Incl}$.*

- *A set of transactions T is block-feasible if $\sum_{t \in T} s_t \leq C_{Block}$.*

Definition 4. *When the types of the block producer and the includers are implied by the text, **the inclusion list vector** $\vec{\alpha}_t \in \{0,1\}^{m+1}$ indicates whether the block producer and includers included transaction t. If and only if the block producer included transaction t in its block B_k, then $\vec{\alpha}_t[0] = 1$, and 0 otherwise. Similarly, if and only if the jth includer included transaction t in its inclusion list, IL_j, $\vec{\alpha}_t[j] = 1$, and 0 otherwise. When the types are not implied we write $\vec{a}_{t,\mu_{BP}^{Bribe},\mu_{CM_1}^{Bribe},...,\mu_{CM_m}^{Bribe}}$.*
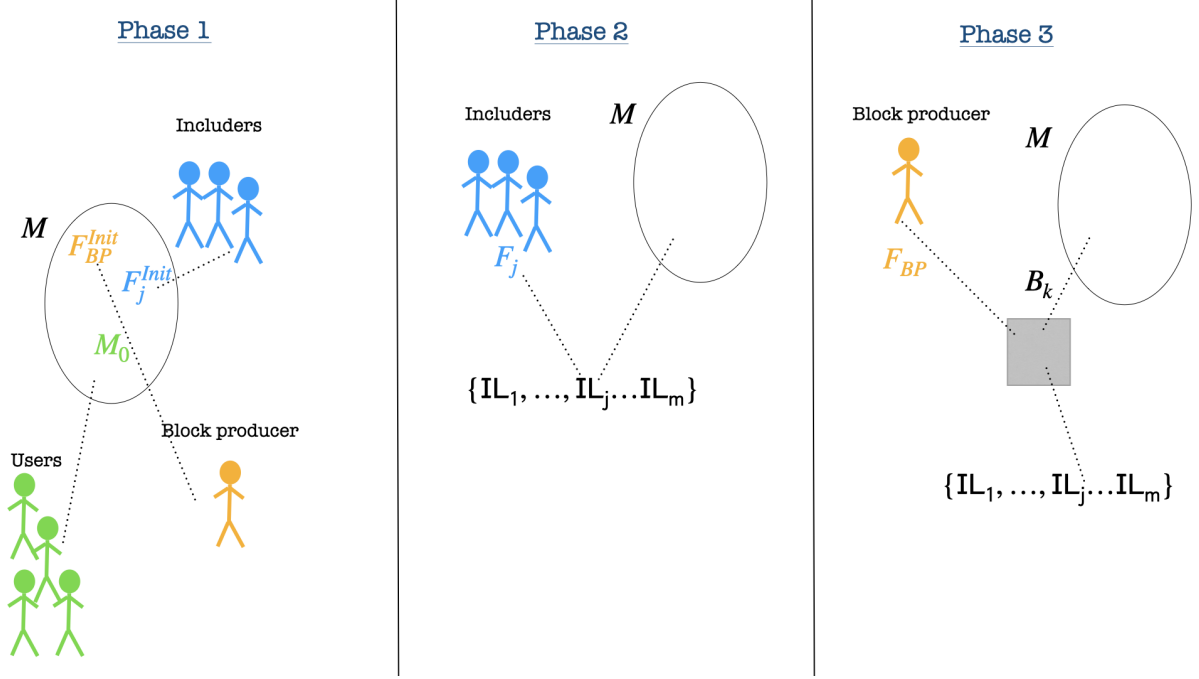

Figure 2: Model Phases. In the first phase, users, includers, and the block producer send transactions to the mempool M. Transactions originating from the includers and the block producer are referred to as fake. In the second phase, includers create inclusion lists with transactions from the mempool M and/or fake transactions issued by themselves during this phase. In the third phase, the block producer constructs their block including transactions from the mempool M, the inclusion lists and/or fake transactions issued by themselves during this phase. The sets $F_{BP}^{Init}, F_j^{Init}$ include the fake transactions submitted by the block producer and includer j respectively during the first phase. M_0 is the set with transactions sent by the users. F_j is the set with the fake transactions includer j adds directly (without sending to the mempool) to their inclusion list and F_{BP} the set with the fake transactions the block producer includes directly in their block.

3.3 Payments and Costs

At the end of the game, the parties receive some payments and incur some costs based on their strategy and the strategies of the other parties.

Payments when the block is approved (not ignored) by the attesters:

Assume that the types of the parties are implied by the context.

Definition 5. *The payment rule for the block producer is a function $p^{BP}(H, B_k, \alpha)$ that takes as input H, B_k, α and outputs the payment $p_t^{BP}(H, B_k, \alpha)$ of the block producer per unit of size for the transaction $t \in B_k$, if the attesters approve block B_k.*

Definition 6. *The payment rule for the includer j is a function $p^{CM}(H, B_k, \alpha, j)$ that takes as input H, B_k, α, j and outputs the payment $p_t^{CM}(H, B_k, \alpha, j)$ of the includer j per unit of size for the transaction $t \in B_k$, if the attesters approve block B_k.*

Costs when the block is approved by the attesters:

1. The sender of the transaction pays an amount that is burnt by the system (for instance, in Ethereum, this is the base fee, a protocol-computed reserve price determined by the burning rule of EIP-1559 [11]).

   Definition 7. *The burning rule is a function $q(H, B_k)$ that takes as input H and B_k and outputs the amount $q_t(H, B_k)$ that is burnt per unit of size for every transaction $t \in B_k$.*

2. The block producer incurs cost μ_{BP}^{Cost} per unit of size for every transaction they include in their block. This cost does not apply to their fake transactions.

Costs regardless whether the block is approved by the attesters:

Assume that the types of the parties are implied by the context.

1. The block proposer pays for every fake transaction t they have included in the mempool during Phase 1 ($t \in F_{BP}^{Init}$) γ fraction of the payment awarded to the block producer and the committee for this transaction ($p_t^{BP}(H, B_k, \alpha)$ and $\sum_{j=1}^{m} p_t^{CM}(H, B_k, \alpha, j)$ respectively, multiplied by s_t). This captures the scenario where the block producer is unsure whether they will be the creator of B_k so that they can invalidate their initial fake transactions. As a result, they risk forfeiting the associated fees, which would otherwise go to the creator of B_k and the includers. If the block producer is certain they will be the creator of B_k, then $\gamma = 0$.

2. If the includers and the block producer include a transaction initiated by the users in their inclusion list or block respectively, they forfeit the reward they would have received from the briber if they had excluded it.

   Definition 8. *Assuming that the types of the parties are implied by the context, the loss of bribe is the following:*

   - *For every transaction $t \in B_k \cap M_0$, the block producer of type μ_{BP}^{Bribe} incurs bribe loss $\mu_{BP}^{Bribe}(s_t, b_t, p_t, \vec{\alpha}_t, H, M_0)$.*
   - *For every transaction $t \in \mathsf{IL_j} \cap M_0$ an includer j of type $\mu_{CM_j}^{Bribe}$ incurs bribe loss $\mu_{CM_j}^{Bribe}(s_t, b_t, p_t, \vec{\alpha}_t, H, M_0)$.*

3. Every includer incurs cost μ_{CM}^{Cost} per unit of size for every transaction they include in their inclusion list, not originated from them (regardless of whether this transaction is included in the block).

3.4 Utilities

Let us first define the utilities of the parties when the types of all the parties are fixed (denoted by $\mu_{BP}^{Bribe}, \mu_{CM_1}^{Bribe}, \ldots \mu_{CM_m}^{Bribe}$) and known to all the other parties.

Utility of the user when the types of the parties are fixed and known:

At a high level, when the transaction of the user is included in the current block and the block is approved by the attesters, they gain the value of the transaction per unit of size. Moreover, they pay the priority fee to the includers and the block producers (if any, depending on the payment mechanism), and the burning fee, per unit of size.

Definition 9. *Utility of a user who sent a transaction t with value v_t and size s_t.*

- *If $t \in B_k$ and B_k meets protocol's predetermined criteria for inclusion lists (this means that it is approved by the attesters) then*

$$u_t(b_t, H, B_k, \alpha) = \left(v_t - p_t^{BP}(H, B_k, \alpha) - \sum_{j \in \{1, \ldots, m\}} p_t^{CM}(H, B_k, \alpha, j) - q_t(H, B_k)\right) \cdot s_t$$

- *Otherwise: $u_t(b_t, H, B_k, \alpha) = 0$.*

Utility of includer j when the types of the parties are fixed and known:

At a high level, if B_k is approved by the attesters, for every transaction in B_k not originated from the includer (this means that it does not belong to $F_j \cup F_j^{Init}$), the includer receives the corresponding transaction fee. In addition, for every transaction from M_0 in their inclusion list, they lose the bribe. Furthermore, for every transaction in their inclusion list, not created by them, they lose the per unit of size cost μ_{CM}^{Cost}. Finally, if B_k is approved by the attesters, they pay the burning fee and the payment for the block producer and the other includers, per unit of size for every fake transaction in B_k they have submitted to the mempool or they have included in their inclusion list.

Definition 10. *Utility of the includer j.*

- *If B_k meets protocol's predetermined criteria for inclusion lists:*

$$u_{CM}(b_t, H, B_k, \alpha, j) =$$
$$\sum_{t \in B_k \cap \neg(F_j \cup F_j^{Init})} [p_t^{CM}(H, B_k, \alpha, j) \cdot s_t]$$
$$- \sum_{t \in \mathsf{IL_j} \cap M_0} [\mu_{CM_j}^{Bribe}(s_t, b_t, p_t, \vec{\alpha}_t, H, M_0)] - \sum_{t \in \mathsf{IL_j} \cap \neg(F_j \cup F_j^{Init})} [\mu_{CM}^{Cost} \cdot s_t]$$
$$- \sum_{t \in B_k \cap (F_j \cup F_j^{Init})} \left[q_t(H, B_k) + p_t^{BP}(H, B_k, \alpha) + \sum_{i \in \{1, \ldots, m\} \setminus j} p_t^{CM}(H, B_k, \alpha, i)\right] \cdot s_t$$

- *Otherwise: The same as above with the difference that the first and the third term are equal to 0.*

> **Utility of the producer when the types of the parties are fixed and known**:
>
> At a high level, if B_k is approved by the attesters, for every transaction in B_k, the block producer receives the corresponding fee and incurs the cost μ_{BP}^{Cost}, per unit of size (except for the transactions that originated from the block producer). Moreover, regardless whether B_k is approved by the attesters, for every transaction in M_0, the block producer loses the bribe. Additionaly, if B_k is approved by the attesters, for every fake transaction in B_k created by them, they pay the burning fee and the fee for the includers per unit of size. Finally, for every transaction they submitted to the mempool in Phase 1, they pay γ fraction of the fee that corresponds to the block producer and the committee.
>
> **Definition 11.** *Utility of the block producer.*
> *Let Fee_t be the total fee per unit of size that a transaction t gives to the committee and the block producer when it is included in both an inclusion list and a block. The structure of this fee depends on the specifics of the bid b_t and the fee mechanism under examination.*
>
> - *If B_k meets protocol's predetermined criteria for inclusion lists:*
>
> $$
> \begin{aligned}
> & u_{BP}(b_t, H, B_k, \alpha) \\
> &= \sum_{t \in B_k \cap \neg (F_{BP} \cup F_{BP}^{Init})} [(p_t^{BP}(H, B_k, \alpha) - \mu_{BP}^{Cost}) \cdot s_t] \\
> &\quad - \sum_{t \in B_k \cap M_0} [\mu_{BP}^{Bribe}(s_t, b_t, p_t, \vec{\alpha}_t, H, M_0)] \\
> &\quad - \sum_{t \in B_k \cap (F_{BP}^{Init} \cup F_{BP})} \left[\left(q_t(H, B_k) + \sum_{i \in \{1,\dots,m\}} p_t^{CM}(H, B_k, \alpha, i) \right) \cdot s_t \right] \\
> &\quad - \sum_{t \in F_{BP}^{Init}} [\gamma \cdot Fee_t \cdot s_t]
> \end{aligned}
> $$
>
> - *Otherwise: The same with the difference that the first and the third term are equal to 0.*

Utilities when the users and the includers do not know the type of the other includers and the block producer; they know only their type. The utility is defined in the same way as in interim stage Bayesian games. The final utility for each type of user and includer is the sum of the utilities for all possible combinations of the other parties' types (based on $\text{Bribe}^{CM}, \text{Bribe}^{BP}$), weighted by the probability that they believe each combination occurs.

3.5 Formal Definition of the Multiple Proposer Transaction Fee Mechanism and its Properties

Assume

- Sets of candidate bribe functions $\text{Bribe}^{CM}, \text{Bribe}^{BP}$.

- Beliefs of the parties about the bribe functions of the other parties, denoted by $\{\text{Belief}_{\text{User}_i \to \text{Users}}, \text{Belief}_{\text{User}_i \to \text{CM,BP}}\}_{j \in \{1, \ldots n\}}, \text{Belief}_{CM}$.

- Parameter γ related to the probability that the block producer is not the creator of the block.

Multiple Proposer Transaction Fee Mechanism A Multiple Proposer Transaction Fee Mechanism (TFM) under the above sets and parameters is the following tuple :

$$(\{x^{BP, \mu_{BP}^{Bribe}}\}_{\mu_{BP}^{Bribe} \in \text{Bribe}^{BP}}, \{x^{j, \mu_{CM_j}^{Bribe}}\}_{\forall \mu_{CM_j}^{Bribe} \in \text{Bribe}^{CM}}, p^{CM}, p^{BP}, q)$$

Note that we consider Transaction Fee Mechanisms where all the includers of the same type have the same allocation rule.

Dominant-Strategy Incentive Compatible (DSIC) A Multiple Proposer Transaction Fee Mechanism is DSIC under the above sets and parameters if the following holds:

Assuming that the includers and the block producer of all types in $\text{Bribe}^{CM}, \text{Bribe}^{BP}$ follow the indicated allocation, every user has a dominant strategy no matter their beliefs for the transactions and the types of the other users.

Myopic Committee Bayesian-Nash Incentive Compatible (MCBN) A Multiple Proposer TFM is MCBN under the above sets and parameters if the following holds for an includer j:

For every H, M_0, assume that:

- Every type of block producer in Bribe^{BP} follows the indicated allocation rule and does not add any fake transactions to their block and the mempool.

- Every type of the other includers in Bribe^{CM} follows the indicated allocation rule and does not add any fake transactions to their inclusion list and the mempool.

Then, for every type in Bribe^{CM}, the best response for the includer j of this type, based on their beliefs Belief_{CM}, is to follow the indicated allocation rule and refrain from adding fake transactions to the mempool and their inclusion list (F_j, F_j^{Init} are empty).

Myopic Block Producer Bayesian-Nash Incentive Compatible (MBBN) A Multiple Proposer TFM is MBBN under the above sets and parameters if the following holds:

For every H, M_0, if all the types of the includers follow the indicated allocation rules and do not add any fake transactions to their inclusion lists and the mempool then: for every type in Bribe^{BP}, the best response for the block producer of this type is to follow the indicated allocation rule and refrain from adding fake transactions to the mempool and to their block (F_{BP}, F_{BP}^{Init} are empty).

Myopic Block Producer Incentive Compatible (MBIC) A Multiple Proposer TFM is MBIC under the above sets and parameters if the following holds:

For every H, M_0 and strategy of the includers, for every type in Bribe^{BP}, the best response for the block producer of this type is to follow the indicated allocation rule and refrain from adding fake transactions to the mempool and to their block (F_{BP}, F_{BP}^{Init} are empty).

MBBN vs MBIC Note that MBBN is a weaker property than MBIC because it makes a (Nash equilibrium related) assumption for the strategy of the includers. Moreover, if MCBN is combined with MBBN, then this means that the strategy profile where (i) all the types of the includers follow the indicated allocation and they do not add fake transactions to the mempool and their inclusion lists and (ii) all the types of the block producer follow the indicated allocation rule and they do not add fake transactions to the mempool and their block is a Bayesian Nash equilibrium.

Censorship resistant A Multiple Proposer TFM is Censorship resistant under the above sets and parameters if the following holds:

The allocation rules of all the types in Bribe^{CM} of the includers and the types in Bribe^{BP} of the block producer ignore the bribing functions.

Fair-under-congestion A Multiple Proposer TFM is fair-under-congestion under the above sets and parameters if the following holds:

Assume arbitrary H, M_0 that is not block-feasible and types of includers and block producer in Bribe^{CM}, Bribe^{BP} respectively. Let

- $\{\mathsf{IL}_1, \ldots, \mathsf{IL_d}\}$ be the inclusion lists if all the includers follow the indicated allocation rule and do not add fake transactions to the mempool and their inclusion list.

- B_k be the block if the block proposer follows the indicated allocation rule and does not add any fake transactions to the mempool and the block.

Then, for every $t \in M_0 \backslash B_k$, there is a bidding strategy the user could follow for their transaction to be included in at least one inclusion list and the block, assuming that all the other transactions remain the same and the includers and block producer adhere to the indicated allocation rules and they do not add any fake transactions.

Block producer and committee fee In the definition of the Multiple Proposers TFMs that we introduce, we use the following terms:

Definition 12. *Block producer fee of a transaction t is the amount the sender of t will pay to the block producer if they include the transaction in their block.*

*Committee fee of a transaction t is the amount the sender of t will pay to the committee if the transaction is included in an inclusion list **and** the block.*

In our proofs, for simplicity, we assume that all the transactions have the same size denoted by s, but in Section 4.3, we explain how our theorems are affected if we remove this assumption. Moreover, we denote by r the burning fee per unit of size.

4 Double TFM

In this section, we examine the Double Multiple Proposer TFM. In this TFM, a transaction's bid is defined as $b_t = (\delta_t^{CM}, \delta_t^{BP}, c_t)$, where δ_t^{CM} is the maximum fee per unit of size for the committee, δ_t^{BP} is the maximum fee per unit of size for the block producer, and c_t is the maximum amount per unit of size the user is willing to pay for all the fees and the burning fee. The block producer fee (Definition 12) is equal to $\max\{\min\{\delta_t^{BP} \cdot s, c_t \cdot s - r \cdot s\}, 0\}$, and the committee fee (Definition 12) is equal to $\max\{\min\{\delta_t^{CM} \cdot s, c_t \cdot s - r \cdot s - \min\{\delta_t^{BP} \cdot s, c_t \cdot s - r \cdot s\}\}, 0\}$. The entire committee fee is awarded to the includer (if any) with the smallest order who includes the transaction in their inclusion list.

- Let t_0 be the target transaction that the external briber seeks to censor by offering bribes to the includers and/or block producer.

- Let $c_{Incl} := \lfloor C_{Incl}/s \rfloor$ be the maximum number of transactions an inclusion list can store.

- Let $c_{block} := \lfloor C_{block}/s \rfloor$ be the maximum number of transactions a block can store.

- Let $r := q_t(H, B_k) = q_t(H)$ be the burning fee per unit of size for a transaction t included in B_k according to EIP-1559. Recall that H is the history of blocks.

- Let w be the number of transactions in M_0.

- Given M_0, we define the following two ordered lists of transactions:

    - L_{BP}: This list consists of the transactions in M_0 that have block producer fee no smaller than $\mu_{BP}^{Cost} \cdot s$. This list is ordered by the block producer fee. The ordering is decreasing. The ties break according to a deterministic rule. The block producer fee corresponding to position j is denoted by $f_{j,BP}$. If there is no position j in the list, we consider that $f_{j,BP} = 0$.

    - $L_{CM,c_{block}}$: This list consists of the transactions in M_0 that (i) belong to the first c_{block} positions in L_{BP} (or to L_{BP} if L_{BP} has fewer than c_{block} positions) (ii) have committee fee no smaller than $\mu_{CM}^{Cost} \cdot s$. This list is ordered by the committee fee. The ordering is decreasing. The ties break according to a deterministic rule. The committee fee corresponding to position j is denoted by $f_{j,CM}$.

    We assume that t_0 belongs to the first $\min\{c_{Incl} \cdot m, size_{L_{CM,c_{block}}}\}$ positions in $L_{CM,c_{block}}$, where $size_{L_{CM,c_{block}}}$ is the size of $L_{CM,c_{block}}$. We adopt this assumption because, under the allocation rule defined below, any transaction that fails to meet these requirements would not be included in either the inclusion list or the block, even in the absence of a bribe.

- Let $size_{L_{BP}}$ be the size of L_{BP}.

- Let $sum_{max,c_{block}}$ be the sum of the rewards (block producer fee minus $\mu_{BP}^{Cost} \cdot s$ per transaction) the block producer will receive if they include the first $\min\{c_{block}, size_{L_{BP}}\}$ transactions of L_{BP} in their block.

- Let o be the order of t_0 in $L_{CM,c_{block}}$ and o_{BP} be the order of t_0 in L_{BP}.

- Let f_{CM}, f_{BP} be the committee and the block producer fee of t_0 respectively.

4.1 Formal Definition of Double TFM

Let us first define the parameters, bribe functions and beliefs for the Double TFM. We assume an arbitrary parameter γ related to the probability that the block producer is not the creator of the block.

Sets of candidate bribe functions $\mathbf{Bribe}^{CM}, \mathbf{Bribe}^{BP}$ At a high level, when $w \leq c_{block}$, the block producer's bribe function offers a bribe that does not exceed the loss incurred by

omitting a transaction from the inclusion list by:

- Ignoring the target transaction without adding any fake transactions (thereby their block being rejected by the the attesters).

- Adding fake transactions to the block to fill its capacity and thereby being able to omit the target transaction without their block being rejected by the attesters. For every fake transaction they add to the block, they pay the burning fee $r \cdot s$.

- Adding fake transactions to the mempool to make the includers ignore the target transaction. To achieve this they need to:

  - Assign a committee fee to the fake transactions that is sufficiently high to render them more profitable for includers than the target transaction.

  - Assign a block producer fee to the fake transactions such that includers are led to believe they will be included in the block. Note that includers have no incentive to include transactions that are unlikely to be selected by the block producer, as they would receive no fees from such transactions.

  - Add a fake transaction to the block to invalidate the previously inserted fake transactions in the mempool, thereby avoiding payment of the committee fee and the block producer fee they had set. They still pay a γ fraction of these fees to account for the possibility that the block producer may not be the proposer for the current slot, in which case the transactions could be included in the subsequent block. The number of fake transactions that must be added to the block in order to invalidate those previously placed in the mempool - and thus the incurred cost —depends on whether multiple inclusion list entries from the same sender are permitted.

[2] When $w > c_{block}$ the intuition behind the bribe function is as follows: when the mempool contains more transactions than can be included in a block (i.e., under congestion), the block producer can omit a transaction in order to accept a bribe, without needing to insert fake transactions into either the mempool or the block to avoid rejection by attesters. However, if the bribe does not cover the amount the block producer will lose if they include the transaction with order $c_{block} + 1$ in L_{BP} instead of t_0, the bribe is disregarded.

---

[2]Note that when $w \leq c_{block}$, if the target transaction is **not** included in an inclusion list, then the block producer loses $f_{BP} - \mu_{BP}^{Cost} \cdot s$ by censoring it. This amount is lower than the bribe specified above. However, as we use the above bribe functions to prove that the Double TFM is MBBN, the bribe function does not need to take into account this fact; the includers always include the target transaction in their inclusion lists when they follow the indicated allocation rule that we describe below. On the other side, if we wanted to prove that the Double TFM is MBIC then the value of the bribe function would be at most $f_{BP} - \mu_{BP}^{Cost} \cdot s$, when $w \leq c_{block}$.

Set Bribe^{CM}

The Bribe^{CM} consists of the following three functions.

- $\mu_{1,CM}^{Bribe}$: This function gives to the includer $f_{CM} - \max\{f_{g,CM}, \mu_{CM}^{Cost} \cdot s\}$, where $g = c_{Incl} \cdot \lceil \frac{o}{c_{Incl}} \rceil + 1$ if they omit this transaction (regardless of the strategy of the other includers).

- $\mu_{2,CM}^{Bribe}$: This function gives to the includer $f_{CM} - \max\{f_{g,CM}, \mu_{CM}^{Cost} \cdot s\}$, where $g = c_{Incl} \cdot \lceil \frac{o}{c_{Incl}} \rceil + 1$ if they omit this transaction and all the other includers and the block producer do the same.

- $\mu_{3,CM}^{Bribe}$: This function gives an X to the includer if they omit this transaction (regardless of the strategy of the other includers). X can be any non negative real number.

<u>Set Bribe^{BP}</u>

Bribe^{BP} consists of the following bribe function $\mu_{1,BP}^{Bribe}$.

- When $w > c_{block}$: This function gives to the block producer

$$f_{BP} - \max\{f_{c_{block}+1,BP}, \mu_{BP}^{Cost} \cdot s\}$$

  if they omit the transaction regardless of the strategy of the includers.

- When $w \leq c_{block}$.

  If at most one transaction per sender is allowed to be added to an inclusion list, the function $\mu_{1,BP}^{Bribe}$ gives to the block producer:

$$\min\{f_{BP} - \mu_{BP}^{Cost} \cdot s + r \cdot s \cdot (c_{block} - w + 1),$$

$$sum_{max,c_{block}},$$

$$f_{BP} - \mu_{BP}^{Cost} \cdot s$$

$$+ (c_{block} - o_{BP} + 1) \cdot \gamma \cdot f_{BP} + \lceil \frac{(c_{block} - o_{BP} + 1)}{m} \rceil \cdot r \cdot s,$$

$$f_{BP} - \mu_{BP}^{Cost} \cdot s +$$

$$\gamma \cdot (\min\{m \cdot c_{Incl}, size_{L_{CM},c_{block}}\} - o + 1) \cdot$$

$$(f_{CM} + \max\{f_{c_{block}-(\min\{m \cdot c_{Incl}, size_{L_{CM},c_{block}}\}-o+1)+1,BP}, \mu_{BP}^{Cost} \cdot s\})$$

$$+ \lceil \frac{(\min\{m \cdot c_{Incl}, size_{L_{CM},c_{block}}\} - o + 1)}{m} \rceil \cdot r \cdot s\}$$

  If multiple transactions per sender are allowed to be added to an inclusion list, the function $\mu_{1,BP}^{Bribe}$ gives to the block producer:

$$\min\{f_{BP} - \mu_{BP}^{Cost} \cdot s + r \cdot s \cdot (c_{block} - w + 1),$$

$$sum_{max,c_{block}},$$

$$f_{BP} - \mu_{BP}^{Cost} \cdot s + (c_{block} - o_{BP} + 1) \cdot \gamma \cdot f_{BP} + r \cdot s,$$

$$f_{BP} - \mu_{BP}^{Cost} \cdot s + \gamma \cdot (\min\{m \cdot c_{Incl}, size_{L_{CM},c_{block}}\} - o + 1) \cdot$$

$$(f_{CM} + \max\{f_{c_{block}-(\min\{m \cdot c_{Incl}, size_{L_{CM},c_{block}}\}-o+1)+1,BP}, \mu_{BP}^{Cost} \cdot s\}) + r \cdot s\}$$

Types of the includers and the block producer The block producer is of type $\mu_{1,BP}^{Bribe}$. The includer with order $\lceil \frac{o}{c_{Incl}} \rceil$ is of type $\mu_{1,CM}^{Bribe}$ or of type $\mu_{2,CM}^{Bribe}$. The other includers can be of type $\mu_{1,CM}^{Bribe}$, $\mu_{2,CM}^{Bribe}$ or $\mu_{3,CM}^{Bribe}$.

Beliefs of the parties about the bribe functions of the other parties The beliefs of the users for the other users are arbitrary. The users and the includers know that the type of the block producer is $\mu_{1,BP}^{Bribe}$ with probability 1. Every user and every includer believes that the every other includer is of type $\mu_{1,CM}^{Bribe}$, $\mu_{2,CM}^{Bribe}$ or $\mu_{3,CM}^{Bribe}$ with arbitrary probability.

Double TFM   The *Double TFM* under the above parameters, bribe functions and beliefs is defined as follows:

$$(\{x^{BP,\mu_{BP}^{Bribe}}\}_{\mu_{BP}^{Bribe}\in\text{Bribe}^{BP}}, \{x^{j,\mu_{CM_j}^{Bribe}}\}_{\mu_{CM_j}^{Bribe}\in\text{Bribe}^{CM}}, p^{CM}p^{BP}, q)$$

where:

- μ_{BP}^{Bribe} is always equal to $\mu_{1,BP}^{Bribe}$ defined above.

- For every includer j, $\mu_{CM_j}^{Bribe}$ is equal to:

    - $\mu_{1,CM}^{Bribe}$ or $\mu_{2,CM}^{Bribe}$ if the order of the includer is equal to $\lceil\frac{o}{c_{Incl}}\rceil$.
    - $\mu_{1,CM}^{Bribe}$ or $\mu_{2,CM}^{Bribe}$ or $\mu_{3,CM}^{Bribe}$ otherwise.

- Burning rule q is the Ethereum's burning rule (EIP-1559).

- p^{CM}: For every transaction not included in the block, they receive zero fees. For every transaction t with a bid $b_t = (\delta_t^{CM}, \delta_t^{BP}, c_t)$ added to the block, the includer is paid as follows: If this includer is the member with the smallest order who has added this transaction to their inclusion list, they receive the entire committee fee - namely $\max\{\min\{\delta_t^{CM}\cdot s, c_t\cdot s - r\cdot s - min\{\delta_t^{BP}\cdot s, c_t\cdot s - r\cdot s\}\}, 0\}$. Otherwise, they receive zero fees.

- p^{BP}: For every transaction included in their block, they receive the block producer fee, regardless of whether this transaction has been included in an inclusion list. Recall that this fee is equal to $\max\{\min\{\delta_t^{BP}\cdot s, c_t\cdot s - r\cdot s\}, 0\}$.

- For the type in Bribe^{BP}, t**he allocation rule for the block producer** is the following: They select transactions satisfying

  ($c_t \geq r + \mu_{BP}^{Cost}, \delta_t^{BP} \geq \mu_{BP}^{Cost}$), prioritizing those with the highest block producer fee until they make their block full or there are no other available transactions.

- For every type in Bribe^{CM}, **the allocation rule of every includer** is the following:

  Every includer with order j (the best order is 1) chooses the following deterministic algorithm: First, the includer computes the set of transactions that a block producer, adhering to the specified allocation rule, would include in their block. The includer then removes from the mempool all transactions not belonging to this set. Additionally, the includer excludes any transactions offering a committee fee lower than $\mu_{CM}^{Cost}\cdot s$. After that the includer:

    - Computes the subset of transactions from the mempool M that maximise the utility of includer with order 1, if they are included in their inclusion list. As we have assumed that every transaction has the same size, this corresponds to the set of transactions offering the highest committee fees.
    - Removes these transactions from the mempool M.
    - Repeats the same procedure for the includers with order $2, \ldots, j-1$.
    - Selects the transactions that yield the highest committee fees for inclusion.

4.2 Properties of Double TFM

"Usually" DSIC   EIP-1559 mechanism is proved to be "usually" DSIC in [13]. With "usually" the author means that EIP-1559 is DSIC under the following assumptions: Let us fix a history of blocks H.

- The burning fee r per unit of size in this slot is not excessively low, meaning that the total size of all the transactions in the mempool satisfying $v_t \geq r$ (recall v_t is the value of transaction t) does not exceed the available space in the current block.

- The users cannot overbid, which means that they cannot set for their transaction t a total fee c_t that is higher than their transaction value v_t.

Theorem 1. *Assume a history of block H and a set of transactions T of the same size. If the users cannot overbid and the burning fee r per unit of size for this slot is not excessively low then: assuming that all the types of includers and the block producer adhere to the indicated allocation rules, the following bidding strategy for a transaction t: $b_t = (\delta_t^{CM}, \delta_t^{BP}, c_t) = (0, \mu_{BP}^{Cost}, \min\{v_t, r + \mu_{BP}^{Cost}\})$ constitutes a dominant strategy for every user, irrespective of their beliefs.*

For the proof cf. Appendix B.1.

Note that in the current model, the inclusion lists are conditional. If they were unconditional and also the following hold:

- $c_{block} > m \cdot c_{Incl} \geq w$

- The indicated allocation rule for the block producer was to include all the transactions from the inclusion lists even if the transactions offer a block producer fee lower than $\mu_{BP}^{Cost} \cdot s$,

then under the same assumptions as the above theorem, the dominant strategy of the users would be:

- $b_t = (\delta_t^{CM}, \delta_t^{BP}, c_t) = (0, \mu_{BP}^{Cost}, \min\{v_t, r + \mu_{BP}^{Cost}\})$, if $\mu_{BP}^{Cost} \leq \mu_{CM}^{Cost}$, and

- $b_t = (\delta_t^{CM}, \delta_t^{BP}, c_t) = (\mu_{CM}^{Cost}, 0, \min\{v_t, r + \mu_{CM}^{Cost}\})$, if $\mu_{BP}^{Cost} > \mu_{CM}^{Cost}$.

The intuition behind this result is that, given the allocation rules followed by the includers and the block producer, any transaction included in an inclusion list will also be included in the block. Therefore, the user's most profitable strategy is to cover either the minimum cost required by the includer or the minimum cost required by the block producer.

Myopic Committee Bayesian-Nash Incentive Compatible

Theorem 2. *Double TFM is Myopic Committee Bayesian-Nash Incentive Compatible (MCBN), under the bribe functions and beliefs specified above.*

For the proof cf. Appendix B.2.

Myopic Block Producer Bayesian-Nash Incentive Compatible

Theorem 3. *Double TFM is Myopic Block Producer Bayesian-Nash Incentive Compatible (MBBN) under the bribe functions and beliefs specified above.*

For the proof cf. Appendix B.3.

Censorship resistant   The Double TFM is censorship resistant because the allocation rules of all the types of the includers and the block producer ignore bribes.

Fair-under-congestion

Theorem 4. *Double TFM is fair-under-congestion under the bribe functions and beliefs specified above.*

For the proof cf. Appendix B.4.

4.3   Variations of our Results

Removing the assumption that all the transactions have the same size   In our proofs, for simplicity, we assume that all the transactions have the same size. If we removed this assumption:

- Instead of selecting the transactions with the highest fee, the allocation rule of includers and the block producer would select the set of transactions that maximise the sum of the fees (taking into account also the size of the transaction sizes and C_{block}, C_{Incl}).

- For some mempools, includers would have incentives to add fake transactions to the mempool to "steal" a transaction t_1 from another member with a smaller order. To steal this transaction, they should create a fake transaction t_f that has a size and a committee fee that make t_f more desirable than t_1 for the other includer. This deviation is not significant in the context of censorship, as it does not negatively affect the utility of other includers; in fact, it results in a utility gain for both parties involved.

Allocation rules that do not exclude transactions with a block producer fee lower than $\mu_{BP}^{Cost} > 0$ Note that the above indicated allocation rules of both the includers and the block producer exclude all the transactions with a block producer fee lower than $\mu_{BP}^{Cost} > 0$.

However, when the block is not full, the block producer will lose the block rewards if they omit a transaction from the inclusion list, even if this transaction has a block producer fee lower than $\mu_{BP}^{Cost} > 0$. This means that the indicated allocation rule of the block producer that excludes transactions with a block producer fee lower than $\mu_{BP}^{Cost} > 0$ is not a dominant strategy.

Moreover, at a Nash equilibrium, we can have a variation of the above indicated allocation rules where both the includers and the block producers include transactions with a block producer fee lower than $\mu_{BP}^{Cost} > 0$ in the following case: if the block rewards are higher than the loss the block producer incurs by adding these transactions. Intuitively, this happens because it is more profitable for the block producer to incur some loss from this type of transaction to avoid rejection by the attesters.

The amount of bribe in the bribe functions is tight   The amount of bribe in the bribe functions of the includers and the block producer we have defined is the maximum that can be set so that the theorems still hold.

The impact of adding some includers that always include the target transaction Even if we added this type of includer, the bribe of the block producer specified in their bribe function could not increase. The reason is that in this notion we examine whether the utility of the block producer increases when they deviate assuming that all the types of includers follow the indicated allocation rule, which already ignores bribes.

However, adding these includers could decrease the bribe of the block producer when we try to prove that the Double TFM is MBIC. This notion examines the utility of the block producer for every strategy of includers. If there is no includer that includes the target transaction, then the maximum cost of the block producer to deviate is $f_{BP} - \mu_{BP}^{Cost} \cdot s$. If at least one member includes the target transaction in their block, their cost is the same as this one in the bribe function we use for proving MBBN.

5 Single TFM

In this section, we examine a TFM, denoted by Single TFM, where the user sets a single fee for their transaction and the system determines how this fee will be shared among the committee and the block producer (after the burning fee is subtracted). In more detail, transaction's bid is $b_t = (c_t)$, where c_t is the maximum amount per unit of size the user is willing to pay.

The system splits the fee as follows: after subtracting the burning fee, the block producer receives an amount that is equal to the cost they incur for processing each transaction - namely $\mu_{BP}^{Cost} \cdot s$. If the remaining amount after burning is less than $\mu_{BP}^{Cost} \cdot s$, the block producer receives the entire remaining amount. Any residual amount beyond this is then distributed as follows: z fraction of this amount is allocated to the committee and $(1 - z)$ fraction to the block producer. In Appendix C.5, we examine how z affects the minimum bribe needed for a briber to make a transaction be omitted from a block.

The committee fee is shared in the same way as the previous payment mechanism: it is allocated to the includer with the smallest order who includes this transaction in their inclusion list, if this transaction is included in the block. If no includer includes this transaction in their inclusion list, the user does not pay the committee fee. Formally, the block producer fee is equal to $\max\{\min\{\mu_{BP}^{Cost} \cdot s, c_t \cdot s - r \cdot s\} + \max\{(c_t \cdot s - r \cdot s - \mu_{BP}^{Cost} \cdot s), 0\} \cdot (1 - z), 0\}$, and the committee fee equal to $\max\{(c_t \cdot s - r \cdot s - \mu_{BP}^{Cost} \cdot s), 0\} \cdot z$.

5.1 Notation

We adopt the same notation as in Section 4. In this setting, there is a single fee per transaction that is split according to a fixed rule across all transactions. As a result, the lists $L_{BP}, L_{CM,c_{block}}$ are both ordered by this unified fee. Consequently, ordering by the block producer fee or the committee fee yields the same result. Therefore, the order of t_0 in $L_{CM,c_{block}}$ (denoted by o) and the order of t_0 in L_{BP} (denoted by o_{BP}) are equal.

5.2 Formal Definition of Single TFM

It is everything the same as the definition of the Double Fee TFM apart from the following:

- The definition of the payment functions. In this case, the payment functions are as follows:

  - p^{CM}: For every transaction not included in the block they receive zero fees. For every transaction t with bid $b_t = (c_t)$ added to the block, an includer is paid as follows: If this includer is the committe member with the smallest order who has added this transaction to their inclusion list, they receive the entire committee fee - namely $\max\{(c_t \cdot s - r \cdot s - \mu_{BP}^{Cost} \cdot s), 0\} \cdot z$. Otherwise, they receive zero fees.

  - p^{BP}: For every transaction included in their block, they receive the block producer fee - namely $\max\{\min\{\mu_{BP}^{Cost} \cdot s, c_t \cdot s - r \cdot s\} + \max\{(c_t \cdot s - r \cdot s - \mu_{BP}^{Cost} \cdot s), 0\} \cdot (1 - z), 0\}$.

- The block producer's allocation rule remains the same, except that in this case, they only verify whether $c_t \geq r + \mu_{BP}^{Cost}$, not if $\delta_t^{BP} \geq \mu_{BP}^{Cost}$, as the bid does not contain a separate δ_t^{BP} field.

- In this case, the relation between f_{CM}, f_{BP} is determined by the system rather than the user.

5.3 Properties of Single TFM

"Usually" DSIC

Theorem 5. *Assume a history of block H and a set of transactions T that have the same size. If the users cannot overbid and the burning fee r per unit of size for this slot is not excessively low, then: assuming that all the types of includers and the block producer follow the indicated allocation rules, the following bidding strategy for a transaction t: $b_t = (c_t) = (\min\{v_t, r + \mu_{BP}^{Cost}\})$ is a dominant strategy for every user regardless of their beliefs.*

For the proof cf. Appendix C.1.

Myopic Committee Bayesian-Nash Incentive Compatible

Theorem 6. *Single TFM is Myopic Committee Bayesian-Nash Incentive Compatible (MCBN) under the bribe functions and beliefs specified above.*

For the proof cf. Appendix C.2.

Myopic Block Producer Bayesian-Nash Incentive Compatible

Theorem 7. *Single TFM is Myopic Block Producer Bayesian-Nash IncentiveCompatible (MBBN) under the bribe functions and beliefs specified above.*

For the proof cf. Appendix C.3.

Censorship resistance   Single TFM is censorship resistant because the allocation rules of all the types of includers and the block producer ignore bribes.

Fair-under-congestion

Theorem 8. *Single TFM is fair-under-congestion under the bribe functions and beliefs specified above.*

For the proof cf. Appendix C.4.

6   Single Prioritized TFM

In this section, we show that a TFM with the following characteristics, called *Single Prioritized TFM*, is not fair-under-congestion if $\mu_{BP}^{Cost} > 0$:

- The users set a single fee and the system splits this fee between the block producer and the committee so that:
    - If the transaction is included in an inclusion list and the block, the entire fee ia allocated to the committee.
    - If the transaction is included in the block but is not included in any inclusion list, the entire fee is awarded to the block producer.

- The indicated allocation rule for the block producer is to select the transactions that yield the highest block producer fees.

For the proof cf. Appendix D.

7 Excluding Strategies that Add Fake Transactions to the Mempool

In this section, we consider a simplified model that excludes strategies in which the block producer adds "fake transactions" to the mempool. Under this model, we prove that unconditional inclusion lists increase significantly the minimum bribe an external briber needs to offer to censor a transaction t_0. In more detail, this bribe should be at least the minimum between the block rewards and $m \cdot f_{CM}$, where f_{CM} is the committee fee of t_0. However, in our original model that accounts for strategies in which the block producer adds fake transactions to the mempool the results are different. In both conditional and unconditional inclusion lists, when there is no congestion, the minimum bribe is approximately the cost of this deviation (adding fake transactions to the mempool) plus the block producer fee of this transaction. For the theorems and the proofs cf. Appendix E.

Acknowledgments

References

[1] Berger, B., Felten, E.W., Mamageishvili, A., Sudakov, B.: Economic censorship games in fraud proofs (2025), `https://arxiv.org/abs/2502.20334`

[2] Chung, H., Shi, E.: Foundations of transaction fee mechanism design (2022), `https://arxiv.org/pdf/2111.03151`

[3] Cullen, A., Camargo, D., Vigneri, L.: A purely posted-price transaction fee mechanism for leaderless blockchains. 2024 6th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS) (2024), `https://api.semanticscholar.org/CorpusID:273902575`

[4] Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., Juels, A.: Flash boys 2.0: Frontrunning, transaction reordering, and consensus instability in decentralized exchanges (2019), `https://arxiv.org/abs/1904.05234`

[5] Fox, E., Pai, M., Resnick, M.: Censorship resistance in on-chain auctions (2023), `https://arxiv.org/abs/2301.13321`

[6] Heimbach, L., Kiffer, L., Ferreira Torres, C., Wattenhofer, R.: Ethereum's proposer-builder separation: Promises and realities. In: Proceedings of the 2023 ACM on Internet Measurement Conference. p. 406–420. IMC '23, Association for Computing Machinery, New York, NY, USA (2023), `https://doi.org/10.1145/3618257.3624824`

[7] Karakostas, D., Kiayias, A., Zacharias, T.: Blockchain bribing attacks and the efficacy of counterincentives. In: Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security. p. 1031–1045. CCS '24, Association for Computing Machinery, New York, NY, USA (2024). https://doi.org/10.1145/3658644.3670330, `https://doi.org/10.1145/3658644.3670330`

[8] Ma, J., Monnot, B., Thiery, T.: Uncrowdable inclusion lists: The tension between chain neutrality, preconfirmations and proposer commitments (2024), `https://ethresear.ch`

/t/uncrowdable-inclusion-lists-the-tension-between-chain-neutrality-preco
nfirmations-and-proposer-commitments/19372

[9] Neuder, M., Buterin, V., D'Amato, F., Tsao, T., Darji, M.: EIP-7547: Inclusion lists
(2023), `https://eips.ethereum.org/EIPS/eip-7547`

[10] Neuder, M., Resnick, M.: Concurrent block proposers in ethereum (2024), `https://ethr
esear.ch/t/concurrent-block-proposers-in-ethereum/18777`

[11] Roughgarden, T.: Transaction fee mechanism design for the ethereum blockchain: An
economic analysis of EIP-1559 (2020), `https://timroughgarden.org/papers/eip1559.
pdf`

[12] Roughgarden, T.: Transaction fee mechanism design. In: Proceedings of the 22nd ACM
Conference on Economics and Computation. p. 792. EC '21, Association for Computing
Machinery, New York, NY, USA (2021), `https://doi.org/10.1145/3465456.3467591`

[13] Roughgarden, T.: Transaction fee mechanism design (2023), `https://arxiv.org/abs/21
06.01340`

[14] Thiery, T.: Towards attester-includer separation (2024), `https://ethresear.ch/t/tow
ards-attester-includer-separation/21306`

[15] Thiery, T., D'Amato, F., Ma, J., Monnot, B., Tsao, T., Kaufmann, J., Song, J.: EIP-7805:
Fork-choice enforced inclusion lists (FOCIL) (2024), `https://eips.ethereum.org/EIPS
/eip-7805`

[16] Wadhwa, S., Ma, J., Thiery, T., Monnot, B., Zanolini, L., Zhang, F., Nayak, K.: AUCIL:
An inclusion list design for rational parties. Cryptology ePrint Archive, Paper 2025/194
(2025), `https://eprint.iacr.org/2025/194`

[17] Wahrstätter, A., Ernstberger, J., Yaish, A., Zhou, L., Qin, K., Tsuchiya, T., Steinhorst, S.,
Svetinovic, D., Christin, N., Barczentewicz, M., Gervais, A.: Blockchain censorship (2023),
`https://arxiv.org/abs/2305.18545`

Appendix

A   Overview of Roughgarden's Model [12]

- Every user has a transaction with the following characteristics:
  - s_t: size of the transaction.
  - Value v_t: maximum amount per unit of size that the user is willing to pay for its
    inclusion in the current block B_k. This value is not affected by the position of the
    transaction in the block.

- The users send their transaction t to the mempool M along with a bid b_t that specifies
  the price per unit of size the user offers for this transaction to be included in the current
  block B_k.

- The block producer decides which transactions they will include in their block. In more
  detail, they decide:
  - On an allocation rule x that determines if a transaction from the mempool will be
    added to the current block or not.

- If they include fake transactions created by themselves.

- For every transaction the block producer includes in their block, they incur a cost μ per unit of size. This reflects the minimum amount the block producer is willing to accept to include this transaction in their block if the maximum block size does not play a role in the selection of transactions. The paper assumes that this is the same for all the block producers and known to the users.

- At the end of the game:

  - The block producer is paid for every transaction they include in their block according to a payment rule p. The payment rule is a function that takes as input the history H of the preceding blocks, and the current block B_k and outputs $p_t(H, B_k)$ for every transaction $t \in B_k$ (payment per unit of size in the native currency).

  - The burning rule q determines the amount burnt per unit of size for a transaction t to be included in the current block. It is a function that takes as input (H, B_k) and outputs $q_t(H, M)$, for every transaction t. This amount is paid by the user via the bid.

  - If a user's transaction is included in the current block, the user gains an amount equal to the value v_t and pays an amount no higher than the amount specified by the bid b_t. This amount is determined by the payment rule p and the burning rule q.

  - If a user's transaction is not included in the block, they do not gain or lose anything.

- The Transaction Fee Mechanism (TFM) consists of (x, p, q).

- A TFM (x, p, q) is Dominant-Strategy Incentive Compatible (DSIC) when assuming that the block producer follows the allocation rule x, every user has a dominant strategy, no matter the transaction values or the bids of the other users.

- A TFM (x, p, q) is incentive compatible for a myopic block producer (MMIC), if for every history H and mempool M, the miner maximises their utility:

  - If they follow the allocation rule x.

  - They do not add any fake transactions.

  "myopic" means that they do not consider what will happen in the following slots.

- Roughgarden in [12] proposes a property of a TFM, called Off-Chain Agreement (OCA) that, at a high level, examines whether a coalition between the block producer and the users can increase all their utilities via off-chain payments. More formally:

  - A bidding strategy is a function that on input the value of a transaction outputs its bid.

  - Individual rational bidding strategy is a strategy that offers non-negative utility for all the users if it is collectively implemented.

  - A TFM is OCA if, for every history H, there is an individual rational bidding strategy such that for every set of transactions in the mempool and values, there is no off-chain agreement that can increase strictly the joint utility of all the users and the block producer.

- EIP-1559 mechanism satisfies OCA, MMIC, and "usually" DSIC. By "usually" they mean that the base fee is not excessively low and the users do not overbid [12].

B Proofs for Double TFM

B.1 "Usually" DSIC

Proof. As all the types of includers and block producer adhere to the indicated allocation rule, they ignore bribes. Moreover, all the types of includers and the types of the block producer follow the same indicated allocation rule. Thus the beliefs of the user for the types of includers and the block producer do not affect their utility.

As the base fee is not excessively low, transactions with values higher than r are fewer than c_{block}. Moreover, as the users do not overbid, transactions with $c_t > r$ are also fewer than c_{block}. This means that a block producer who follows the indicated allocation rule, regardless of their type, will include a transaction in their block *if and only if* it holds ($\delta_t^{BP} \geq \mu_{BP}^{Cost}$ and $c_t \geq \mu_{BP}^{Cost} + r$). Furthermore, as the includers follow the indicated rule, they include a transaction in their inclusion list *only if* the block producer fee is higher than $\mu_{BP}^{Cost} \cdot s$.

We have the following cases:

1. $\min\{v_t, r + \mu_{BP}^{Cost}\} = r + \mu_{BP}^{Cost}$: The current utility of a user who bids $b_t = (\delta_t^{CM}, \delta_t^{BP}, c_t) = (0, \mu_{BP}^{Cost}, \min\{v_t, r + \mu_{BP}^{Cost}\})$ in this case is $v_t - r - \mu_{BP}^{Cost} \geq 0$ regardless of their beliefs, because their transaction will be included in the block by the block producer irrespective of the bids of the other users and the type of the block producer. The utility of the user when their transaction is not included in the block is 0. Thus, the user can increase their utility only if they can set a lower c_t and make their transaction still included in the block. The burning fee is r which means that regardless of their choice of $\delta_t^{CM}, \delta_t^{BP}$, if they decrease c_t, the block producer fee becomes lower than $\mu_{BP}^{Cost} \cdot s$. This means that this transaction will not be included in the block.

2. $\min\{v_t, r + \mu_{BP}^{Cost}\} = v_t$. The current utility of the user in this case is zero because the transaction will not be included in the block regardless of the type of the block producer and the other bids. Note that the block producer fee of this transaction is lower than $\mu_{BP}^{Cost} \cdot s$. The only way for the user's transaction to be included in the block is if the user increases c_t. However, if the user increases c_t, then their utility will become negative if this transaction is included in the block.

As a result bid b_t maximises the user's utility regardless of the other bids and their beliefs for the includers and the block producer. □

B.2 Myopic Committee Bayesian-Nash Incentive Compatible (MCBN)

Proof. Assume arbitrary H, M_0 and that every type of all but one includers and block producer follow the indicated allocation rule and do not add fake transactions. We need to prove that every type of the remaining includer denoted by j cannot increase their utility by deviating from the indicated allocation strategy or by adding fake transactions to their inclusion list or to the mempool.

For all the types of includer j, it holds that their beliefs do not affect their utility because all the types of the other includers and the block producer follow the same indicated allocation rule.

Now we prove that the includer cannot increase their utility by deviating from the indicated allocation rule.

If the order of j is not $\lceil \frac{o}{c_{Incl}} \rceil$

- t_0 is not in their inclusion list when they follow the indicated allocation rule, and thus they do not incur any bribe loss. This means that the bribe function that determines their type does not affect their utility. Note that when all the includers follow the indicated allocation

rule, t_0 is included in the inclusion list of the member with order $\min\{\lceil\frac{o}{c_{Incl}}\rceil, m\}$. For example, if $o = 10$ and $c_{Incl} = 3$, then t_0 is included in the inclusion list of the member with order 4.

- All their current transactions offer them a committee fee no smaller than cost $\mu_{CM}^{Cost} \cdot s$. Thus, their utility cannot increase by omitting them.

- They cannot add a transaction already included by an includer with a higher order to their inclusion list, because they have no space (if they had space, then the includers with a higher order would have no transactions in their inclusion lists). If they choose to replace one (or more) of their current transactions with such a transaction, their utility cannot increase; the members with a worse (higher) order include transactions with lower committee fees than their current transactions.

- If they choose to add one (or more) transactions already included by an includer with a smaller order, then their utility will decrease because they will take zero fees for this transaction, and they will incur cost $\mu_{CM}^{Cost} \cdot s$.

- If they choose to add a transaction not included by any includer, then their utility will decrease because this transaction either has a very low block producer fee and thus will not be included in the block (which means that it will give them zero fees) or has a committee fee lower than μ_{CM}^{Cost}.

If the order of j is equal to $\lceil\frac{o}{c_{Incl}}\rceil$

- The includer j incurs bribe loss equal to $f_{CM} - \max\{f_{g,CM}, \mu_{CM}^{Cost} \cdot s\}$, where $g = c_{Incl} \cdot \lceil\frac{o}{c_{Incl}}\rceil + 1$, as they have included t_0 in their inclusion list.

- If they omit t_0, their utility will not increase because they will gain the bribe loss plus $\mu_{CM}^{Cost} \cdot s$, but they will lose f_{CM}.

- If they replace t_0 with a transaction included by an includer with a smaller order then their utility will decrease, as they will receive zero fees from this transaction.

- If they replace t_0 with a transaction included by an includer with a higher order, or a transaction not included in an inclusion list, then the maximum fee they will gain from this transaction will be $\max\{f_{g,CM}, \mu_{CM}^{Cost} \cdot s\}$ and they will lose f_{CM}. $f_{CM} - \max\{f_{g,CM}, \mu_{CM}^{Cost} \cdot s\}$ is no smaller than the bribe loss. Thus, their utility cannot increase.

- Regarding the other transactions, the proof that their utility cannot increase by deviating from the indicated allocation rule is the same as the case when the order of j is not $\lceil\frac{o}{c_{Incl}}\rceil$.

Regardless of their order, includer j cannot increase their utility by adding fake transactions to their inclusion list, because these transactions will give them no extra reward. Moreover, they cannot increase their utility by adding fake transactions to the mempool, because:

1. When this fake transaction does not affect which transactions the other includers or the block producer include in their inclusion list and block respectively, it cannot affect their utility.

2. In order for the fake transaction to affect which transactions the other includers or the block producer include in their inclusion list and block respectively, they need to give a committee fee or a block producer fee that will be paid by includer j.

- When this fake transaction has a committee fee that makes another includer with a smaller order prefer it over another transaction t', then their utility can be affected if they "steal" t'. However, their utility cannot increase because (i) the maximum includer j can gain by this deviation is the committee fee of the omitted transaction t' and (ii) includer j needs to pay the committee fee, the block producer fee and the burning fee of this omitted transaction t'. This means that the utility of the includer will decrease.

- When this fake transaction has a block producer fee that makes another includer with a smaller order prefer it over another transaction t'': recall that the includers who follow the indicated allocation rule choose a transaction only if it belongs to the c_{block} transactions with the highest block producer fee (which is also higher than $\mu_{BP}^{Cost} \cdot s$). In this case, the other includer will prefer the fake transaction over t'' only if, after the addition of the fake transaction, t'' does not belong to the best c_{block} transactions in terms of block producer fee. This means, that even if includer j steals t'', this transaction will give them no reward because it will not be added to the block by the block producer (the block producer will prefer the fake transaction as well).

- When this fake transaction has a block producer fee that makes the block producer omit some other transaction in favour of this fake transaction, then the utility of includer j cannot increase.

$\square$

B.3 Myopic Block Producer Bayesian-Nash Incentive Compatible (MBBN)

Proof. Assume that all the types of includers follow the indicated allocation rule and they do not add fake transactions. This means that transaction t_0 has been included in an inclusion list. Moreover, if the block producer follows the indicated allocation rule and does not add any fake transactions then t_0 will be included in their block.

We prove that the block producer cannot increase their utility by deviating from the indicated allocation rule or by adding fake transactions to the mempool or their block. Note that the utility of the block producer does not depend on their beliefs for the type of includers because all the types follow the same indicated allocation rule.

1. The block producer cannot increase their utility by replacing transactions different from t_0 with other transactions because their indicated allocation rule chooses the set of transactions that offer them the highest block producer fee.

2. The block producer cannot increase their utility by adding more transactions, because there is no other space or available transactions with a block producer fee of at least $\mu_{BP}^{Cost} \cdot s$. Recall that for every transaction in their block, they incur cost $\mu_{BP}^{Cost} \cdot s$.

3. The block producer cannot increase their utility by omitting transactions, because all their current transactions have a block producer fee of at least $\mu_{BP}^{Cost} \cdot s$.

4. The block producer cannot increase their utility by omitting or replacing transaction t_0 regardless of whether there is congestion ($w > c_{block}$) or not.

The proof for the last claim is the following:

When $w > c_{block}$

- If the block producer omits t_0 without adding a new transaction, then they will lose $sum_{max,c_{block}}$ and they will gain the bribe loss which is no higher. Thus, their utility will not increase.

- If the block producer replaces t_0 with another transaction:

  - If $size_{L_{BP}} \geq c_{block}+1$: The most profitable deviation the block producer can perform is to replace transaction t_0 with the transaction that has position $c_{block} + 1$ in L_{BP} . If they do so, they will gain the bribe loss $f_{BP} - \max\{f_{c_{block}+1,BP}, \mu_{BP}^{Cost} \cdot s\} = f_{BP} - f_{c_{block}+1,BP}$ but they will lose $f_{BP} - f_{c_{block}+1,BP}$ because t_0 has a higher block producer fee. Moreover, the block producer incurs the same cost $\mu_{BP}^{Cost} \cdot s$ for both t_0 and the transaction with position $c_{block} + 1$ in L_{BP} . This means that their utility will not increase.

  - If $size_{L_{BP}} < c_{block} + 1$: There are no other transactions with block producer fee at least $\mu_{BP}^{Cost} \cdot s$ to replace t_0. If the block producer replaces t_0 with a transaction that has lower block producer fee than $\mu_{BP}^{Cost} \cdot s$, they will gain the bribe loss $f_{BP} - \max\{f_{c_{block}+1,BP}, \mu_{BP}^{Cost} \cdot s\} = f_{BP} - \mu_{BP}^{Cost} \cdot s$, but they will lose an amount of at least $f_{BP} - \mu_{BP}^{Cost} \cdot s$ from the difference between the block producer fee of t_0 and of the newly added transaction. Thus, their utility will not increase.

When $c_{block} \geq w$ Recall that o is the order of t_0 in $L_{CM,c_{block}}$ and o_{BP} the order of t_0 in L_{BP}. We examine the following two variants of the FOCIL protocol:

- **Multiple transactions per sender are allowed to be added to an inclusion list**: The utility of the block producer when they do not deviate is $sum_{max,c_{block}}$ minus the bribe loss for the transaction t_0. Let us examine what deviations the block producer can make:

  - They can omit transaction t_0 (losing their fee f_{BP}) and add $c_{block} - w + 1$ fake transactions to their block so that they do not get penalised by the attesters (recall that w is the number of the transactions in the mempool including t_0). For every fake transaction, they need to pay $r \cdot s$ for the burning fee. The amount they gain via this deviation is equal to the bribe loss plus $\mu_{BP}^{Cost} \cdot s$, and the amount they lose is equal to $f_{BP} + r \cdot s \cdot (c_{block} - w + 1)$. As the bribe loss is no higher than $f_{BP} - \mu_{BP}^{Cost} \cdot s + r \cdot s \cdot (c_{block} - w + 1)$, their utility cannot increase.

  - They can omit transaction t_0 (losing its fee f_{BP}) and add no fake transaction. This means that they will lose their entire block rewards. Their utility in this case becomes 0, which is not higher than their current utility if the bribe loss is no higher than $sum_{max,c_{block}}$.

  - They can omit transaction t_0 (losing its fee f_{BP}) and avoid penalisation by the attesters in the following way: by adding fake transactions to the mempool so that includers do not include t_0 in their inclusion lists, and later invalidating them via a single fake transaction. To make the committee ignore t_0, the block producer needs:

    * (First deviation): To exclude t_0 from the first c_{block} positions of L_{BP}. They can do this by adding $c_{block} - o_{BP} + 1$ fake transactions with a block producer fee at least f_{BP}.

    * (Second deviation): To create $\min\{m \cdot c_{Incl}, size_{L_{CM,c_{block}}}\} - o + 1$ fake transactions that (i) have committee fee at least f_{CM}, (ii) belong to the first c_{block} transactions that give the highest block producer fee which means that they have a block producer fee at least $\max\{f_{y,BP}, \mu_{BP}^{Cost} \cdot s\}$, where $y = c_{block} - (\min\{m \cdot c_{Incl}, size_{L_{CM,c_{block}}}\} - o + 1) + 1$.

Note that here we take the worst-case scenario where the fake transactions that offer the same fee as the real transactions are preferred by the includers and the block producer.

When the block producer performs the above deviations, they gain the bribe loss plus $\mu_{BP}^{Cost} \cdot s$, but they lose f_{BP} plus γ fraction of the fees of the fake transactions plus the base fee $r \cdot s$ for the transaction that invalidates the fake transactions. The later amount is equal to $(c_{block} - o_{BP} + 1) \cdot \gamma \cdot f_{BP} + r \cdot s$ for the first deviation and equal to $\gamma \cdot (\min\{m \cdot c_{Incl}, size_{L_{CM,c_{block}}}\} - o + 1) \cdot (f_{CM} + \max\{f_{y,BP}, \mu_{BP}^{Cost} \cdot s\}) + r \cdot s$ for the second deviation. This means that if the bribe loss is at most

$$
\min\{(c_{block} - o_{BP} + 1) \cdot \gamma \cdot f_{BP} + r \cdot s,
$$
$$
\gamma \cdot (\min\{m \cdot c_{Incl}, size_{L_{CM,c_{block}}}\} - o + 1) \cdot (f_{CM}
$$
$$
+ \max\{f_{y,BP}, \mu_{BP}^{Cost} \cdot s\}) + r \cdot s\} + f_{BP} - \mu_{BP}^{Cost} \cdot s
$$

the block producer cannot increase their utility by deviating.

- **Single sender per inclusion list**: The proofs are the same except for the last point where the block producer tries to exclude t_0 from the inclusion lists by adding fake transactions to the mempools and later invalidating them with other transactions in the block. In this case, as every inclusion list can include transactions from a single sender then the cost for the block producer to deviate is higher. This happens because the block producer will need to add $\lceil Y/m \rceil$ transactions to the block to invalidate Y fake transactions in the mempool. At most m fake transactions from the same sender can be included in the inclusion lists (one per inclusion list).

$\square$

B.4 Fair-under-congestion

Proof. Assume arbitrary H, mempool M_0 that is not Block-feasible, lists $L_{CM,c_{block}}, L_{BP}$, and types of includers and block producer in $\text{Bribe}^{CM}, \text{Bribe}^{BP}$ respectively. As we have assumed that every transaction has the same size, the fact that M_0 is not Block-feasible means that $w > c_{block}$. Let

- $\{\mathsf{IL}_1, \ldots, \mathsf{IL}_d\}$ be the inclusion lists if all the includers follow the indicated allocation rule and do not add fake transactions to the mempool and their inclusion list.

- B_k the block if the block proposer follows the indicated allocation rule and does not add any fake transactions to the mempool and the block.

We want to prove that for every $t \in M_0 \setminus B_k$ there is a bidding strategy the user could follow for their transaction to be included in at least one inclusion list and the block, assuming that: (i) all the other transactions remain the same, and (ii) the includers and block producer follow the indicated allocation rules and they do not add any fake transactions.

Note that if all the types of includers follow the indicated allocation rules and do not add fake transactions, the inclusion lists consist of the transactions that belong to the first $\min\{m \cdot c_{Incl}, size_{L_{CM,c_{block}}}\}$ positions in $L_{CM,c_{block}}$. Recall that these transactions belong to c_{block} transactions with the highest block producer fee and their block producer fee is at least $\mu_{BP}^{Cost} \cdot s$. This means that if the block producer follows the indicated allocation rule and does not add any fake transactions, they include all the transactions from the inclusion lists. Thus, the fact that t does not belong to the block means that one of the following holds:

1. It does not belong to $L_{CM,c_{block}}$ because it has a block producer fee lower than $\max\{\mu_{BP}^{Cost} \cdot s, f_{c_{block},BP}\}$.

2. It does not belong to $L_{CM,c_{block}}$ because it has a committee fee lower than $\mu_{CM}^{Cost} \cdot s$.

3. It belongs to $L_{CM,c_{block}}$, but it has a committee fee lower than $f_{m \cdot c_{Incl},CM}$.

If the sender of transaction t gives a bid $b_t = (\delta_t^{CM}, \delta_t^{BP}, c_t)$, such that:

- $c_t = \delta_t^{BP} + \delta_t^{CM} + r$

- $\delta_t^{BP} \cdot s > \max\{\mu_{BP}^{Cost} \cdot s, f_{c_{block},BP}\}$

- $\delta_t^{CM} \cdot s > \max\{f_{m \cdot c_{Incl},CM}, \mu_{CM}^{Cost} \cdot s\}$

their transaction will be included in both an inclusion list and the block. □

C Proofs for Single TFM

C.1 "Usually" DSIC

Proof. The proof is similar to the proof for the Double TFM. Note that the block producer fee and the committee fee under bidding strategy $\min\{v_t, r + \mu_{BP}^{Cost}\}$ in the Single TFM and bidding strategy $(0, \mu_{BP}^{Cost}, \min\{v_t, r + \mu_{BP}^{Cost}\})$ in the Double TFM offer the same block producer and committee fee. In both cases, if the block producer include this transaction in their block, they will collect $\max\{(\min\{v_t, r + \mu_{BP}^{Cost}\} - r) \cdot s, 0\}$, and the includer will receive zero fees. □

C.2 Myopic Committee Bayesian-Nash Incentive Compatible (MCBN)

Proof. The first part of the proof, given below, is the same as the proof for the Double TFM because the committee fee is shared among the includers in the same way as in the Double TFM, $L_{BP}, L_{CM,c_{block}}$ consist of the same transactions, and the bribe functions are defined with respect to f_{CM}, f_{BP}.

" Assume arbitrary H, M_0 and that every type of all but one includers and block producer follow the indicated allocation rule and do not add fake transactions. We need to prove that every type of the remaining includer denoted by j cannot increase their utility by deviating from the indicated allocation strategy or by adding fake transactions to their inclusion list or to the mempool.

For both types of includer j, it holds that their beliefs do not affect their utility because all the types of the other includers and the block producer follow the same indicated allocation rule.

If the order of j is not $\lceil \frac{o}{c_{Incl}} \rceil$

- t_0 is not in their inclusion list when they follow the indicated allocation rule, and thus they do not incur any bribe loss. This means that the bribe function that determines their type does not affect their utility. Note that when all the includers follow the indicated allocation rule, t_0 is included in the inclusion list of the member with order $\min\{\lceil \frac{o}{c_{Incl}} \rceil, m\}$. For example, if $o = 10$ and $c_{Incl} = 3$, then t_0 is included in the inclusion list of the member with order 4.

- All their current transactions offer them a committee fee no smaller than cost $\mu_{CM}^{Cost} \cdot s$. Thus, their utility cannot increase by omitting them.

- They cannot add a transaction already included by an includer with a higher order to their inclusion list, because they have no space (if they had space, then the includers with a higher order would have no transactions in their inclusion lists). If they choose to replace one (or more) of their current transactions with such a transaction, their utility cannot increase; the members with a worse (higher) order include transactions with lower committee fees than their current transactions.

- If they choose to add one (or more) transactions already included by an includer with a smaller order, then their utility will decrease because they will take zero fees for this transaction, and they will incur cost $\mu_{CM}^{Cost} \cdot s$.

- If they choose to add a transaction not included by any includer, then their utility will decrease because this transaction either has a very low block producer fee and thus will not be included in the block (which means that it will give them zero fees) or has a committee fee lower than μ_{CM}^{Cost}.

If the order of j is equal to $\lceil \frac{o}{c_{Incl}} \rceil$

- The includer j incurs bribe loss equal to $f_{CM} - \max\{f_{g,CM}, \mu_{CM}^{Cost} \cdot s\}$, where $g = c_{Incl} \cdot \lceil \frac{o}{c_{Incl}} \rceil + 1$, as they have included t_0 in their inclusion list.

- If they omit t_0, their utility will not increase because they will gain the bribe loss plus $\mu_{CM}^{Cost} \cdot s$, but they will lose f_{CM}.

- If they replace t_0 with a transaction included by an includer with a smaller order then their utility will decrease, as they will receive zero fees from this transaction.

- If they replace t_0 with a transaction included by an includer with a higher order, or a transaction not included in an inclusion list, then the maximum fee they will gain from this transaction will be $\max\{f_{g,CM}, \mu_{CM}^{Cost} \cdot s\}$ and they will lose f_{CM}. $f_{CM} - \max\{f_{g,CM}, \mu_{CM}^{Cost} \cdot s\}$ is no smaller than the bribe loss. Thus, their utility cannot increase.

- Regarding the other transactions, the proof that their utility cannot increase by deviating from the indicated allocation rule is the same as the case when the order of j is not $\lceil \frac{o}{c_{Incl}} \rceil$.

Regardless of their order, includer j cannot increase their utility by adding fake transactions to their inclusion list, because these transactions will give them no extra reward. Moreover, they cannot increase their utility by adding fake transactions to the mempool, because:

- When this fake transaction does not affect which transactions the other includers or the block producer include in their inclusion list and block respectively, it cannot affect their utility.

- In order for the fake transaction to affect which transactions the other includers or the block producer include in their inclusion list and block respectively, they need to have a fee that will be paid by includer j."

    The remaining part of the proof has some differences and is as follows:

    – When this fake transaction gives a committee fee that makes another includer with a smaller order prefer it over another transaction t', then their utility can be affected if they "steal" t'. However, their utility cannot increase because (i) the maximum includer j can gain by this deviation is the committee fee of the omitted transaction t' and (ii) includer j needs to pay the committee fee of this omitted transaction t', the burning fee, μ_{BP}^{Cost}, and $(1 - z)/z$ times the committee fee of t' (this is the fee that is awarded to the block producer apart from μ_{BP}^{Cost}). This means that the utility of includer j will decrease.

– When this fake transaction has a block producer fee that makes another includer with a smaller order prefer it over another transaction t' (because t', after the addition of the fake transaction, will not belong to the first c_{block} positions of L_{BP}): In this case, also the committee fee of the fake transaction will be higher than the committee fee of t'. Thus, the utility of includer j will decrease.

– When this fake transaction has a block producer fee that makes the block producer omit some other transactions in favour of this fake transaction, then the utility of includer j cannot increase.

$\square$

C.3 Myopic Block Producer Bayesian-Nash Incentive Compatible (MBBN)

Proof. The proof is similar to the proof for the Double TFM, because the committee fee is shared among the includers in the same way as in the Double TFM, $L_{BP}, L_{CM,c_{block}}$ consist of the same transactions, and the bribe functions are defined with respect to f_{CM}, f_{BP}. The difference is that there is a dependency between f_{CM} and f_{BP} but this does not affect the proofs. $\square$

C.4 Fair-under-congestion

Proof. Assume arbitrary H, mempool M_0 that is not Block-feasible, lists $L_{CM,c_{block}}, L_{BP}$ and types of includers and block producer in $\text{Bribe}^{CM}, \text{Bribe}^{BP}$ respectively. As we have assumed that every transaction has the same size, then the fact that M_0 is not Block-feasible means that $w > c_{block}$. Let

- $\{\mathsf{IL_1}, \ldots, \mathsf{IL_d}\}$ be the inclusion lists if all the includers follow the indicated allocation rule and do not add fake transactions to the mempool and their inclusion list.

- B_k the block if the block proposer follows the indicated allocation rule and does not add any fake transactions to the mempool and the block.

We want to prove that for every $t \in M_0 \setminus B_k$ there is a bidding strategy the user could follow for their transaction to be included in at least one inclusion list and the block, assuming that all the other transactions remain the same, and the includers and block producer follow the indicated allocation rules and they do not add any fake transactions.

Recall that all the types of includers who follow the indicated allocation rules and do not add fake transactions include in their inclusion lists the transactions that belong to the first $\min\{m \cdot c_{Incl}, size_{L_{CM,c_{block}}}\}$ positions in $L_{CM,c_{block}}$. This means that if the block producer follows again the indicated allocation rule and does not add any fake transactions, they include all the transactions from the inclusion lists. Thus, the fact that t does not belong to the block means that at least one of the followings hold:

1. It does not belong to $L_{CM,c_{block}}$ because it has a block producer fee lower than $\max\{\mu_{BP}^{Cost} \cdot s, f_{c_{block},BP}\}$.

2. It does not belong to $L_{CM,c_{block}}$ because it has a committee fee lower than $\mu_{CM}^{Cost} \cdot s$.

3. It belongs to $L_{CM,c_{block}}$, but it has a committee fee lower than $f_{m \cdot c_{Incl},CM}$.

If the sender of transaction t gives a bid $b'_t = (c'_t)$, such that:

- $c'_t > r + \mu_{BP}^{Cost}$

- $(c'_t - r - \mu_{BP}^{Cost}) \cdot z \geq \mu_{CM}^{Cost}$

- c'_t belongs to the $\min\{m \cdot c_{Incl}, size_{L_{CM,c_{block}}}\}$ highest bids

this transaction will be included in both an inclusion list and the block. $\square$

C.5 Intuition about How the Choice z, c_{t_0} Affect the Minimum Bribe Needed for Censorship

Based on Theorems 9, 11 we prove in Section 7 for conditional inclusion lists, assuming that $\mu_{CM}^{Cost} = \mu_{BP}^{Cost} = 0$ and $w = c_{block}$, it holds that: if a briber gives a sum of bribes higher than $min\{m \cdot f_{CM}, r \cdot s\} + f_{BP}$, there is no Nash equilibrium where the target transaction t_0 is included in the block. In this section, we examine how this amount is affected by the choice of c_{t_0} or z. In the Single TFM, this amount is equal to

$$min\{m \cdot f_{CM}, r \cdot s\} + f_{BP} = \tag{1}$$

$$min\{m \cdot (c_{t_0} - r) \cdot s \cdot z, r \cdot s\}+ \tag{2}$$

$$(c_{t_0} - r) \cdot (1 - z) \cdot s \tag{3}$$

Note that $f_{CM} = (c_{t_0} - r) \cdot s \cdot z$ and $f_{BP} = (c_{t_0} - r) \cdot (1 - z)$, because t_0 belongs to first $min\{m \cdot c_{Incl}, size_{L_{CM, c_{block}}}\}$ positions in $L_{CM, c_{block}}$ and thus it holds $c_{t_0} \geq r$.

If we fix z, and the mempool M apart from the target transaction, then the higher the c_{t_0}, the higher the above amount is.

Now we fix M, c_{t_0}, r and we examine for which z the above formula is maximised. We prove that it is maximised for $z_0 = \min\{\frac{\frac{r \cdot s}{m}}{(c_{t_0} - r)}, 1\}$.

Note that:

- The latter amount depends on r, c_{t_0}, which means that it does not apply to every target transaction.

- It holds that the higher r, the higher z_0. The intuition about this is the following: when r is very high $min\{m \cdot f_{CM}, r \cdot s\} = m \cdot f_{CM}$, which means that equations $2, 3$ depend not only on the block producer fee but also on the committee fee.

Proof. We have the following two cases:

- $\frac{r}{m} > c_{t_0} - r$. In this case, it holds $0 \leq z \leq \min\{1, \frac{\frac{r}{m}}{(c_{t_0} - r)}\}$, because it holds $z \leq 1$.

- $\frac{r}{m} \leq c_{t_0} - r$. In this case, we have either:

  - $0 \leq z \leq \frac{\frac{r}{m}}{(c_{t_0} - r)}$, or

  - $\frac{\frac{r}{m}}{(c_{t_0} - r)} < z \leq 1$.

Thus,

- When $\frac{r}{m} \leq c_{t_0} - r$ and $1 \geq z > \frac{\frac{r}{m}}{(c_{t_0} - r)}$, the equation $2, 3$ is equal to

$$r \cdot s + (c_{t_0} - r) \cdot (1 - z) \cdot s$$

  This is maximised for $z_0 = \frac{\frac{r}{m}}{(c_{t_0} - r)}$.

- When $[\frac{r}{m} > c_{t_0} - r]$ OR $[\frac{r}{m} \leq c_{t_0} - r$ and $0 \leq z \leq \frac{\frac{r}{m}}{(c_{t_0} - r)}]$ the equation $2, 3$ is equal to

$$m \cdot (c_{t_0} - r) \cdot s \cdot z + (c_{t_0} - r) \cdot (1 - z) \cdot s$$

The above formula is maximised for $z_0 = \min\{\frac{\frac{r}{m}}{(c_{t_0} - r)}, 1\}$. $\qquad \square$

D Proof that Single Prioritized is not fair-under-congestion

Proof. When the block producer follows the indicated allocation rule, they include only transactions that do not belong to an inclusion list in their block. This happens because if they include a transaction that belongs to an inclusion list, they receive zero fees and incur a cost $\mu_{BP}^{Cost} \cdot s$. Thus, if the block producer follows the indicated allocation rule, no bidding strategy can make this transaction be included in both an inclusion list and the block. $\qquad \square$

E Theorems and Proofs for Simplified Model

In this section, we restrict the strategy space of both includers and the block producer by excluding strategies that involve adding fake transactions to the mempool. However, we still allow strategies that add fake transactions directly to the block or inclusion list. We analyse how the minimum bribe required by a briber to censor a transaction varies based on whether the inclusion lists are conditional or unconditional.

- Let M be an arbitrary mempool and t_0 be the target transaction the briber tries to censor.

- Let s be the size of every transaction in the mempool M.

- $r \cdot s$ the burning fee per transaction.

- Let c_{block}, c_{Incl} be the maximum number of transactions the block and the inclusion list can store respectively.

- Let sum be the block rewards (block producer fees minus costs).

- Let w be the number of transactions in M.

- Let f_{CM} be the fee the committee receives if t_0 is included in an inclusion list and the block.

- Let f_{BP} be the fee the block producer receives if t_0 is included in the block regardless of whether this transaction is included in an inclusion list.

- Let us assume $\mu_{BP}^{Cost} = \mu_{CM}^{Cost} = 0$.

- The includers and the block producer have only one type that known to the other parties. Thus, we use the notion of Nash equilibrium instead of Bayesian Nash equilibrium.

- The bribe function of the block producer offers them bribe B_1 when they omit transaction t_0 from their block.

- The bribe function of a includer j gives them bribe B^j when they omit transaction t_0 from their block.

E.1 Conditional Lists

Theorem 9. *Regardless of the payment rule, if $B_1 > f_{BP} + r \cdot s \cdot (\max\{c_{block} - w + 1, 0\})$, it is a dominant strategy for the block producer to censor t_0, which means that there is no Nash equilibrium where t_0 is included in the block.*

Proof. This holds because regardless of whether t_0 has been included in an inclusion list, the block producer can omit t_0 without being rejected by the attesters by adding fake transactions to their block. The maximum cost the block producer incurs when they omit t_0 is $f_{BP} + r \cdot s \cdot (\max\{c_{block} - w + 1, 0\})$. Thus, it is more profitable for them to receive the bribe and omit t_0. $\qquad \square$

Theorem 10. *Regardless of the payment rule, if $B_1 > f_{BP}$, there is a Nash equilibrium where both the includers and the block producer censor t_0.*

Proof. This holds because: (i) when the block producer omits t_0 then the committee does not receive f_{CM} even if they include t_0 in an inclusion list and (ii) when t_0 is not in an inclusion list, the maximum cost of the block producer to omit it is f_{BP}. $\qquad\square$

Theorem 11. *Regardless of the payment rule, if $B_1 > f_{BP}$ and $\forall j \in \{1, \ldots m\} : B^j > f_{CM}$ there is no Nash equilibrium where t_0 is included in the block.*

Proof. We will prove it by contradiction. Let us assume that there exist such a Nash equilibrium. This means that in this strategy profile the block producer has included t_0 in the block. Moreover, as $\forall j \in \{1, \ldots m\} : B^j > f_{CM}$, it holds that no includer has included t_0 in their inclusion list; otherwise they could increase their utility by omitting t_0 and receiving the bribe. Note that regardless of the payment rule, the reward of an includer who includes t_0 cannot be more than f_{CM}. As t_0 is not in an inclusion list, the block producer can omit it and incur maximum cost f_{BP}. We reach a contradiction because the block producer can increase their utility by omitting it. $\qquad\square$

E.2   Unconditional Lists

Theorem 12. *When $m \cdot c_{Incl} \leq c_{block}$, regardless of the payment rule, if $B_1 < sum$, it is a dominant strategy for the block producer to follow an allocation rule that includes t_0 if it is included in an inclusion list.*

Proof. This holds because if the block producer ignores any transaction from an inclusion list, they will lose their block rewards. Recall that in this section we have excluded strategies where the block producer can add fake transactions to the mempool to capture space in the inclusion lists, thereby allowing them to omit t_0 at a lower cost. $\qquad\square$

Theorem 13. *Assume $m \cdot w \leq m \cdot c_{Incl} \leq c_{block}$. Under the payment rule where the committee fee is awarded to the includer with the smallest order who includes it, if ($B_1 < sum$ AND $\sum_{j \in \{1, \ldots m\}} \cdot B^j < m \cdot f_{CM}$), there is no Nash equilibrium where t_0 is not included in the block.*

Proof. We will prove it by contradiction. Assume that such a Nash equilibrium exists. As it holds $B_1 < sum$, we know by the previous theorem that at a Nash equilibrium, the block producer follows an allocation rule that includes t_0 if it is included in an inclusion list. As t_0 has not been included in the block, this means that no includer has included t_0 in their inclusion list. As it holds $\sum_{j \in \{1, \ldots m\}} \cdot B^j < m \cdot f_{CM}$, there is at least one includer j with $B^j < f_{CM}$. We reach a contradiction because this includer can increase their utility by deviating and including t_0 in their inclusion list, as they know that this transaction will be included in the block and will give them committee fee f_{CM}. $\qquad\square$

Note that in [16], the authors propose a notion for censorship resistance based on the minimum amount required to censor a transaction.

E.3   Conclusion

Based on the above theorems, we conclude that unconditional lists can significantly increase the cost of bribing at a Nash equilibrium provided we exclude strategies where the block producer can add fake transactions to the mempool. However, if we include the latter strategy in the strategy space, the cost of bribing between conditional and unconditional lists becomes similar. This holds because, in both cases, adding fake transactions to the mempool and later invalidate them is the lowest-cost strategy that allows the block producer to omit a transaction from an inclusion list.