CENSORSHIP RESISTANCE IN ON-CHAIN AUCTIONS

MALLESH M. PAI[A] Ⓡ, MAX RESNICK[B] Ⓡ, AND ELIJAH FOX[C]

ABSTRACT: Smart contracts offer a way to credibly commit to a mechanism, as long as it can be expressed as an easily computable mapping from inputs, in the form of transactions on-chain, to outputs: allocations and payments. But proposers decide which transactions to include, allowing them to manipulate these mechanisms and extract temporary monopoly rents known as MEV. Motivated by both general interest in running auctions on-chain, and current proposals to conduct MEV auctions on-chain, we study how these manipulations effect the equilibria of auctions.

Formally, we consider an independent private value auction where bidders simultaneously submit private bids, and public tips, that are paid to the proposer upon inclusion. A single additional bidder may bribe the proposer to omit competing bids.

We show that even if bids are completely sealed, tips reveal bids in equilibrium, which suggests that encrypting bids may not prevent manipulation. Further, we show that collusion at the transaction inclusion step is extremely profitable for the colluding bidder: as the number of bidders increases, the probability that the winner is not colluding and the economic efficiency of the auction both decrease faster than $1/n$. Running the auction over multiple blocks, each with a different proposer, alleviates the problem only if the number of blocks is larger than the number of bidders. We argue that blockchains with more than one concurrent proposer can credibly execute auctions on chain, as long as tips can be conditioned on the number of proposers that include the transaction.

KEYWORDS: auctions, blockchain, MEV, on-chain, censorship

JEL CLASSIFICATION: D82.

1. INTRODUCTION

This paper considers the problem of running an auction via a smart contract on-chain. From an academic perspective, smart contracts provide tools to ensure *credible commitment* to a mechanism. By encoding the underlying mechanism in a smart contract, the principal can commit to the rules, and the underlying blockchain will faithfully execute them as written. However, modern blockchains are typically leader driven. By this, we mean that they select a rotating proposer who has absolute power over which transactions are included in each slot. Since smart contracts can only compute based on transactions that make it onto the chain, these proposers can manipulate the outcome of on-chain mechanisms by censoring some of their inputs. This leads to the general question of whether economically valuable mechanisms, such as auctions, are manipulable by the proposer, and how these manipulations can warp the outcomes.

A reason to study auctions specifically, as opposed to general mechanisms, is driven by recent interest in auctions as a solution to Miner Extractable Value (MEV), a form of value extraction similar to high frequency trading in traditional finance Daian et al. (2019).[1] MEV arises from the proposer's power to include and order transactions in any way they see fit, which gives them a source of temporary monopoly rents. Flashbots estimates that over 600 million USD of MEV has been extracted on Ethereum since 2020.[2] One proposed solution has been to auction off the right to be the proposer. For example, MEV-boost, the mechanism responsible for deciding the contents of more than 4 out of every 5 new Ethereum blocks,[3] is effectively a sealed-bid first-price auction for the right to decide the content of a block. The creators of MEV-boost, Flashbots, have announced plans to move this process on-chain Flashbots (2022). At the application level, Maker DAO, the entity behind popular stablecoin DAI, uses Dutch clock auctions to sell the right to liquidate collateral for distressed loans, which have historically been a major source of MEV.[4]

Censorship concerns are particularly salient today given the increasing super-majority of Ethereum validators who have switched to MEV-Boost clients in order to opt in to proposer builder separation (PBS). Senior Researchers within the Ethereum Foundation identified the proposer's temporary monopoly on inclusion as a centralizing force within Ethereum's consensus network. Among them was Ethereum co-founder Vitalik Buterin, who authored a forum post suggesting Proposer Builder Separation (PBS) as a solution to this centralization.[5] Instead of requiring proposers to run sophisticated, computationally

---

[1]Of course other digital goods such as NFTs may also be auctioned off on-chain, we describe some related work below.

[2]See, https://explore.flashbots.net.

[3]Source: https://dune.com/ChainsightAnalytics/mev-after-ethereum-merge

[4]See, https://docs.makerdao.com/keepers/the-auctions-of-the-maker-protocol.

[5]See, https://ethresear.ch/t/proposer-block-builder-separation-friendly-fee-market-designs/9725.

intensive algorithms to maximize their MEV, under PBS, the building of blocks would be outsourced to a community of builders, proposers would then have the simple task of selecting the highest revenue block from among those offered by the builders. These ideas were built into MEV-boost which today is responsible for deciding the contents of over 80% of new Ethereum blocks. While PBS was successful in reducing the sophistication required to run an Ethereum node, its effects on decentralization are mixed. The centralization that Vitalik feared would play out at the validator level has instead occurred at the builder level, with half of all new blocks at the time we write this being built by the Flashbots relay.[6] More importantly for our purposes, PBS created a direct channel through which proposers could collude with bidders to manipulate the outcome of an auction. In fact, proposers who collude with bidders through MEV-boost aren't even aware that they have colluded until after they have signed the block header, effectively committing them to collusion before they realize what they have done.

Formally, we consider a seller who holds a second-price auction for a single unit of an indivisible good on-chain. The seller encodes the rules of the second-price auction in a smart contract. The contract selects the bidder who submitted the highest bid over a predefined period, and sets the payment to the second-highest bid. But, since this all takes place on a blockchain, before a bid can be submitted to the auction, it must be included in a transaction on-chain. Valid transactions are submitted to a *mempool*. Each slot, the proposer gathers transactions from the mempool into a block that will eventually be added to the chain. Proposers have complete autonomy over which transactions to include.

The power of the proposer to determine the contents of the block—and therefore the outcome of the auction—sets up a competition for inclusion. Bidders include tips for the proposer along with their bids. The proposer receives these tips if and only if the corresponding transactions are included in his block. We suppose that there is a single colluding bidder who may offer a bribe to the proposer in exchange for omitting certain transactions. In the auction setting, tips for inclusion are a public good, since they provide security to other transactions and only benefit the bidder who pays the tip if they win the auction. On the contrary bribes for omission are purely for private benefit and make other bidders worse off in equilibrium. Consequently, our results suggest that the colluding bidder is highly advantaged in this game. In particular, we show that as the number of honest bidders increases, the colluding bidder wins the auction increasingly often, and collects an increasingly large share of the surplus created by the auction.

Notably, we assume that bids are sealed, i.e., that the colluding bidder must choose which transactions to try and omit based solely on the associated tip. We show that the

---

[6]As reported by https://transparency.flashbots.net.

colluding bidder can back out the private bids (and therefore whether it is profitable to attempt to censor these bids) based on these public tips. This suggests that cryptographic approaches (e.g. commit-reveal schemes) are not a silver bullet for resolving censorship concerns in such settings.

We then consider two ways to restore the security of the auction. The first is to run the auction over multiple slots with a different proposer for each. We find that this achieves credibility, only if the number of blocks is larger than the number of bidders. This is undesirable for reasons external to our model, for example, executing the auction in a short window is important for financial applications. MEV auctions in particular are concerned about speed since they clear at least once every slot—once every 12 seconds on Ethereum.

The second is to have blockchains with multiple concurrent block proposers, $k > 1$, and allow bidder tips to be conditioned not only on inclusion, but also on the number of proposers who include the bid within a slot. This allows bidders to set up a sort of "prisoner's dilemma" among the proposers by proposing to pay a large tip T when only one proposer includes, and a small tip $t \ll T$ if multiple proposers include. Each proposer is incentivized to include since if they are alone in including the transaction, there is a high tip attached. All proposers therefore include the bid in equilibrium. This leads to a low expected tip of kt but an asymmetrically expensive censorship cost of $kT \gg kt$. This asymmetry allows for a pooling equilibrium in which the probability of censorship is 0, tips no longer reveal bids, and expected total tips are low.

We are not aware of any blockchains that currently allow multiple concurrent block proposers. Representatives from at least one major chain, however, mentioned concurrency as a goal going forward, in order to scale throughput and decrease latency from the user to the nearest proposer within a given slot.[7] The co-founder, and CEO of Solana even mentioned MEV resistance as a motivation for the desirability of multiple concurrent block proposers.[8] Our results suggest that progress in this direction could reduce MEV.

2. RELATED LITERATURE

Early scholars of auctions identified a fundamental tension between incentive compatibility for bidders and credibility for auctioneers Vickrey (1961); Rothkopf et al. (1990), more recently formalized in Akbarpour and Li (2018, 2020). A common method for

---

[7]See, e.g., https://blog.chain.link/execution-and-parallelism-for-dag-based-bft-consensus/.
[8]See https://twitter.com/aeyakovenko/status/1584676110948012032.

resolving this tension is to use a trusted third party to oversee the auction.[9] Using a blockchain as this third party is attractive, since the assumptions required to trust a blockchain are weaker than those required to trust an individual Galal and Youssef (2019); Blass and Kerschbaum (2018).[10]

In online auctions, bids are seldom announced simultaneously, and maintaining the seal on bids transmitted through public channels requires cryptography. For example a simple cryptographic second-price sealed-bid auction involves bidders submitting the hash of their bids rather than the bids themselves and then revealing the hash after all bids have been submitted. Ferreira and Weinberg (2020) showed that, using a cryptographically secure commitment scheme, it is possible to design an auction that is optimal, strategy proof and credible, but only when the number of bidders is known in advance. More complicated cryptographic approaches can eliminate the need to reveal any information beyond the results of the auction and can accommodate combinatorial auctions as well Lee et al. (2001); Elkind and Lipmaa (2004); Suzuki and Yokoo (2003). However, these still require that the bidder set is known in advance and struggle to accommodate scenarios when bidders may drop and never submit a bid, where blockchains have an advantage.

Auctions commonly cited as use case for the verifiable computation that smart contracts provide Galal and Youssef (2019); Blass and Kerschbaum (2018).[11] Auctions have also been suggested as a desirable mechanism for deciding ordering and inclusion of transactions to mitigate MEV Kulkarni et al. (2022). Historically, these were decided by a combination of auction and speed based mechanisms, leading Daian et al. (2019) to compare MEV to high frequency trading as described in Budish et al. (2015). Initially inclusion and priority within the block were decided by priority gas auctions (PGAs), since most validators gathered transactions directly from the mempool and ordered them according to their miner tips, breaking ties using a first come first serve rule Daian et al. (2020). But recently, a super-majority of validators have switched their execution clients to MEV-boost compatible versions meaning the right to decide inclusion and ordering for most blocks is sold to the highest bidder. These bidders are typically established builders who specialize in extracting the maximum value from each block. The leading advocate

---

[9]For e.g., Vickrey (1961) notes "To prevent the use of a "shill" to jack up the price... it would probably be desirable to have all bids ... certified by a trustworthy holder who would then deliver all the bids simultaneously to the seller."

[10]Originally envisaged in Szabo (1997), who noted that "... a blockchain with a built-in fully fledged Turing-complete programming language that can be used to create "contracts" ... simply by writing up the logic in a few lines of code."

[11]See, e.g., https://a16zcrypto.com/hidden-in-plain-sight-a-sneaky-solidity-implementation-of-a-sealed-bid-auction/.

for this approach has been Flashbots, the company behind the initial open source MEV client. Their next product SUAVE, aims to move these auctions on-chain Flashbots (2022).

Prior MEV mitigation research has focused on fairness rather than on censorship Kelkar et al. (2020, 2021). But Ferreira and Parkes (2022) showed that for every sequencing rule of trades through a liquidity pool, there exists a way for the proposer to obtain non-zero risk-free profits suggesting that ordering based MEV is inevitable with current on chain financial application design. In response to this, researchers have suggested that Frequent Batch Auctions or other order agnostic mechanisms might alleviate the MEV that arises from transaction ordering power Johnson et al. (2022).

On-chain auctions have also been studied as a mechanism for the sale of non-fungible tokens (NFTs) Milionis et al. (2022). Gradual dutch auctions (GDAs) Frankie et al. (2022), are a dynamic mechanism for selling multiple NFTs. Kulkarni et al. (2023) explores the credibility of GDAs, and finds that an auctioneer can bid to artificially raise the sale price and create the appearance of demand.

3. MODEL

We consider a traditional independent private values setting. There is a single seller with a single unit of an indivisible good for sale. There are $n + 1$ buyers for the good, $n \geq 1$— we denote the set of bidders by $N = \{0, 1, \ldots, n\}$. Each of these buyers $i \in N$ has a private value for the good, v_i. We suppose buyer 0's value v_0 is drawn from a distribution with CDF F_0 and density f, and the other buyers' values are are drawn i.i.d. from a distribution with CDF F and density f. Both distributions have bounded support, we normalize these to be equal to the unit interval $[0, 1]$. Several of our results will be for the special case $F = F_0 = U[0, 1]$. Bidders know their own v_i; and n, F, and F_0 are common knowledge among all bidders and the seller.

The seller wishes to run a sealed-bid second-price auction with reserve price r. As described in this introduction, the point of departure of our model is that this auction runs on a blockchain. Initially, we consider an auction that accepts bids in a single designated designated block. Below we formally define this game and our solution concept.

In an idealized world with honest/ non-strategic proposers, the auction would run as follows:

(1) The seller announces the auction.
(2) All buyers privately commit bids to the auction as transactions.
(3) Proposer(s) include these transactions on relevant block(s).[12]
(4) The second-price auction is computed based on the included bids, i.e., the highest bid is selected to win if this bid $\geq r$, in this case paying a price of $\max\{r, \text{other bids}\}$.

---

[12]We abstract away from issues such as block size constraints/ congestion.

In particular, we assume that the idealized sealed-bid nature of off-chain auctions can be achieved on-chain via cryptographic methods.[13] We also assume that the set of bids submitted for the auction are public (the bid itself may be private, but the fact that it exists as a bid is public).

Our main concern is that bids submitted for this auction may be censored, that is, omitted from a block. More specifically, we suppose that after all other bids are submitted, but before they are revealed, a designated bidder, bidder 0, can pay the proposer of the block to *censor* bids. These censored bids are then excluded from the block and have no impact the auction. We assume that the proposer is purely profit focused and that bidder's utilities are quasilinear.

Formally, we consider the following game:

(1) The seller announces second-price sealed-bid auction with reserve price r to be conducted over a single block.
(2) Buyers learn their values $v_i \leftarrow F$.
(3) Buyers $1, \ldots, n$ each simultaneously submit a private bid b_i and a public tip t_i.
(4) Buyer 0 observes all the other tips t_i and can offer the proposer of the block a take-it-or-leave-it-offer of a subset $S \subseteq \{1, \ldots, n\}$ of bidders and a bribe p to exclude that subset's bids. Bidder 0 also submits their own bid b_0.
(5) The proposer accepts or rejects bidder 0's bribe and constructs the block accordingly, either including $N \setminus S$ if he accepts or N otherwise.
(6) The auction is computed based on the bids included in the block.

In the next section, we consider the case of auctions over multiple sequential blocks with independent proposers, and the case of simultaneous proposers. Those games are variants of the game above. We describe them in-line.

Formally, pure strategies in this game are:

- For players $i \in \{1, \ldots, n\}$: A tuple of bidding and tipping strategies $\beta_i : [0, 1] \rightarrow \Re_+$, $\tau_i : [0, 1] \rightarrow \Re_+$ for players $i \in \{1, \ldots n\}$, i.e., player i with value v_i bids $\beta_i(v_i)$ and tips $\tau_i(v_i)$.
- For player 0: an offer to the proposer $\theta_0 : \Re_+^n \times [0, 1] \rightarrow 2^N \times \Re_+$, and a bid function $\beta_0 : \Re_+^n \times [0, 1] \rightarrow \Re_+$, i.e. as a function of tips $\mathbf{t} = (\tau_1(v_1), \ldots, \tau_n(v_n))$ and his own value v_0, an offer $\theta_0(\mathbf{t}, v_0)$ and a bid $\beta_0(\mathbf{t}, v_0)$.
- For proposer, given the tips $\mathbf{t}$ and offer from player 0, $\theta_0(\mathbf{t}, v_0)$, a choice of which bids to include.

Since our game is an extensive-form game of incomplete information, our solution concept is Perfect Bayes-Nash Equilibrium (PBE). This requires strategies to be mutual best-responses as is standard in equilibrium. Additionally, for each player, it requires the

---

[13]This can be practically achieved by submitting the hash of the bid and revealing it later.

player to have beliefs about unknowns at every information set (on-, and off-, path) at which they are called upon to play such that their strategy maximizes their expected utility given the beliefs and others' strategies. Beliefs are correct on path (i.e., derived from the prior, and Bayesian updating given agents' strategies), and unrestricted off path.

Note that the proposer has multiple potential indifferences: e.g. should they include a bid with 0 tip? Should they censor a set of bids if bidder 0's offered bribe exactly equals the total tip from that set? We assume that given tips $\mathbf{t}$ from bidders $\{1, \ldots, n\}$ and an offered from bidder 0 to censor subset S for a bribe of p, the proposer includes the bids of $N - S$ if and only if $p \geq \sum_{i \in S} t_i$, and includes bids from all N otherwise (i.e. we are breaking proposer indifferences in favor of bidder 0 so that best responses are well defined).

There are multiple PBEs of the game, driven in part by the fact that there are multiple equilibria in a second-price auction (for instance it is an equilibrium in the second price auction for one player to bid a high value, and all others to bid 0). However, most of these equilibria are in weakly dominated strategies. We therefore focus on the following class of equilibria:

(1) Bidders $\{1, \ldots n\}$ submit a truthful bid, i.e. $\beta_i(v_i) = v_i$. Note that this is a weakly dominant strategy for them. Further, these bidders use a symmetric tipping function τ, i.e., $\tau_i(\cdot) = \tau(\cdot)$.

(2) Bidder 0 bids equal to his value if he believes, given the tips of $\{1, \ldots n\}$, that there is a non-zero probability that he could win the auction, otherwise he bids 0 or does not bid.

In what follows we simply refer to a PBE that satisfies this refinement as an *equilibrium* of the game (with no qualifier). We reiterate that there are multiple PBEs of the original game, we are simply restricting attention to these "reasonable" equilibria for tractability.

4. RESULTS

Our results are easiest for the case that n=1, i.e., there are two bidders. We present that as an illustration before considering the general case.

4.1. *Two Bidder Case*

Suppose there are only two bidders, one "honest" bidder 1 with value drawn according to distribution F, and one "colluding" bidder who has the opportunity to collude with the proposer, bidder 0, with value drawn independently from distribution F_0. We assume that F_0 satisfies a regularity condition, i.e., that $F_0(t)/f_0(t)$ is non-decreasing in t.

The equilibrium in this case is easy to describe:

PROPOSITION 1. *The following constitutes an equilibrium of the game with 2 bidders, i.e. $N = \{0,1\}$, when the seller announces a second-price auction with a reserve price $r = 0$:*

- *Bidder 1 submits a truthful bid, and his tipping strategy as function of his value v_1 is given by $t_1(v_1)$ solves $(v_1 - t) - \frac{F_0(t)}{f_0(t)} = 0$.*
- *Bidder 0's strategy as function of the observed tip t_1 and his value v_0 is given by*

$$\sigma_0(t_1, v_0) = \begin{cases} \textit{bribe} & t_1 \leq v_0, \\ \textit{don't bribe} & t_1 > v_0. \end{cases}$$

where bribe is shorthand for paying t_1 to the proposer in exchange for omitting bidder 1's transaction. Further bidder 0 submits a non-zero bid in the auction if and only if he bribes the proposer.

- *The proposer accepts bidder 0's bribe whenever it is offered and omits bidder 1's bid, otherwise the proposer includes both bids.*

Before providing a proof of this result, the following corollary summarizes the outcome that results in this equilibrium when $F = F_0 = \text{Uniform}[0, 1]$. For comparison, recall that in the (standard) second price auction when both buyers have values drawn i.i.d. from $\text{Uniform}[0, 1]$, the expected revenue is $1/3$ and each bidder has an *ex ante* expected surplus of $1/6$.

COROLLARY 1. *Bidder 0 wins the object with probability $\frac{3}{4}$, and has an expected surplus of $\frac{13}{48}$, while bidder 1 wins the auction with probability $\frac{1}{4}$ and has an expected surplus of $\frac{1}{12}$. The revenue to the seller in this auction is 0, and the expected tip revenue to the proposer is $\frac{1}{4}$.*

In short, the proposer collects all of the revenue from this auction, while the seller collects none. Bidder 0 is substantially advantaged by his ability to see bidder 1's tip and then decide whether to bribe the proposer or not (wins the auction with higher probability, collects more of the surplus). Our results for the $n > 1$ are similarly stark except for the fact that the auctioneer collects some positive revenue when $n > 1$, although this revenue rapidly decreases as n increases.

PROOF. The proof of the proposition is straightforward so we describe it briefly in line. First to see that bidder 1 should bid his value (our refinement restricts attention to these) note that bidder 1 has two actions, he privately submits a bid b_1 and publicly submits a tip t. Since bids only matter after inclusion has been decided, which is also after tips have been paid, tips are a sunk cost and what remains is simply a second price auction, in which truthful bidding is a weakly dominant strategy. Therefore it is (part of) an equilibrium for bidder 1 to bid his value.

Notice that bidder 1 does not benefit from submitting a tip $t > v_1$ since even if he wins, he will end up paying more in tips (in addition to possible fees from the auction) than he values the item. Knowing this, it is always weakly better for player 0 to pay t to omit player 1's bid when $v_0 \geq t$. Thus player 0 bribes the proposer if and only if $v_0 \geq t$. In that case player 1's expected utility as a function of his tip is:

$$\mathbb{E}[U_1(v_1, t)] = F_0(t)(v_1 - t).$$

Taking the derivative with respect to t, and setting it equal to 0, we get, as desired, that

$$t_1(v_1) \text{ solves } (v_1 - t) - \frac{F_0(t)}{f_0(t)} = 0.$$

Now that we have found a candidate equilibrium, we have some more work to do to verify that it is in fact a PBE. Formally, bidder 1's beliefs at his only information set are that $v_0 \sim \text{Uniform}[0, 1]$. By our regularity condition, $t_1(\cdot)$ is strictly increasing. Bidder 0's beliefs, conditional on bidder 1's tip being t_1 are given by

$$v_1 = \begin{cases} t_1^{-1}(t_1) & t_1 \leq t_1(1), \\ 1 & \text{otherwise.} \end{cases}$$

Notice that the case of $t_1 > t_1(1)$ is off the equilibrium path. Finally note that Bidder 0's strategy to bribe whenever his value exceeds bidder 1's tip, and to bid only if he is willing to bribe, constitutes a best response. This concludes the proof. ∎

Notice that even though bids are completely private in this model, because of the transaction inclusion micro-structure, bids are effectively revealed by the tips attached to them. This calls into question whether we can conduct sealed bid auctions of any type on chain.

We can also describe the equilibrium for the case where the seller chooses an auction with a reserve price $r > 0$. For brevity we describe this informally:

$$t_1(v_1) \text{ solves } (v_1 - r - t)f_0(r + t) - F_0(r + t) = 0 \text{ if solution exists,}$$
$$t_1(v_1) = 0 \text{ otherwise.}$$

Our regularity condition implies that there exists $\underline{v} = r + \frac{F_0(r)}{f_0(r)} > r$ such that $t_1(v_1) = 0$ for $v \leq \underline{v}$ and strictly increasing for $v > \underline{v}$. Bidder 0's strategy is to bribe and submit a bid only if his value $v_0 > t_1 + r$ where t_1 is the observed tip.

PROPOSITION 2. *The following constitutes an equilibrium of the game with 2 bidders, i.e., $N = \{0, 1\}$, when the seller announces a second-price auction with a reserve price $r > 0$:*

- *Bidder 1 submits a truthful bid, and his tipping strategy as function of his value v_1 is given by $t_1(v_1) = v_1/2 - r$ whenever $v_1 > 2r$ and 0 otherwise.*
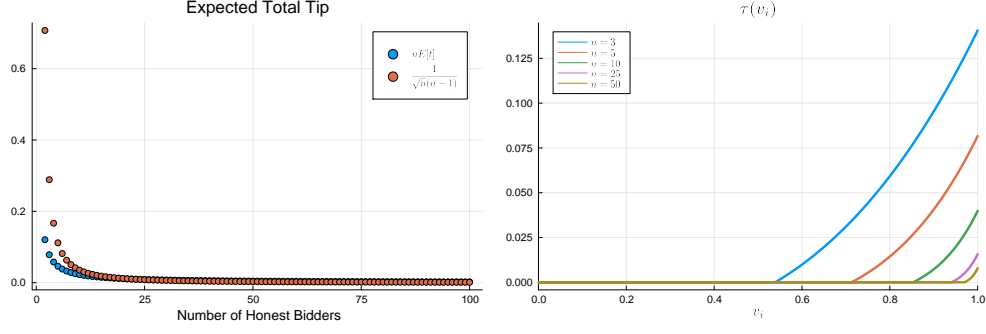
FIGURE 1. Expected Total Tips and Tipping functions for $F = F_0 \sim$ Uniform$[0,1]$

- *Bidder 0's strategy as function of the observed tip t_1 and his value v_0 is given by*

$$\sigma_0(t_1, v_0) = \begin{cases} \text{bribe} & t_1 + r \leq v_0 \\ \text{don't bribe} & \text{o.w.} \end{cases}$$

  where bribe is shorthand for paying t_1 to the proposer in exchange for omitting bidder 1's transaction. Further bidder 0 submits a non-zero bid in the auction if and only if he bribes the proposer.
- *The proposer accepts bidder 0's bribe whenever it is offered and omits bidder 1's bid, otherwise the proposer includes both bids.*

Note that while the seller does receive positive revenue in this case, they do not realize any "benefit" from running an auction relative to posting a "buy it now" price of r. We formalize this in the following corollary:

COROLLARY 2. *Suppose buyer values are i.i.d. Uniform$[0,1]$. Assuming $r \leq \frac{1}{2}$, Bidder 0 wins the object with ex-ante probability $(1-r)(1-(\frac{1}{2}-r)^2)$, while bidder 1 wins the object with ex-ante probability $(1-2r)(\frac{r}{2}+\frac{1}{4})$. The expected revenue of the seller is $r(1-r^2)$, which is the same as the revenue for posting a "buy it now" price of r. The proposer makes an expected revenue of $\frac{1}{4}(1-2r)^2$.*

Again bidder 0 has a strong advantage in this auction. Tips are no longer perfectly revealing, since a non-empty interval of bidder values tip 0, but remain weakly monotone in bid and perfectly revealing when strictly positive.

4.2. *Three or more bidders*

We now turn to the case where $n \geq 2$, i.e., $N = \{0, 1, \dots, n\}$.

At first the problem of finding an equilibrium may appear intractable since bidder 0's best-response problem is itself complicated: there are 2^n possible subsets of $\{1, \dots, n\}$ and the problem of finding the best subset to buy out is therefore non-trivial. The tipping

function of bidders $\{1, \ldots, n\}$ needs to be a best response to this (accounting for how changing their tip changes the probability that they are censored given a distribution of other tips). Nevertheless, there is an easy to describe equilibrium. In order to construct it, the following lemma is useful:

LEMMA 1. *Suppose that the tipping strategy of buyers $1 \ldots n$ is such that $t(v) \leq v/n$. Then we have that the best response for bidder 0, as a function of his own value v_0 and observed vector of tips $\mathbf{t} = (t_1 \ldots t_n)$ can be described as:*

$$\sigma_0(v_0, t_1, \ldots, t_n) = \begin{cases} bribe, & \sum_{i=1}^n t_i \leq v_0 \\ don't\ bribe, & \sum_{i=1}^n t_i > v_0 \end{cases}$$

where bribe is shorthand for paying the proposer $\sum_i t_i$ in exchange for omitting all of bidder 1 through n's transactions.

PROOF. To see this note that:

$$\sum_{i=1}^n t(\theta_i) \leq \sum_{i=1}^n \frac{\theta_i}{n} \leq \sum_{i=1}^n \frac{\max(\theta_1, \theta_2, \ldots, \theta_n)}{n} = \max(\theta_1, \theta_2, \ldots, \theta_n).$$

and therefore bribing the proposer and buying out all the bids (and therefore winning the object for free in the auction) is more profitable than buying out any subset of the bids and possibly losing the auction or having to pay more than the bribes for that subset would have cost. ∎

This lemma is useful because, in equilibrium, the tipping strategy of bidders 1 through n will satisfy this property. Bidder 0's strategy is therefore straightforward (analogous to the case $N = \{0, 1\}$). We are now in a position to describe equilibrium in this game.

PROPOSITION 3. *The following constitutes an equilibrium of the game with $n + 1$ bidders, $N = \{0, 1, \ldots, n\}$, and buyer values drawn i.i.d. from Uniform$[0, 1]$ when the seller announces a second-price auction with a reserve price $r = 0$:*

- *Bidders 1 through n submit truthful bids, and their tipping strategy as function of their value v_i is given by:*

$$t(v) = \begin{cases} 0 & v < \underline{v}, \\ \frac{1}{2n}\left(v^n - \underline{v}^n\right) & o.w. \end{cases} \tag{1}$$

where $\underline{v}$ solves

$$(n+1)\frac{\underline{v}^n}{n(n-1)} - \frac{\underline{v}^{n+1}}{(n+1)} - \frac{1}{n(n+1)} = 0. \tag{2}$$

- *Bidder 0's strategy as function of the observed tips $t_1, \ldots, t_n$ and their value v_0 is given by*

$$\sigma_0(v_0, t_1, \ldots, t_n) = \begin{cases} bribe, & \sum_{i=1}^n t_i \leq v_0 \\ don't\ bribe, & \sum_{i=1}^n t_i > v_0 \end{cases}$$

  where bribe is shorthand for paying $\sum_i t_i$ to the proposer in exchange for omitting bidder 1 through n's transactions. Further bidder 0 submits a truthful non-zero bid in the auction if and only if he bribes the proposer.
- *The proposer accepts bidder 0's bribe whenever it is offered and omits the other bids, otherwise the proposer includes all bids.*

It is easy to see that (2) has exactly 1 root in $[0,1]$ by observing that the left hand side is increasing in v on $[0,1]$, and evaluates to a negative number at $v = 0$ and a positive number for $\theta = 1$. Unfortunately we cannot analytically derive these roots for arbitrary n since polynomials of order ≥ 5 don't have explicit roots (and even for $n = 2, 3$ these are not particularly nice); however, we can use a zero finding algorithm to compute these numerically. Results for the uniform case are presented in Figure 1.

Analytically, we can bound how this root varies with n. Note that the expected total tip is $n\mathbb{E}[t(v)]$ and substituting in (1) and simplifying via (2), we have that the expected total tip $= \frac{v^n}{n-1}$. The following proposition describes the asymptotic behavior of the expected total tip:

PROPOSITION 4. *Let $\underline{v}(n)$ describe the solution to (2) as a function of n. There exists $\underline{n}$ large enough such that for $n > \underline{n}$, we have that $\frac{1}{n} \leq \underline{v}(n)^n \leq \frac{1}{\sqrt{n}}$.*

Proposition 4 is particularly useful when you consider the fact that for large n, by the law of large numbers, the total tip concentrates around the expected tip with high probability (buyer values are i.i.d. bounded random variables). Further by Proposition 4, this is decreasing at rate at least $1/n\sqrt{n}$: as n grows, individual bidders are willing to tip less. To see why tipping is only profitable when it leads to the bid not being censored *and* winning the auction, but increasing the tip increases the probability of all bids not being censored. In short, tips have public goods type properties. Indeed, the rate of tipping shrinks fast enough so that the total tip is also decreasing. Therefore bidder 0 wins the auction with increasing probability in n, asymptotically tending to 1. Note that the seller only receives revenue when there is more than one bidder in the auction (or more generally, in the auction with a reserve price r, makes revenue larger than the reserve price)—and this happens with vanishing probability as n grows large.

PROPOSITION 5. *As n grows large, the expected revenue of the auction with reserve price r reduces asymptotically to the expected revenue of a posted price of r.*
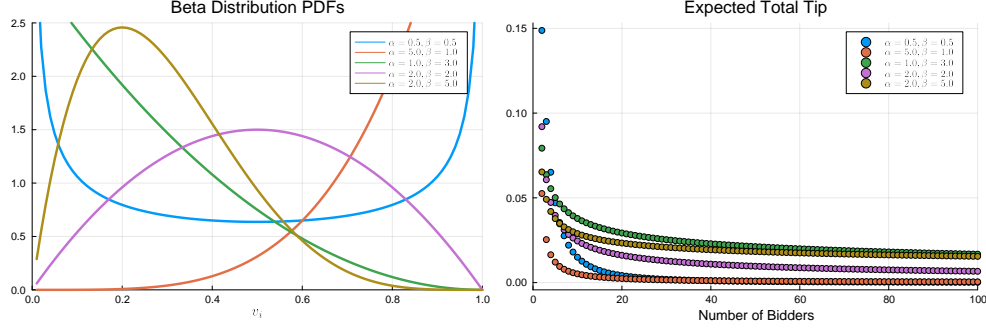
FIGURE 2. Expected Total Tips for $F_0 \sim \text{Uniform}[0,1]$, $F \sim \text{Beta}(\alpha, \beta)$

4.3. *General Distributions*

It is straightforward to generalize our results to the case where bidders $\{1, \ldots, n\}$ are distributed according to some general distribution with density f and CDF F on $[0,1]$.

ASSUMPTION 1. *We assume throughout that F satisfies $\int_0^v F^{n-1}(\theta)d\theta \leq \frac{v}{n}$ for all $v \in [0,1]$.*

Formally, we have the following Proposition:

PROPOSITION 6. *The following constitutes an equilibrium of the game with $n + 1$ bidders, i.e. $N = \{0, 1, \ldots, n\}$, when the seller announces a second-price auction with a reserve price $r = 0$, bidder 0 has a value $\text{Uniform}[0,1]$ and bidders 1 through n have values distributed i.i.d. according to a distribution with density f and CDF F satisfying Assumption 1:*

- *Bidders 1 through n submit truthful bids, and their tipping strategy as function of their value v_i is given by:*

$$t(v) = \begin{cases} 0 & v < \underline{v}, \\ \frac{1}{2} \int_{\underline{v}}^v F^{n-1}(\theta)d\theta & o.w. \end{cases} \tag{3}$$

where $\underline{v}$ solves

$$\int_0^1 F^{n-1}(\theta)d\theta - \int_{\underline{v}}^1 F^n(\theta)d\theta = \frac{n+1}{n-1} \int_0^{\underline{v}} F^{n-1}(\theta)d\theta. \tag{4}$$

- *Bidder 0's strategy as function of the observed tips $t_1, \ldots, t_n$ and their value v_0 is given by*

$$\sigma_0(v_0, t_1, \ldots, t_n) = \begin{cases} \text{bribe}, & \sum_{i=1}^n t_i \leq v_0 \\ \text{don't bribe}, & \sum_{i=1}^n t_i > v_0 \end{cases}$$

where bribe is shorthand for paying $\sum_i t_i$ to the proposer in exchange for omitting bidder 1 through n's transactions. Further bidder 0 submits a truthful non-zero bid in the auction if and only if he bribes the proposer.

13

- *The proposer accepts bidder 0's bribe whenever it is offered and omits the other bids, otherwise the proposer includes all bids.*

This proposition allows us to numerically solve for tipping behavior in this auction. Using the flexible Beta distribution for a range of parameters, we compute $n\mathbb{E}[t]$ as a function of n in Figure 2.

Analytical results for the case where bidder 0's value is distributed non-uniformly appear out of reach. To see why—for bidders 1 through n, part of the payoff of increasing their tip is increasing the probability that bidder 0 chooses not to buy them out. When bidder 0's value is distributed uniformly, the increase in probability is constant and independent of others' tips (which from the perspective of the bidder is a random variable). This simplifies the optimality condition and makes it analytically tractable. Nevertheless, the intuition above suggests that our qualitative results (seller expected revenue drops to close to the posted price, tips do not offer much "protection" due to the public goods nature of tips suggests, bidder 0 has a strong advantage in the auction) carry over to this case as well.

5. RESTORING AUCTION CREDIBILITY

We now discuss possible design choices to restore auction credibility, so that an auction can be run on chain with the desired results.

5.1. *Auction over Multiple Blocks*

The source of the popularly stylized *eventual censorship resistance* of blockchains, a.k.a *liveness*, is that even though a single proposer is the "monopolist" over one block, over a longer period, multiple proposers get a chance to make a block. In order for a specific transaction to be censored, multiple proposers will have to be incentivized to exclude it. Motivated by this, we now investigate whether running the auction over multiple blocks restores the desired behavior.

Formally we consider the following dynamic game corresponding to an auction being run over m blocks. We assume that each of these blocks is produced by an independent proposer.[14]

(1) Period 0: Bidders learn their values v_i. Bidders $1, \ldots, n$ each submit simultaneously a private bid b_i and a public tip t_i.
(2) Period j for j in 1 to k: Bidder 0 observes which bids from $1, \ldots n$ have not been included in a block in periods 1 to $j - 1$. They offer Proposer j a take-it-or-leave-it-offer of a subset S_j of the unincluded bids and a payment p_j to exclude that subset.

---

[14]In practice, an majority of blocks on major blockchains is produced by one of a small oligopoly of proposers. We discuss the implications of this in the sequel.

The proposer j observes the tips and the offer from Bidder 0 and decides which bids if any to include.

(3) Period $m + 1$: The seller's auction is run on blocks produced in periods 1 to m.

If a transaction is included in period j, it is removed from the set of bids in the mempool, its tip is attributed to proposer j where j is the block it was included in, it is included in the auction, and it cannot be included in subsequent blocks.

Note that the game we describe is a natural extension of the previous game to the case of an auction over $m > 1$ blocks. In particular, it reduces to the original game for the case of $m = 1$. We consider the same refinement as before, which applies to this game in a similar fashion.

Note that there are two possible sources of additional security in this auction. The first is mechanical: in order to censor a transaction, intuitively, bidder 0 has to bribe m proposers, which is more expensive for a given tip. The second is that the marginal returns to a tip have increased (increasing a tip by q increases the cost to censor for bidder 0 by mq, and decreases the probability they can afford it correspondingly).

In our results, we show that the latter effect is null. In particular, we show that for $m < n$, the tipping behavior of bidders $1, \ldots n$ stays unaffected.

Formally, we have the following result:

PROPOSITION 7. *Suppose buyers 1 to n have values drawn i.i.d. $U[0,1]$ and buyer 0 has value drawn i.i.d. $U[0, \kappa]$ for $\kappa > m$. The following constitutes an equilibrium of the game with $n + 1$ bidders, i.e. $N = \{0, 1, \ldots, n\}$, when the seller announces a second-price auction with a reserve price $r = 0$ to be run over m blocks for $m < n$: Bidders 1 through n and the proposers have the same strategy as in Proposition 3.*

Bidder 0's strategy as function of the observed tips $t_1, \ldots, t_n$ and his value v_0 is given by

$$\sigma_0(v_0, t_1, \ldots, t_n) = \begin{cases} bribe, & m \sum_{i=1}^{n} t_i \leq v_0, \\ don't\ bribe, & otherwise, \end{cases}$$

Before we proceed, we comment on the assumption that bidder 0's value is distributed $U[0, \kappa]$. Suppose bidder 0 is distributed $U[0, 1]$, but bidders 1 to n tip as in Proposition 3. Note that with positive probability the total tip could exceed 1 when $m > 1$. Therefore, given bidders 2 to n follow the tipping strategy of Proposition 3, bidder 1 will have incentives to shade their tip relative to $t(\cdot)$. After all, the marginal value of a tips depends on the how they increase the probability of not being censored. From the Proof of 3, in the case of $m = 1$, increasing one's tip on the margin always increases the probability that the bids are not censored, because the total tip is strictly smaller than 1 with probability 1 on path. Intuitively, therefore if bidder 0 is distributed $U[0, 1]$, and the auction is conducted over $m > 1$ blocks, the equilibrium tipping strategy for bidders 1 to n is weakly lower

than the corresponding tipping strategy for $m = 1$ (Proposition 3). This can be shown numerically, but is out of reach analytically.

Note that we had already shown that expected total tip of n bidders was smaller than $1/n^{3/2}$. Therefore, the probability that bidder 0 does not censor the remaining bids collapses to 0 as n grows large, as long as m grows sublinearly with n. To see that we had already shown that expected total tip of n bidders was smaller than $1/n^{3/2}$. Therefore m times this for $m < n$ still grows smaller than $1/\sqrt{n}$.

Put differently, guaranteeing the auction outcome is "as desired" requires $m > n$. This comes with its own costs: for example, the auction would have to remain open for a relatively long time which may be undesirable, particularly for financial applications.

5.2. *Multiple Concurrent Block Proposers*

Depending on the number of bidders and the time constraints inherent to the specific auction application, it may not be feasible to hold the auction for long enough to achieve the desired censorship resistance level.

A different solution we now consider would be to allow more than one proposer within a single slot. Formally, we now consider k concurrent block proposers (by analogy to our previous section where we considered k sequential block producers). The seller announces an auction which will execute within the single slot, i.e. the bids included on at least one of the k concurrent produced blocks will be included in the auction.

In view of the concurrency, we allow bidders to submit conditional tips, which depend on the number of proposers who include the transaction. For simplicity, we consider a *twin tip*, i.e., each bidder submits a conditional tip of the form (t, T), where T is paid if only a single proposer includes bidder 1's transaction and t is paid if more than one proposer includes the transaction. After the honest bidder observes v_1 and submits his private bid b_1 and public tip (t, T), the bribing bidder submits a bribe to each proposer.

Formally, we first consider the following game:

(1) Seller announces second-price sealed-bid auction with reserve price r to be conducted over a single slot.
(2) Buyers learn their values $v_i \sim F$.
(3) Buyers $1, \ldots, n$ each submit simultaneously a private bid b_i and a public tip t_i, T_i.
(4) Buyer 0 observes all the other tips t_i, T_i and simultaneously offers each proposer a take-it-or-leave-it-offer of a subset $S \subseteq \{1, \ldots, n\}$ of bidders and a payment p to exclude that subset's bids. Bidder 0 also submits his own bid b_0.
(5) Each Proposer simultaneously accepts or rejects bidder 0's offer and constructs the block accordingly i.e., either containing bids of set $N \setminus S$ or N.

(6) The auction is computed based on the union of the bids included in all blocks, tips are paid based on the inclusion behavior.

As before we focus our attention on equilibria where Bidders $\{1, \ldots, n\}$ bid truthfully in the auction. Note that each proposer, in choosing whether to censor a transaction, needs to reason about the behavior of other proposers since that potentially affects their tip if they include the transaction.

PROPOSITION 8. *Consider the Multiple Concurrent Block Proposer game, with m proposers and $n = 1$ honest bidder, i.e., $N = \{0, 1\}$, with bidder i's value drawn from a distribution with CDF F_i and PDF f_i.*

This game has an equilibrium where the outcome of the auction is the same as a standard second price auction without a censorship step and where the expected tip by each bidder to each proposer is $\underline{t}$.

In particular, bidders 1's tipping strategy in equilibrium is given by:

$$t_1(v_1) = 0, \qquad\qquad T_1(v_1) = 1 \tag{5}$$

Bidder 0's offer strategy to the proposer based on their own value v_0 and the observed tips (t, T) is

$$z_0(t, T, v_0) = \begin{cases} 0 & C(v_0) < mT \\ T & C(v_0) \geq mT. \end{cases} \tag{6}$$

Here $C(v_0)$ is buyer 0's net value to censoring bidder 1's bid (i.e., the difference their profit from censoring the competing bid and winning in the auction for free (v_0); and their expected surplus from competing with bidder 1 in the auction). Finally, the proposer's strategies are to censor transactions with the following probabilities:

$$p(z, t, T) = \begin{cases} 0 & z < t \\ \left(\frac{z-t}{T-t}\right)^{\frac{1}{m-1}} & t \leq z < T \\ 1 & z \geq T \end{cases} \tag{7}$$

The above proposition may admittedly appear a little dense. We provide the following corollary regarding (on-path) equilibrium behavior.

COROLLARY 3. *Consider the equilibrium proposed in Proposition 8 for any $m \geq 2$. On path, bidder 0 does not bribe the proposers and instead competes in the second-price auction. All bidders pay 0 in tips on path. Equilibrium tips do not reveal bids.*

Further, a careful study of the proof of Proposition 8 shows that the Corollary continues to hold even when $n > 1$. Therefore even 2 concurrent block proposers restore the "desired" outcome relative to a single block proposer system. This is partly driven

by concurrency of block proposers which removes the "monopoly" that they have over transaction inclusion, and partly by the conditional tip. The conditional tip allows bidder 1 to get security via a high-tip offer conditional on inclusion by only a single proposer. This high tip offer makes it very expensive for bidder 0 to attempt censor bidder 1's bid since they would need to pay m times the high tip to censor the bid by all m producers. Therefore, no bribe is offered. Further, this tip never needs to be paid, since both proposers find it weakly dominant to include the bid and pick up the low tip.[15] As an aside, note that this also restores equilibrium bid privacy, since tips no longer reveal bids.

6. DISCUSSION

Our results suggest that single proposer blockchains are not ideal for holding time sensitive auctions when the number of potential bidders is large. In our results, collusion arrangements are extremely profitable for the colluding bidder but only marginally profitable for the proposer. However, this is because we restrict the model to have one potential colluding bidder who can bribe the proposer. In reality, there are many possible colluding bidders, and only one proposer in each slot, the proposer could end up charging for the right to collude and extract a significant portion of the value that the colluding bidder gains from the arrangement. In fact, the predominant block building system, MEV-boost, can be thought of as a direct channel through which the proposer can sell the right to censor transactions to the highest bidder. This suggests that one driver of MEV is the proposer's right to determine inclusion. Previous work has focused on a different source: the proposer's right to order transactions within a block. From the position that proposer ordering power is the source, order agnostic mechanisms should solve MEV. But if censorship power is the source, these order agnostic mechanisms, including the second price auction we study here, could be just as susceptible to value extraction.

Another proposed source for MEV is the public nature of transactions in the mempool. The argument is, transactions in the mempool are sitting ducks, waiting to be front-ran. It follows that, if transactions are encrypted while in the mempool, they will be less susceptible to MEV. But our results demonstrate that even when bids in the auction are encrypted, public tips may reveal private bids.

6.1. *Future Directions*

From a theoretical perspective, this work leaves open questions of how censorship in on chain auctions might effect the equilibria of auctions with different assumptions about

---

[15]Note that $t = 0$ supports alternative asymmetric equilibria in the inclusion subgame where only a single proposer includes the transaction. In the broader game, these would correspond to the equilibria in the single proposer cases where T substitutes for the old single dimensional tip. However, when t is bounded away from 0, these equilibria disappear, since it is now strictly dominant for the proposer to include the bid in the inclusion subgame.

bidder valuations. For example a natural extension to our results would be to consider honest bidders with interdependent or common values. This may be a better model for on chain order flow auctions and collateral liquidation auctions.

Our results are based on the assumption that a single bidder has been selected as the colluding bidder in advance, but an assumption that would track more closely to the realities of MEV-boost would be to have the right to collude be auctioned off after bids have been submitted. If the right to collude is auctioned off before the bids are submitted, then our results would still hold, since our result would simply be a subgame of the larger game being considered, and the result would be that proposers end up with a larger share of their monopoly rents; however, when the right to collude is auctioned off after transactions have been submitted, and therefore after bidders discover their types, the players who are willing to pay to collude are more often those who value the item more. This could warp the equilibrium slightly.

Outside of mechanism design, this work provides a strong theoretical justification for investigating multiple concurrent block proposer based consensus frameworks as a tool for MEV mitigation. Specifically, we identify conditional tipping as a powerful tool to combat censorship in situations where there are more than one block proposer.

Another potential tool for combating censorship on chain, that we have not discussed, is a data availability layer. Instead of being submitted to a blockchain directly, bids could be submitted to a data availability layer, nodes could then compute the results of the auction based on whichever transactions were included on the data availability layer. This is similar to holding the auction directly on chain except that the nodes tasked with curating a data availability layer do not necessarily need to participate in consensus. The requirements for a data availability layer are weaker than those required for a full blockchain so it may be easier to integrate multiple proposer architecture on data availability layers than on blockchains themselves.

REFERENCES

Akbarpour, Mohammad and Shengwu Li, "Credible Mechanisms.," in "EC" 2018, p. 371.

_____ **and** _____ , "Credible auctions: A trilemma," *Econometrica*, 2020, *88* (2), 425–467.

Blass, Erik-Oliver and Florian Kerschbaum, "Strain: A secure auction for blockchains," in "European Symposium on Research in Computer Security" Springer 2018, pp. 87–110.

Budish, Eric, Peter Cramton, and John Shim, "The high-frequency trading arms race: Frequent batch auctions as a market design response," *The Quarterly Journal of Economics*, 2015, *130* (4), 1547–1621.

Daian, Philip, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels, "Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges," 2019.

_____ , _____ , _____ , _____ , _____ , _____ , _____ , **and** _____ , "Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability," in "2020 IEEE Symposium on Security and Privacy (SP)" IEEE 2020, pp. 910–927.

Elkind, Edith and Helger Lipmaa, "Interleaving cryptography and mechanism design: The case of online auctions," in "Financial Cryptography: 8th International Conference, FC 2004, Key West, FL, USA, February 9-12, 2004. Revised Papers 8" Springer 2004, pp. 117–131.

Ferreira, Matheus VX and David C Parkes, "Credible Decentralized Exchange Design via Verifiable Sequencing Rules," *arXiv preprint arXiv:2209.15569*, 2022.

_____ **and S Matthew Weinberg**, "Credible, truthful, and two-round (optimal) auctions via cryptographic commitments," in "Proceedings of the 21st ACM Conference on Economics and Computation" 2020, pp. 683–712.

Flashbots, "The future of MeV is suave: Flashbots," Nov 2022.

Frankie, Dan Robinson, Dave White, and andy8052, "Gradual Dutch Auctions," Apr 2022.

Galal, Hisham S and Amr M Youssef, "Verifiable sealed-bid auction on the ethereum blockchain," in "Financial Cryptography and Data Security: FC 2018 International Workshops, BITCOIN, VOTING, and WTSC, Nieuwpoort, Curaçao, March 2, 2018, Revised Selected Papers 22" Springer 2019, pp. 265–278.

Johnson, Nicholas AG, Theo Diamandis, Alex Evans, Henry de Valence, and Guillermo Angeris, "Concave Pro-rata Games," 2022.

Kelkar, Mahimna, Fan Zhang, Steven Goldfeder, and Ari Juels, "Order-fairness for byzantine consensus," in "Annual International Cryptology Conference" Springer 2020, pp. 451–480.

———, **Soubhik Deb, Sishan Long, Ari Juels, and Sreeram Kannan**, "Themis: Fast, strong order-fairness in byzantine consensus," *Cryptology ePrint Archive*, 2021.

Kulkarni, Kshitij, Matheus VX Ferreira, and Tarun Chitra, "Credibility and Incentives in Gradual Dutch Auctions," *arXiv*, 2023.

———, **Theo Diamandis, and Tarun Chitra**, "Towards a theory of maximal extractable value i: Constant function market makers," *arXiv preprint arXiv:2207.11835*, 2022.

Lee, Byoungcheon, Kwangjo Kim, and Joongsoo Ma, "Efficient public auction with one-time registration and public verifiability," in "Progress in Cryptology—INDOCRYPT 2001: Second International Conference on Cryptology in India Chennai, India, December 16–20, 2001 Proceedings 2" Springer 2001, pp. 162–174.

Milionis, Jason, Dean Hirsch, Andy Arditi, and Pranav Garimidi, "A Framework for Single-Item NFT Auction Mechanism Design," in "Proceedings of the 2022 ACM CCS Workshop on Decentralized Finance and Security" 2022, pp. 31–38.

Rothkopf, Michael H, Thomas J Teisberg, and Edward P Kahn, "Why are Vickrey auctions rare?," *Journal of Political Economy*, 1990, *98* (1), 94–109.

Suzuki, Koutarou and Makoto Yokoo, "Secure generalized vickrey auction using homomorphic encryption," in "Financial Cryptography: 7th International Conference, FC 2003, Guadeloupe, French West Indies, January 27-30, 2003. Revised Papers 7" Springer 2003, pp. 239–249.

Szabo, Nick, "Formalizing and securing relationships on public networks," *First monday*, 1997.

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

7. OMITTED PROOFS

7.1. *Proof of Proposition 3*

PROOF. We first need consider the tipping strategy $t(v)$. To do this we first work out the expected utility for player 1 when all other $n - 1$ "honest" bidders are bidding according to $t(\cdot)$ and bidder 0 is following the strategy above, i.e., censoring all the bids whenever the total tip doesn't exceed their value:

$$U(v, t) = \int_0^v \ldots \int_0^v \left(F_0(\sum_{j=2}^n t(v_j) + t)(v - \max(v_j)) \right) dv_2 \ldots dv_n \tag{8}$$

$$- t\mathbb{E}\left[F_0(\sum_{j=2}^n t(v_j) + t) \right].$$

Here the first term is expected profit of the buyer *in the auction*, and the second term is the expected cost of the tip: tip times the probability that the bid is not censored and the tip is therefore charged. Note that since the buyer 0's value is distributed uniformly, so $F_0(\sum_{j=2}^n t(v_j) + t) = \sum_{j=2}^n t(v_j) + t.$[16]

$$\implies U(v, t) = \int_0^v \ldots \int_0^v \left((\sum_{j=2}^n t(v_j) + t)(v - \max(v_j)) \right) dv_2 \ldots dv_n$$

$$- t\mathbb{E}\left[(\sum_{j=2}^n t(v_j) + t) \right].$$

Differentiating with respect to t

$$\frac{\partial U(v, t)}{\partial t} = \int_0^v \ldots \int_0^v \left((v - \max(v_j)) \right) dv_2 \ldots dv_n - \mathbb{E}\left[(\sum_{j=2}^n t(v_j)) \right] - 2t.$$

Therefore optimality implies that $t(v)$ must solve:

$$\implies \frac{v^n}{n} - \mathbb{E}\left[(\sum_{j=2}^n t(v_j)) \right] - 2t(v) \leq 0.$$

with the inequality binding when $t(v) > 0$.

Let us denote $\mathbb{E}[t(v_j)]$ by c.

$$\implies \frac{v^n}{n} - (n - 1)c - 2t = 0.$$

---

[16]Formally, this is only true as long as $\sum_{j=2}^n t(v_j) + t < 1$, but our solution will be such that $\sum_1^n t(v_i) \leq 1$ for any profile of values i.

Therefore we have that:

$$t(v) = \begin{cases} 0 & v < \underline{v}, \\ \frac{1}{2}\left(\frac{v^n}{n} - (n-1)c\right) & \text{o.w.} \end{cases}$$

where $\underline{v} = ((n^2 - n)c)^{1/n}$. Finally, since $\mathbb{E}[t(v_j)] = c$, it must be that

$$\int_{\underline{v}}^{1} \frac{1}{2}\left(\frac{v^n}{n} - (n-1)c\right) dv = c,$$

$$\implies \frac{1}{n(n+1)}(1 - \underline{v}^{n+1}) - (n-1)c(1 - \underline{v}) = 2c.$$

Putting together we have that

$$\frac{\underline{v}^{n+1}}{n(n+1)} + (n+1)c - (n-1)c\underline{v} = \frac{1}{n(n+1)}. \tag{9}$$

Recall that $\underline{v} = ((n^2 - n)c)^{1/n} \implies c = \frac{\underline{v}^n}{n(n-1)}$. Substituting this into (9) we have

$$\frac{\underline{v}^{n+1}}{n(n+1)} + (n+1)\frac{\underline{v}^n}{n(n-1)} - (n-1)\cdot\frac{\underline{v}^n}{n(n-1)}\cdot\underline{v} = \frac{1}{n(n+1)}.$$

$$\implies (n+1)\frac{\underline{v}^n}{n(n-1)} - \frac{\underline{v}^{n+1}}{(n+1)} - \frac{1}{n(n+1)} = 0, \tag{10}$$

as desired.

Further by observation, we have that the assumption of Lemma 1 is satisfied, i.e., $t(v) \leq \frac{v}{n}$ and therefore we have from Lemma 1 that Bidder 0's bribing strategy is a best response to these tips. ∎

As an aside, we note that the the first step in the proof, i.e. noting that $F_0(\sum_{j=2}^{n} t(v_j) + t) = \sum_{j=2}^{n} t(v_j) + t$ under the uniform distribution, allows to make the $\mathbb{E}[F_0(\sum_{j=2}^{n} t(v_j) + t)]$ in the first expression analytically tractable. This is the reason we are unable to generalize beyond the uniform distribution for bidder 0

7.2. *Proof of Proposition 4*

First suppose $\underline{v}^n = 1/\sqrt{n}$. Substituting in to the left hand side of (10), we have

$$\frac{n+1}{n(n-1)\sqrt{n}} - \frac{1}{(n+1)(\sqrt{n})^{\frac{n+1}{n}}} - \frac{1}{n(n+1)}.$$

Note that the first term is $O(1/n^{3/2})$, and the latter two terms are smaller. So the left hand side is always positive.

Therefore we have that $\underline{v}^n \leq \frac{1}{\sqrt{n}}$ (since the left hand side of (10) goes from negative to positive and is 0 at the unique root).

This in turn implies that $nc \leq \frac{1}{(n-1)\sqrt{n}}$.

By a similar argument we can argue that $\underline{v}^n > 1/n$. To see this, note that substituting into left hand side of (10), we have

$$\frac{n+1}{n^2(n-1)} - \frac{1}{(n+1)(n)^{\frac{n+1}{n}}} - \frac{1}{n(n+1)},$$

$$= \frac{(n+1)^2 - n(n-1)}{n^2(n-1)(n+1)} - \frac{1}{(n+1)(n)^{\frac{n+1}{n}}},$$

$$= \frac{3n+1}{n^2(n-1)(n+1)} - \frac{1}{(n+1)(n)^{\frac{n+1}{n}}}.$$

Note that the first term is $O(1/n^3)$, while the second term is $\approx O(1/n^2)$, so for n large this will be negative.

7.3. *Proof of Proposition* 5

Repeating the calculation of the proof of Proposition 3, we have that a bidder of value v' indirect utility from a tip of t given all other $n - 1$ bidders tip according to $t(\cdot)$ is given by

$$U(v,t) = \int_r^v \ldots \int_r^v \left(P_0(v_0 < r + \sum_{j=2}^n t(v_j) + t)(v - \max(v_j)) \right) dv_2 \ldots dv_n$$

$$+ P_0(v_0 < r + t)r^{n-1}(v - r) - t\mathbb{E}\left[F_0(r + \sum_{j=2}^n t(v_j) + t) \right] t.$$

Again, the buyer 0's value is distributed uniformly, so $F_0(r + \sum_{j=2}^n t(v_j) + t) = r + \sum_{j=2}^n t(v_j) + t$.

$$\implies U(v,t) = \int_r^v \ldots \int_r^v \left((r + \sum_{j=2}^n t(v_j) + t)(v - \max(v_j)) \right) dv_2 \ldots dv_n$$

$$+ (r + t)r^{n-1}(v - r) - t\mathbb{E}\left[(r + \sum_{j=2}^n t(v_j) + t) \right].$$

Differentiating with respect to t, we have

$$\frac{\partial U(v,t)}{\partial t} \int_r^v \ldots \int_r^v ((v - \max(v_j))) \, dv_2 \ldots dv_n + r^{n-1}(v - r) - \mathbb{E}\left[r + (\sum_{j=2}^n t(v_j)) \right] - 2t.$$

The first two terms are just the interim expected surplus of a bidder with value v in a second price auction with n bidders and reserve price r, which by revenue equivalence is the integral of the allocation of lower types, i.e.,

$$\int_r^v \ldots \int_r^v ((v - \max(v_j))) \, dv_2 \ldots dv_n + r^{n-1}(v - r)$$

$$= \int_r^v \theta^{n-1} d\theta,$$

$$= \frac{v^n}{n} - \frac{r^n}{n}.$$

Therefore, substituting back in, optimality of $t(\cdot)$ requires that

$$\frac{v^n}{n} - \frac{r^n}{n} - r - \mathbb{E}\left[\sum_{j=2}^n t(v_j)\right] - 2t(v) \leq 0,$$

with equality whenever $t(v) > 0$. Therefore we have that:

$$t(v) = \begin{cases} \frac{1}{2}\left(\frac{v^n}{n} - (n-1)c_r - (r + \frac{r^n}{n})\right) & v \geq (n((n-1)c_r + (r + \frac{r^n}{n}))^{1/n} \\ 0 & \text{otherwise} \end{cases}$$

where $c_r = \mathbb{E}[t(v)]$.

Therefore we have $t(v) = \frac{1}{2}\left(\frac{v^n}{n} - (n-1)c_r - (r + \frac{r^n}{n})\right)$ when $v > \underline{v}$ and 0 otherwise. Recall that when $r = 0$, $t(v) = \frac{1}{2}\left(\frac{v^n}{n} - (n-1)c\right)$. Therefore $c_r < c$ and $(n-1)c_r - (r + \frac{r^n}{n}) > n - 1c$.

Therefore the equilibrium tipping function $t(v)$ when $r > 0$ are first order stochastically dominated by the tipping function when $r = 0$. We already showed in Proposition 4 that the tipping function when $r = 0$ as a function of n implies that total tips collapse to 0 at a super-linear rate. Therefore that continues to be the case here, and the Proposition follows.

7.4. *Proof of Proposition 6*

Repeating the calculation of the Proof of Proposition 3 but assuming that the bidders are now distributed according to some distribution F, an taking first order conditions, we must have that

$$\int_0^v F^{n-1}(v)dv - c - 2t(v) \leq 0$$

with it binding whenever $t(v) > 0$.

So we must have:

$$t(\theta) = \begin{cases} 0 & v \leq \underline{v} \\ \frac{1}{2}\left(\int_0^v F^{n-1}(v)dv - (n-1)c\right) & \text{o.w.} \end{cases}$$

where $c, \underline{v}$ jointly solve

$$\int_0^v F^{n-1}(v)dv = (n-1)c,$$

25

$$\int_0^1 t(v)dF(v) = c.$$

Note that the latter equation can be written as:

$$\int_{\underline{v}}^1 \frac{1}{2} \left(\int_0^v F^{n-1}(v)dv - (n-1)c \right) dF(v) = c$$

$$\implies \int_{\underline{v}}^1 \left(\int_0^v F^{n-1}(v)dv - (n-1)c \right) dF(v) = 2c,$$

$$\implies \int_{\underline{v}}^1 \left(\int_0^v F^{n-1}(v)dv \right) dF(v) = (2 + (n-1)(1 - F(\underline{v}))) c,$$

writing $\int_0^v F^{n-1}(v)dv = S(v)$ and doing integration by parts

$$\implies S(1) - S(\underline{v})F(\underline{v}) - \int_{\underline{v}}^1 F^n(v)dv = (2 + (n-1)(1 - F(\underline{v}))) \frac{S(v)}{n-1},$$

$$\implies S(1) - \int_{\underline{v}}^1 F^n(v)dv = \frac{n+1}{n-1} S(\underline{v}),$$

as desired.

Note that under Assumption 1, 1, this implies that the assumption of Lemma 1 continues to be satisfied, i.e., $t(v) \le \frac{v}{n}$ and therefore we have from Lemma 1 that Bidder 0's bribing strategy is a best response to these tips.

7.5. *Proof of Proposition 7*

The proof follows from the Proof of Proposition 3. To see this, note that if bidder 0 is distributed $U[0, \kappa]$, given the conjectured strategies of 1 to n, we have the total tip is always smaller than the highest possible value of bidder 0. Therefore the proof continues to hold as written: bidder 0 being distributed $U[0, \kappa]$ changes (8) by a multiplicative constant $\frac{1}{\kappa}$, and therefore this does not affect the optimization.

7.6. *Proof of Proposition 8*

PROOF. We proceed by backward induction. First consider the subgame where tips (t, T), and bribe z have already been offered. Given that all other proposers are censoring with probability p. The expected utility for proposer i as a function of censoring probability p_i is given by:

$$p_i z + (1 - p_i)(p^{m-1})T + (1 - p_i)(1 - p^{m-1})t.$$

Differentiating this with respect to p_i we have

$$z - p^{m-1}T - t + p^{m-1}t.$$

Therefore for a symmetric mixed equilibrium of the subgame it must be that

$$0 = z - t - (T - t)p^{m-1}$$

$$\implies p = \left(\frac{z-t}{T-t}\right)^{\frac{1}{m-1}}$$

Given this, the probability of successfully censoring the bid for a given bribe $z \in [t, T]$ is

$$p^m = \left(\frac{z-t}{T-t}\right)^{\frac{m}{m-1}}$$

If the value of censorship to the bribing bidder is C relative to the no censorship case, then the expected utility of the bribing bidder relative to the no censorship case as a function of z is

$$Cp^m - mzp = C\left(\frac{z-t}{T-t}\right)^{\frac{m}{m-1}} - mz\left(\frac{z-t}{T-t}\right)^{\frac{1}{m-1}}$$

Define $u \equiv \frac{1}{T-t}^{1/m-1}$, and $q \equiv z - t$. Substituting in to the latter expression, we have

$$u^m Cq^{\frac{m}{m-1}} - u\left(mtq^{\frac{1}{m-1}} + mq^{\frac{m}{m-1}}\right)$$

Note that this is convex in q, and therefore the solution is to either tip t (which effectively is the same as tip 0), or tip T. Finally, note that $C \leq v_0$ by definition.

Given this, the strategy of $(t, T) = (0, 1)$ is a best response for bidder 1 since it will result in bidder 0 offering a bribe of 0. ∎