Redesigning Bitcoin's fee market

Ron Lavi[1], Or Sattath[2,3], and Aviv Zohar[2]

[1]Technion
[2]The Hebrew University
[3]MIT

September 27, 2017

Abstract

The security of the Bitcoin system is based on having a large amount of computational power in the hands of honest miners. Such miners are incentivized to join the system and validate transactions by the payments issued by the protocol to anyone who creates blocks. As new bitcoins creation rate decreases (halving approximately every 4 years), the revenue derived from transaction fees start to have an increasingly important role. We argue that Bitcoin's current fee market does not extract revenue well when blocks are not congested. This effect has implications for the scalability debate: revenue from transaction fees may decrease if block size is increased.

The current mechanism is a "pay your bid" auction in which included transactions pay the amount they suggested. We propose two alternative auction mechanisms: The Monopolistic Price Mechanism, and the Random Sampling Optimal Price (RSOP) Mechanism (due to Goldberg*et al.*). In the monopolistic price mechanism, the miner chooses the number of accepted transactions in the block, and all transactions pay exactly the smallest bid included in the block. The mechanism thus sets the block size dynamically (up to a bound required for fast block propagation and other security concerns). We show, using analysis and simulations, that this mechanism extracts revenue better from users, and that it is nearly incentive compatible: the profit due to strategic bidding relative to honest biding decreases as the number of bidders grows. Users can then simply set their bids truthfully to exactly the amount they are willing to pay to transact, and do not need to utilize fee estimate mechanisms, do not resort to bid shading and do not need to adjust transaction fees (via replace-by-fee mechanisms) if the mempool grows.

We discuss these and other properties of our mechanisms, and explore various desired properties of fee market mechanisms for crypto-currencies.

1 Introduction

The Bitcoin system is known to be more secure against double spending attacks as more computational power is invested by honest miners [Nak08]. Miners are nodes in Bitcoin's network that solve proof-of-work puzzles that are required by the protocol. To improve the network's security it is important to attract miners and to incentivize them to invest large amounts of computational power. Nakamoto's approach was to pay miners to partake in the security of the system: a miner that solves a proof-of-work puzzle successfully is allowed to create a block within Bitcoin's blockchain. The block, which is a collection of approved transactions, awards the lucky miner with a block reward of newly minted bitcoins plus the sum of all the fees included in the transactions within that block.

Two main problems in today's Bitcoin system are (i) obtaining sufficient revenue for the miners as the block reward gradually decreases, and (ii) throughput limitation as a result of the maximal block size. More specifically, the block reward which started as ฿50 per block is cut in half approximately every 4 years.[1] Therefore, in the long run, transaction fees will become the dominating source of miners' income and thus the main determinant of the security of the system. To circumvent double spending attacks, and maintain the security of the system, it is crucial that this source of income will be significant. In fact, the security of bitcoin is in some sense a public good, enjoyed by all who transact with the currency, and collectively paid for by its users. Bitcoin's fee mechanism is a way to combat *the tragedy of the commons*: each individual user wishes to pay low fees, while still enjoying the security that is purchased with the fees of others. If each acted "selfishly" and did not pay, security would decline. Competition in the fee market is what keeps the rational behavior of Bitcoin's users (partially) aligned with the goal of buying enough security for the entire system.

The second problem, of the limited throughput, is in fact related to the first. Indeed, one of the main arguments against a block-size increase in Bitcoin had been that the fees for transactions may drop to the point where not enough security is purchased for the system. In this paper we essentially show how a different fee market mechanism can extract revenue which does not decrease as block size increases. Hence, decoupling the effect block size increases would have on the fee market from other considerations (like block propagation times, or the fairness of the reward distribution under larger blocks) and providing scalability from the economic perspective of the fee market.

Our contributions: In this paper we reconsider the design of Bitcoin's fee market. We propose a conceptual framework which uses auction theory to determine which transactions will be included in each block. Our main contribution is the proposal and analysis of two auction-based mechanisms for the fee market: the *monopolistic price mechanism*, and the *RSOP mechanism* which is based on the Random Sampling Optimal Price (RSOP) auction defined by Goldberg *et al.* [GHK+06]. These two mechanisms essentially decouple the revenue from fees from the block-size which can be freely determined according to other security

[1] The symbol ฿ represents 1 bitcoin. We use ฿ or bitcoin to represent the currency, and Bitcoin to represent the Bitcoin network or the protocol.

considerations.

We analyze the properties of these two mechanisms using a combination of analytical tools and simulations. In particular, we show several key properties, primarily (i) a high revenue extraction from the users of the system (which will imply a high level of security for the protocol), (ii) incentivizing the miner in its role as an auctioneer to follow the protocol, and (iii) simplicity for transaction issuers: Both mechanisms encourage participants to simply reveal their true preferences – in this case to plainly state how much they are willing to pay in transaction fees. While in Bitcoin wallets today, fee estimation mechanisms cause the wallet to use different transaction fees as a response to the current congestion level, our design implies that the wallet software can run independently of the behavior of others and of external conditions.

Along the way we clearly define the desiderata for such mechanisms including resilience to the various ways participants may deviate and manipulate the protocol. Also, we examine the benefits and faults of the mechanism currently used by Bitcoin.

The blockchain as a single monopolist While the miners in the Nakamoto consensus are separate entities, the protocol itself allows them to act in concert and to reach consensus. We therefore consider the collective of miners as a single monopolist that can coherently charge non-competitive prices from the users. This can be implemented if miners enforce such pricing schemes as part of the consensus mechanism and consider blocks that deviated from these mechanisms as invalid. In this sense, we conceptually consider the monopolist as a single entity acting on behalf of the entire system (in practice, individual miners still obtain the rewards, and we must ensure that individual miners do not deviate).

The Monopolistic Price Mechanism. Our first mechanism operates according to the following rules:

- Each transaction specifies a bid which is the maximal fee it is willing to pay.[2]
- Miners can choose which subset of transactions they include in their block.
- All transactions in the block pay the exact same fee, which is given by the lowest bid contained in the block.
- Miners are expected to choose transactions in a way that will maximize the revenue obtained, i.e., maximize the number of included transactions times the minimal bid – see Eq. (2.1).

As the mechanism above provides miners the maximal revenue (by allowing them to select the set of included transactions and effectively set the monopolistic price), myopic miners gain nothing from a range of manipulations of the protocol, mainly, adding fake transactions,

[2]This deviates from the current way Bitcoin transactions are structured, and requires some architectural modifications.

or excluding legitimate ones. The main issue we address is therefore the manipulations of the users. We focus on *impatient users*, defined as those who desire that their transaction will be included in the next block, and have no utility from inclusion in later blocks. This effectively makes it a single shot game, rather than a repeated game which is often much harder to analyze. For these users we show that honest (truthful) behavior is nearly an equilibrium: our analysis shows, both analytically (for more details on the assumptions and the results, see Thm. 2.3) and empirically (see Section 4), that relative gains from strategic bidding go to 0 as the number of transactions increases. We further show that the monopolistic price protocol collects at least as much revenue from impatient users (and hence buys at least as much security) as Bitcoin's current mechanism.

The RSOP Mechanism We consider the following mechanism.

- Partition the transactions in each block to two sets using a random assignment.
- Compute the monopolistic price (see Eq. (2.2)) for each set.
- Apply the price computed for each set to the complementary set (i.e., only transactions that bid higher than the monopolistic price in the complementary set are accepted, and all pay that same price).

This auction still focuses on obtaining some price that is close to the monopolist's price. The main difference is that it removes (by design) the ability of an individual transaction to affect the price that it pays, as the price is always determined by transactions in the complementary set. Therefore, it is not beneficial to shade the true maximal willingness to pay, as such bid modifications cannot affect the price for that user (although we must still consider splitting transactions, since a single Bitcoin user may have several pseudo-entities). Instead, miners may again benefit from inserting some additional transactions, or ignoring valid transactions, to manipulate their revenue. We conjecture that such manipulations are not severe[3].

A major practical limitation of the RSOP mechanism is that it usually includes many transactions in the blocks that are not eventually considered valid into the ledger. While clever use of cryptographic techniques may alleviate this concern, we currently leave a comprehensive solution as an open problem. For this reason, we believe that the monopolistic price mechanism will be more practical, at least as a first attempt. We discuss other advantages and disadvantages of this mechanism at greater length later in the paper.

1.1 Bitcoin's current fee mechanism

The current design of Bitcoin's fee mechanism requires users to set a fee that they are willing to pay for each transaction. This fee is encoded in the transaction message itself. Once a transaction is included in a block, the fee is awarded automatically to the miner that

[3]More precisely, we conjecture that the ratio between the revenue of an honest miner and a strategic miner goes to 1 as the number of players goes to infinity. This is partly supported by Theorem 5.2.

successfully created that block. Transactions are thus effectively given as take-it-or-leave-it offers to miners. We thus name the current fee mechanism that is used in Bitcoin *Pay-your-Bid*. Since the size of each block is capped, each miner's transaction inclusion strategy is straightforward: they gain most if they first include transactions that pay higher fees (fees are actually sorted by the payment per KB that the transaction takes up as transactions sizes may vary as well). As demand for transferring bitcoins increases, transaction fees are expected to increase as users compete for limited space in blocks. For simplicity, we assume from now on that all transactions are of fixed size, and are thus sorted by the amount they pay. Adapting the mechanisms we propose to varying transaction sizes is trivial (substituting cost per Byte instead of cost per transaction).

Critique of the current mechanism There are several significant disadvantages to the current fee market design. The main one is that the revenue extraction is often deficient. In the following we describe the two main downsides of the current design.

- Bid shading, and frequent bid updates. Unlike in the first-price sealed bid auction, where users pay the amount they bid but do not see the bids of other before hand, Bitcoin users can see the transactions that are queued for inclusion, and may use this information to set their own fee. In particular, a user who is willing to pay a high fee sees that a lower amount will still guarantee that her transaction will get included, will shade her bid, and offer a smaller fee that is currently sufficient. Thus, the fees observed on the network are in fact not truthful representation of the actual amounts users are willing to bid, but rather provide a lower bound which may in fact be far from the truth. This in itself is not problematic, however, as more transactions arrive and are queued for inclusion in the next block, the threshold price of transactions that enter the block grows. Users may then wish to re-transmit their transactions and offer a higher fee[4]. This requires that they remain online and continually monitor the memory pool (the buffer used to hold bitcoin transactions), or settle for either higher fees than are absolutely necessary to get into the block (or alternatively lower the certainty that they would enter a block)

- Poor revenue extraction. Consider for example a situation in which blocks could contain 2000 transactions, but only 1000 users are interested in sending money. As each user sees that the next block is not expected to be full, they can offer an arbitrarily small fee. Regardless of how low the fee is, the miner's incentive is to accept this transaction, as no alternative one can take its place.[5] Overall, all users will bid low, and provide negligible revenue for the miner. If this state persists, miners who receive little reward, but still exert effort to create blocks, will withdraw from mining, which in turn will lower security guarantees.

[4]Older versions of the Bitcoin client did not allow fee readjustments, but current miners adapted a "replace-by-fee" policy that transactions can opt-in for, as the rational step to increase their profit. See `http://www.webcitation.org/6qnP9ROYL`.

[5]Here we neglect communication effects due to larger block size [Riz15].

In general, if a block can contain ℓ transactions, the fee paid by each transaction will be determined by the $\ell+1^{th}$ highest bidder, as shading will occur. It may happen that a smaller block size would yield more revenue for the miner.

To emphasize the problem with the current market, consider the following thought experiment: If some technological advancement allows for larger blocks to be used in the protocol with no additional security risk, then the fees collected by much larger blocks can decrease to 0 if there is no demand for all of the newly available space. This is because the Bitcoin block size serves as the effective price-setting rule for the transaction given a particular distribution of users. Thus, in general, the block size that is used for security purposes due to block propagation [DW13, SZ15] is not necessarily the one that would yield a high-enough revenue. We therefore advocate for a separation of the block size mechanism for security purposes (which we take as an upper bound on the blocks that are produced in practice) from any economic mechanism that selects transactions for inclusion and may decide not to allocate all available space within that limit for transactions.

We demonstrate this point in Figure 1, where we compare the revenue of the current pay-your-bid strategy to the one obtained by the monopolistic price mechanism. For the former, we assume that bids are shaded by the participants so that they all match the one needed to enter the block, i.e., these are equilibrium bids that are equivalent to the $\ell+1$'th valuation (assuming ℓ is the number of transactions can enter a block). The revenue for the monopolistic price assumes honest bids. We demonstrate the revenue assuming utilities that were sampled randomly from the interval $[0,1]$. As can be seen from the graph, the revenue of both mechanisms is (roughly) the same, as long as the block size is small. At some point, the monopolistic price mechanism no longer uses the extra block size, and maintains its high revenue whereas the pay-your-bid mechanism accepts more transactions and suffers from prices that fall dramatically.

In spite of our critique of the current mechanism, it is important to note its obvious benefits: It is relatively simple, the fee a transaction will pay is known in advance, and there are no manipulations that could be made by the miners (e.g., if they add fake transactions to blocks they have little to gain).

1.2 Desiderata

Next we provide the desired properties of a fee mechanism in Bitcoin. We note that some of the properties mentioned below may conflict with others, and it may well be that no single mechanism provides them simultaneously.

High social welfare The sum of valuations of accepted transactions should be large. In this sense, the system is providing a high level of utility to its users. In particular, an efficient allocation is warranted: transactions with higher fees should be included before those with lower fees (assuming both are available at the same time) as this clearly improves the social welfare.

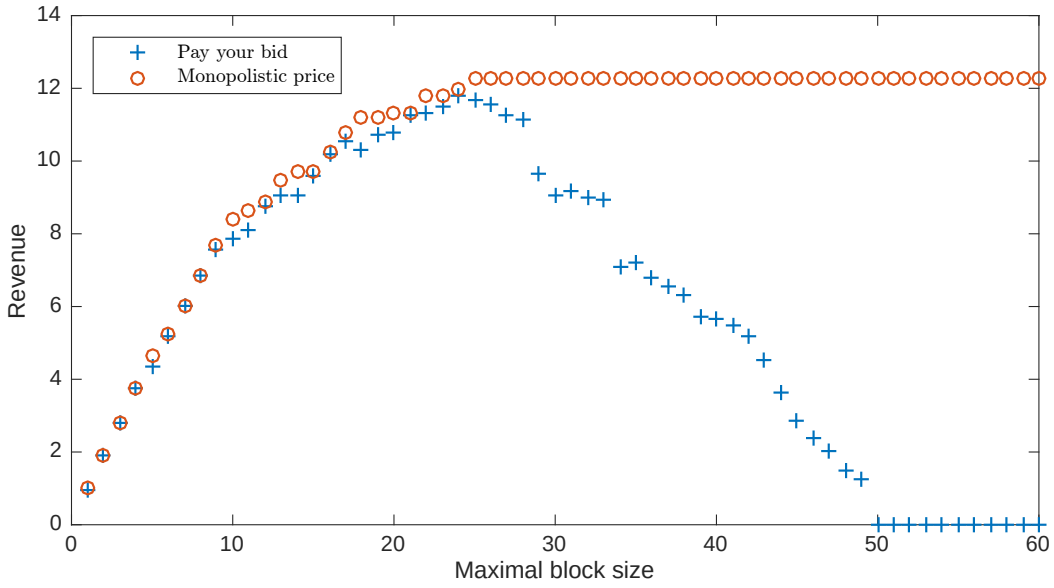


Figure 1: The revenue of the pay-your-bid and monopolistic price mechanisms for various block sizes. Utilities were sampled i.i.d. from the $[0, 1]$ interval. The x-axis denotes the number of transactions that can fit into a block.

Revenue extraction The amount of money transfered to the miners is high, which would buy more security for the system. Stated another way: the revenue of miners should be part of the social welfare measure of the system.

Direct revelation by the users and truthful bidding An ideal mechanism would allow users to state their preferences clearly and would encourage honest reporting. The main advantage would be that users do not need to "overthink" how they should act. Simply state their true preferences. Furthermore, there is no need to monitor the network for price, perform estimates of the threshold fee needed to get accepted into a block, and no need to perform fee updates for the transaction.

Additionally, no manipulation by users should be profitable: splitting a single transaction into two transfers of smaller amounts, adding more transactions between two bitcoin addresses of the same client, etc.

Resistance to manipulation by miners The mechanism should be resistant to selfish behavior by the miners. Such behavior can include miners adding transactions of their own into their own blocks, miners withholding transactions and selecting other sets of transactions, etc.

Resistance to manipulation via side payments Some mechanisms may seem to provide good fees, but in fact may encourage miners and users to circumvent the fee system

altogether. For example, if a miner has to give half of the revenue from his block to the miner that creates the next block in the chain, then he can offer users a deal: The miner will include transactions with 0 fees in his block in exchange for a side payment that will be given to him via a separate and direct transaction. In this manner, he does not need to share the rewards with others.

Adaptivity to changing demand, network conditions, block sizes, etc. It is important to avoid hard-coded magic numbers (such as hard-coded minimal fees) in the protocol as much as possible. Given that the protocol is hard to update, as it requires wide adoption of new code, any hard-coded number is difficult to adjust. A minimal fee, for example, which may need adjusting from time to time (e.g., when the exchange rate fluctuates, or demand increases) would insert inefficiency when it is not set in accordance with market conditions.

Accounting for temporal considerations Users may have different levels of urgency for their transactions. A good fee mechanism will take into account the willingness of users to delay the acceptance of their transactions, e.g., in exchange for paying lower fees. In Bitcoin, transactions that were not added to the blockchain persist with the same fee and may be included in other blocks (without a discount). Our own analysis in this paper considers only impatient users who only desire that their transactions will be included in the next block. We believe that such temporal considerations are an important issue to tackle in future work.

1.3 Related Work

There are relatively few works that analyze the Bitcoin fee market, and fewer still that offer modifications to the basic mechanism.

Kroll *et al.* [KDF13] provided an early analysis of the economics of Bitcoin mining, including some game theoretic analysis of the incentives to mine on the longest chain. Babaioff *et al.* [BDOZ12] consider the incentives of miners to distribute transactions to each other and design ways to share the fees in exchange for distribution. Carlsten *et al.* [CKWN16] explore the security of Bitcoin and the incentive to mine blocks properly when block rewards diminish and fees dominate the revenue of miners. They show that variance in fees may undermine the security of the protocol and subject it to different forms of deviations and attacks. Bonneau [Bon16] explores related bribery attacks on the protocol that are paid for through promises of higher rewards for attackers that construct blocks off the longest chain. A work by Rizun [Riz15] considers the removal of the block limit altogether, arguing that delays in the propagation time of large blocks, which in turn imply a higher likelihood that the block is abandoned (often referred to as an orphaned block), will result in miners restricting their own block size. The paper analyzes the fee market that results. Huberman *et al.* [HLM17] model the transaction fee market assuming that users benefit less if their transactions are delayed. They show that this, together with congestion that may naturally occur in blocks due to queuing effects can lead to non-zero bids for transacting users even if blocks are not completely full.

As far as we are aware, no previous work has explored a different mechanism for the fee market in crypto-currencies.

An important approach to resolve Bitcoin's scalability problem is off-chain transactions, such as the Lightning network [PD15]. The idea is that the vast majority of the transactions are to be made off-line, in so-called *payment channels*, without including them in a block. In this setting, settlements are needed only in rare cases (for example, opening and closing channels). It is unclear how this change would affect Bitcoin's fee market, and more specifically, the miners' revenue.

2 The Monopolistic Price Mechanism

In this section we describe our first mechanism for the fee market, the monopolistic price mechanism and define our model.

We consider n users, each with her own transaction to include in the block, and a miner that is now constructing the block. We assume that every user i has a maximum fee, v_i, that she is willing to pay for her transaction to be included in the block. Our approach is as follows: every transaction includes a bid (maximum fee) and all transactions that are chosen to be included in the block pay the *minimal* bid included in the block. Formally, suppose the bids in the block are $b_1 \geq b_2 \geq ... \geq b_k$, then everyone pays b_k. Given the bids of all users $\boldsymbol{b} = (b_1, \ldots, b_n)$ where $b_1 \geq \ldots \geq b_n$, define the monopolistic revenue as:

$$R(\boldsymbol{b}) = max_{k \in [n]} k \cdot b_k \tag{2.1}$$

(where $[n] \equiv \{1, ..., n\}$). Given the vector of bids $\boldsymbol{b}$, if a miner will be restricted by the Bitcoin protocol to charge the same payment from all transactions in the block, the optimal revenue that the miner can achieve is $R(\boldsymbol{b})$.[6] Denote by $k^*(\boldsymbol{b})$ the number of users that maximize the monopolistic revenue $R(\boldsymbol{b})$ (in case of ties, k^* is taken to be the maximal one). The monopolistic price is

$$p^{monopolistic}(\boldsymbol{b}) = b_{k^*(\boldsymbol{b})}. \tag{2.2}$$

A user, however, might wish to submit a bid that is lower than her true maximum fee, i.e. $b_i < v_i$ (this is sometimes termed "bid shading"). To see why bid shading is profitable for the user, consider the following examples:

Example 2.1. Suppose all users $1, \ldots, n$, have the same maximum fee $v_i = 1$. If all users bid $b_i = v_i$ then $R(\boldsymbol{b}) = n, k^*(\boldsymbol{b}) = n$, and $p^{monopolistic}(\boldsymbol{b}) = 1$. I.e., all users get accepted to the block and they all pay 1. However, in such a case, a strategic user, say user 1, can reduce her payment a bit by reducing her bid to be $b_1 = \frac{n-1}{n}$. With such a bid, notice that the monopolistic price decreases to $\frac{n-1}{n}$: if all bids of value 1 are accepted the miner's revenue is $n-1$ and if all bids of value at least $b_1 = \frac{n-1}{n}$ are accepted the miner's revenue is still $n-1$. Thus, being strategic helped user 1 to reduce her payment.

[6] This assumes that the miner is myopic, i.e., she does not expect to create another block in the near future.

This example suggests that a user can indeed benefit from bid shading but the possible gain from it vanishes as the number of users (and the block size) increases. We will establish later that this observation in fact holds in many realistic settings under reasonable distributional assumptions. However, in the worst case, there could be cases where the manipulations yield significant gains, as the following example shows:

Example 2.2. Suppose users $v_1 = 2, \ldots, v_{\frac{n}{2}+1} = 2, v_{\frac{n}{2}+2} = 1, \ldots, v_n = 1$. If user 1 is strategic, she can significantly reduce her payment by submitting a smaller bid $\frac{n-1}{n} \approx 1$ instead of 2.

The point that we make here is that, although in the worst case users can manipulate, "usually" (under various reasonable distributional assumptions), this will not happen as the possible gain from such a manipulation becomes very close to zero when there are many users in each block. We first show a theoretical result and then describe an extensive empirical analysis to validate this claim.

To continue with the formal discussion, we first define a few notions. Fix a user i and a vector of bids $\boldsymbol{b}_{-i} \equiv (b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_n)$ of the other users. Let $p^{honest}(v_i, \boldsymbol{b}_{-i}) \equiv p^{monopolistic}(v_i, \boldsymbol{b}_{-i})$ and

$$p^{strategic}(\boldsymbol{b}_{-i}) \equiv \min\{b_i \in \mathbb{R} \mid p^{monopolistic}(b_i, \boldsymbol{b}_{-i}) \leq b_i\}.^{78} \tag{2.3}$$

As an illustration, Figure 2 presents $p^{monopolistic}(b_1, 1)$, and Figure 3 presents the strategic prices in an example with $n = 256$ users. As can be seen from this example, $p^{strategic}$ is monotonically decreasing among the winning users (higher winning bids imply lower strategic prices) but not among all users (this property will be proved later in Claim A.8). It is also interesting to note that, in this example (as well as in other simulations), almost all winning users have the same strategic prices, the exception being the very few winning users with the lowest bids (i.e., prices slightly higher than the monopolistic price), whose strategic prices are higher (i.e., they can gain less from being strategic). A similar situation holds for the losing users. Most of them have the same strategic price, except for the few highest ones.

We next define the "discount ratio" from strategic bid shading. In words, this is 0 if the the user does not get into the block, even if she is honest. Otherwise, it is one minus the ratio between the monopolistic price when the user is strategic,and the monopolistic price when the user is honest. Formally,

$$\delta_i(v_i, \boldsymbol{b}_{-i}) = \begin{cases} 1 - \frac{p^{strategic}(\boldsymbol{b}_{-i})}{p^{honest}(v_i, \boldsymbol{b}_{-i})} & \text{if } v_i \geq p^{strategic}(\boldsymbol{b}_{-i}) \\ 0 & \text{otherwise.} \end{cases} \tag{2.4}$$

[7] Here the strategic user chooses the lowest possible bid that would get her included in the block. This is indeed the optimal strategy, assuming that the user can only provide one bid. See an additional discussion in the sequel regarding the case that the user can split her bid.

[8] The minimum is well defined by Claim B.1, using $f(b_i) = p^{monopolistic}(b_i, b_{-i})$. Claim A.13, shows that $f(b_i)$ satisfies the property required by Claim B.1, and clearly there exists b_i such that $b_i \geq f(b_i)$, e.g., taking any $b_i > \max_{j \neq i} b_j$.

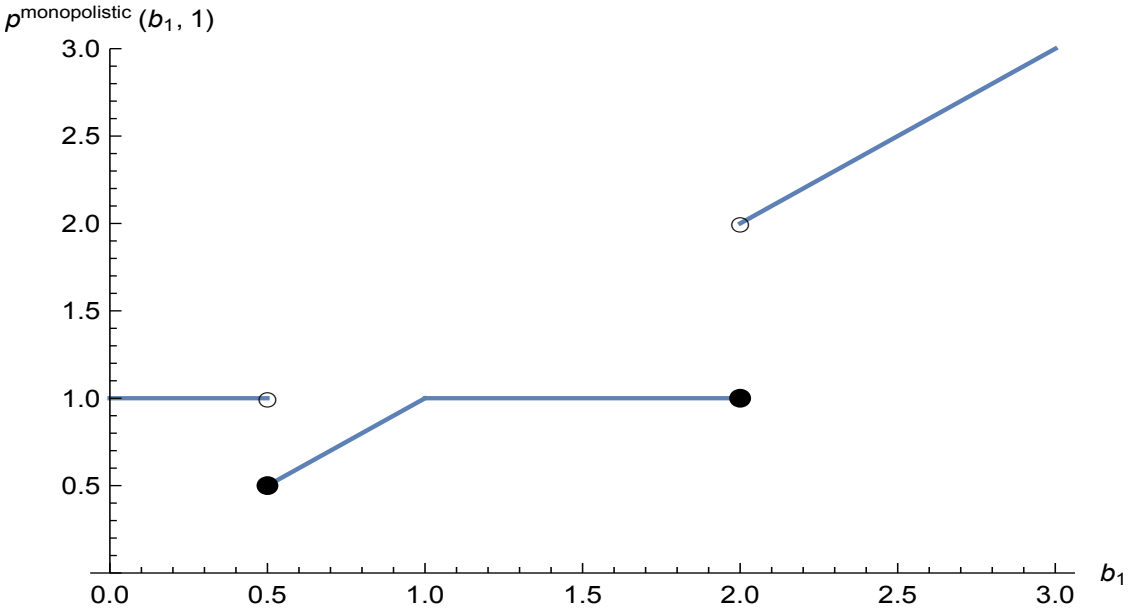


Figure 2: The function $p^{monopolistic}(b_1, 1)$ as a function of b_1. This demonstrates that $p^{monopolistic}$ is not monotone and not continuous. As can be seen, the strategic price of the first bidder is 0.5.

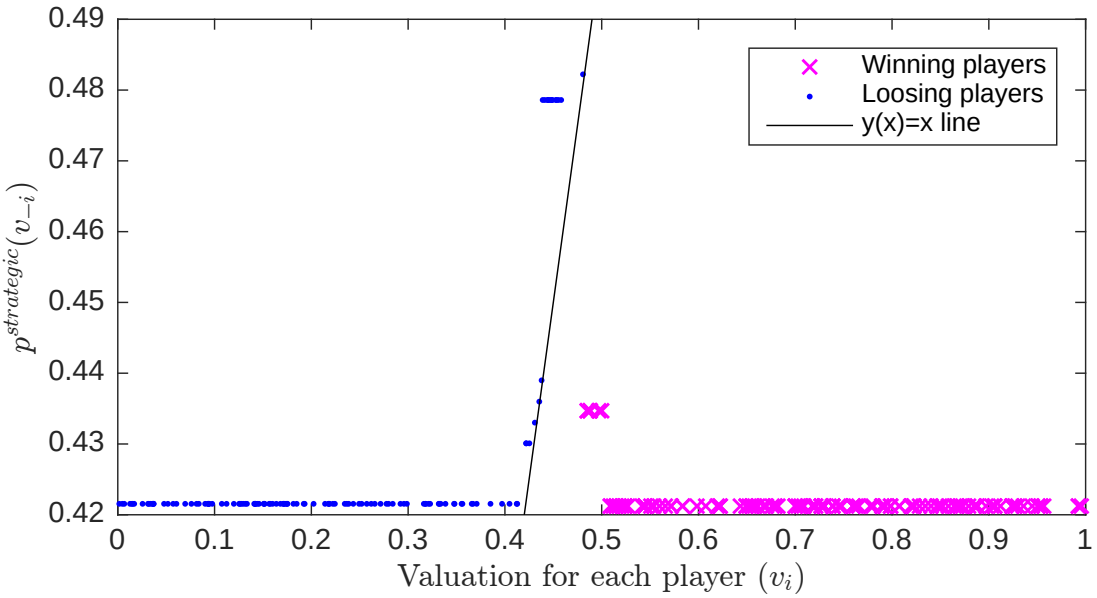


Figure 3: An example with $n = 256$ bids sampled i.i.d from the uniform distribution on $[0, 1]$. For each user, the x-axis shows her values and the y-axis shows her strategic price. Winning bids, which are marked with 'x', must be at least as high as their respective strategic price, i.e., to the right of the black line.

Note that $0 \leq \delta_i(v_i, \boldsymbol{b}_{-i}) \leq 1$. The discount ratio captures the gain that a user can obtain from strategic bidding: if $v_i < p^{strategic}(\boldsymbol{b}_{-i})$, there is no way for user i to win with a bid of at most v_i, and therefore her gain is 0. If $v_i \geq p^{strategic}(\boldsymbol{b}_{-i})$, user i can win and pay $p^{strategic}(\boldsymbol{b}_{-i})$, but with an honest bid she will pay $p^{honest}(v_i, \boldsymbol{b}_{-i})$. She can thus save a percentage of $1 - \frac{p^{strategic}(\boldsymbol{b}_{-i})}{p^{honest}(v_i, \boldsymbol{b}_{-i})}$ from her payment by strategically adjusting her bid.

Our goal is to quantify how large the discount factor will typically be. The claims will be distributional, and not worst case. In this section we assume that all true values are drawn i.i.d from some distribution F on $\mathbb{R}_{>0}$. We will bound the average discount ratio which, as a first attempt, can be defined as:

$$\Delta_n^{average} = \mathbb{E}_{(v_1,\ldots,v_n)\sim F}[\delta_1(v_1, \boldsymbol{v}_{-1})]$$

(The choice of user 1 is arbitrary since all users are symmetric a-priori.)

We will in fact consider two stronger definitions to measure the maximal and worst-case discount ratios. In the first extension, for each realization of the values, we consider the maximum discount ratio among all players. This is obviously always larger than the previous definition, and thus claiming that this goes to zero as n increases is stronger.

$$\begin{aligned} \delta_{max}(\boldsymbol{v}) &= \max_i \delta_i(v_i, \boldsymbol{v}_{-i}) \\ \Delta_n^{max} &= \mathbb{E}_{(v_1,\ldots,v_n)\sim F}[\delta_{max}(\boldsymbol{v})] \end{aligned}$$

Clearly, it holds for every n that $\Delta_n^{max} \geq \Delta_n^{average}$ since for every $\boldsymbol{v}$ and every i, $\delta_{max}(\boldsymbol{v}) \geq \delta_i(v_i, \boldsymbol{v}_{-i})$.

Theorem 2.3. For any distribution F with a finite support size, $\lim_{n\to\infty} \Delta_n^{max} = 0$.

In the second extension, defined only for distributions with a finite bounded support, we fix player 1, and assume that she deterministically has a value that maximizes her discount ratio (the worst possible value for her, from our perspective), while all other values are probabilistic. This captures a situation where a user knows her own value but only knows a distribution over the other values. As we show below, even in this case the discount ratio goes to zero as the number of users increases.

$$\begin{aligned} \delta_n^{worst-case}(\boldsymbol{b}_{-1}) &= \max_{v_1 \in \text{Support}(F)} \delta_1(v_1, \boldsymbol{b}_{-1}) \\ \Delta_n^{worst-case} &= \mathbb{E}_{(v_2,\ldots,v_n)\sim F}[\delta_n^{worst-case}(\boldsymbol{v}_{-1})] \end{aligned}$$

The relation between $\Delta_n^{worst-case}$ and Δ_n^{max} depends on the distribution, as the following example shows:

Example 2.4. Consider the distribution $Pr(v_i = 1) = p$ and $Pr(v_i = \epsilon) = 1 - p$ where $0 < \epsilon < 1$. In this case, if $p < 0.5$ then $\Delta_{n=2}^{worst-case} > \Delta_{n=2}^{max}$ and if $p > 0.5$ then $\Delta_{n=2}^{worst-case} < \Delta_{n=2}^{max}$, as the following calculation shows.

$$\begin{aligned}\Delta_{n=2}^{worst-case} =& \mathbb{E}_{v_2\sim F}[\max_{v_1\in\{\epsilon,1\}} \delta_1(1,v_2)] = \mathbb{E}_{v_2\sim F}[\delta_1(1,v_2)] \\ &= p\delta(1,1) + (1-p)\delta(1,\epsilon) \\ &= p\cdot\frac{1}{2} + (1-p)\cdot(1-\frac{\epsilon}{2})\end{aligned}$$

$$\begin{aligned}\Delta_{n=2}^{max} =& \mathbb{E}_{(v_1,v_2)\sim F}[\max_i \delta_i(v_1,v_2)] = p^2\delta_i(1,1) + (1-p)^2\delta_1(\epsilon,\epsilon) + 2p(1-p)\max_i \delta_i(1,\epsilon) \\ =& p^2\delta_i(1,1) + (1-p)^2\delta_1(\epsilon,\epsilon) + 2p(1-p)\delta_1(1,\epsilon) \\ =& (1-2p(1-p))\cdot\frac{1}{2} + 2p(1-p)\cdot(1-\frac{\epsilon}{2})\end{aligned}$$

Similarly to Theorem 2.3, it is also the case that $\Delta_n^{worst-case}$ goes to zero as n goes to infinity, when user values are drawn i.i.d. from a distribution F with a finite support size. The proof is very similar to the proof in Section 2.1, and is omitted here.[9] Because both quantities go to zero as n increases, clearly the difference between them also goes to zero as n increases. In the empirical analysis that will be presented in the next section we will focus on Δ_n^{max}, mainly because it is more convenient to work with when the distribution has unbounded support.

As a last note, we remark that we believe that these theoretical conclusions could be further extended, as follows.

Conjecture 2.5.

1. For any distribution F, $\lim_{n\to\infty} \Delta_n^{average} = 0$. Specifically, $\Delta_n^{average} = O\left(\frac{1}{n}\right)$.[10]
2. If F has a bounded support (which may still give probability on an infinite set of values) $\lim_{n\to\infty} \Delta_n^{\max} = 0$. Specifically, $\Delta_n^{\max} = O\left(\frac{1}{n}\right)$.
3. There exists a distribution F with an unbounded support such that $\lim_{n\to\infty} \Delta_n^{\max} > 0$.

2.1 Proof of Theorem 2.3

The get intuition for the proof, consider the following example. The distribution F assigns the probability p to the value 1 and the probability $1-p$ to the value 2. If $p > \frac{1}{2}$, and as n increases, the probability that the monopolistic price is 1 with probability very close to 1, and the strategic price in this case is $1 - \frac{1}{n}$. Therefore, $\delta_n^{max} = \frac{1}{n}$ which, indeed, decreases

[9] The main change is that we need to set the value of the first user to the maximal value in the support of F, and all statements hold with respect to the first player, instead of player i^* as defined in Section 2.1.

[10] The coefficient in the $O(\cdot)$ notation may depend on F.

to 0. If $p > \frac{1}{2}$, the monopolistic price is 2 with high probability, and the strategic price is slightly below 2 (to be more precise, it is $2 - \frac{1}{k^*}$): the value 1 yields a revenue of n, wheres a value of 2 yields a higher value, of about $2(1-p)$. The case where $p = \frac{1}{2}$ is slightly more complicated. In some cases, there would be more players with value 1, and then the strategic price would be $1 - \frac{1}{n}$, and in some cases there would be more players bidding 2, and in this case the strategic price would be roughly 2. But, in some rare cases there would be ties (or a tie up to one player). For example, there could be 5 players with value 1 and 6 players with value 2. In this case, the monopolistic price is 2, but the strategic price for a 2 player is $1 - \frac{1}{11}$, and therefore $\delta_n^{max} \approx \frac{1}{2}$. The probability of having these close ties is the same as the probability that a random walk returns to 0 after exactly n steps, which is $O(\frac{1}{\sqrt{n}})$, and therefore diminishes as n grows. When F has a finite support, the argument is similar and uses a union bound over all possible pairs of values (which is also finite).

Proof For a given tuple $\boldsymbol{v}$ of n values, let $i^* = \text{argmax}_{i=1,\ldots,n} v_i$ and let $k^* = k^*(\boldsymbol{v}_{-i^*})$ be the optimal block size for $\boldsymbol{v}_{-i^*}$. In addition let $p^{honest} = p^{honest}(\boldsymbol{v})$ and $p^{strategic} = p^{strategic}(\boldsymbol{v}_{-i^*})$. We first show two lemmas:

Lemma 2.6. For any F with finite support size, there exists a constant $c > 0$ (which may depend on F but not on n) such that

$$\lim_{n\to\infty} \Pr[k^* < c \cdot n] = 0.$$

This lemma shows that when F has finite support, and when the user which is willing to pay the most is removed, the number of winners grows linearly with n,.

Proof Let $v_{max} = \max \text{Support}(F)$, k_{max} be the number of bidders in $\boldsymbol{v}$ who bid v_{max}, and $p_{max} = \Pr_{v_i \sim F}[v_i = v_{max}]$. By linearity of expectation, $\mathbb{E}[k_{max}] = p_{max} \cdot n$. Using the Chernoff bound, it follows that

$$\lim_{n\to\infty} \Pr\left(k_{max} < \frac{9np_{max}}{10}\right) = 0.$$

Clearly, the bidders who bid v_{max} win, and therefore $k^* + 1 \geq k_{max}$. Therefore,

$$\lim_{n\to\infty} \Pr\left(k^* + 1 < \frac{9np_{max}}{10}\right) = 0.$$

Choosing $c = \frac{8p_{max}}{10}$ completes the proof of the lemma. □

Lemma 2.7. $\lim_{n\to\infty} \Pr(p^{strategic} < \frac{k^*}{k^*+1} p^{honest}) = 0$.

Proof Define A as the event where $p^{strategic} < \frac{k^*}{k^*+1} p^{honest}$. The proof will define an event B and show two facts: (i) $\lim_{n\to\infty} \Pr(B) = 0$, and (ii) $A \subseteq B$. This implies that $\lim_{n\to\infty} \Pr(A) = 0$ as claimed.

To define event B, fix any arbitrary $x > y$ in the support of F. Define $\text{num}(\boldsymbol{v}, z) \equiv |\{v_i | v_i \geq z\}|$. Let the random variables $n_z = \text{num}(\boldsymbol{v}, z)$ for any real number z. Let $h(x) = n_x \cdot x$ and $g(x) = (n_x - 1) \cdot x$. This is the same as $n_x > \frac{y}{x} n_y \geq n_x - 1$ which implies $n_x = \lfloor \frac{y}{x} n_y + 1 \rfloor$. The triple $(n_x, n_y - n_x, n - n_y)$ is a multinomial (specifically, trinomial) distribution with probabilities $p_1 = \Pr_{v_i \sim F}(v_i \geq x), p_2 = \Pr_{v_i \sim F}(x > v_i \geq y), p_3 = \Pr_{v_i \sim F}(v_i < y)$ (note that the p_i's depend on F but do not depend on n). Claim B.3 in Appendix B therefore implies, taking $f(n_y) = \lfloor \frac{y}{x} n_y + 1 \rfloor$,

$$\lim_{n \to \infty} \Pr(h(x) > h(y) \geq g(x)) = 0. \tag{2.5}$$

Let B be the event in which $\exists x > y \in \text{Support}(F)$ s.t. $h(x) > h(y) \geq g(x)$. Since the support is of finite size, there is a fixed number of such pairs $x > y \in \text{Support}(F)$. By Eq. (2.5) and the union bound we conclude that $\lim_{n \to \infty} \Pr(B) = 0$.

We show next that $A \subseteq B$, i.e., that $p^{strategic} < \frac{k^*}{k^*+1} p^{honest}$ implies that $\exists x > y \in \text{Support}(F)$ s.t. $h(x) > h(y) \geq g(x)$. Let $x = p^{honest}$ and let y be the smallest element in the support of F which is at least $p^{strategic}$. By Claim A.6, the event $p^{strategic} < \frac{k^*}{k^*+1} p^{honest}$ implies that $x > y$. Since $p^{monopolistic}(v_{i^*}, \boldsymbol{v}_{-i^*}) = x$ it follows that $h(x) = n_x \cdot x > n_y \cdot y = h(y)$. Furthermore,

$$\begin{aligned}
h(y) &\geq h(p^{strategic}) \\
&= n_{p^{strategic}} \cdot p^{strategic} \\
&= \text{num}(\boldsymbol{v}, p^{strategic}) \cdot p^{strategic} \\
&= \text{num}((p^{strategic}, \boldsymbol{v}_{-i^*}), p^{strategic}) \cdot p^{strategic} \\
&\geq \text{num}((p^{strategic}, \boldsymbol{v}_{-i^*}), x) \cdot x \\
&= (n_x - 1) \cdot x = g(x)
\end{aligned}$$

where the first step follows since $n_y = n_{p^{strategic}}$ and $p^{strategic} \leq y$, the fourth step follows since $v_{i^*} \geq x > y \geq p^{strategic}$, the fifth step follows from Claim A.5 that shows that $p^{monopolistic}(p^{strategic}, \boldsymbol{v}_{-i^*}) = p^{strategic}$, and the sixth step follows since $v_{i^*} \geq x > y \geq p^{strategic}$. □

These two lemmas imply the theorem, as follows. Define the "bad" event E_1 to be the case where $k^* < c \cdot n$ (where c is the constant that is guaranteed to exist from Lemma 2.6) and the "bad" event E_2 as the case where $p^{strategic} < \frac{k^*}{k^*+1} p^{honest}$.

By Claim A.9, $\delta_{max}(\boldsymbol{v}) = \delta_{i^*}(\boldsymbol{v})$. Therefore, $\Delta_n^{max} = \mathbb{E}_{\boldsymbol{v}}[\delta_{i^*}(\boldsymbol{v})]$.

If E_2 does not hold, then $p^{strategic} \geq \frac{k^*}{k^*+1} p^{honest}$ and therefore $\delta_{i^*}(\boldsymbol{v}) \leq \frac{1}{k^*+1}$. Thus,

$$\begin{aligned}
\lim_{n\to\infty} \Delta_n^{max} &= \lim_{n\to\infty} \left[\Pr[E_1 \cup E_2]\, \mathbb{E}_v[\delta_{i^*}(v_{i^*}, v_{-i^*})|E_1 \cup E_2] + \Pr[E_1^c \cap E_2^c]\, \mathbb{E}_v\left[\delta_{i^*}(v_{i^*}, v_{-1})|E_1^c \cap E_2^c\right]\right] \\
&\leq \lim_{n\to\infty} \left[\Pr[E_1] + \Pr[E_2] + \Pr[E_1^c \cap E_2^c] \cdot \mathbb{E}_v[\frac{1}{k^*+1}|E_1^c \cap E_2^c]\right] \\
&\leq \lim_{n\to\infty} \left[\Pr[E_1] + \Pr[E_2] + \Pr[E_1^c \cap E_2^c] \cdot \frac{1}{c\cdot n}\right] \\
&\leq \lim_{n\to\infty} \left[\Pr[E_1] + \Pr[E_2] + \frac{1}{c\cdot n}\right] \\
&= 0
\end{aligned}$$

□

2.2 Multiple strategic bids

The following example demonstrates that there are cases where it is beneficial to split one's bid to several separate transactions with several separate bids. In fact, such a strategy sometimes enables a losing transaction to be included in the block.

Example 2.8. Suppose $v = (5, 2, 1, 1)$. If all users submit truthful bids, the monopolistic price will be 5 and the second user will not be included. However, if the second user submits two separate transactions, both of them with a bid of 1, then the monopolistic price will be 1 and all bids will be included.

The empirical evaluation accounts for such situations and shows that the benefit from using multiple bids also goes to zero as n increases, in a similar way to the case where multiple bids are not considered. In this section we generalize the definition of $p^{strategic}$ to capture the possible benefit from splitting the bid. This is captured by the following definition:

$$p^{multibid}(\boldsymbol{b}_{-i}) = \min\{u \cdot b_i^{(u)} |\, u \in \mathbb{N}^+,\ b_i^{(1)} \geq \ldots \geq b_i^{(u)} \in \mathbb{R},\ b_i^{(u)} \geq p^{monopolistic}(b_i^{(1)}, \ldots, b_i^{(u)}, \boldsymbol{b}_{-i})\}$$

In this definition, user i splits her bid to u different bids such that all of them are accepted, and because of that she pays at most $u \cdot b_i^{(u)}$. Clearly $p^{strategic}(\boldsymbol{b}_{-i}) \geq p^{multibid}(\boldsymbol{b}_{-i})$ because the case of $u = 1$ results in $p^{strategic}$. Example 2.8 shows that there are cases in which the inequality is strict. The following definition is a more natural version of the previous one, and it is straightforward to show the equivalence of the two:

$$p^{multibid}(\boldsymbol{b}_{-i}) = \min\{u \cdot b_i \mid u \in \mathbb{N}^+,\ b_i \in \mathbb{R},\ b_i \geq p^{monopolistic}(\overbrace{b_i, \ldots, b_i}^{\text{u times}}, \boldsymbol{b}_{-i})\}.^{11} \tag{2.6}$$

[11] The minimum is well defined using an argument similar to that used for $p^{strategic}$. In particular, for any positive integer u, use $f_u(b_i) = p^{monopolistic}(b_i, ..., b_i, b_{-i})$ (where b_i appears u times). By Claim A.10, $u \in \{1, ..., n\}$. Since for every u, the infimum is contained in the set, then so is the infimum over the union over $u \in \{1, ..., n\}$.

We believe that Theorem 2.3 and Conjecture 2.5 hold in the case of multiple bids, where in the definition of δ, $p^{multibid}$ replaces $p^{strategic}$. In our empirical evaluation we use $p^{multibid}$ instead of $p^{strategic}$. In all the distributions we examined, except the discrete distribution, we have never encountered a case in which the strategic player has an advantage placing multiple bids. Even in the discrete case, the effect of such multiple bids was negligible.

3 An efficient algorithm for computing $p^{multibid}$

Equations (2.3) and (2.6) define the strategic and multi-bid strategic price of each player, but give little information on how to algorithmically compute such a price (since the optimization is done on an infinite set). In this section we provide an alternative form for Eq. (2.6) which lends itself to a direct algorithmically efficient implementation. This will also be used in the empirical analysis in Section 4.

For the computation of $p^{multibid}$, fix a player i, and let $\boldsymbol{w} = \boldsymbol{v}_{-i}$. From now on we assume w.l.o.g. that $\boldsymbol{w}$ is sorted, $w_1 \geq w_2, \ldots, \geq w_{n-1}$. Define

$$f(j) \equiv \max\left\{\left\lceil \frac{R(\boldsymbol{w})}{w_j} \right\rceil, j+1\right\}.$$

Theorem 3.1. $p^{multibid}(\boldsymbol{w}) = \min_{k^*(\boldsymbol{w}) \leq j \leq n-1} \frac{R(\boldsymbol{w})}{f(j)}(f(j)-j)$. Furthermore, if j^* is the index that minimizes this term, then taking $b^* = \frac{R(\boldsymbol{w})}{f(j^*)}$ and $u^* = f(j^*) - j^*$ minimizes the r.h.s. in Eq. (2.6).

3.1 Proof of Theorem 3.1

We begin with a useful Lemma:

Lemma 3.2. Let b, u be the arguments which minimize Eq. (2.6), j be the integer which satisfies $w_j \geq b > w_{j+1}$ and $u^* = f(j) - j$. Then, $u^* \geq 1$ and $u \geq u^*$.

Proof Since $f(j) \geq j+1$, $u^* \geq 1$. If $f(j) = j+1$, $u^* = 1$ and the claim immediately follows. Thus assume that $f(j) = \lceil \frac{R(\boldsymbol{w})}{w_j} \rceil$. Suppose towards a contradiction that $u \leq u^* - 1$. Then,

$$R(\overbrace{b, \ldots, b}^{\text{u times}}, \boldsymbol{w}) = b \cdot (u+j) \leq w_j \cdot (u^* - 1 + j) = w_j \cdot (f(j) - 1) < R(\boldsymbol{w}) \tag{3.1}$$

where the first step follows since by Claim A.11

$$b = p^{monopolistic}(\overbrace{b, \ldots, b}^{\text{u times}}, \boldsymbol{w})$$

and since there are exactly j bids in $\boldsymbol{w}$ that are at least b; and the last inequality follows from $f(j) < \frac{R(\boldsymbol{w})}{w_j} + 1$.

However Eq. (3.1) shows a contradiction since adding bids can only increase the monopolistic revenue. □

Proof We now prove the theorem. Let b, u be the arguments that determine $p^{multibid}(\boldsymbol{w})$ (i.e., (b, u) minimizes Eq. (2.6)). Let j be the integer that satisfies $w_j \geq b > w_{j+1}$ (where $j = n-1$ if $w_{n-1} \geq b$). By Claim A.12, $j \geq k^*(\boldsymbol{w})$. Let $u^* = f(j) - j$ and $b^* = \frac{R(\boldsymbol{w})}{f(j)}$. Then,

$$b \cdot (u + j) = R(\overbrace{b, \ldots, b}^{\text{u times}}, \boldsymbol{w}) \geq R(\boldsymbol{w}) = b^* \cdot (u^* + j)$$

where the first step is the same as the first step in Eq. (3.1) above. Thus, $b \cdot u \geq b^* \cdot u^* + j \cdot (b^* - b)$. By Lemma 3.2, $u \geq u^*$, which implies $b \cdot u \geq b^* \cdot u^*$ (since $b \cdot u < b^* \cdot u^*$ and $u \geq u^*$ implies $b < b^*$ and $b \cdot u < b^* \cdot u^* + j \cdot (b^* - b)$, a contradiction). Thus,

$$p^{multibid}(\boldsymbol{w}) = b \cdot u \geq b^* \cdot u^* \geq \min_{k^*(\boldsymbol{w}) \leq j \leq n-1} \frac{R(\boldsymbol{w})}{f(j)}(f(j) - j),$$

and the first part of the theorem follows. The second part follows in a straight-forward way from the first part. □

4 Empirical Evaluation

In this section we provide an empirical evaluation of the monopolistic price mechanism. The overall goal is to show that the discount ratio of strategic players becomes negligible, in accordance with the theoretical analysis and conjectures made in the previous sections. We provide empirical evidence supporting the above conjectures, and give more details on the rate at which the discount ratio converges to zero.

The empirical evaluation uses both synthetic data as well as transaction data taken from the Bitcoin blockchain. The synthetic data is generated using four distributions:

1. A uniform discrete distribution over the integers $1, \ldots, 100$. This distribution has a finite support size and therefore satisfies the requirements of Theorem 2.3.

2. The uniform distribution over $[0, 1]$. Notice that, here, the support size is infinite.

3. The half normal distribution. This represents the case where the probability for maximum fee x decreases exponentially with x. Thus, in this case, even though arbitrarily high transaction fees will be seen, they are highly unlikely.

4. The inverse distribution $F(x) = 1 - \frac{1}{x}$ for $x \in [1, \infty)$. This represents the case where the probability for maximum fee x decreases polynomially with x.[12]

[12]The uniform distribution has no tail, the half normal distribution has a light tail because it decreases exponentially fast, and the inverse distribution has a heavy tail. We will see that Δ_n^{max} does not go to 0 as n grows for the inverse distribution, as a result of its heavy tail. Indeed, it is the most difficult distribution

In addition to the synthetic data, we also used real data from the Bitcoin blockchain. The data was collected from 1000 consecutive blocks which constitute roughly one week of activity ending in October 28th 2016. The data obviously does not contain the maximum transaction fee (the maximum willingness to pay for the transaction) since this is not how Bitcoin operates. In the simulations we estimate the user's maximum willingness to pay, v, as a function $v = v(x)$ of the transaction size x.[13] We use three alternative functions: $v(x) = \log x, v(x) = \sqrt{x}, v(x) = x$.[14]

We next present three sets of results to evaluate the actual discount ratios for these distributions. Recall that the discount ratio of a player measures the possible gain, in percentages, that a user can achieve by submitting a strategic bid instead of her true maximum willingness to pay, as explained in detail in Section 2). In Eq. (2.4), we use $p^{multibid}$ instead of $p^{strategic}$ to take into account the most general manipulation possible. $p^{multibid}$ is defined and discussed in Section 2.2. The efficient algorithm used for computing it is described in Section 3.

The following figures show $\Delta_n^{average}$ and Δ_n^{max} as a function of the number of users, n. Recall that $\Delta_n^{average}$ is the average discount ratio over all players, and Δ_n^{max} is the maximal discount ratio over all players. For each point $n = 2^i$ $(i = 3, \ldots, 17)$ we conducted 100 simulation runs. In each simulation we sampled n points from the bid distribution and calculated the empirical discount ratios for each of the n users. Based on the empirical ratios we calculated the empirical $\Delta_n^{average}$, which is the average over the n individual discount ratios, and Δ_n^{max} , which is the maximum over the n individual discount ratios. Each point in the graph is the average over the 100 simulation runs.

The average discount ratio. Figure 4 shows $\Delta_n^{average}$ as a function of the number of users, n. As can be seen from the graph, $\Delta_n^{average}$ behaves very similarly for all the tested distributions. In particular, as stated in the first part of Conjecture 2.5, $\Delta_n^{average}$ decreases linearly with the number of users for all distributions, even those with an infinite and unbounded support size.

The maximal discount ratio. Figure 5 shows Δ_n^{max} as a function n. As can be seen from the graph, Δ_n^{max} behaves differently for some of the tested distributions. For the uniform distribution, Δ_n^{max} decreases linearly with the number of users, supporting the second part of Conjecture 2.5. The half normal distribution behaves similarly (even though it is not bounded). For the inverse distribution, Δ_n^{max} does not seem to decrease with the number

for the proposed mechanism, since for any price $x \geq 1$, the revenue of the mechanism would be roughly $x \cdot (1 - F(x)) = x \cdot 1 - \frac{1}{x} = 1$, thus (up to noise) all prices yield the same revenue, which makes it easy for players to manipulate the prices by changing a single transaction. While we do not think that this distribution represents the actual distribution of maximum transaction fees, we include it here to demonstrate that there may indeed be bad cases for our mechanism.

[13] More specifically, x is the sum of all outputs of the Bitcoin transaction.

[14] Note that multiplying $v(x)$ by a scalar does change the discount ratio. Therefore our results hold even if $v(x)$ is multiplied by some factor $\alpha > 0$.

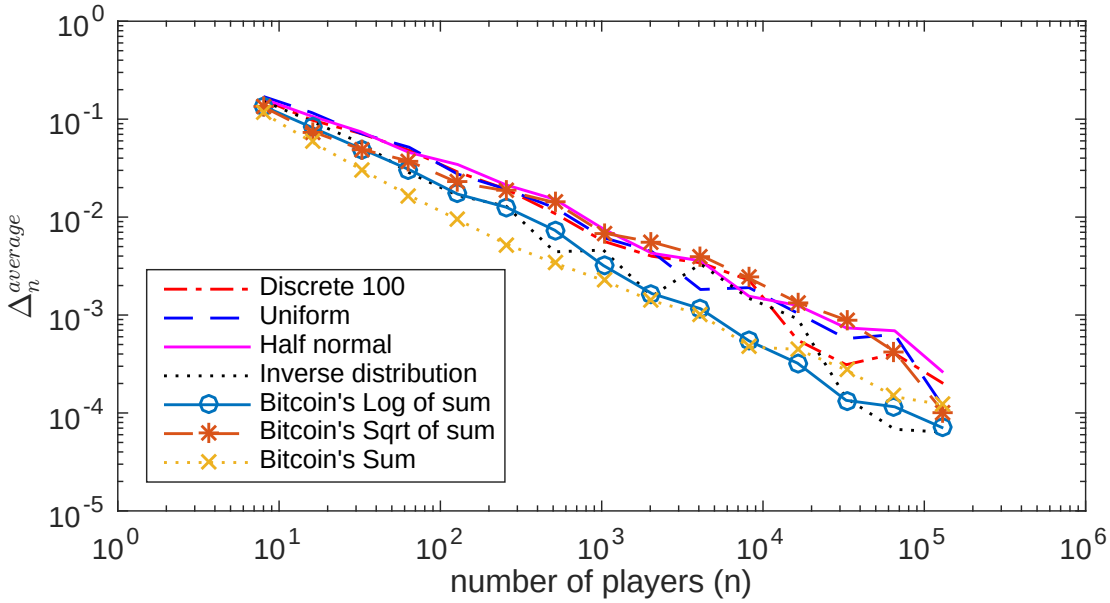


Figure 4: The average discount ratio of a player from selfish bidding as a function of the number of players that participate.

of users, and we believe that this is in fact an example that supports the third part of Conjecture 2.5.

The three Bitcoin distributions behave as follows: the log of sum decreases fastest, the square root of sum decreases in a slower fashion, and the sum decreases in the slowest fashion. For example, when the number of players $n = 2048$ (which is roughly the current Bitcoin block-size), the typical maximal discount factor is about of $0.2\%, 5\%, 19\%$ for the three distributions, respectively. When $n = 2^17 \approx 130,000$, the typical maximal discount factor is about $0.0007\%, 0.05\%, 1\%$.

This shows a qualitative difference between $\Delta_n^{average}$ and Δ_n^{max} when looking at some of the distributions, mainly, for the inverse distribution and for the Bitcoin distribution with $v(x) = x$. In these distributions, the average user will benefit very little from strategically shading down her bid, but some users can benefit from strategizing. This difference between $\Delta_n^{average}$ and Δ_n^{max} can in principle be the result of two different reasons. First, $\Delta_n^{average}$ takes into account also the losing bidders, whose discount ratio is zero. Second, Δ_n^{max} takes into account only the single winning bidder with the maximal discount ratio. However, the typical behavior (which was demonstrated in Figure 3) shows that almost all winning users have the lowest strategic price and therefore highest discount ratio. Thus, the main reason for the difference between $\Delta_n^{average}$ and Δ_n^{max} is the first reason.

Figure 6 shows all simulation points for two distributions, the Bitcoin log of sum and the Bitcoin sum, where the x-axis is the block size of the simulation run and the y-axis is the maximal discount ratio of the simulation run. This figure demonstrates three main points: First, the block sizes (number of winners) range from 1 to about 25,000 when $v(x) = \log x$,

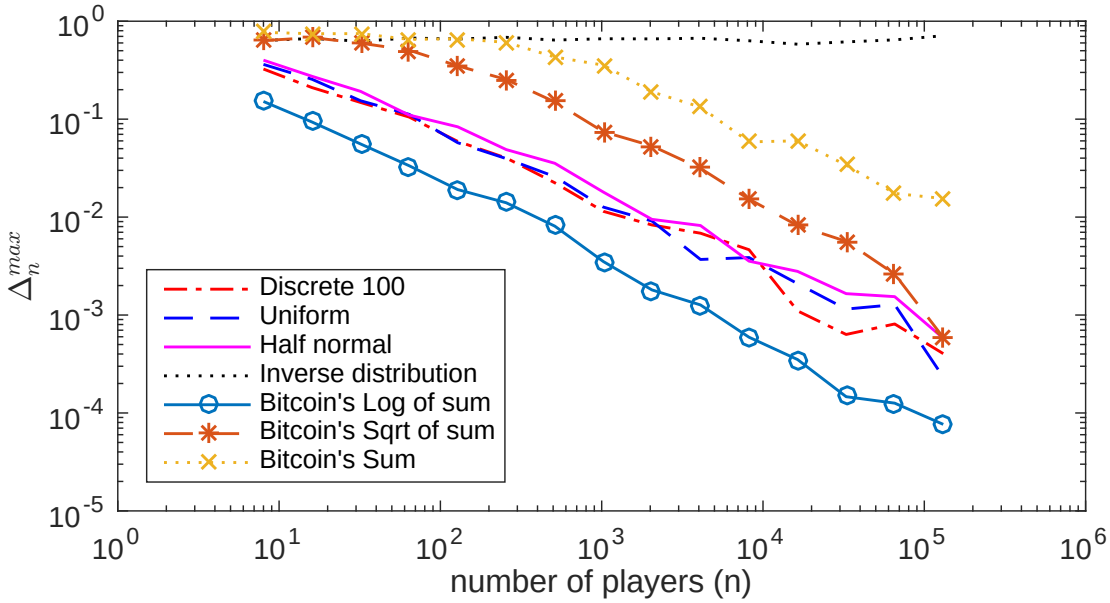


Figure 5: The maximal discount ratio of a player from selfish bidding as a function of the number of players that participate.

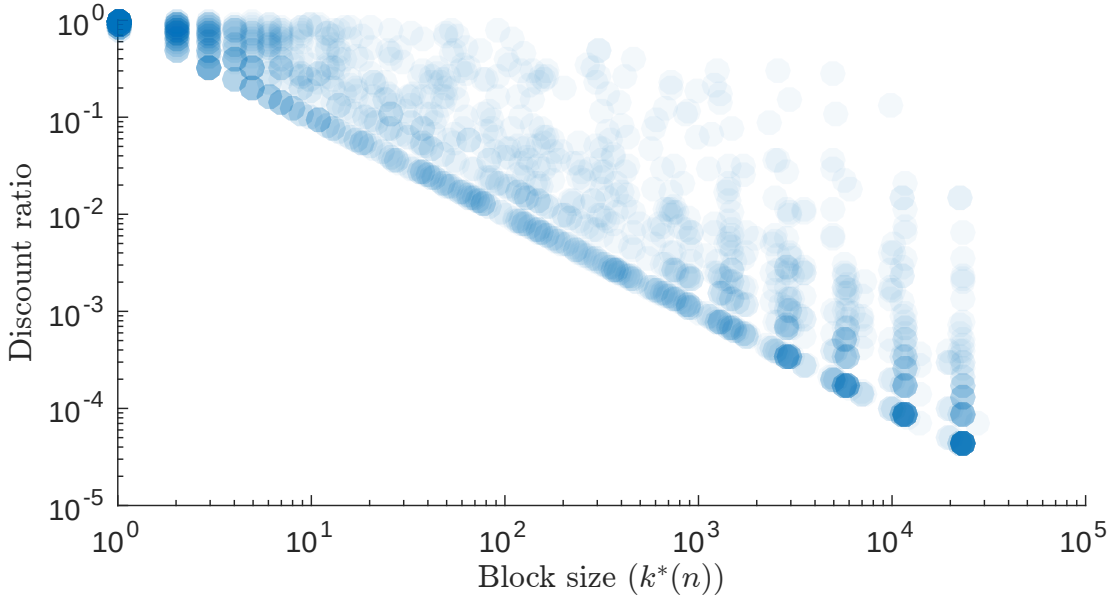
and from 1 to about 1,500 when $v(x) = x$ (recall that the total number of users ranges from 2^3 to 2^{17}).[15] Second, this difference in block sizes is the main reason why Δ_n^{max} is smaller in the Bitcoin log of sum distribution (larger block sizes imply smaller discount factors, as discussed also in Section 2). Third, the distribution of simulation points is not normal, and with outlier points. We do not have an explanation for this. The last two remarks apply to all the distributions we sampled.

5 The RSOP Mechanism

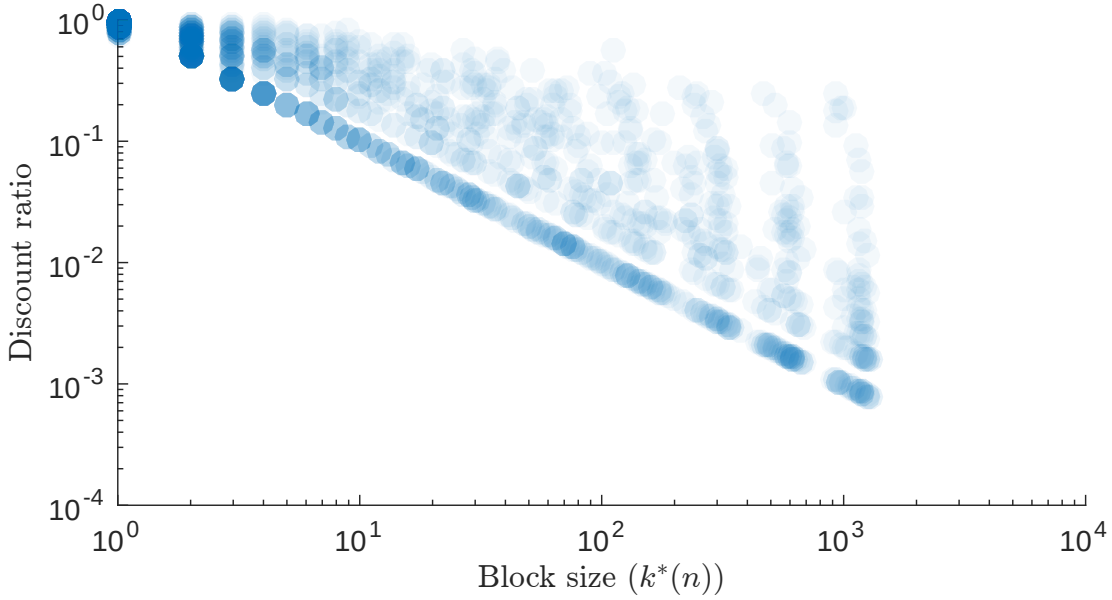
The monopolistic-price mechanism that was previously described is miner-honest in the sense that a myopic miner cannot increase her revenue by diverging from the suggested protocol (for example, add false bids or delete existing bids). However, as discussed above, even impatient users can sometimes benefit from submitting a strategic bid which is different than their true maximum willingness to pay.

In this section we discuss an alternative approach in which we use a well-known auction which is truthful for impatient users. That is, an impatient user will maximize her gain by simply submitting her maximal willingness to pay. On the other hand, in this second mechanism the challenge is to show that miners will be honest and will not manipulate the protocol, as we further discuss below. In particular, we will show empirical evidence

[15] This clearly impacts the throughput of the suggested protocol: it will be about $0.1n$ (where n is the number of all bidders) when $v(x) = \log x$ and about $0.01n$ when $v(x) = x$.



(a)



(b)

Figure 6: A scatter plot of all simulation points for the Bitcoin distribution with (a) $v(x) = \log x$ and (b) $v(x) = x$.

suggesting that the profit for the miners from such manipulations becomes negligible as the number of users increases.

More specifically, our second suggested mechanism uses the following RSOP (Random Sampling Optimal Price) auction, defined by [GHK+06]. In the definition, the following notation is used: For a subset $A \subseteq [n]$ of users, and a bid vector $\boldsymbol{b}$, let $\boldsymbol{b}_A = (b_i)_{i \in A}$. We define $p_A^{monopolistic}(\boldsymbol{b}) \equiv p^{monopolistic}(\boldsymbol{b}_A)$. When $\boldsymbol{b}$ is clear from the context, we simply write $p_A^{monopolistic}$.

Definition 5.1 (The RSOP auction [GHK+06])**.** Upon receiving n bids, $\boldsymbol{b} = b_1, ..., b_n$, the auctioneer performs the following:

1. Randomly partition the bids to two disjoint sets A and B (each bid is placed in A with probability $\frac{1}{2}$, otherwise it is placed in B).

2. Compute the monopolistic price for each set: $p_A^{monopolistic}, p_B^{monopolistic}$. The monopolistic price of an empty set is defined to be zero.

3. The set of winning bids is $A' \cup B'$, where:

$$A' = \{i \in A : b_i \geq p_B^{monopolistic}\} \quad ; \quad B' = \{i \in B : b_i \geq p_A^{monopolistic}\}.$$

   The bidders in A' each pay $p_B^{monopolistic}$, and the bidders in B' pay $p_A^{monopolistic}$ each. The revenue obtained in the auction is therefore

$$RSOP(\boldsymbol{b}) = |A'| \cdot p_B^{monopolistic} + |B'| \cdot p_A^{monopolistic}.$$

For the RSOP mechanism, Goldberg *et al.*provide the following results that hold under "the usual" auction theory assumptions, most notably that: (1) the auctioneer is honest; (2) bidders do not collude; (3) each bidder can submit exactly one bid; (4) bidders are impatient, i.e. they do not obtain utility from winning in future auctions (we discuss these assumptions further below).

Theorem 5.2 ([GHK+06], Observation 6.2 and Theorem 6.4)**.**

1. *Truthfulness.* The RSOP auction is truthful, i.e., a bidder maximizes her utility by reporting her true maximal willingness to pay, even when the other bidders do not reveal their true maximal willingness to pay.

2. *Maximal Revenue.* Fix any parameter h. Let $\boldsymbol{b}$ be any bid vector of n bids with $b_i \in [1, h]$ for all i. Then

$$\lim_{n \to \infty} \max_{\boldsymbol{b}} \frac{R(\boldsymbol{b})}{RSOP(\boldsymbol{b})} = 1.$$

To instantiate the RSOP-based mechanism, users must specify their maximal willingness to pay for the transactions, and the miners are asked to create a block with all transactions they wish to *potentially* include. Unlike the current Bitcoin protocol, here not all transactions in a block are valid. After the block is mined, and propagated to the Bitcoin nodes in the network, they determine which transactions are valid, by running Algorithm 1.

Algorithm 1 RSOP block verification

1: A node receives a new block B.
2: Check validity of the block and of all the included transactions according to Bitcoin's current rules. When referring to transactions in previous blocks, consider only valid transactions (as explained below).
3: Compute the sets A and B using the block hash as a seed to a Cryptographically Secure Pseudo-Random Number Generator (CSPRNG).
4: The transactions that are considered valid are the ones in A' and B' as in Def. 5.1.
5: Transactions in A' pay $p_B^{monopolistic}$ and transactions in B' pay $p_A^{monopolistic}$ as a fee. A fraction $1-\alpha$ of that revenue goes to the miner who mined the current block, and the rest goes to the future miner who would mine the next valid block. Invalid transactions do not pay anything. The parameter $0 \leq \alpha \leq 1$ needs to be specified as part of the protocol.

The algorithm has the following advantages. Since the source of the randomness (block hash) used in line 3 is the same for all the Bitcoin nodes, all nodes will reach consensus on the set of valid transactions. Notice that the block hash is determined by its contents including the solution to a proof-of-work puzzle. A miner cannot easily manipulate the choice of the sets A and B to maximize revenue[16] (if she could, it could destroy the truthfulness of the protocol). She *can* choose to forgo a block in which A and B were not set to her liking but will need to generate the proof-of-work from scratch, which is extremely costly. There are however several concerns with the proposed algorithm:

User truthfulness. The assumption that users cannot send multiple bids is unrealistic in the Bitcoin setting. Therefore, we do not know whether the suggested protocol is truthful even for impatient users and honest miners. Under the assumption that the user cannot control which bids will be associated with subset A and which with subset B, we do not know how to construct even tailored worst-case examples or if there exists an efficient algorithm to find beneficial deviations.[17]

Auctioneer honesty: adding false bids. Miners are able to manipulate the protocol by adding false bids, especially if $\alpha = 0$. The purpose of choosing $\alpha > 0$ is to eliminate this problem. The following example demonstrates this issue:

[16] A more careful cryptographic analysis is required to establish this statement, but is outside the scope of this work. This statement is fairly simple to show in the random oracle model.

[17] We discuss this type of manipulation in the other protocol, see the discussion in Sections 2.2, 3.1 and 4.

Example 5.3. Suppose $\alpha = 0$. There are two users with maximal willingness $b_1 = h,\ b_2 = \ell$ where $h > 2\ell$. With probability $\frac{1}{2}$ both users will fall to the same set, and the revenue for the miner would be 0. If they fall into different sets, only the h user will be included, and will pay ℓ. Therefore, the expected revenue is $\frac{\ell}{2}$. A strategic miner can create many false bids with a maximal willingness to pay h, by this receiving a revenue of approximately h, which is the true bid of the high bidder. The false bids clearly cannot create a profit for the miner but also do not harm the miner because the miner pays them to herself.

As α increases, the profitability of the strategy in the example decreases. More generally, a dishonest auctioneer can always use the following simple strategy to increase revenue: (1) Compute the monopolistic price over all bids; (2) Add many false bids with a fee which is equal to the monopolistic price. Adding sufficiently many false bids will change the RSOP revenue to that of the monopolistic price mechanism. We conjecture that this strategy is always beneficial to the miner:

Conjecture 5.4. For every $\boldsymbol{b}$ and all choices of A and B, the RSOP revenue is at most the monopolistic revenue. In particular, $RSOP(\boldsymbol{b}) \leq R(\boldsymbol{b})$.

The right hand side ($R(\boldsymbol{b})$) is the revenue a manipulating miner can obtain with the strategy above, and the left hand side is the RSOP revenue, for *any* allocation of the sets A,B (even one chosen adversarially)

In the empirical evaluation reported below, we have never encountered a counterexample to this conjecture. To measure the expected "gain ratio" from performing this strategy, we define

$$\Delta_n^{RSOP} = \mathbb{E}_{(v_1,\ldots,v_n)\sim F}\left[\frac{R(\boldsymbol{v})}{RSOP(\boldsymbol{v})} - 1\right].$$

For distributions with bounded support sizes Theorem 5.2 proves that Δ_n^{RSOP} goes to zero as n goes to infinity. Furthermore, Figure 7 demonstrates that this indeed happens in a reasonably fast manner for almost all the distributions we considered in Section 4, with the only exception being the inverse distribution. To summarize this issue:

- In the RSOP mechanism the miner can gain from adding false bids with a fee equal to the monopolistic price. This is an easy strategy to perform, and as far as we can tell, it never harms the miner when $\alpha = 0$. If the miner does so, the mechanism changes and becomes similar to the monopolistic-price mechanism. This, in turn, may harm the bidder-truthfulness property.

- However, the gain ratio from performing this strategy decreases as the number of users increases.

- Furthermore, we conjecture that, for many bid distributions and when the number of users is fairly large, it is possible to set $\alpha > 0$ in a way that will eliminate the profitability of this strategy. Note that if $\alpha > 0$, the miner needs to pay some of her false bids to other miners.

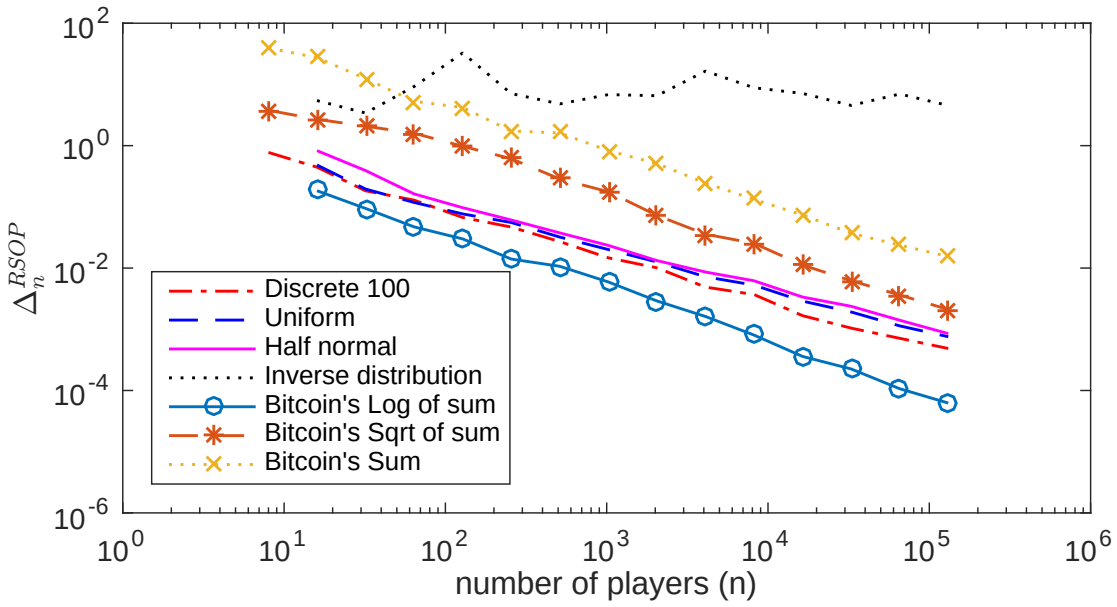


Figure 7

- On the other hand, setting $\alpha > 0$, and especially high values (say, $\alpha = 0.9$), introduces risks of side-payments. A miner may provide the following service. She asks users to submit transactions with 0 fee, and pay directly to the miner a fixed per transaction fee. The miner will guarantee that she will eventually include these transactions in a block which contain only other 0 fee transactions (which will then all be valid). In such a case the miner gets all the revenue for herself, whereas if she follows the protocol she will only receive a factor of $1 - \alpha$ of the fee. If α is low, this is less likely to happen, as this requires non-trivial coordination between the miner and the user (e.g., trust regarding the transfer of payments, regarding inclusion in the block, etc).

Auctioneer honesty: removing true bids. The auctioneer might also be able to increase her profit by removing true bids. The following example demonstrates this:

Example 5.5. There are n bids with value 2 and n bids with value 1. The auctioneer can obtain a revenue of $2n$ w.h.p. by removing all bids of value 1. The expected revenue for the honest miner is always at most $2n$, and in the limit of large n, the revenue is $2n - \frac{2^{3/4}\sqrt{n}}{\sqrt{\pi}} + o(\sqrt{n})$, see Appendix C Cor. C.2.

Note that the maximal revenue that can be obtained in this example by removing bids is exactly the monopolistic revenue. We do not know if this is true in general, however we strongly suspect that this is the case. More specifically, we conjecture:

Conjecture 5.6. For any vector of bids $\boldsymbol{b}$, $\max_{\boldsymbol{b}' \subseteq \boldsymbol{b}} RSOP(\boldsymbol{b}') \leq R(\boldsymbol{b})$.

In fact, Conjectures 5.4 and 5.6 are equivalent: by choosing $\boldsymbol{b}' = \boldsymbol{b}$, Conjecture 5.6 implies 5.4. To show the other direction, Conjecture 5.4 implies that $RSOP(\boldsymbol{b}') \leq R(\boldsymbol{b}')$ and by the monotonicity of $R(\cdot)$, we reach $RSOP(\boldsymbol{b}') \leq R(\boldsymbol{b}') \leq R(\boldsymbol{b})$, as required.

Note that under this conjecture, the gain ratio Δ_n^{RSOP} goes to zero for any distribution with finite support even if the miner can remove true bids, using Theorem 5.2. Note that this form of the conjecture is harder to verify empirically as it requires considering different subsets for removal. But the equivalence to Conjecture 5.4, and the empirical evaluation performed above provides some supporting evidence for it.

We do not know an efficient algorithm to find the best bids to remove, and therefore the strategy for the miner is left open. We do not have any suggestions regarding how to mitigate this case. Unlike the previous case (adding false bids) α is irrelevant to this strategy by the miner. Perhaps it can be shown that removing true bids rarely beneficial, under some distributional assumptions.

Block size. Notice that in the RSOP mechanisms blocks may contain many transactions that do not get accepted (their bid may be below the price that is eventually determined). One possible way to prevent this is to commit to all transactions in the Merkle tree in some canonical order of bid size and then eventually only reveal transactions that are needed to establish the monopolistic price and transactions that win this bid. While we do not have a fully fleshed out scheme, we do believe that clever use of data structures and cryptographic schemes may help in reducing the amount of wasted space in blocks in this way.

6 Discussion

In this paper we have proposed an auction based framework to redesign Bitcoin's fee market. Our conceptual framework proposes to use an auction in order to determine which transactions are included in each block. We have proposed and analyzed two such auctions, our primary candidate from these two is the monopolistic price auction. We have shown that it satisfies several important properties: it is auctioneer-truthful, it maximizes the revenue of the auctioneer under the maximal block size constraint, and, while, it is not bidder-truthful, we have shown via theoretical analysis as well as an empirical evaluation that the incentives of the impatient users to shade their bids decreases to zero as the number of transactions increase. By redesigning Bitcoin's fee market in this way, we propose a way to decouple the issue of miners' revenues from the block-size debate.

One restriction of our analysis is our assumption of impatient users, which care only about the next block. We believe that it is important to tackle this restriction in future work, either theoretically or empirically. For example, it will be interesting to analyze, via simulations, the possible gain for patient users, and the way that the distribution of bids changes if rejected bids stay in the system and continue to participate in subsequent blocks.

Different types of off-chain transaction channels are currently under development (see, e.g. [PD15, DW15]) and might radically change the transaction fee market. Several aspects of the demand for blockchain transactions would be affected: the level of patience of users for transactions that set up payment channels, the willingness to pay fees, and the basic demand for transacting on-chain may differ from the pre-lightning fee market. An interesting direction for future work is hence to explore the interaction of auction based mechanisms for on-chain transactions with off-chain channels.

As was mentioned, computational power invested in computing buys security for the network. But, how much security should be achieved? Perhaps the network spends too much on its security.

7 Acknowledgments

We thank Alaa Mozalbat, who designed and implemented the simulations code, and Reshef Meir for valuable discussions. Ron Lavi was partly supported by a Marie-Curie fellowship "Advance-AGT", and by an ARCHES award from the MINERVA foundation. Or Sattath is supported by ERC Grant 280157. Aviv Zohar is supported by the Israel Science Foundation (grant 616/13) and by a grant from the HUJI Cyber Security Research Center in conjunction with the Israel National Cyber Bureau (grant 039-9230).

References

[BDOZ12] M. Babaioff, S. Dobzinski, S. Oren, and A. Zohar. On Bitcoin and red balloons. In *ACM Conference on Electronic Commerce, EC '12, Valencia, Spain, June 4-8, 2012*, pages 56–73, 2012.

[Bon16] J. Bonneau. Why Buy When You Can Rent? - Bribery Attacks on Bitcoin-Style Consensus. In *Financial Cryptography and Data Security - FC 2016 International Workshops, BITCOIN, VOTING, and WAHC, Christ Church, Barbados, February 26, 2016, Revised Selected Papers*, pages 19–26, 2016.

[CKWN16] M. Carlsten, H. A. Kalodner, S. M. Weinberg, and A. Narayanan. On the Instability of Bitcoin Without the Block Reward. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*, pages 154–167, 2016.

[DW13] C. Decker and R. Wattenhofer. Information propagation in the Bitcoin network. In *13th IEEE International Conference on Peer-to-Peer Computing, IEEE P2P 2013, Trento, Italy, September 9-11, 2013, Proceedings*, pages 1–10, 2013.

[DW15] C. Decker and R. Wattenhofer. A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels. In *Stabilization, Safety, and Security of Distributed Systems - 17th International Symposium, SSS 2015, Edmonton, AB, Canada, August 18-21, 2015, Proceedings*, pages 3–18, 2015.

[GHK+06] A. V. Goldberg, J. D. Hartline, A. R. Karlin, M. E. Saks, and A. Wright. Competitive auctions. *Games and Economic Behavior*, 55(2):242–269, 2006.

[HLM17] G. Huberman, J. D. Leshno, and C. C. Moallemi. Monopoly without a monopolist: An economic analysis of the bitcoin payment system. `https://ssrn.com/abstract=3025604`, 2017.

[KDF13] J. A. Kroll, I. C. Davey, and E. W. Felten. The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In *Proceedings of WEIS*, volume 2013, 2013.

[Nak08] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.

[PD15] J. Poon and T. Dryja. The Bitcoin lightning network: Scalable off-chain instant payments, 2015.

[Riz15] P. R. Rizun. A Transaction Fee Market Exists Without a Block Size Limit. 2015.

[SZ15] Y. Sompolinsky and A. Zohar. Secure High-Rate Transaction Processing in Bitcoin. In *Financial Cryptography and Data Security - 19th International Conference, FC 2015, San Juan, Puerto Rico, January 26-30, 2015, Revised Selected Papers*, pages 507–527, 2015.

A Properties of p^{honest}, $p^{strategic}$, and δ

Recall that $\text{num}(\boldsymbol{v}, z) \equiv |\{v_i | v_i \geq z\}|$.

Claim A.1. If $p^{monopolistic}(\boldsymbol{v}_{-i}) \leq v_i$, then $p^{monopolistic}(\boldsymbol{v}_{-i}) \leq p^{monopolistic}(\boldsymbol{v})$. Furthermore, if $p^{monopolistic}(\boldsymbol{v}_{-i}) = v_i$, then $p^{monopolistic}(\boldsymbol{v}_{-i}) = p^{monopolistic}(\boldsymbol{v})$.

Proof Let $x = p^{monopolistic}(\boldsymbol{v}_{-i})$ and $y = p^{monopolistic}(\boldsymbol{v})$. Assume by contradiction that $x > y$. By definition of the monopolistic price for $\boldsymbol{v}_{-i}$, $x \cdot \text{num}(\boldsymbol{v}_{-i}, x) > y \cdot \text{num}(\boldsymbol{v}_{-i}, y)$. Since $v_i \geq x > y$, $\text{num}(\boldsymbol{v}, x) = \text{num}(\boldsymbol{v}_{-i}, x) + 1$ and $\text{num}(\boldsymbol{v}, y) = \text{num}(\boldsymbol{v}_{-i}, y) + 1$. Thus, $x \cdot \text{num}(\boldsymbol{v}, x) > y \cdot \text{num}(\boldsymbol{v}, y) - y + x > y \cdot \text{num}(\boldsymbol{v}, y)$, contradicting $y = p^{monopolistic}(\boldsymbol{v})$. □

Claim A.2. For any $\boldsymbol{v}$ and any i, $p^{strategic}(\boldsymbol{v}_{-i}) < p^{monopolistic}(\boldsymbol{v}_{-i})$.

Proof Let $k^* = k^*(\boldsymbol{v}_{-i})$, and $b^* = \frac{k^*}{k^*+1} p^{monopolistic}(\boldsymbol{v}_{-i})$. Suppose by contradiction that $p^{monopolistic}(b^*, \boldsymbol{v}_{-i}) > b^*$. This would imply that $p^{monopolistic}(b^*, \boldsymbol{v}_{-i}) = p^{monopolistic}(\boldsymbol{v}_{-i})$. But this is a contradiction since $\text{num}((b^*, v_{-i}), b^*) \cdot b^* \geq (k^* + 1) \cdot b^* = k^* \cdot p^{monopolistic}(\boldsymbol{v}_{-i})$. Thus, $p^{monopolistic}(b^*, \boldsymbol{v}_{-i}) \leq b^*$. Since $p^{strategic}(\boldsymbol{v}_{-i}) = \min_b p^{monopolistic}(b, \boldsymbol{v}_{-i}) \leq p^{monopolistic}(b^*, \boldsymbol{v}_{-i})$, the claim follows. □

Corollary A.3. Fix $v_1, ..., v_n$ and let $i^* = \text{argmax}_{i=1,...,n} v_i$. Then,

$$p^{strategic}(\boldsymbol{v}_{-i*}) < p^{monopolistic}(\boldsymbol{v}_{-i*}) \leq p^{monopolistic}(\boldsymbol{v}).$$

This is an immediate consequence of Claims A.2 and A.1.

Claim A.4. For any $\boldsymbol{v}$ and any i, let $x = p^{monopolistic}(\boldsymbol{v})$. Then, $p^{monopolistic}(x, \boldsymbol{v}_{-i}) \leq x$

Proof Suppose towards a contradiction that $y = p^{monopolistic}(x, \boldsymbol{v}_{-i}) > x$. Therefore $y \cdot \text{num}((x, \boldsymbol{v}_{-i}), y) > x \cdot \text{num}((x, \boldsymbol{v}_{-i}), x)$. Note that $\text{num}(\boldsymbol{v}, y) \geq \text{num}((x, \boldsymbol{v}_{-i}), y)$ and $\text{num}(\boldsymbol{v}, x) \leq \text{num}((x, \boldsymbol{v}_{-i}), x)$. This implies $y \cdot \text{num}(\boldsymbol{v}, y) \geq y \cdot \text{num}((x, \boldsymbol{v}_{-i}), y) > x \cdot \text{num}((x, \boldsymbol{v}_{-i}), x) \geq x \cdot \text{num}(\boldsymbol{v}, x)$. Therefore $y \cdot \text{num}(\boldsymbol{v}, y) > x \cdot \text{num}(\boldsymbol{v}, x)$ which contradicts the fact that $x = p^{monopolistic}(\boldsymbol{v})$. □

Claim A.5. For any $\boldsymbol{v}$ and any i, $p^{monopolistic}(p^{strategic}(\boldsymbol{v}_{-i}), \boldsymbol{v}_{-i}) = p^{strategic}(\boldsymbol{v}_{-i})$.

Proof Recall the definition, $p^{strategic}(\boldsymbol{v}_{-i}) \equiv \min\{b \mid p^{monopolistic}(b, \boldsymbol{v}_{-i}) \leq b\}$. It immediately follows that $p^{monopolistic}(p^{strategic}(\boldsymbol{v}_{-i}), \boldsymbol{v}_{-i}) \leq p^{strategic}(\boldsymbol{v}_{-i})$. Assume towards a contradiction that the inequality is strict, and let $x = p^{monopolistic}(p^{strategic}(\boldsymbol{v}_{-i}), \boldsymbol{v}_{-i})$. But then Claim A.4 implies that $p^{monopolistic}(x, \boldsymbol{v}_{-i}) \leq x$, which is a contradiction since $p^{strategic}(\boldsymbol{v}_{-i})$ is supposed to be the minimal such x. □

Claim A.6. Fix any $\boldsymbol{v}$, let $i^* = \text{argmax}_{i=1,\ldots,n} v_i$, $k^* = k^*(\boldsymbol{v}_{-i^*})$, $x = p^{honest}(\boldsymbol{v})$ and let y be the smallest element in the support of F which is at least $p^{strategic}(\boldsymbol{v}_{-i^*})$. Then, $x = y$ implies that $p^{strategic}(\boldsymbol{v}_{-i^*}) \geq \frac{k^*}{k^*+1} \cdot p^{honest}(\boldsymbol{v})$.

Proof By Corollary A.3,

$$p^{strategic}(\boldsymbol{v}_{-i^*}) < p^{monopolistic}(\boldsymbol{v}_{-i^*}) \leq p^{monopolistic}(v_{i^*}, \boldsymbol{v}_{-i^*}) = p^{honest}(\boldsymbol{v}). \tag{A.1}$$

I.e., $y \leq p^{monopolistic}(\boldsymbol{v}_{-i^*}) \leq x$ (because $p^{monopolistic}(\boldsymbol{v}_{-i^*})$ is in the support of F). Thus, since $x = y$,

$$p^{monopolistic}(\boldsymbol{v}_{-i^*}) = x = p^{honest}(\boldsymbol{v}). \tag{A.2}$$

By definition of k^*, there exist k^* values in $\boldsymbol{v}_{-i^*}$ that are at least $p^{monopolistic}(\boldsymbol{v}_{-i^*})$. Overall,

$$\text{num}(\boldsymbol{v}_{-i^*}, p^{strategic}(\boldsymbol{v}_{-i^*})) = \text{num}(\boldsymbol{v}_{-i^*}, y) = \text{num}(\boldsymbol{v}_{-i^*}, x) = k^*. \tag{A.3}$$

Therefore, $R(p^{strategic}(\boldsymbol{v}_{-i^*}), \boldsymbol{v}_{-i^*}) = (k^*+1)p^{strategic}(\boldsymbol{v}_{-i^*})$: this follows from Claim A.5, and Eq. (A.3). Thus, for any number $z > p^{strategic}(\boldsymbol{v}_{-i^*})$, $(k^*+1)p^{strategic}(\boldsymbol{v}_{-i^*}) \geq z \cdot \text{num}(\boldsymbol{v}_{-i^*}, z)$ (since $z > p^{strategic}(\boldsymbol{v}_{-i^*})$, the number of bids in $(p^{strategic}(\boldsymbol{v}^*_{-i}), v_{-i^*})$ that are at least z is exactly $\text{num}(\boldsymbol{v}_{-i^*}, z)$).

Taking $z = p^{honest}(\boldsymbol{v})$ (which satisfies $z > p^{strategic}(\boldsymbol{v}_{-i^*})$ by Eq.(A.1)), $\text{num}(\boldsymbol{v}_{-i^*}, p^{honest}(\boldsymbol{v})) = k^*$ (where here we used Eq. (A.2)). It follows that $x = y$ implies that $(k^*+1)p^{strategic}(\boldsymbol{v}_{-i^*}) \geq k^* \cdot p^{honest}(\boldsymbol{v})$, and the claim follows. □

Claim A.7. For any $\boldsymbol{v} = (v_1, ..., v_n)$, and any v'_i such that $v_i \geq v'_i \geq p^{monopolistic}(\boldsymbol{v})$, $p^{monopolistic}(\boldsymbol{v}) \geq p^{monopolistic}(v'_i, \boldsymbol{v}_{-i})$.

We remark that $p^{monopolistic}(\boldsymbol{v})$ is not necessarily monotonically increasing as a function of v_i, for example, $p^{monopolistic}(2, 0) = 2 > 1 = p^{monopolistic}(2, 1)$. Hence, the importance of the condition $v'_i \geq p^{monopolistic}(\boldsymbol{v})$.

Proof Denote $x = p^{monopolistic}(\boldsymbol{v})$ and $y = p^{monopolistic}(v_i', \boldsymbol{v}_{-i})$. Assume towards a contradiction that $x < y$. Therefore

$$y \cdot \text{num}(\boldsymbol{v}, y) \geq y \cdot \text{num}((v_i', \boldsymbol{v}_{-i}), y) > x \cdot \text{num}((v_i', \boldsymbol{v}_{-i}), x) = x \cdot \text{num}(\boldsymbol{v}, x)$$

where the first step follows since $v_i \geq v_i'$, the second step follows since y is the monopolistic price for $(v_i', \boldsymbol{v}_{-i})$ (the inequality is strict because $y > x$), and the third step follows since $v_i \geq v_i' \geq x$. However $y \cdot \text{num}(\boldsymbol{v}, y) > x \cdot \text{num}(\boldsymbol{v}, x)$ contradicts the fact that x is the monopolistic price for v. □

Claim A.8. For any $v_1, ..., v_n$ and i, j, $v_i > v_j \geq p^{strategic}(\boldsymbol{v}_{-j})$ implies that $p^{strategic}(\boldsymbol{v}_{-j}) \geq p^{strategic}(\boldsymbol{v}_{-i})$.

We remark that the condition $v_j \geq p^{strategic}(\boldsymbol{v}_{-j})$ is important as without it the claim is not true. For example, take $\boldsymbol{v} = (2, 1, 0)$:

$$p^{srategic}(\boldsymbol{v}_{-2}) = p^{srategic}(2, 0) = 1 > \frac{2}{3} = p^{strategic}(2, 1) = p^{strategic}(\boldsymbol{v}_{-3}).$$

Proof Let $b = p^{strategic}(\boldsymbol{v}_{-j})$. We will prove that $b \geq p^{monopolistic}(b, v_{-i})$, which implies the claim since $p^{strategic}(\boldsymbol{v}_{-i}) \equiv \min\{b \mid b \geq p^{monopolistic}(b, v_{-i})\}$.

By applying Claim A.7 with respect to $\boldsymbol{u} = (v_1, \ldots, v_{j-1}, b, v_{j+1}, \ldots, v_n)$ and $u' = (v_1, \ldots, v_{i-1}, v_j, v_{i+1}, \ldots, v_{j-1}, b, v_{j+1}, \ldots, v_n)$ implies that $p^{monopolistic}(\boldsymbol{u}) \geq p^{monopolistic}(\boldsymbol{u}')$ (note that $v_i \geq v_j \geq b \geq p^{monopolistic}(b, \boldsymbol{v}_{-j})$ where the last inequality follows from the definition of $p^{strategic}()\boldsymbol{v}_{-j})$; therefore $u_i \geq u_i' \geq p^{monopolistic}(\boldsymbol{u})$). Thus

$$b \geq p^{monopolistic}(\boldsymbol{u}) \geq p^{monopolistic}(\boldsymbol{u}') = p^{monopolistic}(b, v_{-i})$$

and the claim follows. □

Claim A.9. For any $v_1, ..., v_n$ and i, j, $v_i \geq v_j$ implies $\delta_i(v_i, \boldsymbol{v}_{-i}) \geq \delta_j(v_j, \boldsymbol{v}_{-j})$.

Proof If $v_j < p^{strategic}(v_{-j})$, $\delta_j(v_j, \boldsymbol{v}_{-j}) = 0$ and the claim follows. Thus assume $v_j \geq p^{strategic}(\boldsymbol{v}_{-j})$, and we have $v_i > v_j \geq p^{strategic}(\boldsymbol{v}_{-j}) \geq p_i^{strategic}(\boldsymbol{v}_{-i})$ where the last inequality follows from Claim A.8. Since p^{honest} is the same in both terms, and $p^{strategic}(v_{-j}) \geq p^{strategic}(v_{-i})$, we have $\delta_i(v_i, v_{-i}) \geq \delta_j(v_j, v_{-j})$. □

Claim A.10. For any $\boldsymbol{b}_{-i}$ and $u \in \mathbb{N}^+$, define[18]

$$p_u^{multibid}(\boldsymbol{b}_{-i}) = \min\{u \cdot b_i \mid b_i \in \mathbb{R},\ b_i \geq p^{monopolistic}(\overbrace{b_i, \ldots, b_i}^{\text{u times}}, \boldsymbol{b}_{-i})\}.$$

Then, for any $u \geq n + 1$, $p_u^{multibid}(\boldsymbol{b}_{-i}) > p_1^{multibid}(\boldsymbol{b}_{-i})$.

[18]The minimum is well defined – see the argument next to Eq. (2.6).

Proof Let $b = \frac{p_u^{multibid}(\boldsymbol{b}_{-i})}{u}$. Then, $b \cdot (u + \text{num}(\boldsymbol{b}_{-i}, b) \geq k^*(\boldsymbol{b}_{-i}) \cdot p^{monopolistic}(\boldsymbol{b}_{-i})$. Therefore,

$$p_u^{multibid}(\boldsymbol{b}_{-i}) = b \cdot u \geq \frac{k^*(\boldsymbol{b}_{-i}) \cdot p^{monopolistic}(\boldsymbol{b}_{-i})}{u + \text{num}(\boldsymbol{b}_{-i}, b)} \cdot u \tag{A.4}$$

If $k^*(\boldsymbol{b}_{-i}) \geq 2$ then $\frac{u}{u+\text{num}(\boldsymbol{b}_{-i},b)} \cdot k^*(\boldsymbol{b}_{-i}) > 1$ since $u > n > \text{num}(\boldsymbol{b}_{-i}, b)$. Therefore Eq. (A.4) implies that $p_u^{multibid}(\boldsymbol{b}_{-i}) > p^{monopolistic}(\boldsymbol{b}_{-i}) > p^{strategic}(\boldsymbol{b}_{-i}) = p_1^{multibid}(\boldsymbol{b}_{-i})$, implying the claim.

If $k^*(\boldsymbol{b}_{-i}) = 1$ then $\frac{u}{u+\text{num}(\boldsymbol{b}_{-i},b)} \cdot k^*(\boldsymbol{b}_{-i}) > \frac{1}{2}$. Therefore Eq. (A.4) implies that $p_u^{multibid}(\boldsymbol{b}_{-i}) > \frac{p^{monopolistic}(\boldsymbol{b}_{-i})}{2} \geq p^{strategic}(\boldsymbol{b}_{-i}) = p_1^{multibid}(\boldsymbol{b}_{-i})$, implying the claim. (Here, in the second inequality we used the fact that $k^*(\boldsymbol{b}_{-i}) = 1$, and bidding half of the highest bid will win in this case.) □

Claim A.11. Fix any $\boldsymbol{b}_{-i}$ and let b, u be the arguments which minimize Eq. (2.6). Then,

$$b = p^{monopolistic}(\overbrace{b, \ldots, b}^{\text{u times}}, \boldsymbol{b}_{-i}).$$

Proof By definition $b \geq p^{monopolistic}(\overbrace{b, \ldots, b}^{\text{u times}}, \boldsymbol{b}_{-i})$. Suppose towards a contradiction that the inequality is strict, and take some b' such that

$$b > b' \geq p^{monopolistic}(\overbrace{b, \ldots, b}^{\text{u times}}, \boldsymbol{b}_{-i}).$$

Claim A.7 implies that

$$b' \geq p^{monopolistic}(\overbrace{b', \ldots, b'}^{\text{u times}}, \boldsymbol{b}_{-i}),$$

contradicting the minimality of (b, u) since $b \cdot u > b' \cdot u$. □

Claim A.12. Fix any $\boldsymbol{b}_{-i}$ and let (b, u) be the arguments which minimize Eq. (2.6). Then,

$$b \leq p^{monopolistic}(\boldsymbol{b}_{-i}).$$

Proof Let $b' = p^{monopolistic}(\boldsymbol{b}_{-i})$. Then, the second part of Claim A.1 implies that $b' = p^{monopolistic}(b', \boldsymbol{b}_{-i})$. Thus $(b', u' = 1)$ satisfies the requirement of Eq. (2.6). Hence $b \cdot u \leq b'$ and the claim follows. □

Claim A.13. Fix any $\boldsymbol{b}_{-i}$ and any $b_i < p^{monopolistic}(b_i, \boldsymbol{b}_{-i})$. Then there exists $\delta > 0$ such that for any $0 < \epsilon < \delta$, $p^{monopolistic}(b_i + \epsilon, \boldsymbol{b}_{-i}) = p^{monopolistic}(b, \boldsymbol{b}_{-i})$.

Proof Let $\boldsymbol{v} = (b_i, \boldsymbol{b}_{-i})$ and assume w.l.o.g. that v is ordered, i.e., $v_1 \geq v_2 \geq ... \geq v_n$. Let k be such that $v_k = p^{monopolistic}(\boldsymbol{v})$. Let j be the minimal index of bid b_i in $\boldsymbol{v}$, i.e., $v_{j-1} > v_j = b_i$. Note that $j > k$ since $v_j < v_k$ by assumption. Also note that $v_j \cdot j < v_k \cdot k$ since the monopolistic price is v_k. Choose $\delta > 0$ such that $v_j + \delta < v_{j-1}$ and $(v_j + \delta) \cdot j < v_k \cdot k$. By definition, for any $0 < \epsilon < \delta$, $p^{monopolistic}(v_j + \epsilon), \boldsymbol{v}_{-j}) = p^{monopolistic}(\boldsymbol{v})$, and the claim follows. □

B A few mathematical facts

Claim B.1. Let $f : \Re_{\geq 0} \to \Re_{\geq 0}$ be any function that satisfies the following property: If $x < f(x)$ there exists $\delta > 0$ such that for any $0 < \epsilon < \delta$, $f(x + \epsilon) = f(x)$. Let $A = \{x \in \Re_{\geq 0} \mid x \geq f(x)\}$. Then, if A is not empty, $\inf A \in A$.

Proof Note that if A is not empty than the infimum of A is well defined since A is bounded from below by 0. Let $x^* = \inf A$. Assume towards a contradiction that $x^* \notin A$, i.e., $x^* < f(x^*)$. Thus, by the property of f, there exists $\epsilon > 0$ such that $x^* + \epsilon < f(x^*)$ and $f(x) = f(x^*)$ for every $x^* < x < x^* + \epsilon$. Since $x^* = \inf A$ there exists $x \in A$, $x^* < x < x^* + \epsilon$. For this x, $f(x) \leq x < x^* + \epsilon < f(x^*) = f(x)$, a contradiction. □

Claim B.2. Let $X \sim B(n, p)$ be a binomial random variable. For every i, $\Pr(X = i) = O\left(\frac{1}{\sqrt{n}}\right)$.

Proof If np is an integer, the mode (most likely value of the distribution) is its mean np.[19] The case where np is not an integer can be handled is a similar manner. Therefore, our goal is to show that $\Pr(X = np) = O\left(\frac{1}{\sqrt{n}}\right)$. By using Stirling's approximation,

$$\begin{aligned}\Pr(X = np) &= \binom{n}{np} p^{np}(1-p)^{n(1-p)} \\ &\approx \frac{1}{\sqrt{2\pi np(1-p)}} = O\left(\frac{1}{\sqrt{n}}\right).\end{aligned}$$

Of course, this is only valid when p is treated as a constant. □

Claim B.3. Let $(X_1, X_2, X_3) \sim Trinomial(n, p_1, p_2, p_3)$ be a triple of trinomial random variables where $p_1, p_2 > 0$. For every function f, $\Pr(X_1 = f(X_1 + X_2)) = O\left(\frac{1}{\sqrt{n}}\right)$.

Proof

$$\begin{aligned}\Pr(X_1 = f(X_1 + X_2)) &= \sum_{z=0}^{n} \Pr(X_1 = f(X_1 + X_2) | X_3 = z) \Pr(X_3 = z) \\ &= \sum_{z=0}^{n} \Pr(X_1 = f(n - z) | X_3 = z) \Pr(X_3 = z)\end{aligned}$$

Using Chernoff bound, and $p_3 < 1$ (since $p_1, p_2 > 0$ and $p_1 + p_2 + p_3 = 1$), for $\alpha = \frac{p_3+1}{2} < 1$, $\Pr(X_3 \geq \alpha n) = O(\frac{1}{\sqrt{n}})$. Conditioned that $X_3 = z$, X_1 has a Binomial distribution: $X_1 \sim B(n - z, \frac{p_1}{1-p_3})$ (here we use the condition $p_1,\ p_2 > 0$ to conclude that $0 < \frac{p_1}{1-p_3} < 1$). By

[19] This can be shown directly by computing $\frac{\Pr(X=i)}{\Pr(X=i+1)}$.

Claim B.2,

$$\begin{aligned}
\Pr(X_1 = f(X_1 + X_2)) &= \sum_{z=0}^{n} \Pr(X_1 = f(X_1 + X_2) | X_3 = z) \Pr(X_3 = z) \\
&\leq \sum_{z=0}^{\lfloor \alpha n \rfloor} \Pr(X_1 = f(n - z) | X_3 = z) \Pr(X_3 = z) + O\left(\frac{1}{\sqrt{n}}\right) \\
&\leq \sum_{z=0}^{\lfloor \alpha n \rfloor} O\left(\frac{1}{\sqrt{n - z}}\right) \Pr(X_3 = z) + O\left(\frac{1}{\sqrt{n}}\right) \\
&\leq \sum_{z=0}^{\lfloor \alpha n \rfloor} O\left(\frac{1}{\sqrt{(1-\alpha)n}}\right) \Pr(X_3 = z) + O\left(\frac{1}{\sqrt{n}}\right) = O\left(\frac{1}{\sqrt{n}}\right)
\end{aligned}$$

□

C Analysis of Example 5.5

Claim C.1.

$$\lim_{n \to \infty} \frac{RSOP(\overbrace{2, \ldots, 2}^{n \text{ times}}, \overbrace{1, \ldots, 1}^{n \text{ times}}) - 2n}{\sqrt{n}} = -\frac{2^{3/4}}{\sqrt{\pi}} \tag{C.1}$$

Proof Let X_i be the indicator variable whether the i'th 2-bidder is in group A, and similarly Y_i for the i'th 1-bidder. Let $Z_i = X_i - Y_i$. Let $X = \sum_{i=1}^{n} X_i$, $Y = \sum_{i=1}^{n} Y_i$ and $Z = \sum_{i=1}^{n} Z_i$.

Note that the revenue for any realization of the coin toss is exactly $2n - |Z|$. Suppose first that $Z \geq 0$, i.e., $X \geq Y$. In this case, the monopolistic price in A is 1 and the monopolistic price in B is 2. Thus, the revenue is $1 \cdot (X + Y) + 2 \cdot (n - X) = 2n - Z$. Similarly, if $Z < 0$, the revenue is $2n + Z$. This shows that in all cases, the revenue is $2n - |Z|$.

Since $\mathbb{E}[Z_i] = 0$ and $\mathrm{Var}(Z_i) = \frac{1}{2}$, by the central limit theorem, $\frac{1}{\sqrt{n}} Z$ converges in distribution to $N(0, \sigma^2 = \frac{1}{2})$ as n goes to infinity. Using the properties of the half-normal distribution, the expected value of $\frac{|Z|}{\sqrt{n}}$ is $\frac{2\sqrt{\sigma}}{\sqrt{\pi}} = \frac{2^{3/4}}{\sqrt{\pi}}$. This completes the proof, since $RSOP(\overbrace{2, \ldots, 2}^{n \text{ times}}, \overbrace{1, \ldots, 1}^{n \text{ times}}) = 2n - \mathbb{E}[|Z|]$. □

Corollary C.2. $RSOP(\overbrace{2, \ldots, 2}^{n \text{ times}}, \overbrace{1, \ldots, 1}^{n \text{ times}}) = 2n - \frac{2^{3/4}}{\sqrt{\pi}} \sqrt{n} + o(\sqrt{n})$.