Redesigning Bitcoin's fee market

Ron Lavi
Technion
Israel
ronlavi@technion.ac.il

Or Sattath
Ben-Gurion University of the Negev
Israel
sattath@post.bgu.ac.il

Aviv Zohar
The Hebrew University of Jerusalem
Israel
avivz@cs.huji.ac.il

ABSTRACT

The Bitcoin payment system involves two agent types: Users that transact with the currency and pay fees and miners in charge of authorizing transactions and securing the system in return for these fees. Two of Bitcoin's challenges are (i) securing sufficient miner revenues as block rewards decrease, and (ii) alleviating the throughput limitation due to a small maximal block size cap. These issues are strongly related as increasing the maximal block size may decrease revenue due to Bitcoin's pay-your-bid approach. To decouple them, we analyze the "monopolistic auction" [8], showing: (i) its revenue does not decrease as the maximal block size increases, (ii) it is resilient to an untrusted auctioneer (the miner), and (iii) simplicity for transaction issuers (bidders), as the average gain from strategic bid shading (relative to bidding one's true maximal willingness to pay) diminishes as the number of bids increases.

CCS CONCEPTS

• **Theory of computation → Algorithmic mechanism design**; **Exact and approximate computation of equilibria**; **Computational pricing and auctions**; • **Computer systems organization → Peer-to-peer architectures**.

KEYWORDS

Bitcoin; Cryptocurrency; Blockchain; Auction-Theory; Fee-market

ACM Reference Format:
Ron Lavi, Or Sattath, and Aviv Zohar. 2019. Redesigning Bitcoin's fee market. In *Proceedings of the 2019 World Wide Web Conference (WWW'19), May 13–17, 2019, San Francisco, CA, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3308558.3313454

1 INTRODUCTION

Bitcoin's security relies on its ability to attract honest miners and to incentivize them to invest large amounts of computational power [13]. This is done by rewarding miners for the creation of new blocks. The payment comprises a block reward that is a fixed amount per block, and a fee that each transaction pays for its inclusion in the block. Since the block reward is cut in half approximately every 4 years, transaction fees gradually become the miners' main incentive to participate. The decision on which transactions to include in the block is made using a "pay-your-bid" auction: each transaction submits its fee for its inclusion in the block. A miner, in turn, includes the highest bidding transactions that fit in the block. In this auction, larger block sizes imply smaller transaction fees, since all transactions will aim to pay the lowest possible fee for its inclusion in the block. The Bitcoin block size therefore significantly influences miners' revenue. Indeed, one of the main arguments against a block-size increase in Bitcoin has been that it may cause transaction fees to drop significantly. Thus, two of the Bitcoin system's main problems, i.e., obtaining sufficient revenue for the miners as the block reward gradually decreases and the throughput limitation as a result of the maximal block size, are in fact strongly related. This connection, however, is a major obstacle to their resolution. Our motivation in this paper is to decouple the issues of revenue and maximal block size (which should be determined according to other technical considerations, like block propagation times) and to provide scalability from the economic perspective of the fee market.

While most of auction theory assumes a trusted auctioneer that honestly follows the protocol, a miner (the auctioneer of the block) cannot be trusted. If adding fake bids can increase profit, a miner can add transactions by moving funds from one of its accounts to another. Similarly, a miner can ignore bids. An untrusted auctioneer can manipulate a 2^{nd} price auction, for example, by adding a fake bid that is very close to the highest bid. Bidders will realize that and shade down their bids. Though cryptography can, in general, help resolve some of these issues, as far as the authors are aware, cryptographic techniques are not applicable to Bitcoin: they assume a trusted setup, that the auctioneer is known in advance, or multiple communication rounds between all parties as in secure multi-party computation [1, 4, 12, 14].

We analyze here a potential solution to these issues, the *monopolistic auction* [8].[1] We observe that in the Bitcoin setting, the monopolistic auction is immune to untrusted auctioneers, on the one hand, and it decouples the revenue issue from the maximal block size issue, on the other. In this auction, given bids $b_1, ..., b_n$, the miner chooses which transactions to include in the block. All chosen transactions pay the same fee – the lowest bid in the block (as must be verified by the protocol). The maximal revenue resulting from this method cannot be increased by adding fake bids or by ignoring true bids. Other manipulations like side payments between miners and users are also not beneficial. In fact, we are not aware of any beneficial miner manipulation that can be exploited in the frame of this auction. Additionally and in contrast to a pay-your-bid auction, increasing the maximal block size does not decrease the revenue of the monopolistic auction. Choosing a threshold price is conceptually similar to dynamically choosing the block size – the miner chooses the size of the block it creates as a function of the

[1] Termed the "optimal single price omniscient auction" in [8], this auction was suggested as a benchmark, and as far as we know, its game-theoretic properties have not been analyzed in the Bitcoin context.

WWW '19, May 13–17, 2019, San Francisco, CA, USA

ACM ISBN 978-1-4503-6674-8/19/05.
https://doi.org/10.1145/3308558.3313454

bids received. In some bid instances, blocks will be small, while in others they will be large.

In a pay-your-bid auction, a user must strategically determine the lowest bid it can submit such that it will be included in the block ("bid shading"). Indeed, Bitcoin wallets use various fee estimation techniques. It is not clear how to do this optimally, and in any case, it requires some non-trivial computational effort (data gathering, statistical analysis, etc). Bid shading can also help in worst-case instances of the monopolistic auction, and as a result, [8] do not analyze its strategic properties but suggest it only as a benchmark for other truthful auctions they define. These other truthful auctions from [8] are less applicable vis-a-vis our needs (see Section 5). Although the approach is not truthful, in the monopolistic auction, a user, rather than paying her bid, pays some threshold value (a function of all bids) which w.h.p is only remotely related to one's bid. The main technical novelty of this paper is to show that the expected gain from optimal bid shading relative to truthfully bidding the maximal willingness to pay decreases to zero as the number of bids grows. On average, all users will benefit very little, if at all, from bid shading in the monopolistic auction. Since a near optimal strategy is to bid the maximal willingness to pay, bidding in the monopolistic auction is simpler. Section 2 defines the formal framework used and proves this statement, and Section 4 verifies it via simulations using synthetic and actual Bitcoin bid distributions. The greater simplicity of the monopolistic auction is another of its advantages over the pay-your-bid auction.

This analyzes a single block creation. "Patient users", who willing to wait for future blocks, might lower their bids if they anticipate less competition in the future. Two important issues that remain to be investigated in future research are (1) how patient users shade down their bids and (2) how non-myopic bidders who create persistent transactions affect the bid distribution. Note that these issues affect the revenue not only of the monopolistic auction, but also of the pay-your-bid auction. We do not know, however, which of the two auctions is more strongly affected. Our analytical results suggest that the monopolistic auction collects at least as much revenue from impatient users as Bitcoin's current mechanism.

Related Work. There are relatively few works devoted to analyses of the Bitcoin fee market and fewer still that suggest modifications to the basic mechanism. [10] provided an early analysis of the economics of Bitcoin mining, including a game theoretic analysis of the incentives to mine on the longest chain. [2] considered the incentives of miners to distribute transactions to each other and designed ways to share the fees in exchange for distribution. [6] explored the security of Bitcoin and the incentive to mine blocks properly when block rewards diminish and fees dominate the revenue of miners. They showed that variance in fees may undermine the security of the protocol and subject it to different forms of deviations and attacks. [5] explored related bribery attacks on the protocol that are paid for through promises of higher rewards for attackers that construct blocks off the longest chain. [15] considered the removal of the block limit altogether, arguing that delays in large block propagation times, which, in turn, imply a higher likelihood that the block is abandoned (often referred to as an orphaned block), will cause miners to restrict their own block sizes. The paper analyzed the resultant fee market that emerges. [9] modeled the transaction fee market and assumed that users benefit less if their transactions are delayed. They showed that such delays together with the 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.

After the preprint version of this manuscript was published, Andrew Chi-Chih Yao [17] further analyzed the monopolistic price as a fee mechanism for Bitcoin, in the process resolving our main conjecture, Conjecture 2.6 – see the discussion there.

Basu, Easley, O'Hara and Sirer [3] used a modified monopolistic price auction to determine inclusion in the block. They penalize miners if the blocks are not full, and additionally, they average the reward from blocks between different miners. Their goal is to maximize social welfare rather than the miners' revenue. The main analytical difference between their work and ours is that theirs is based mostly on simulations while ours is proved for the most part formally. In terms of abstract conclusions, our results agree with theirs: they also establish that the incentive of miners and users to manipulate diminishes as n grows.

A full version with greater detail and the full proofs is in Ref. [11].

2 THE MONOPOLISTIC AUCTION

There are n transactions, each of which has a privately known maximal willingness to pay v_i for its inclusion in the block, e.g., an alternative transaction cost via a bank, credit card, etc. Transactions submit bids, and based on these, the miner decides which transactions to include in the block. The bid vector is sorted so that $\boldsymbol{b} = (b_1, \ldots, b_n)$ satisfies $b_1 \geq \ldots \geq b_n$. Let $k^*(\boldsymbol{b})$ be the index k that maximizes $k \cdot b_k$. In case of ties, k^* is chosen to be the maximal such index. Define:

$$R(\boldsymbol{b}) = k^*(\boldsymbol{b}) \cdot b_{k^*(\boldsymbol{b})} \ , \ p^M(\boldsymbol{b}) = b_{k^*(\boldsymbol{b})}, \tag{1}$$

where $R(\boldsymbol{b})$ is termed the "monopolistic revenue" and $p^M(\boldsymbol{b})$ is termed the monopolistic price. In the monopolistic auction, the miner includes in the block the $k^*(\boldsymbol{b})$ transactions who submitted the highest bids and charges a payment of $p^M(\boldsymbol{b}) = b_{k^*(\boldsymbol{b})}$ from each of these transactions. The miner's revenue from this block is therefore $R(\boldsymbol{b})$.

An untrusted auctioneer that can add fake bids does not have any incentive to do so in this auction. Specifically, the Bitcoin protocol can verify that all transactions in the same block pay the same price. However, it cannot prevent miners from adding fake bids by exploiting transactions that move funds between two accounts of the same miner. These fake bids can affect the payments of the "real" bids and increase the revenue of the auctioneer, as is the case in a second-price auction. In the monopolistic auction,in contrast, the addition of fake bids cannot increase the revenue: given any vector of real bids $\boldsymbol{b}$, since all transactions in the block pay the same price, the maximal revenue is $R(\boldsymbol{b})$ if the miner does not create another block in the near future. However, a bidder might benefit from submitting $b_i < v_i$, as demonstrated by the following examples:

Example 2.1. Suppose n bidders that have the same maximum fee $v_i = 1$. If all bids are $b_i = v_i$, then $R(\boldsymbol{b}) = n, k^*(\boldsymbol{b}) = n$, and

$p^M(\boldsymbol{b}) = 1$, i.e., all bids get accepted to the block and they all pay 1. A strategic bidder, say 1, can reduce her payment by reducing her bid to $b_1 = \frac{n-1}{n}$. With this bid, the monopolistic price decreases to $\frac{n-1}{n}$: if all bids of value 1 are accepted, the revenue is $n-1$, and if all bids of value at least $b_1 = \frac{n-1}{n}$ are accepted, the revenue is still $n-1$.

The gain from bid shading in this example vanishes as the number of users (and the block size) increases. In other cases, gains do not vanish even when the number of bidders grows:

Example 2.2. $v_1 = \ldots = v_{\frac{n}{2}+1} = 2, v_{\frac{n}{2}+2} = \ldots = v_n = 1$. Bidder 1 can reduce her price by bidding $\frac{n-1}{n}$ instead of 2.

However, if the values for example 2.2 are taken from realistic distributions, then the probability that it will be realized will usually be very small.

Therefore, rather than allege that there are no profitable deviations from truth-telling, we will only claim that the expected gain from any non-truthful bid diminishes as n grows. For example, if the distribution of values has a finite support, bidding the next lower value in the support *weakly dominates* truth-telling. Though more pronounced bid shading may be beneficial, it will not be a dominant strategy. We will show, however, that the expected gain from such a deviation or from any other deviation becomes extremely small as n grows. Therefore, we believe that it makes sense to conclude that only small deviations will likely happen.

Example 2.3. Consider the simplest equal-revenue distribution F with a finite support: $\Pr[v = 1] = 0.5, \Pr[v = 2] = 0.5$. For simplicity, assume that bidders can only submit bids of 1 or 2. Every bidder with $v = 2$ has a dominant strategy to bid 1, since she derives 0 utility when the monopoly price is set to be 2, and by bidding 1 she increases the chance that the monopoly price will be 1. The probability that a bidder with $v = 2$ can improve the outcome (i.e., change the empirical monopoly price from 2 to 1) by bidding b=1 in a 2n bidder auction is $\frac{\binom{2n}{n+1}}{2^{2n}} = \Theta\left(\frac{1}{\sqrt{n}}\right)$.

We validate this intuition more generally via both theoretical and empirical analyses. First we define some terms. 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.

$$p^S(\boldsymbol{b}_{-i}) \equiv \min\{b_i \in \mathbb{R} \mid p^M(b_i, \boldsymbol{b}_{-i}) \leq b_i\}.$$

In words, $p^S(\boldsymbol{b}_{-i})$ is the lowest possible bid for i to be included in the block. Figure 1 gives an example. This definition does not capture a case where a bidder can provide false-name bids (i.e., can split her transaction into several transactions), which is discussed in Section 3.

Figure 2 presents the strategic prices in an example with $n = 256$ users. In this example, p^S is monotonically decreasing among winning bidders (higher winning bids imply lower strategic prices) but not among all bidders. This property is formally proved in the full version [11]. Additionally, here and in most other simulations, almost all winning bids have the same strategic price, the exception being the very few lowest winning bids (i.e., those with prices slightly higher than the monopolistic price). The strategic price of these bids is higher, i.e., they gain less from being strategic.

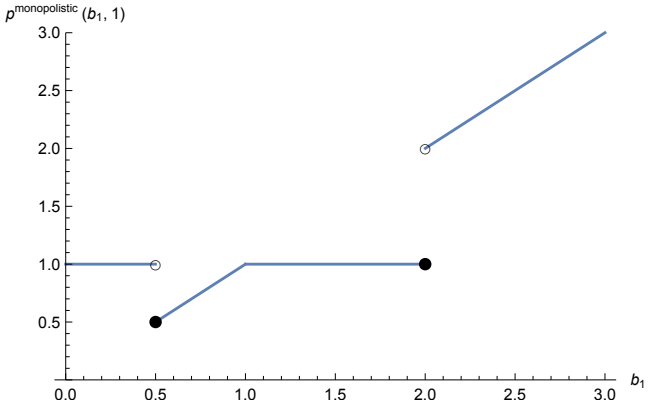

Figure 1: The function $p^M(b_1, 1)$ as a function of b_1, demonstrating that p^M is neither monotone nor continuous. As can be seen, the strategic price of the first bidder is 0.5.

While $p^S(\boldsymbol{b}_{-i})$ is the minimal price that bidder i must pay to be included in the block, she will pay $p^M(v_i, \boldsymbol{b}_{-i})$ if she bids her true maximal willingness to pay. This possible gain from bid shading is captured by the notion of the "discount ratio":

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

Clearly, $0 \leq \delta_i(v_i, \boldsymbol{b}_{-i}) \leq 1$. If $v_i < p^S(\boldsymbol{b}_{-i})$, every bid of at most v_i loses. Hence, the gain from bid shading is 0. If $v_i \geq p^S(\boldsymbol{b}_{-i})$, bidder i can win and pay $p^S(\boldsymbol{b}_{-i})$. With an honest bid, she will pay $p^M(v_i, \boldsymbol{b}_{-i})$. She can thus save a percentage of $1 - \frac{p^S(\boldsymbol{b}_{-i})}{p^M(v_i, \boldsymbol{b}_{-i})}$ from her price by strategic bid shading.

As we showed above that the discount factor can be large in the worst case, we therefore conduct an average-case analysis. Assume that all true values are drawn i.i.d. from some distribution F on $\mathbb{R}_{>0}$. The average discount ratio is then $\Delta_n^{average} = \mathbb{E}_{(v_1,\ldots,v_n)\sim F}[\delta_1(v_1, \boldsymbol{v}_{-1})]$ (the choice of bidder 1 is arbitrary since all are symmetric a-priori).

We also consider two stronger notions. In the first, for each realization $v_1, \ldots, v_n$, we consider the maximal discount ratio among all bidders:

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

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

Theorem 2.4. *For any distribution F with a finite support size,* $\lim_{n\to\infty} \Delta_n^{max} = 0$.

Section 2.1 proves this theorem.

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 depicts a situation commonly assumed in game theory wherein a user knows her own value and (only) the

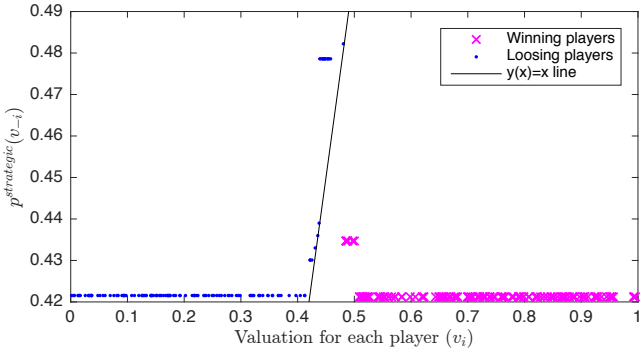

Figure 2: An example with $n = 256$ bids sampled i.i.d. from the uniform distribution on $[0, 1]$. For each user, the x-axis shows her values and the y-axis shows her strategic price. Winning bids, which are marked with 'x', must be at least as high as their respective strategic price, i.e., to the right of the black line.

distribution of the other values.

$$\delta_n^{GT}(\boldsymbol{b}_{-1}) = \max_{v_1 \in \text{Support}(F)} \delta_1(v_1, \boldsymbol{b}_{-1})$$

$$\Delta_n^{GT} = \mathbb{E}_{(v_2,\ldots,v_n)\sim F}[\delta_n^{GT}(\boldsymbol{v}_{-1})]$$

Theorem 2.5. *For any distribution F with a finite support size, $\lim_{n\to\infty} \Delta_n^{GT} = 0$.*

The proof of this theorem is very similar to that of Theorem 2.4.

Our empirical analysis focuses on Δ_n^{max}, since it is well-defined even for distributions with unbounded support.

While $\lim_{n\to\infty} |\Delta_n^{GT} - \Delta_n^{max}| = 0$, the relation between Δ_n^{GT} and Δ_n^{max} depends on the distribution, i.e., one term is not always larger than the other – see the full version for concrete examples. The e-print version contained the following conjectures:

Conjecture 2.6 (Nearly Bayesian-Nash Incentive-Compatibility).

1. *For any distribution F, $\lim_{n\to\infty} \Delta_n^{average} = 0$. In particular, $\Delta_n^{average} = O\left(\frac{1}{\sqrt{n}}\right)$, where the constant in the $O(\cdot)$ notation may depend on F.*
2. *If F has a bounded support (still possibly with an infinite cardinality) $\lim_{n\to\infty} \Delta_n^{\max} = 0$. In particular, $\Delta_n^{\max} = O\left(\frac{1}{\sqrt{n}}\right)$. The same holds for Δ_n^{GT}.*
3. *There exists a distribution F with unbounded support such that $\lim_{n\to\infty} \Delta_n^{\max} > 0$. The same holds for Δ_n^{GT}.*

The $O\left(\frac{1}{\sqrt{n}}\right)$ in the above conjecture can be achieved by Example 2.3.

Recently, Andrew Chi-Chih Yao resolved many issues that were left open in this work. Indeed, "The main purpose [of Yao's paper] is to settle the Nearly IC Conjecture for the monopolistic price in the positive" [17]. Specifically, the first sentences in items 1 and 2 were proved, and a slightly weaker claim was shown than the "in particular" claims in these items. This was proved also when accounting for multiple strategic bids – see Section 3. Item 3 was proved for the inverse distribution (see Eq. (3)), which was our primary candidate for this conjecture based on numerical data – see Section 4.

2.1 Proof of Theorem 2.4

Given $\boldsymbol{v}$, define: $i^* = \text{argmax}_{i=1,\ldots,n} v_i$, $k^* = k^*(\boldsymbol{v}_{-i^*})$, $p^H = p^M(\boldsymbol{v})$, and $p^S = p^S(\boldsymbol{v}_{-i^*})$.

Lemma 2.7. *For any F with finite support size, there exists a constant $c > 0$ (which may depend on F but not on n) s.t. $\lim_{n\to\infty} \Pr[k^* < c \cdot n] = 0$.*

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, $\mathbb{E}[k_{max}] = p_{max} \cdot n$. A Chernoff bound implies that $\lim_{n\to\infty} \Pr\left(k_{max} < \frac{9np_{max}}{10}\right) = 0$. Bidders who bid v_{max} win; therefore, $k^* + 1 \geq k_{max}$. Thus, $\lim_{n\to\infty} \Pr\left(k^* + 1 < \frac{9np_{max}}{10}\right) = 0$. Choosing $c = \frac{8p_{max}}{10}$ completes the proof of the lemma. □

The following three claims are proved in the full version [11]:

Claim 1. $\forall \boldsymbol{v}, i,\ p^M(p^S(\boldsymbol{v}_{-i}), \boldsymbol{v}_{-i}) = p^S(\boldsymbol{v}_{-i})$.

Claim 2. $\forall \boldsymbol{v}, i, j$: *$v_i \geq v_j$ implies $\delta_i(v_i, \boldsymbol{v}_{-i}) \geq \delta_j(v_j, \boldsymbol{v}_{-j})$.*

Claim 3. *Let y be the smallest element in the support of F that is at least p^S. Then, $y = p^H$ implies $p^S \geq \frac{k^*}{k^*+1} \cdot p^H$.*

With these claims, we prove a second lemma:

Lemma 2.8. $\lim_{n\to\infty} \Pr(p^S < \frac{k^*}{k^*+1} p^H) = 0$.

Proof. Define A as the event where $p^S < \frac{k^*}{k^*+1} p^H$. The proof defines an event B s.t. (i) $\lim_{n\to\infty} \Pr(B) = 0$, and (ii) $A \subseteq B$. This implies $\lim_{n\to\infty} \Pr(A) = 0$ as claimed.

To define event B, fix any arbitrary two $x, y \in \text{Support}(F)$ such that $x > y$. Define $\text{num}(\boldsymbol{v}, z) \equiv |\{v_i | v_i \geq z\}|$. Define the random variables $n_z = \text{num}(\boldsymbol{v}, z)$ for any real number z, $h(x) = n_x \cdot x$, and $g(x) = (n_x - 1) \cdot x$. We first aim to bound the probability that $h(x) > h(y) \geq g(x)$. This is the same as the probability that $n_x > \frac{y}{x} n_y \geq n_x - 1$, which is true only if $n_x = \lfloor \frac{y}{x} n_y + 1 \rfloor$. The triple $(n_x, n_y - n_x, n - n_y)$ is a trinomial distribution with probabilities $p_1 = \Pr_{v_i\sim F}(v_i \geq x), p_2 = \Pr_{v_i\sim F}(x > v_i \geq y), p_3 = \Pr_{v_i\sim F}(v_i < y)$ (p_i depends on F but not on n). By simple analysis of the trinomial distribution, we show in the full version that

$$\lim_{n\to\infty} \Pr(h(x) > h(y) \geq g(x)) = 0. \tag{2}$$

Let B be the event in which $\exists x, y \in \text{Support}(F)$ s.t. $x > y$ and $h(x) > h(y) \geq g(x)$. Since the support is of finite size, there is a fixed number of such pairs $x > y \in \text{Support}(F)$. By Eq. (2) and the union bound, we conclude that $\lim_{n\to\infty} \Pr(B) = 0$. We show that $A \subseteq B$, i.e., $p^S < \frac{k^*}{k^*+1} p^H$ implies $\exists x > y \in \text{Support}(F)$ s.t. $h(x) > h(y) \geq g(x)$. Let $x = p^H$ and let y be the smallest element in the support of F, which is at least p^S. By Claim 3, the event $p^S < \frac{k^*}{k^*+1} p^H$ implies $x > y$. Since $p^M(v_{i^*}, \boldsymbol{v}_{-i^*}) = x$, it follows that $h(x) = n_x \cdot x > n_y \cdot y = h(y)$. Furthermore,

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

where the first step follows since $n_y = n_{p^S}$ and $p^S \le y$, the fourth step follows since $v_{i^*} \ge x > y \ge p^S$, the fifth step follows from Claim 1 that shows that $p^M(p^S, \boldsymbol{v}_{-i^*}) = p^S$, and the sixth step follows since $v_{i^*} \ge x > y \ge p^S$. □

Let the "bad" event E_1 be the case where $k^* < c \cdot n$ (c is taken from Lemma 2.7) and the "bad" event E_2 be the case where $p^S < \frac{k^*}{k^*+1} p^H$. By Claim 2, $\delta_{max}(\boldsymbol{v}) = \delta_{i^*}(\boldsymbol{v})$. Therefore, $\Delta_n^{max} = \mathbb{E}_{\boldsymbol{v}}[\delta_{i^*}(\boldsymbol{v})]$. If E_2 does not hold, then $p^S \ge \frac{k^*}{k^*+1} p^H$, and therefore, $\delta_{i^*}(\boldsymbol{v}) \le \frac{1}{k^*+1}$. To conclude:

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

implying Theorem 2.4.

3 MULTIPLE STRATEGIC BIDS

In some cases, it is beneficial to split one's bid into separate transactions with several separate bids. In fact, such a strategy sometimes enables a losing transaction to be included in the block:

Example 3.1. Let $\boldsymbol{v} = (5, 2, 1, 1)$. With bids $\boldsymbol{b} = \boldsymbol{v}$, the monopolistic price is 5 and the second bidder loses. However, if she submits two separate bids of 1 each, the monopolistic price will be 1 and all bids will be included.

Our empirical evaluation below accounts for such situations, showing that the benefit from using multiple bids also goes to zero as n increases. In all the distributions we examined, except the discrete distribution, we *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. See the full version for more detail.

4 EMPIRICAL EVALUATION

We provide empirical evidence to support the above conjectures and to supply greater detail on the rate at which the discount ratio converges to zero. We use both synthetic data as well as transaction data taken from the Bitcoin blockchain. The synthetic data are 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 2.4.
(2) The uniform distribution over $[0, 1]$. Notice that here the support size is infinite.
(3) The half normal distribution. Here, the probability for maximum fee x decreases exponentially with x, hence, even though arbitrarily high transaction fees will be seen, they are highly unlikely.

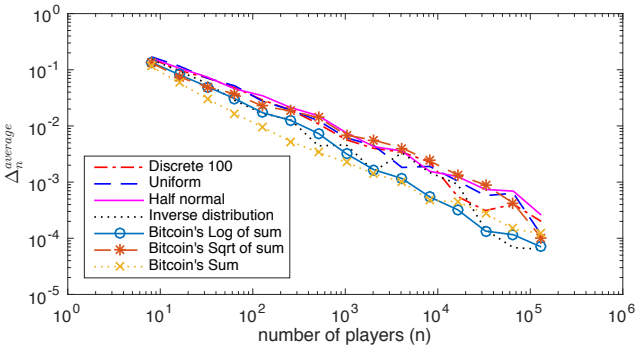

Figure 3: The average discount ratio of a player from selfish bidding as a function of the number of players that participate.

(4) The inverse distribution

$$F(x) = 1 - \frac{1}{x}, \quad x \in [1, \infty). \tag{3}$$

Here, the probability for a maximum fee x decreases polynomially with x.

The uniform distribution has no tail, the half normal distribution has a light tail (it decreases exponentially fast), and the inverse distribution has a heavy tail.

Bitcoin blockchain data was collected from 1000 consecutive blocks, which constitute roughly one week of activity ending on October 28th, 2016. The data obviously do not contain the maximum willingness to pay, since this is not how Bitcoin operates. The simulations estimate the maximum willingness to pay, v, as a function $v = v(x)$ of the transaction size x (x is the sum of all outputs of the Bitcoin transaction). We use three alternative functions: $v(x) = \log x, v(x) = \sqrt{x}, v(x) = x$. Note that multiplying all bids by a scalar does not change the discount ratio, which is the case when, e.g., the maximum willingness to pay is some percentage of $v(x)$.

We empirically evaluated $\Delta_n^{average}$ and Δ_n^{max} as a function of the number of bids, n. For each $n \in \{2^3, 2^4, \ldots, 2^{17}\}$, we conducted 100 simulation runs. Each run samples n bids and calculates the n empirical discount ratios. $\Delta_n^{average}$ is the average of the n individual discount ratios and Δ_n^{max} is the maximum over the n individual discount ratios. Each point in the graph is the average of 100 runs.

Figure 3 shows that $\Delta_n^{average}$ behaves almost identically for all tested distributions. In particular, as stated in the first part of Conjecture 2.6, $\Delta_n^{average}$ decreases linearly with the number of bids n and for all distributions, even those with an infinite and unbounded support size.

Figure 4 shows that Δ_n^{max} behaves differently for some of the tested distributions. For the uniform distribution, Δ_n^{max} decreases linearly with the number of bids, supporting the second part of Conjecture 2.6. 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 of users, and we believe that this is in fact an example that supports the third part of Conjecture 2.6. The three Bitcoin distributions behave as follows: the log of the sum decreases the fastest, the square root of the sum decreases

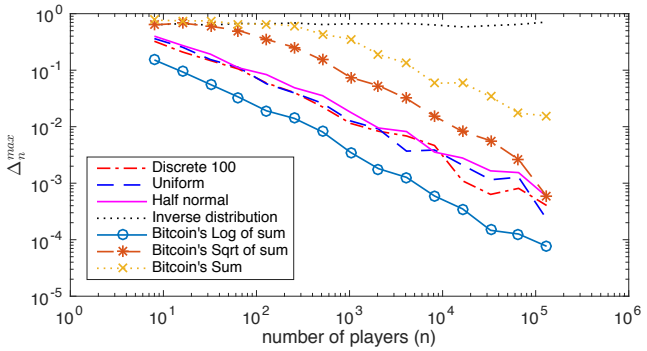

Figure 4: The maximal discount ratio of a player from selfish bidding as a function of the number of players.

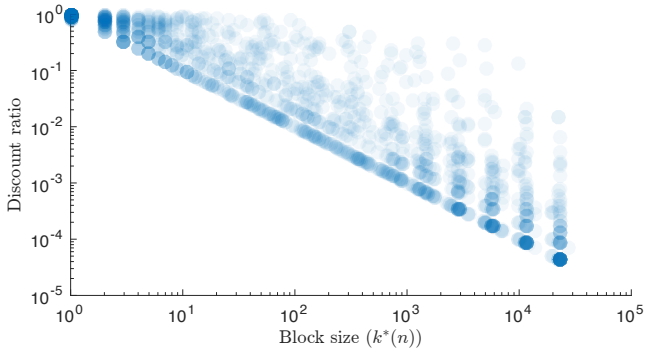

Figure 5: A scatter plot of all simulation points for the Bitcoin distribution with $v(x) = \log x$.

more slowly, and the sum decreases the slowest. For example, for $n = 2048$ (roughly the current Bitcoin block-size), Δ_n^{max} is about 0.2%, 5%, and 19% for the three distributions, respectively. When $n = 2^{17} \approx 130,000$, Δ_n^{max} is about 0.0007%, 0.05%, and 1%.

These findings show that there is a qualitative difference between $\Delta_n^{average}$ and Δ_n^{max}, mainly for the inverse distribution and for the Bitcoin distribution with $v(x) = x$. In these distributions, although the average transaction will benefit very little from bid shading, some transactions can nonetheless obtain significant benefit. This outcome can, in principle, result from two different reasons. The first is that $\Delta_n^{average}$ also accounts for the losing bidders, whose discount ratio is zero. The second is that Δ_n^{max} only accounts for the single winning bidder with the maximal discount ratio. However, typical bidder behavior (as demonstrated in Figure 2) shows that almost all winning bids have the lowest strategic price and, therefore, the highest discount ratio. Thus, the explanation for the difference between the two discount ratios seems to be the first.

Figure 5 shows all simulation points for the Bitcoin log of of sum distribubtion. The x-axis is the resulting *block size* of the simulation run (in the previous figures it was n) and the y-axis is the maximal discount ratio of the simulation run. Three main conclusions can be drawn from Figure 5. First, block sizes (number of winners) range from 1 to about 25,000 when $v(x) = \log x$ (recall that the total number of bids ranges from 2^3 to 2^{17}).[2] Second, this range in block sizes is the main reason why Δ_n^{max} is smaller in the Bitcoin log of the distribution of sums, as larger block sizes imply smaller discount factors. Third, the distribution of the simulation points, which include outliers, is not normal. We do not have an explanation for this finding. The last two remarks apply to all tested distributions.

5 SUMMARY AND CONCLUDING REMARKS

The simple pay-your-bid fee mechanism used in Bitcoin has several disadvantages: (i) A fixed (hard-coded) maximal block size implies non-optimal revenue extraction when the pre-fixed block-size is too small or too large for the current bid instance, (ii) Bitcoin wallets must invest computational effort in bid shading, and (iii) deciding on the maximal block size involves economic rather than purely technological considerations (e.g., block propagation time [7, 16]). For single block creation, the proposed monopolistic auction effectively solves all these issues while maintaining miner non-manipulability.

The monopolistic auction is ϵ-truthful (ϵ goes to zero as the number of bidders grows). Alternatively, we can take a truthful auction where a bidder cannot influence its winning price, e.g., the RSOP auction is truthful and its revenue $RSOP(\boldsymbol{v})$ satisfies $\lim_{n\to\infty} \max_{\boldsymbol{v}} \frac{R(\boldsymbol{v})}{RSOP(\boldsymbol{v})} = 1$ [8]. The full version describes an implementation in Bitcoin (e.g., the required randomness needs to be verified by other miners) and discusses major drawbacks of it. In light of these shortcomings, we believe that the monopolistic auction is better suited to implement improvements in Bitcoin's fee market.

Future Work. One important issue we did not cover is that of the temporal implications of patient users who are willing to wait for transactions to be included in future blocks, as in the current analysis we only address impatient users. The monopolistic auction can also be explored further via a careful equilibrium analysis. The astute reader may notice that the current model allows for an equilibrium in which all bidders bid 0, an unrealistic setting since in practice there exists a maximum limit on the block size, and not all transactions can be included in the block. We believe that in such a setting, no other meaningful equilibria exist other than truthfulness, which is an ϵ-BNE. To reach a definitive conclusion, however, a careful analysis is required.

6 ACKNOWLEDGMENTS

We thank Alaa Mozalbat, who designed and implemented the simulation code, and Reshef Meir for valuable discussions. R.L. was partly supported by a Marie-Curie fellowship "Advance-AGT", by an ARCHES award from the MINERVA foundation, and by the ISF-NSFC joint research program (grant No. 2560/17). O.S. was supported by ERC Grant 280157, by the Israel Science Foundation (grant 682/18), and by the Cyber Security Research Center at Ben-Gurion University. A.Z. was 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).

[2]The throughput when $v(x) = \log x$ will therefore be about $0.1n$ (n is the number of all transactions). For $v(x) = x$, block sizes range from 1 to about 1,500, implying a throughput of about $0.01n$.

REFERENCES

[1] Abe, M., Suzuki, K.: M+1-st price auction using homomorphic encryption. In: International Workshop on Public Key Cryptography. pp. 115–124. Springer (2002)

[2] Babaioff, M., Dobzinski, S., Oren, S., Zohar, A.: On Bitcoin and red balloons. In: ACM Conference on Electronic Commerce, EC '12, Valencia, Spain, June 4-8, 2012. pp. 56–73 (2012). https://doi.org/10.1145/2229012.2229022, http://doi.acm.org/10.1145/2229012.2229022

[3] Basu, S., Easley, D., O'Hara, M., Sirer, E.G.: Towards a functional fee market for cryptocurrencies (2019), http://arxiv.org/abs/1901.06830

[4] Bogetoft, P., Damgård, I., Jakobsen, T., Nielsen, K., Pagter, J., Toft, T.: A practical implementation of secure auctions based on multiparty integer computation. In: International Conference on Financial Cryptography and Data Security. pp. 142–147. Springer (2006)

[5] Bonneau, J.: 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. pp. 19–26 (2016). https://doi.org/10.1007/978-3-662-53357-4_2, https://doi.org/10.1007/978-3-662-53357-4_2

[6] Carlsten, M., Kalodner, H.A., Weinberg, S.M., Narayanan, A.: 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. pp. 154–167 (2016). https://doi.org/10.1145/2976749.2978408, http://doi.acm.org/10.1145/2976749.2978408

[7] Decker, C., Wattenhofer, R.: 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. pp. 1–10 (2013). https://doi.org/10.1109/P2P.2013.6688704, https://doi.org/10.1109/P2P.2013.6688704

[8] Goldberg, A.V., Hartline, J.D., Karlin, A.R., Saks, M.E., Wright, A.: Competitive auctions. Games and Economic Behavior **55**(2), 242–269 (2006). https://doi.org/10.1016/j.geb.2006.02.003, http://dx.doi.org/10.1016/j.geb.2006.02.003

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

[10] Kroll, J.A., Davey, I.C., Felten, E.W.: The economics of bitcoin mining, or bitcoin in the presence of adversaries. In: Proceedings of WEIS. vol. 2013 (2013)

[11] Lavi, R., Sattath, O., Zohar, A.: Redesigning bitcoin's fee market (2017), http://arxiv.org/abs/1709.08881

[12] Lipmaa, H., Asokan, N., Niemi, V.: Secure vickrey auctions without threshold trust. In: International Conference on Financial Cryptography. pp. 87–101. Springer (2002)

[13] Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008), http://www.bitcoin.org/bitcoin.pdf

[14] Naor, M., Pinkas, B., Sumner, R.: Privacy preserving auctions and mechanism design. In: Proceedings of the 1st ACM conference on Electronic commerce. pp. 129–139 (1999)

[15] Rizun, P.R.: A transaction fee market exists without a block size limit. Block Size Limit Debate Working Paper (2015), https://www.bitcoinunlimited.info/resources/feemarket.pdf

[16] Sompolinsky, Y., Zohar, A.: 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. pp. 507–527 (2015). https://doi.org/10.1007/978-3-662-47854-7_32, https://doi.org/10.1007/978-3-662-47854-7_32

[17] Yao, A.C.: An incentive analysis of some bitcoin fee designs (2018), http://arxiv.org/abs/1811.02351