# Dynamic Posted-Price Mechanisms for the Blockchain Transaction-Fee Market*

Matheus V. X. Ferreira[†‡1], Daniel J. Moroz[2], David C. Parkes[2], and Mitchell Stern[‡3]

[1]Computer Science, Princeton University
[2]Computer Science, Harvard University
[3]EECS, University of California, Berkeley

March 29, 2021

**Abstract**

In recent years, prominent blockchain systems such as Bitcoin and Ethereum have experienced explosive growth in transaction volume, leading to frequent surges in demand for limited block space, causing transaction fees to fluctuate by orders of magnitude. Under the standard first-price auction approach, users find it difficult to estimate how much they need to bid to get their transactions accepted (balancing the risk of delay with a preference to avoid paying more than is necessary).

In light of these issues, new transaction fee mechanisms have been proposed, most notably EIP-1559, proposed by Buterin et al. [4]. A problem with EIP-1559 is that under market instability, it again reduces to a first-price auction. Here, we propose dynamic posted-price mechanisms, which are *ex post* Nash incentive compatible for myopic bidders and dominant strategy incentive compatible for myopic miners. We give sufficient conditions for which our mechanisms are stable and approximately welfare optimal in the probabilistic setting where each time step, bidders are drawn i.i.d. from a static (but unknown) distribution. Under this setting, we show instances where our dynamic mechanisms are stable, but EIP-1559 is unstable. Our main technical contribution is an iterative algorithm that, given oracle access to a Lipschitz continuous and concave function $f$, converges to a fixed point of $f$.

*The authors thank Cemil Dibek, Vikram V. Ramaswamy and Tim Roughgarden for helpful discussions.
†Contact: mvxf@cs.princeton.edu
‡Part of this work completed while visiting Harvard University.

# 1 Introduction

In recent years, prominent blockchain systems such as Bitcoin and Ethereum have experienced explosive growth in their transaction volume, leading to frequent surges in demand for limited block space and causing transaction fees to fluctuate by orders of magnitude on a regular basis. Under the standard first-price auction approach to transaction fee auctions [18], users find it difficult to estimate how much they need to bid in order to get their transactions accepted. If they bid too low, their transactions can have a long confirmation time. Nevertheless, if they bid too high, they pay larger fees than necessary.

In light of these issues, new transaction-fee mechanisms have been proposed [16, 3, 4]. In particular, to improve a user's experience, there has been a focus on designing transaction-fee mechanisms that are incentive compatible for users. Unfortunately, standard mechanisms, such as second-price auctions, assume the auctioneer can commit to following an auction format. In a decentralized blockchain such as Bitcoin, self-interested miners act as auctioneers, deciding which transactions are included in a block. Due to the flexibility afforded to them in constructing blocks, miners cannot commit to following particular rules when they could do better by deviating. Moreover, there is information asymmetry, where miners control the available information due to deciding which transactions will win. While the correctness of payment rules can be enforced given the winning transactions, miners have complete control over the allocation and can use this to their advantage.

Designing strategyproof auctions that are at the same time robust to strategic auctioneers is a challenging task and closely related to the problem of designing *credible*[1] and *strategyproof* auctions [10, 2]. Akbarpour and Li [2] show that the ascending price auction with reserves is the unique revenue optimal, credible, and strategyproof auction for a computationally unbounded auctioneer. Ferreira and Weinberg [10] propose the *Deferred Revelation Auction* (DRA), which is credible assuming the auctioneer is computationally bounded. However, it is not known how to implement the ascending price auction or DRA in blockchains efficiently. An ideal transaction fee mechanism should require only winning transactions to store information in the blockchain. Still, a naive implementation of the ascending price auction and DRA would require all transactions to do so.[2]

In the face of these challenges, a new opportunity presented by the transaction fee problem on blockchains is to design dynamic mechanisms, wherein the price offered by a mechanism can adapt across auctions based on the transcript of winning bids. We ask whether this ability to use dynamics and adaptation *enables the design of approximately welfare optimal mechanisms that provide a good user experience and are robust to manipulation by miners.*

The recent *EIP-1559 proposal* of Buterin et al. [4] is an example of this idea. This proposal would change the current first-price auction on Ethereum to a hybrid between a *first-price auction* and a *dynamic posted-price* mechanism, which intends to keep block utilization at a target of 1/2 its maximum capacity. In EIP-1559 (described formally in Appendix A), each block has a fixed maximum capacity $m$ and a posted-price $q$ that is a deterministic function

[1]In a credible auction, the auctioneer is allowed to implement any safe deviation — a deviation that cannot be detected by bidders — from the promised auction, and yet, in expectation, the auctioneer gets no more revenue than implementing the promised auction.

[2]Blockchain space is a limited and expensive resource. Each communication with the blockchain is stored in blocks that propagate to the whole network.

of the previous blocks utilization. Every submitted transaction includes a *bid* $b$ as well as a *bid cap* $c$, which is the amount a bidder is willing to spend to have their transaction included. If a transaction's bid cap $c$ is greater than $b+q$, then a miner may choose to include it in the block. The protocol sets the next block's posted-price to be higher if block utilization was above the target and lower if below. The bidder pays $b+q$ to the blockchain, but miners receive only $b$ as revenue. Introducing a price floor via dynamic posted-prices is likely to make payments more predictable and was well received inside the Ethereum community. However, EIP-1559 received negative reception from miners since it significantly reduces their revenue [1]. Incentive alignment with miners is certainly an important component in adoption; therefore, we focus on studying dynamic posted-pricing mechanisms that award the full auction's revenue to miners.[3]

When the posted-price $q$ is stable, EIP-1559's mechanism reduces to a dynamic posted-price mechanism similar to the mechanisms that we study: bidders will bid $b = 0$ and report a bid cap $c$ equals the posted-price $q$.[4] However, under market instability, EIP-1559 reduces to a (non-incentive compatible) first-price auction. Roughgarden [19] formalizes EIP-1559 as a decentralized auction game and provides an economic analysis of the mechanism. Our work is complementary. We design a dynamic posted-price mechanism that succeeds in providing dominant-strategy incentive compatibility (DSIC) for myopic miners and is also *ex post* Nash incentive compatible (IC) for myopic bidders, even as demand fluctuates over time. The main distinction between dynamic-posted-price mechanisms and EIP-1559 is how they handle the case where there is excess demand. While EIP-1559 forces bidders to compete in a first-price auction, we suggest a dynamic posted-price mechanism, maintaining incentive alignment for users by ensuring that it remains a weakly dominant strategy for miners to randomize the allocation whenever there is excess demand.

Regarding the assumption about the myopia of miners, blockchain transaction-fee mechanisms involve multiple miners, from which one is, in effect, chosen at random in each time step. This decentralization of mining power is critical in providing the security of blockchains such as Bitcoin and Ethereum. Additionally, there is a high variance in the time at which a miner is chosen to create a block (and run the mechanism to choose winning transactions); therefore, it is reasonable that miners are myopic and seek to maximize immediate utility when selected to create a block. The user's myopia is a reasonable assumption when prices have low volatility. For this reason, one of our main objectives is to design mechanisms that are not only incentive-aligned but also converge to a stable posted-price.

## 1.1 Brief Technical Overview

The mechanisms that we study are relatively simple. We formalize the *dynamic posted-price* (DPP) mechanism (Definition 3.2) as a posted-price mechanism that is endowed with a price update rule and with an initial price $q_0$. In each time step $t$, the mechanism announces a price $q_t$ and the miner whose turn it is can allocate block space to at most $m$ bidders from

[3] Any mechanism can be modified to award only $\delta \in [0, 1]$ fraction of the auction revenue to miners. In this paper, we consider the case where the mechanism award all the revenue to miners ($\delta = 1$), but our results generalize for any $\delta > 0$.

[4] Here, we assume there is no reserve price, but EIP-1559 supports a hard-coded reserve price for its first-price auction.

those with bids $b_i \geq q_t$. Given the winning bids at time step $t$, the update rule computes the subsequent price $q_{t+1}$.

We say that a dynamic posted-price mechanism is *asymptotically stable with respect to $n$ i.i.d. bids drawn from the distribution $F$ and miner's randomness* if the sequence of expected posted-prices converges to a limit point $z$: that is, if $z$ is the current posted-price, then the expected value of next posted-price is also $z$. We say a mechanism is *approximately welfare optimal with respect to distribution $F^n = F \times \ldots \times F$* if selling at this limit price $z$ gives a constant fraction of the expected optimal welfare.

Our first concern is how to suggest to miners to resolve the allocation if there is excess demand — there are more than $m$ bids with $b_i \geq q_t$. A naive approach is to suggest that miners make use of a *maximum value maximal* (MVM) allocation rule (Definition 2.14). This rule would instruct miners to serve at most $m$ of the highest bidders. But in this case, any bidder with value $v_i \geq q_t$ has an incentive to bid $b_i = \infty$ to increase their chances of receiving block space. To fix this issue, we propose an alternative approach, the *random maximal* (RM) allocation rule (Definition 2.15), which instructs miners to serve a uniformly random maximal set of at most $m$ bidders from those with $b_i \geq q_t$.[5] This allocation rule removes the incentive for bidders to overbid since any bid above $q_t$ has an equal chance of being served. One challenge is to design a price update rule that provides asymptotic stability while also aligning incentives for miners to follow the RM allocation.

We first propose a *Welfare-Based Dynamic Posted-Price* (WDPP) mechanism in Section 4, which converges at an exponential rate to a price equilibrium assuming the revenue curve is Lipschitz continuous. However, the WDPP mechanism is not *ex post* IC for myopic bidders because it adopts the MVM allocation rule — there, we argue why miner's myopia is unreasonable for dynamic posted-price mechanisms using the RM allocation rule and the update rule of the WDPP mechanism. Next, we propose the *Utilization-Based Dynamic Posted-Price* (UDPP) mechanism in Section 5, which uses EIP-1559's price update rule. Although *ex post* IC for myopic bidders and DSIC for myopic miners, we show UDPP is unstable even when the demand is smaller than the supply, Proposition 6.3.

Our main result is the design and analysis of the *Truncated Welfare-Based Dynamic Posted-Price* (TWDPP) mechanism, Section 6, which aligns incentives for both users and miners (Theorem 2), converges to an equilibrium price (Theorem 3), and obtains $1/4$ of the optimal welfare at equilibrium (Theorem 4). For the proof of Theorem 3, our main technical contribution is an iterative algorithm that, given oracle access to a Lipschitz continuous and strictly concave function $f$, converges to a fixed point of $f$, Lemma 6.6.

In Section 7, we simulate the WDPP, UDPP, and TWDPP mechanisms. We find that the TWDPP mechanism achieves the strongest empirical welfare of the group. Throughout the paper, we give an intuition for our theoretical results and defer most proofs to the appendix.

# 2 Preliminaries

We study a setting where there are $m$ identical *block slots* to allocate at each discrete time step. A set of bidders arrive in each step, and one miner is chosen randomly to become

[5] Note that this protocol requires only private randomization and not trusted, public randomness, which is an expensive resource on blockchains.

*active*. We assume miners are myopic and seek to maximize their immediate utility. The number of miners and how they are chosen is not relevant for the model. Later, in Section 8, we discuss the relevance of the miner selection rule in the setting of non-myopic miners.

It is the active miner who determines the allocation of the block slots to bidders. For reasons we will explain, the miners do not have the opportunity to deviate from the mechanism's intended design regarding its payment rule. For this reason, we say that the active miner determines the allocation while "the mechanism" determines the payments to collect from each bidder that receives a slot.

The set of *active bidders* $M_t \subset \mathbb{N}_+$ denotes the bidders who arrive at time $t$. Bidder $i \in \cup_{t=1}^{\infty} M_t$ has a *private value* $v_i \in \mathbb{R}_+$. We assume bidders are myopic, that is, they are only interested in receiving a slot at time $t$. Thus, the sets of active bidders $M_1, M_2, \dots$ are disjoint.

For each $i \in M_t$, let $b_i \in \mathbb{R}_+$ denote bidder's $i$ bid value. We assume lexicographic tie-breaking between identical bid values. An interesting case to consider is when the demand is greater than the supply. Hence, unless otherwise stated, we assume $|M_t| \geq m + 1$ for all time step $t$. For a set of active bidders $M$, we define $M(q) := \{i \in M : b_i \geq q\}$ as the subset of bidders from those with bid $b_i \geq q$.

Crucial to our setting is that bids are public to all miners, but are not available to the mechanism. Rather, the mechanism is only privy to information about the values of bids that are *actually assigned* to slots in period $t$. For this reason, the miners can, collectively, impersonate a set of *fake bidders*, $F_t \subset \mathbb{N}_+$, at time $t$, and each fake bidder $i \in F_t$ submits a *fake bid* $b_i \in \mathbb{R}$. Thus, the set $F_t$ is disjoint from real bidders $M_t$. The *allocation* $B_t \subseteq M_t \cup F_t$ is a set of at most $m$ bids that receive a slot at time $t$. The allocation is chosen by the miner who controls the outcome of the auction in period $t$. It is only once a miner selects the allocation $B_t$ that the mechanism learns the bid $b_i$ for all $i \in B_t$. The mechanism does not learn the bid $b_i$ for $i \in M_t \setminus B_t$.

We now define the allocation rule and payment rule for the family of dynamic mechanisms that we study in this paper.

**Definition 2.1** (Allocation Rule)**.** An *allocation rule* is a vector-valued function $\vec{x}$ from history $B_1, \dots, B_{t-1}$ and active bidders $M_t$ to an indicator $x_i(B_1, \dots, B_{t-1}, M_t) \in \{0, 1\}$ for each active bidder $i \in M_t$. The indicator is 1 if and only if bidder $i \in M_t$ receives a slot at time $t$. An allocation rule is *feasible* if $\sum_{i \in M_t} x_i(B_1, \dots, B_{t-1}, M_t) \leq m$. An allocation rule is *deterministic* if $x_i(B_1, \dots, B_{t-1}, M_t)$ is a deterministic variable, and *randomized* otherwise.

**Definition 2.2** (Payment Rule)**.** A *payment rule* is a vector-valued function $\vec{p}$ from history $B_1, \dots, B_t$ to a payment $p_i(B_1, \dots, B_t)$ for each bidder $i \in B_t$.

Given this, we say that an *intended mechanism* is a tuple $(\vec{x}, \vec{p})$ where $\vec{x}$ is a feasible allocation rule and $\vec{p}$ is a payment rule. Throughout the paper, we use *mechanism* to refer to the blockchain protocol responsible for charging payments to bidders and transferring payments to miners. We now define the sequence of steps in the game.

**Definition 2.3** (Decentralized multi-round auction game)**.** The *decentralized multi-round auction game* is a multi-round game between multiple miners and the mechanism. We are given an allocation rule $\vec{x}$, a payment rule $\vec{p}$, and initially all miners are *inactive* and the time step is $t = 1$. The game proceeds as follows:

1. All miners observe $M_t$ and all bids $b_i \in M_t$.
2. One miner is chosen at random to become *active*.
3. The active miner chooses and announces an allocation

$$B_t := \{i \in M_t : x_i(B_1, \ldots, B_{t-1}, M_t) = 1\}.$$

4. The mechanism observes $B_t$ and all bids $b_i \in B_t$.[6]
5. For each bidder $i \in B_t$, the mechanism charges $p_i(B_1, B_2, \ldots, B_t)$.
6. The active miner receives a payment $\sum_{i \in B_t} p_i(B_1, \ldots, B_t)$.
7. The active miner becomes inactive. Increment $t$ and return to step (1).

Unlike standard mechanism design [17], miners are responsible for choosing $B_t$, and yet at the same time, cannot commit to implementing a particular allocation rule $\vec{x}$; that is, an active miner can corrupt step (3) of the game in any way they want. Miners may even allocate slots to fake bidders, $i \in F_t$.

Once miners choose $B_t$, the mechanism can only observe bids in $B_t$ and does not observe $M_t \setminus B_t$. Thus, the payments must depend on $B_1, \ldots, B_t$, and not on the bids $M_t$ that were active at time $t$. Blockchains can commit to executing honest code and faithfully implement steps (5) and (6); in fact, it is this commitment power to correctly execute code that is one of the biggest appeals of decentralized blockchains. Thus, miners can manipulate the allocation $B_t$ of the intended mechanism but not what the mechanism computes once it learns $B_t$.

**Example 2.4.** Suppose there is a single slot for sale, and the mechanism $(\vec{x}, \vec{p})$ is a first-price auction; i.e., the highest bidder receives the slot and pays his bid. Suppose there are two active bidders at time $t$, $M_t = \{1, 2\}$, with identical values $v_1 = v_2 = 2$ and distinct bids $b_1 = 1$, $b_2 = 2$. While the values are private to bidders, the bids become known to miners at Step (1). At Step 3, the active miner is instructed by the allocation rule to allocate the slot to bidder 2, but he is not constrained to not implementing other allocations. For example, the active miner can: allocate the slot to bidder 1 and receive utility \$1; allocate to bidder 2 and receive utility \$2; allocate the slot to neither bidder and receive utility \$0; or even allocate the slot to a fake bidder with any bid $b$ and receive a utility of $v - v = \$0$; i.e., they pay the mechanism at Step 5, but the mechanism returns the payment at Step 6. In this example, the active miner's optimal action is to allocate the slot to bidder 2 and receive utility \$2. Thus, in this example, the mechanism and the active miner's incentives are aligned.

We assume that bidders have *quasilinear utility*. That is for all bidders $i \in M_t$, we have

$$u_i(v_i, b_i) := x_i(B_1, \ldots, B_{t-1}, M_t) \cdot (v_i - p_i(B_1, \ldots, B_t)). \tag{1}$$

We will only consider mechanisms that transfer all payments from the bidders to the miners.[7] The miner's utility is a function $u_0$ from allocation $B_t$ to the revenue to the miner (and nets

[6] The integrity of bid values can be enforced via digital signatures.

[7] While we transfer all payments to miners, EIP-1559 burns most of payments coming from bidders. In Appendix A, we modify our model to incorporate EIP-1559. Miner's revenue is not relevant for our analysis. All of our results remains untouched if one modify Equation 2 to transfer $\delta \in (0, 1]$ fraction of the revenue to the active miner.

out any payments from fake bids). That is,

$$u_0(B_t) := \sum_{i \in B_t \setminus F_t} p_i(B_1, \ldots, B_t). \tag{2}$$

We study the stability and the expected welfare of a mechanism in the probabilistic setting when $n$ bidders are drawn i.i.d. from a continuous *cumulative density function* $F$ supported on the positive interval $[\underline{a}, \bar{a}]$:

$$F(x) := Pr[v \leq x]. \tag{3}$$

We define $\vec{v} := \{v_1, v_2, \ldots, v_n\} \in \mathbb{R}_+^n$ as an $n$-dimensional random variable, where $v_1, v_2, \ldots, v_n$ are drawn i.i.d. from $F$.

**Definition 2.5** (Social Welfare)**.** For a mechanism $(\vec{x}, \vec{p})$ with history $B_1, B_2, \ldots, B_{t-1}$, let $M_t = [n] = \{1, 2, \ldots, n\}$ be a set of bidders with values $\vec{v} = \{v_1, v_2, \ldots, v_n\}$ drawn i.i.d. from $F$. The expected *social welfare* at time $t$ with respect to allocation rule $\vec{x}$ is

$$\textsc{Welfare}_t(\vec{x}) := \mathbb{E}_{\vec{v} \sim F^n} \left[ \sum_{i=1}^{n} v_i \cdot x_i(B_1, \ldots, B_{t-1}, M_t) \middle| B_1, \ldots, B_{t-1} \right]. \tag{4}$$

We drop the subscript $t$ and write $\textsc{Welfare}(\vec{x})$ when the time step is clear from context. Let $\vec{x}^*(\vec{v})$ be the welfare maximizing feasible allocation for a particular value profile $\vec{v}$, with $\sum_{i=1}^{n} x_i^*(\vec{v}) = m$. The *optimal expected social welfare* is:

$$OPT := \mathbb{E}_{\vec{v} \sim F^n} \left[ \sum_{i=1}^{n} v_i \cdot x_i^*(\vec{v}) \right]. \tag{5}$$

## 2.1 Mechanisms from auction theory

We will consider a mechanism as having *good user experience* if it is *ex post Nash incentive compatible (IC)* and *individually rational* (IR) for bidders — i.e., bidders have an incentive to report their true value, and pay at most their bid.

**Definition 2.6** (Ex Post Nash Equilibrium)**.** A *strategy* for bidder $i$ is a function $b_i^*$ from value $v_i$ to bid $b_i^*(v_i)$. A strategy profile $b^*(\cdot)$ is an *ex post Nash equilibrium* (EPNE) for a mechanism $(\vec{x}, \vec{p})$ if for all histories $B_1, \ldots, B_{t-1}$, for all active bidders $M_t$, for all bidders $i \in M_t$, for all values $v_i$, bidding $b_i^*(v_i)$ maximizes the utility (1) of bidder $i$ conditioned on all $j \neq i \in M_t$ following strategy $b_j^*(v_j)$.

**Definition 2.7** (Ex Post Incentive Compatible)**.** A mechanism $(\vec{x}, \vec{p})$ is *ex post incentive compatible* (IC) for bidders if it has a *truthful ex post* Nash equilibrium where all real bidders bid their true value. That is, $b_i^*(v_i) = v_i$ for all $i \in \cup_{t=1}^{\infty} M_t$.

We work with *ex post* IC rather than dominant-strategy IC on the part of bidders because the pool of bids is public and, in principle, bidders could choose to condition their strategies on the reports of others. *Ex post* IC still provides a useful simplification: it is optimal for a bidder to report truthfully, whatever its actual value and the value of others, as long as others are also truthful.

**Definition 2.8** (Individual Rationality (IR))**.** A mechanism $(\vec{x}, \vec{p})$ is *individually rational* if for all history $B_1, B_2, \ldots$, bidders pay at most their bids, i.e., $p_i(B_1, B_2, \ldots) \leq b_i$ for all bidders $i$.

Mining in a decentralized blockchain is distributed to miners. At each time step $t$, one miner is chosen randomly from a large pool of potential miners, for example, through proof-of-work or proof-of-stake protocols. The elected miner is responsible for picking the allocation $B_t$. Because each miner has a negligible probability of being elected, we assume miners are myopic and maximize their immediate utility without regard for how their strategy in the current time step might affect their utility in the future. Moreover, our mechanism awards all the auction's revenue to miners reducing miner's incentives to follow non-myopic strategies. However, non-myopic miners may collude and implement deviations that increase their future revenue if the gains from deviating outweigh the costs. For a discussion on collusion, see Section 8.

**Definition 2.9** (Dominant Strategy Incentive Compatible (DSIC) for Myopic Miners)**.** A mechanism $(\vec{x}, \vec{p})$ is *DSIC for myopic miners* if for all histories $B_1, \ldots, B_{t-1}$, for all active bidders $M_t$, miners maximize their utility (2) by implementing the allocation rule $\vec{x}$. That is, the miner sets $F = \emptyset$ and chooses $B_t = \{i \in M_t : x_i(B_1, \ldots, B_{t-1}, M_t) = 1\}$.

Next, we highlight how traditional auctions have undesirable properties as a decentralized transaction-fee mechanism to motivate the design of dynamic mechanisms.

**Definition 2.10** (Static mechanism, and Dynamic mechanism)**.** A mechanism $(\vec{x}, \vec{p})$ is *static* if its allocation and payment rule depends only on the most recent bids and allocation. That is, for all histories $B_1, \ldots, B_{t-1}$, $x_i(B_1, \ldots, B_{t-1}, M_t) = x_i(M_t)$ and $p_i(B_1, \ldots, B_t) = p_i(B_t)$. A mechanism is *dynamic* if it is not static.

**Definition 2.11** (First-price auction)**.** A *first-price* (FP) auction is a static mechanism where the top $m$ bidders receive a slot and pay their bid.

Nakamoto [18] proposed the first-price auction as the default transaction-fee mechanism for Bitcoin. An important property of the first-price auction is that it is DSIC for myopic miners. Miners can only lose revenue by replacing a real bid $i \in M_t$ for a fake bid $j \in F_t$. As a downside, the first-price auction is known to provide a bad user experience as a transaction-fee mechanism because it has no *ex post* Nash equilibrium. A bidder wants to bid the minimum possible that would allow her to win a slot, but that requires the bidder to monitor all the other bids and adapt her strategy.

**Definition 2.12** (Second-price auction)**.** A *second-price* (SP) auction is a static mechanism where the top $m$ bidders receive a slot and pay the $(m+1)$-st highest bid.

Unlike the first-price auction, truthful bidding $b_i(v_i) = v_i$ is an *ex post* Nash equilibrium for the second-price auction, making it easy for myopic bidders to participate. However, to implement its payment rule, miners must commit to truthfully reporting the value of $m+1$-st highest bid with the mechanism (note the payment rule depends not only on the allocation $B_t$ but also on unallocated transactions $M_t \setminus B_t$). Thus miners are better off by reporting a fake bid equals the $m$-th highest bid, and the second-price auction is not DSIC for myopic miners.

Next, we consider posted-price mechanisms, and two possible allocation rules.

**Definition 2.13** (Maximal Allocation)**.** For a set of active bidders $M$, we say $S \subseteq M$ is a *maximal allocation* with respect to $M$ if the following is true:

- $S$ contains at most $m$ bidders.
- If $S$ contains less than $m$ bidders, $S = M$.

Let $2^M$ denote the collection of maximal allocations with respect to $M$, i.e.

$$2^M := \{B \subseteq M : |B| \leq m \text{ is a maximal allocation}\}. \tag{6}$$

**Definition 2.14** (Maximum value maximal allocation rule)**.** The *maximum value maximal* (MVM) allocation rule $\vec{x}^{MVM}(M)$ selects a maximal allocation $B \in 2^M$ that maximizes bids values — that is, $B = \arg\max_{B' \in 2^M} \sum_{i \in B'} b_i$.

Let *Unif*$(\{B_1, \ldots, B_\ell\})$ denotes the uniformly random distribution over $\{B_1, \ldots, B_\ell\}$.

**Definition 2.15** (Random maximal allocation rule)**.** The *random maximal* (RM) allocation rule $\vec{x}^{RM}(M)$ samples a maximal allocation $B \in 2^M$ from the distribution *Unif*$(2^M)$.

**Definition 2.16** (Posted-price mechanism)**.** A *posted-price* (PP) mechanism with posted-price $q$ is an static mechanism $(\vec{x}, \vec{p})$ where each bidder that receives a slot pays $q$ and all other bidders pay nothing. We refer to $(\vec{x}(q), \vec{p}(q))$ as the posted-price mechanism with posted-price $q$. A posted-price mechanism with posted-price $q$ is a *randomized posted-price* (RPP) mechanism if for all $M$, $\vec{x}(M) = \vec{x}^{RM}(M(q))$ is the RM allocation rule on bids $M(q) = \{i \in M : b_i \geq q\}$. A posted-price mechanism with posted-price $q$ is a *deterministic posted-price* (DPP) mechanism if for all $M$, $\vec{x}(M) = \vec{x}^{MVM}(M(q))$ is the MVM allocation rule on bids $M(q)$.

Posted-price mechanisms are DSIC for myopic miners since they commit to a fixed-price that miners cannot influence, and thus, the best a miner can do is accept a maximal allocation of bids priced at or above the price $q$. Depending on how the posted-price mechanism allocates slots, the mechanism might also be incentive compatible for bidders. The posted-price mechanism with the RM allocation rule is *ex post* IC since any bidder with $b_i \geq q$ has an equal chance to receive a slot irrespective of its bid. On the other hand, the posted-price mechanism with the MVM allocation rule is not *ex post* IC because whenever more than $m$ bidders have value $v_i \geq q$, there exists a bidder with value $v_i \geq q$ that will not receive a slot. If that bidder bids $b_i = \infty$ instead of $v_i$, they receive the slot and pay $q \leq v_i$.

## 2.2 Desiderata for transaction-fee mechanisms

We summarize the properties of the posted-price, first-price, and second-price auctions in Table 1, and we discuss other proposals in Appendix A. All three mechanisms are individually rational and require little communication with the blockchain. This communication efficiency is a first-order concern for decentralized blockchains because any information stored in the blockchain must propagate through the whole network. In particular, these mechanisms require miners to report order $O(m)$ bids to the mechanism to implement the payment rule — that is, the communication scales as the number of slots, not the number of bidders.

| Static mechanisms | Bidder payment | Miner revenue | IC for bidders | DSIC for miners |
|---|---|---|---|---|
| FP auction (2.11) | $b_i$ | $\sum_{i \in B_t} b_i$ | No | Yes |
| SP auction (2.12) | $\max_{i \in M_t \setminus B_t} b_i$ | $\lvert B_t \rvert \cdot \max_{i \in M_t \setminus B_t} b_i$ | Yes | No |
| Deterministic PP (2.16) | $q_t$ | $\lvert B_t \rvert \cdot q_t$ | No | Yes |
| Randomized PP (2.16) | $q_t$ | $\lvert B_t \rvert \cdot q_t$ | Yes | Yes |
| EIP-1559 (A.1) | $b_i + q_t$ | $\sum_{i \in B_t} b_i$ | Sometimes | Yes |
| Monopolistic price (A.2) | $\min_{i \in B_t} b_i$ | $\lvert B_t \rvert \cdot \min_{i \in B_t} b_i$ | Approximately | Yes |
| RSOP (A.3) | $\min_{i \in B_t} b_i$ | $\lvert B_t \rvert \cdot \min_{i \in B_t} b_i$ | Yes | No |
| Modified GSP (A.4) | $\min_{i \in B_t} b_i$ | $\frac{1}{k} \sum_{i=1}^{k} \lvert B_{t-k} \rvert \cdot \min_{i \in B_{t-k}} b_i$ | Approximately | Approximately |

Table 1: Bidder payments and miner revenue under various static mechanisms. $q_t$ denotes a posted-price. At time $t$, $M_t$ denote the set of active bidders and $B_t$ denotes the allocation.

Posted-price mechanisms are also naturally robust to miners' strategic behavior and are incentive compatible for bidders provided the posted-price is high enough (so that supply is greater than the demand at the posted-price). While first-price auctions are not incentive compatible for bidders, they are resilient to manipulation by miners. Finally, second-price auctions are incentive compatible for bidders but not resilient to manipulation by miners.

A mechanism is *efficient* (or welfare optimal) if, under the assumption, bidders follow an *ex post* Nash equilibrium, it allocates slots to bidders with the highest values. The second-price auction is efficient since truthful bidding is a dominant strategy and the highest bidders receive block slots. In theory, first-price auctions are also efficient assuming bids are drawn i.i.d. from some distribution $F$ and under the assumption bidders follow a Bayes-Nash equilibrium. However, bids in a first-price auction do not typically converge to an equilibrium in repeated settings, as was observed for paid-search engines [7], and the current blockchain transaction fee market is an example of the kind of instability that can occur. Sequential posted-price mechanisms — where the auctioneer visits bidders to make a take or leave offer — can obtain 1/2 fraction of the optimal welfare provided prior knowledge on the distribution $F$ and the demand $n$ [15].

We summarize the desiderata for the design of transaction-fee mechanisms for decentralized blockchains as follows:

- **Communication Complexity.** The mechanism requires $O(m)$ communication between bidders and the blockchain.[8]
- **Ex Post Incentive Compatible for Myopic Bidders.** The mechanism has a truthful *ex post* Nash equilibrium for myopic bidders.
- **Individually Rational.** If bidders receive a slot, they pay at most their bid; otherwise, they pay nothing.
- **DSIC for Myopic Miners.** In each period, it is a weakly dominant strategy for miners to implemented the intended allocation rule.
- **Approximately Welfare Optimal.** If in each period, $n$ i.i.d. bidders are drawn from distribution $F$, then the mechanism converges to a stable equilibrium where the

[8] The second-price, first-price, and posted-price mechanisms have communication complexity $O(m)$. As a distinction, the communication cost between miners and the blockchain on known implementations of credible, strategyproof, optimal auctions would scale with $n$, the number of bidders, not the number of slots.

expected welfare in each time step is $\Omega(OPT)$, where $OPT$ is the optimal expected social welfare.[9]

# 3 Dynamic Posted-Price Mechanisms

Designing a mechanism that is IC for myopic bidders and DSIC for myopic miners is closely related to the problem of designing revenue optimal, strategyproof, and credible auctions [2, 10]. However, all known constructions of credible, strategyproof, and optimal auctions are static[10] and have communication complexity of $\Omega(n)$, i.e., scaling with the number of bidders, not the number of slots. Since we expect demand to be greater than the supply, naive implementations of these mechanisms are impractical as transaction-fee mechanisms on blockchains.

The idea of a dynamic posted-price mechanism is that even though the demand curve is unknown, we can hope to learn a proxy for the market-clearing price from transactions included in preceding blocks. We must be careful, though, since we must align the mechanism with miners' incentives to faithfully implement the allocation rule. Moreover, dynamic mechanisms introduce additional challenges that are not present in static mechanisms. In particular, demand curves change over time, and the mechanism must respond to these changes.

**Definition 3.1** (Update Rule)**.** An *update rule* is a real-valued function $T$ from positive $q$ and feasible allocation $B$ with respect to $q$ to the subsequent price $T(q, B)$ where $b_i \geq q$ for all $i \in B$.

*Remark:* we use $B$ to refer to the bidders that receive a slot. Given $i \in B$, the update rule has access to the bid $b_i$ of bidder $i$.

**Definition 3.2** (Dynamic Posted-Price Mechanism)**.** A *Dynamic Posted-Price* (DPP) mechanism $(\vec{x}, \vec{p}, T)$ is a dynamic mechanism endowed with an update rule $T$. Let positive $q_0$ denote the initial posted-price. Given history $B_1, B_2, \ldots, B_{t-1}$ and active bidders $M_t$, define the posted-price $q_t := T(q_{t-1}, B_{t-1})$ at time $t$. The mechanism $(\vec{x}, \vec{p}, T)$ is a *Randomized Dynamic Posted-Price* (RDPP) mechanism, if at time step $t$, it implements the RM allocation rule:

$$\vec{x}(B_1, B_2, \ldots, B_{t-1}, M_t) := \vec{x}^{RM}(M_t(q_t)).$$

The mechanism $(\vec{x}, \vec{p}, T)$ is a *Deterministic Dynamic Posted-Price* (DDPP) mechanism, if at time step $t$, it is implements the MVM allocation rule:

$$\vec{x}(B_1, B_2, \ldots, B_{t-1}, M_t) := \vec{x}^{MV}(M_t(q_t)).$$

[9] We consider asymptotically stability with respect to the distribution $F^n$ as our formal definition for stable equilibrium (Definition 3.5).

[10] To avoid confusion, we always refer to *static mechanisms* as mechanisms that satisfy Definition 2.10 where the allocation and payment rules depend only on $M_t$ while Akbarpour and Li [2] refers to *static mechanisms* as mechanisms that require a single round of communication from each bidder with the auctioneer.

Because the posted-price change over time adds the constraint that the posted-price must not oscillate when we observe similar demand across time. For this, we study the stability of the expected value for the random operator $T(q, B)$ when each time step, $n$ bidders with values $\vec{v} = (v_1, v_2, \ldots, v_n)$ are drawn from distribution $F^n$ and under the assumption bidders are truthful: bidder $i$ bids $b_i = v_i$ for all $i$. Define the real-valued function $E_T$ to be

$$E_T(q) := \mathbb{E}_{\vec{v}\sim F^n}\left[T(q, B)\right], \tag{7}$$

where the expectation taken is over $v_1, v_2, \ldots, v_n$ and over the allocation rule $\vec{x}(q)$ where the random variable

$$B = \{i \in M : x_i(q) = 1\}.$$

Before we formally define stability for a DPP mechanism, we need to define the fixed point iteration of a real-valued function. Throughout the paper, we use $(X, d)$ to refer to a complete metric space where $X \subseteq \mathbb{R}$ and $d$ is the Euclidean norm.

**Definition 3.3** ($n$-iterate)**.** The *$n$-iterate* of function $f : X \to X$, for integer $n \geq 0$, is the function

$$f^n(q) := \begin{cases} q & \text{for } n = 0, \\ f(f^{n-1}(q)) & \text{for } n \geq 1. \end{cases} \tag{8}$$

A point $x$ is a *fixed point* for function $f : X \to X$ if and only if $f(x) = x$.

**Definition 3.4** (Fixed-point iteration)**.** Given a continuous function $f : X \to X$ and a initial point $q_0 \in X$, the *fixed-point iteration* of $f$ starting from $q_0$ is the sequence of function evaluations

$$q_0, f(q_0), f^2(q_0), f^3(q_0), \ldots \tag{9}$$

If the sequence converges to some $q^*$, from continuity of $f$, $q^*$ is a fixed point of $f$.

**Definition 3.5** (Asymptotically Stability and Welfare at Equilibrium)**.** A DPP mechanism $(\vec{x}, \vec{p}, T)$ is *asymptotically stable* with respect to $F^n$ if, for *any* positive initial price $q_0$, the fixed point iteration of $E_T$ starting from $q_0$ converges to the *equilibrium price* $q^*$. A DDP mechanism is *unstable* if it is not asymptotically stable. A DPP mechanism is *approximately welfare optimal* if it is asymptotically stable with equilibrium price $q^*$ and the welfare at equilibrium $\textsc{Welfare}(\vec{x}(q^*)) \geq \Omega(OPT)$ is a constant approximation of the optimal welfare.

There are two main reasons a DPP mechanism can be unstable: prices grow unbounded, or prices oscillate in a closed orbit. The proofs of Propositions 5.5 and 6.3 give examples of mechanisms that are unstable when the distribution $F$ is a point mass. In practice, prices must remain bounded for the mechanism to be of practical use. The convergence of prices is important in justifying our assumption that bidders are myopic. If prices were to oscillate, bidders might become non-myopic, seeking to time the moment they enter their bids, waiting for moments where prices are lower, driving more instability and uncertainty in the market.

## 3.1 Asymptotically stable update rules via fixed point theory

Here we give a brief introduction on how to construct asymptotically stable mechanisms using the *Banach contraction principle* [20]. There is a rich theory on the study of fixed points [6, 13] for monotone decreasing operators and in many settings, the existence of a fixed point is guaranteed. In general, we do not expect a function $f : \mathbb{R} \to \mathbb{R}$ to have a fixed point, consider $f(x) = x + 1$. But if a continuous function $f$ is non-increasing, then $f$ always intersects the line $y(x) = x$. Let point $z$ denote the $x$ value corresponding to this intersection. Then $z$ is a fixed point for function $f$, since $f(z) = y(z) = z$.

**Definition 3.6** (Lipschitz continuity)**.** A real-valued function $f : X \to \mathbb{R}$ is *$L$-Lipschitz* if for all $x, y \in X$, $|f(x) - f(y)| \leq L \cdot |x - y|$. We say $f$ is *Lipschitz continuous* if there is a positive constant $L$ such that $f$ is $L$-Lipschitz. We say that $f$ is a *constant function* if and only if $f$ is 0-Lipschitz.

**Definition 3.7** (Contractive Mapping)**.** A *contractive mapping* is a function $f : X \to X$ with the property that $f$ is Lipschitz continuous with constant $0 \leq L < 1$.

**Definition 3.8** (Monotone mixture)**.** A *monotone mixture* $f$ with *kernel* $g : X \to X$ is a function $f(x) = \alpha \cdot g(x) + (1 - \alpha) \cdot x$ where the kernel is nonconstant, nonincreasing and $\alpha \in [0, 1]$ is the convergence parameter.

**Observation 3.9.** *If $f(x) = \alpha g(x) + (1 - \alpha)x$, then $x$ is a fixed point for $f$ if and only if $x$ is a fixed point for $g$.*

*Proof.* Assume $x = f(x)$, then $g(x) = x$. Conversely, assume $x = g(x)$, then $f(x) = x$. $\square$

Thus, for any continuous nonincreasing function $g$, we can use Observation 3.9 to construct a function $f$ that has the same fixed point as $g$. Then, we can search for a fixed point for $g$ by searching for a fixed point for $f$. For this, we use the following well known fact:

**Lemma 3.10.** *If $f(x) = \alpha g(x) + (1 - \alpha)x$ is a monotone mixture with a nonconstant $L$-Lipschitz kernel $g$, then for all $0 \leq \alpha \leq \frac{1}{L+1}$, $f$ is $(1 - \alpha)$-Lipschitz. Additionally, if $f$ maps $X$ to itself, the restriction of $f$ to $X$ is a contractive mapping.*

*Proof.* Fix $x, y \in X$ and w.l.o.g, assume $x < y$, then $g(x) \geq g(y)$ is nonincreasing and

$$\begin{aligned}
|f(x) - f(y)| &= |\alpha(g(x) - g(y)) + (1 - \alpha)(x - y)| \\
&= |\alpha(g(x) - g(y)) - (1 - \alpha)(y - x)| \\
&\leq \max\{\alpha|g(x) - g(y)|, (1 - \alpha)|x - y|\} \\
&\leq \max\{\alpha L|x - y|, (1 - \alpha)|x - y|\} \\
&\leq (1 - \alpha)|x - y|.
\end{aligned}$$

The last step is from the assumption $\alpha \cdot L + \alpha \leq 1$. This proves $f$ is $(1 - \alpha)$-Lipstchitz. For the "additionally" part, if $f$ maps $X$ to itself, the fact $g$ is non-constant implies $L > 0$, thus $\alpha < 1$ and the restriction of $f$ to $X$ is a contraction. $\square$

**Lemma 3.11** (Banach Contraction Principle [20]). *If a real-valued function $f : X \to X$ is a contraction, then $f$ has a unique fixed point $x^*$. To find $x^*$, start at any $x_0$, then* $\lim_{n\to\infty} f^n(x_0) = x^*$.

Thus, if we design a DPP mechanism $(\vec{x}, \vec{p}, T)$ such that for distribution $F^n$, the expected value $E_T$ is a monotone mixture with a $L$-Lipschitz kernel and convergence parameter $\alpha \leq \frac{1}{L+1}$, we get that $(\vec{x}, \vec{p}, T)$ is asymptotically stable with respect to $F^n$.

# 4 A Welfare-Based Dynamic Posted-Price Mechanism

This section describes our first proposal and gives sufficient conditions for our mechanism to be asymptotic stable and obtain a 1/2 approximation of the optimal welfare. To maximize social welfare, we must guarantee the highest-valued transactions are included in each block. The challenge is that whenever there is more than $m$ bidders with bids $b_i \geq q_{t-1}$, the mechanism is not *ex post* IC for bidders when miners use the MVM allocation rule. If we use the RM allocation rule, a low bid may receive a slot in place of a high bid. In this case, the mechanism must increase the posted-price. A welfare-based approach uses bids of allocated bidders as a proxy for the degree of excess demand:

**Definition 4.1** (Welfare-Based update rule). The *$\alpha$-welfare-based update rule* is the update rule:

$$\mathrm{T}_{\mathrm{W}}^{\alpha}(q, B) := \alpha \frac{1}{m} \sum_{i \in B} b_i + (1-\alpha)q, \tag{10}$$

where $\alpha \in [0, 1]$ is the convergence parameter.

Observe that whenever $|B_t| = m$, $q_t = \mathrm{T}_{\mathrm{W}}^{\alpha}(q_{t-1}, B_{t-1}) > q_{t-1}$ unless $b_i = q_t$ for all $i \in B_{t-1}$. Thus the hope is that the mechanism converges to a price $z$ at least as big as the market clearing price — that is, a price where at most $m$ bidders have value $v_i \geq z$.

Unfortunately, miners' myopia is an unreasonable assumption for a dynamic posted-price mechanism with the RM allocation rule and endowed with the welfare-based update rule. To see this, note that if the current price $q_{t-1}$ is smaller than the market-clearing price, there exists a price $q > q_{t-1}$ that also sells to $m$ buyers. Thus under a demand surge, the active miner might have a strict preference for implementing the MVM allocation rule instead of the RM allocation rule to drive prices up for the next time they become the active miner. Once miners signal a preference for adding the highest value bids, each bidder with $v_i \geq q_t$ would have a dominant strategy to bid $b_i > v_i$ to maximize the probability of being selected. Thus the dynamic posted-price mechanism would not be *ex post* IC for myopic bidders.[11]

[11] A possible counterargument to bidders overbidding comes for *Mempools* — a global decentralized database of pending transactions — where Bitcoin and other blockchains store bids until they are processed and added to the blockchain or removed after 48 hours. With Mempools, there is a *carry over* from $M_t \setminus B_t$ to $M_{t+1}$ – i.e., if not served, bidders participate in more than one time step. Thus if a bidder bids $b_i > v_i$ in the hope of increasing their chances of being included in $B_t$, there is a risk their bid will carry over to the next time step. Since there is uncertainty about future prices (since $M_{t+1}, M_{t+2}, \ldots$ are unknown at time $t$), there is a risk bidder $i$ could pay $b_i > v_i$ and receive a negative utility. It is hard to model carry over, and incorporating Mempools in the model is an interesting avenue for future work. Here, we assume each bidder only participates once.

Since a DPP mechanism with the welfare-based update rule and the RM allocation rule reduces to a DPP mechanism with the MVM allocation rule, we study a DPP mechanism endowed with the welfare-based update rule and the MVM allocation rule:

**Definition 4.2** (Welfare-Based Dynamic Posted-Price mechanism)**.** The *welfare-based dynamic posted-price* (WDPP) mechanism is a DDPP mechanism $(\vec{x}, \vec{p}, \mathrm{T}_{\mathrm{W}}^{\alpha})$ endowed with the welfare-based update rule $\mathrm{T}_{\mathrm{W}}^{\alpha}$.

The WDPP mechanism is not *ex post IC*. However, we show, assuming truthful bidding, the WDPP mechanism is asymptotically stable as a warm-up to studying *ex post IC* mechanisms in the following sections.

### 4.0.1 Asymptotic stability of the WDPP mechanism

Next, we show that by setting a sufficiently small $\alpha$, the WDPP mechanism is asymptotically stable and approximately welfare optimal under the mild assumption the revenue curve is Lipschitz continuous.

**Definition 4.3** (Demand Curve)**.** The *demand at price* $q$ is the random variable $N(q) := \sum_{i=1}^{n} \mathbb{1}_{v_i \geq q}$. A *demand curve* is non-increasing real-valued function $D$ mapping a price $q$ to the expected number of buyers $D(q) := \mathbb{E}\left[N(q)\right]$ that would purchase at price $q$. The *demand curve with limited supply* is $\bar{\mathrm{D}}(p) := \mathbb{E}\left[\min\{m, N(q)\}\right]$.

**Definition 4.4** (Revenue Curve)**.** A *revenue curve* is a real-valued function from price $q$ to the expected revenue $\textsc{Rev}(q) := q \cdot \bar{\mathrm{D}}(q)$ when selling a supply of $m$ slots at price $q$.

**Theorem 1.** *If the revenue curve* $\textsc{Rev}$ *is L-Lipschitz and* $\alpha \leq \frac{1}{L/m+1}$*, the WDPP mechanism* $(\vec{x}, \vec{p}, \mathrm{T}_{\mathrm{W}}^{\alpha})$ *is asymptotically stable with respect to* $F^n$ *and has unique equilibrium price* $q^*$*. Moreover, the welfare in the stable equilibrium is* $\textsc{Welfare}(\vec{x}(q^*)) \geq \frac{OPT}{2}$*.*

# 5 An Utilization-Based Dynamic Posted-Price Mechanism

To improve the robustness of the welfare-based dynamic posted-price mechanism to strategic behavior by miners, in turn unraveling the IC property to bidders, we can to remove the influence of bid values on the price update when there is excess demand. That is, we can use a fixed multiplicative price change that is independent of values:

**Definition 5.1** (Utilization-Based Update Rule)**.** The $(\alpha, \delta)$*-utilization-based* update rule is the update rule:

$$\mathrm{T}_{\mathrm{U}}^{\alpha,\delta}(q, B) := \alpha \frac{|B|}{m}(1+\delta)q + (1-\alpha)q. \tag{11}$$

where $\alpha \in (0, 1)$ is the convergence parameter and $\delta \in (0, \infty)$.

The utilization-based update rule with $\delta = 1$ and $\alpha = 1/8$ is the update rule used by EIP-1559 to dynamically set its posted-price. While EIP-1559 uses a first-price auction to choose the allocation when there is excess demand, we adopt as the intended allocation rule the RM allocation rule which, in turn, removes incentives for non-truthful bidding by bidders:

**Definition 5.2** (Utilization-Based Dynamic Posted-Price Mechanism)**.** The *utilization-based dynamic posted-price* (UDPP) mechanism is a RDPP mechanism $\left(\vec{x}, \vec{p}, \mathrm{T}_{\mathrm{U}}^{\alpha,\delta}\right)$ endowed with the utilization-based update rule $\mathrm{T}_{\mathrm{U}}^{\alpha,\delta}$.

**Proposition 5.3.** *The RDPP is ex post IC for myopic bidders and DSIC for myopic miners.*

*Proof.* First, we show the RDPP mechanism is DSIC for myopic miners. For a particular time step, let $M$ denote the set of active bidders and let $q$ denote the current posted-price. The active miner maximizes utility by selecting a maximal allocation from $M(q)$, and any maximal allocation weakly dominates all other allocations. Thus choosing a uniformly random maximal allocation is a weakly dominant strategy. This proves the RDPP mechanism is DSIC for myopic miners.

Next, we show the RDPP mechanism is *ex post* IC for myopic bidders. Given that miners select a uniformly random maximal allocation from $M(q)$, we first consider the case bidder $i$ has value $v_i < q$. If bidder $i$ bids $b_i \geq q$, there is a positive probability the active miner select bidder $i$ to receive a slot and pay $q$ resulting in a negative utility. Thus bidding $v_i$ strictly dominates bidding $b_i \geq q$ and weakly dominates bidding $b_i \in (v_i, q)$. Next, suppose bidder $i$ has value $v_i \geq q$. For bidder $i$ to receive a slot and pay $q$, she must bid $b_i \geq q$. Thus bidding $v_i$ strictly dominates bidding $b_i < q$. For any bid $b_i \geq q$, bidder $i$ has equal probability of winning a slot and paying $q$. Thus bidding $v_i$ weakly dominates bidding $b_i > v_i$. This proves truthful bidding weakly dominates bidding $b_i \neq v_i$, and the mechanism is IC for myopic bidders. □

**Corollary 5.4.** *The UDPP mechanism is* ex post *IC for myopic bidders and DSIC for myopic miners.*

*Remark.* Note a DPP mechanism with the welfare-based update rule, and the RM allocation rule (Definition 2.15) is also DSIC for myopic miners. However, the crucial difference is that there is a clear and sensible out-of-model deviation by non-myopic miners to that rule, while this deviation has gone away in the new design.

Interestingly, the fact the UDPP mechanism ignores bid values when there is excess demand, which is important for incentive alignment, can lead to instability in instances in which the welfare-based dynamic-posted mechanism is asymptotically stable. This motivates the study of more stable update rules in Section 6.

**Proposition 5.5.** *There exists a distribution $F^n$ where the WDPP mechanism $(\vec{x}, \vec{p}, \mathrm{T}_{\mathrm{W}}^{\alpha})$ is asymptotically stable, but the UDPP mechanism $\left(\vec{x}, \vec{p}, \mathrm{T}_{\mathrm{U}}^{\alpha,\delta}\right)$ is unstable.*

*Proof.* For any positive $v$, let $F$ be the distribution where each bidder has value $v$ with probability 1. Suppose there is a single slot for sale and two bidders drawn i.i.d. from $F$

in each time step. For the UDPP mechanism, if the current price $q_t \leq v$, the mechanism observes excess demand the subsequent price increases to $q_t(1+\alpha\delta)$. However, when the current price $q_t > v$, neither bidder will purchase, and the subsequent price decreases to $q_t(1-\alpha)$. This repeats *ad infinitum*, and the utilization-based update rule is unstable with respect to $F^n$.

For the welfare-based dynamic posted-price mechanism, whenever the current price $q_t > v$, neither bidder will purchase, and the subsequent price decreases to $q_t(1-\alpha)$. Thus eventually, the mechanism reaches a price $q_t \leq v$. Whenever the current price $q_t \leq v$, the active miner allocates a single slot and the subsequent price increases to $q_t + \alpha(v - q_t)$ where $v - q_t \geq 0$ is the surplus of the mechanism. Thus the subsequent price is $q_t < q_{t+1} = \alpha v + (1-\alpha) q_t \leq v$ whenever $q_t < v$ (and $q_t = v$ whenever $q_t = v$). By induction, we get that for all time steps $n \geq t$, $q_t \leq v$, and one bidder receives the slot. The sequence $q_t, q_{t+1}, \ldots$ is increasing and bounded by $v$. From completeness of the Euclidean space, the sequence has a limit point $z \leq v$. This proves the welfare-based update rule is asymptotically stable with respect to $F^n$. See Figure 4 for an empirical example of this behavior. $\square$

# 6 The Truncated Welfare-Based Dynamic Posted-Price Mechanism

In this section, we propose the *Truncated Welfare-Based Dynamic Posted-Price* (TWDPP) mechanism that combines desirable features of the WDPP and the UDPP mechanisms. In particular, whenever $m$ or more bidders receive a slot, TWDPP behaves like the UDPP mechanism. Whenever less than $m$ bidders receive a slot, we use bid values to compute the subsequent price just like the WDPP mechanism, but to reduce the variance of the update rule, we will cap how much each bid contributes to the subsequent price:

**Definition 6.1** (Truncated Welfare-Based Update Rule)**.** The *truncated* $(\alpha, \delta)$*-welfare-based* update rule is the update rule:

$$\mathrm{T}_{\mathrm{TW}}^{\alpha,\delta}(q, B) := \begin{cases} \alpha \frac{1}{m} \sum_{i \in B} \min\{b_i, (1+\delta) \cdot q\} + (1-\alpha) \cdot q & \text{for } |B| < m, \\ \alpha(1+\delta) \cdot q + (1-\alpha) q & \text{for } |B| = m, \end{cases} \tag{12}$$

where $\alpha \in (0,1)$ is the convergence parameter and $\delta \in (0, \infty)$ is the truncation parameter.[12]

**Definition 6.2** (Truncated Welfare-Based Dynamic Posted-Price Mechanism)**.** The *truncated welfare-based dynamic posted-price* (TWDPP) mechanism is a RDPP mechanism $(\vec{x}, \vec{p}, \mathrm{T}_{\mathrm{TW}}^{\alpha,\delta})$ endowed with the truncated welfare-based update rule $\mathrm{T}_{\mathrm{TW}}^{\alpha,\delta}$.

Because the TWDPP mechanism uses the RM allocation rule, from Proposition 5.3, we directly obtain:

**Theorem 2.** *The TWDPP mechanism is* ex post *IC for myopic bidders and DSIC for myopic miners.*

[12] An alternative update rule could always round $b_i$ to the interval $[(1-\delta)q, (1+\delta)q]$ so that $T(q, B) = \alpha \frac{1}{m} \sum_{i \in B} \max\{\min\{b_i, (1+\delta)q\}, (1-\delta)q\} + (1-\alpha) \cdot q$. Here we study the update rule in Equation 12 to exclude out-of-model deviations where miners prefer to include higher value bids whenever $|B| = m$.

Recall from Proposition 5.5, there is a distribution where the UDPP mechanism is unstable, but the WDPP mechanism is stable. The following proposition implies there is a distribution $F^n$ where the UDPP is unstable even when the demand $n$ is smaller than the supply $m$. At the same time, the TWDPP mechanism is asymptotically stable with respect to $F^n$.

**Proposition 6.3.** *There exists a distribution $F^n$ with $n < m$ where the TWDPP mechanism $\left(\vec{x}, \vec{p}, \mathrm{T}^{\alpha,\delta}_{\mathrm{TW}}\right)$ is asymptotically stable, but the UDPP $\left(\vec{x}, \vec{p}, \mathrm{T}^{\alpha,\delta}_{\mathrm{U}}\right)$ mechanism is unstable.*

To study the stability of the TWDPP mechanism, we define the expected value of the random operator $\mathrm{T}^{\alpha,\delta}_{\mathrm{TW}}(q, \mathit{Unif}(2^{M(q)}))$:

$$E_{\mathrm{T}^{\alpha,\delta}_{\mathrm{TW}}}(q) := \alpha\, \mathrm{K}_{\mathrm{TW}}(q) + (1-\alpha)q, \tag{13}$$

where $\mathrm{K}_{\mathrm{TW}}$ is the kernel of the TWDPP mechanism:

$$\mathrm{K}_{\mathrm{TW}}(q) := \mathbb{E}\left[\frac{1}{m}\sum_{i=1}^{n} \min\{v_i, (1+\delta)q\} \cdot x_i(q) \cdot \mathbb{1}_{N(q)<m} + (1+\delta)\cdot q \cdot \mathbb{1}_{N(q)\geq m}\right], \tag{14}$$

where the expected value is taken over the values $v_1, v_2, \ldots, v_n$ and random allocation $\mathit{Unif}(2^{M(q)})$. Recall $x_i(q) = 1$ if bidder $i$ with $v_i \geq q$ receives a slot and $N(q) = \sum_{i=1}^{n} \mathbb{1}_{v_i \geq q}$.

## 6.1 Stability

Because the kernel $\mathrm{K}_{\mathrm{TW}}$ is neither increasing nor decreasing, we cannot directly apply the proof sketch in Section 3.1 to show the TWDPP mechanism is asymptotically stable. Instead, we will show the fixed-point iteration on $E_{\mathrm{T}^{\alpha,\delta}_{\mathrm{TW}}}$ starting from a positive $q_0$ converges to a fixed point under the assumption $\mathrm{K}_{\mathrm{TW}}$ is Lipschitz continuous and strictly concave.

**Definition 6.4** (Concave function)**.** A real-valued function $f : X \to \mathbb{R}$ is *concave* if for any $x \neq y \in X$ and $0 < \alpha < 1$, $f((1-\alpha)x + \alpha y) \geq (1-\alpha)f(x) + \alpha f(y)$, and *strictly concave* if we have a strict inequality.

Here, we show that for a function $f$ satisfying Assumption 1, executing the fixed-point iteration on $g(x) = \alpha f(x) + (1-\alpha)x$ (for some positive $\alpha < 1$) starting from a positive $x_0$ converges to a fixed point of $f$.[13]

**Assumption 1.** *Suppose $X = [0, \bar{a}] \neq \emptyset$ is a finite interval and $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is a real-valued function satisfying:*

*(i) $f$ is L-Lipschitz,*

*(ii) The restriction of $f$ to $X$ is strictly concave, and*

[13]It is known that iterating a increasing function $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ will either converge to a fixed-point or diverge [14]. In Section 3.1, we showed that if $f$ is decreasing and Lipschitz continuous, then the fixed-point iteration of $g(x) = \alpha f(x) + (1-\alpha)x$ will converge to a unique fixed point by setting a sufficiently small positive $\alpha$. In other words, we replace the monotonicity assumption by the assumption $f$ is strictly concave.

*(iii)* $f(x) = 0$ *for all* $x \geq \bar{a}$.

The main idea is to reduce the problem of computing a fixed point of $f$ satisfying Assumption 1 to finding a fixed point for another function $g$ satisfying Assumption 2 such that $x$ is a fixed point of $f$ if and only if $x$ is a fixed point of $g$. The main observation is that whenever $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is nonincreasing on some interval $D \subseteq \mathbb{R}_{\geq 0}$, we can force the restriction of $g$ to $D$ to be Lipschitz continuous with Lipschitz constant $L < 1$ by using a similar argument from Lemma 3.10. We can leverage this fact to show that the restriction of $g$ to some rectangle $[a, b] \subseteq D$ is a contraction — i.e., $g$ maps $[a, b]$ to itself and the restriction of $g$ to $[a, b]$ has Lipschitz constant $L < 1$. Then, we show that iterating $g$ starting from any positive $x_0$ will either converge to a point outside $[a, b]$ or eventually visit a point $x_t \in [a, b]$. The moment $x_t \in [a, b]$ for some $t$, from Banach contraction principle and the fact the restriction of $g$ to $[a, b]$ is a contractive mapping implies the fixed point iteration of $g$ starting from $x_t$ will converge to a unique fixed point contained in $[a, b]$.

**Lemma 6.5.** *If* $f : X \to X$ *satisfies Assumption 2, then the fixed-point iteration of* $f$ *starting from any* $x_0 \in X$ *converges to a fixed point of* $f$.

**Assumption 2.** *Assume* $f : X \to X$ *with nonempty interval* $X = [0, \bar{a}]$ *is a real-valued function satisfying:*

*(i)* $f$ *is strictly concave and Lipschitz continuous,*

*(ii)* $f(x) \geq 0$ *for all* $x \in X$,

*(iii) Let* $\bar{x} = \sup_{x \in X} f(x)$. *Strict concavity implies* $f$ *is strictly increasing on interval* $I = [0, \bar{x})$ *and strictly decreasing on interval* $D = [\bar{x}, \sup X]$. *Then assume the restriction of* $f$ *to* $D$ *is* $L$*-Lipschitz with* $L < 1$ *and*

*(iv) There is a positive* $b \in X$ *such that* $f(b) < b$.

**Lemma 6.6.** *Let* $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ *be a function satisfying Assumption 1. By setting* $0 \leq \alpha \leq \frac{1}{L+1}$, *the function* $g(x) = \alpha f(x) + (1 - \alpha)x$ *satisfies Assumption 2. Then, the fixed-point iteration of* $g$ *starting from any positive* $x_0$ *converges to a fixed point of* $f$.

We defer the proof of the Lemmas to Appendix C.1. In Example C.13, we run simulations demonstrating the fixed-point iteration described in Lemma 6.6.

Lemma 6.6 immediately implies that if the kernel $\mathrm{K}_{\mathrm{TW}}$ is Lipschitz continuous and strictly concave on a bounded interval $[0, \bar{a}]$, the TWDPP mechanism is asymptotically stable. We can now state our main theorem.

**Theorem 3.** *Assume the distribution* $F$ *is supported on interval* $[0, \bar{a}]$ *and the distribution* $F^n$ *induces the kernel* $\mathrm{K}_{\mathrm{TW}}$ *to be* $L$*-Lipschitz and strictly concave on interval* $[0, \bar{a}]$. *Then for any* $\alpha \leq \frac{1}{L+1}$, *the TWDPP mechanism is asymptotically stable with respect to* $F^n$.

*Proof.* We first check $\mathrm{K}_{\mathrm{TW}}$ satisfy all the bullets in Assumption 1. The first and second properties are clear. For the third property, $\mathrm{K}_{\mathrm{TW}}(q) \geq 0$, and observe no bidder purchases at price $\geq \bar{a}$. Thus $1 - F(q) = 0$ and $\mathrm{K}_{\mathrm{TW}}(q) = 0$ for all $q \geq \bar{a}$. This proves $\mathrm{K}_{\mathrm{TW}}$ satisfies Assumption 1. From Lemma 6.6, for any $\alpha \leq \frac{1}{L+1}$, the fixed-point iteration of

$$E_{\mathrm{T}^{\alpha,\delta}_{\mathrm{TW}}}(q_0) = \alpha\, \mathrm{K}_{\mathrm{TW}}(q_0) + (1-\alpha) q_0$$

starting from positive $q_0$ converges to a fixed point $q^*$. This proves the intended TWDPP mechanism is asymptotically stable. □

## 6.2 Welfare Guarantee at Equilibrium

Because the active miner selects a random maximal allocation whenever $N(q) > m$, it is more challenging to show the TWDPP mechanism is approximately welfare optimal. That is because the social welfare is not a monotone function of the posted-price: as the posted-price decreases, the welfare might decrease because the active miner has a higher chance to allocate block space to a lower bid instead of a higher bid. The main idea is to show that if $q$ is an equilibrium price, the probability the demand $N(q) \geq m$ is at most $1/(1+\delta)$. Whenever the demand $N(q) \leq m$, miners deterministically allocate slots to the top $N(q)$ bidders. Thus we will show the welfare loss from the cases where $N(q) > m$ is a constant fraction of the optimal welfare.

**Theorem 4.** *If $q$ is an equilibrium price of the TWDPP mechanism $\left(\vec{x}, \vec{p}, \mathrm{T}^{\alpha,\delta}_{\mathrm{TW}}\right)$, then*

$$\textsc{Welfare}(\vec{x}(q)) \geq \frac{OPT}{2(1+\delta)} \min\{1, \delta\}.$$

By setting $\delta = 1$, we get that the TWDPP mechanism obtains $1/4$ of the optimal welfare at equilibrium.

# 7 Experimental Results

In this section, we provide experimental results supporting our theoretical findings. We simulate the following dynamic-posted price mechanisms:

- *Welfare-Based Dynamic Posted-Price* (WDPP) mechanism $(\vec{x}, \vec{p}, \mathrm{T}^{\alpha}_{\mathrm{W}})$: the deterministic dynamic posted-price mechanism with the maximum value maximal allocation rule and the welfare-based update rule.

- *Utilization-Based Dynamic Posted-Price* (UDPP) mechanism $\left(\vec{x}, \vec{p}, \mathrm{T}^{\alpha,\delta}_{\mathrm{U}}\right)$: the randomized dynamic posted-price mechanism with the random maximal allocation rule and the utilization-based update rule.

- *Truncated Welfare-based Dynamic Posted-Price* (TWDPP) mechanism $\left(\vec{x}, \vec{p}, \mathrm{T}^{\alpha,\delta}_{\mathrm{TW}}\right)$: the randomized dynamic-posted-price mechanism with the random maximal allocation rule and the truncated welfare-based update rule.

Note while UDPP and TWDPP mechanisms and are *ex post* IC, the WDPP mechanism is not. However, for the simulations, we always assume truthful bidding. Recall UDPP mechanism is equivalent to EIP-1559 assuming bidder $i$ bids $b_i = 0$ and submit a bid cap $c_i = v_i$.

For the experimental setup, each time step $t$, $n_t$ bidders are drawn i.i.d. from distribution $F_t$. We use the same random seed across all mechanisms to ensure a valid comparison across the same population. We set the convergence parameter $\alpha = 1/16$. Smaller $\alpha$ decreases the price variance and expands the class distribution where our mechanisms are asymptotically stable. We set the truncation parameter $\delta = 1$. Smaller $\delta$ reduces how much each bid contributes to increasing the subsequent price.

Throughout the simulation, we track three quantities in each time step $t$: the demand $n_t$, the posted-price $q_t$, and the ratio between the achieved welfare $\sum_{i \in B_t} v_i$ and the optimal welfare $\sum_{i=1}^{n_t} v_i \cdot x_i^*(\vec{v}_t)$ where $\vec{v}_t$ is drawn from distribution $F_t^{n_t} = \underbrace{F_t \times \ldots \times F_t}_{n_t \text{ times.}}$.

## 7.1 Excess demand

Here, we consider the case with constant demand $n_t = 200$ above the supply of $m = 100$ for three value distributions: a uniform distribution over 0 to 200, an exponential distribution with mean of 100, and a scaled and shifted Pareto distribution with a median around 100. We give the results in Figure 1.

The WDPP mechanism has the fastest convergence for distributions with a low variance but is highly volatile when the distribution has high variance (e.g., Pareto distribution). High price volatility makes the bidder myopia toothless since bidders might time their entry in the auction. Because the UDPP mechanism ignores bid values, it converges to a higher average price than the TWDPP mechanism yielding lower welfare. This phenomenon can be observed clearly for the exponential distribution. Because the TWDPP best adapts to the case where values have high and low variance, the TWDPP mechanism achieves the best empirical welfare.

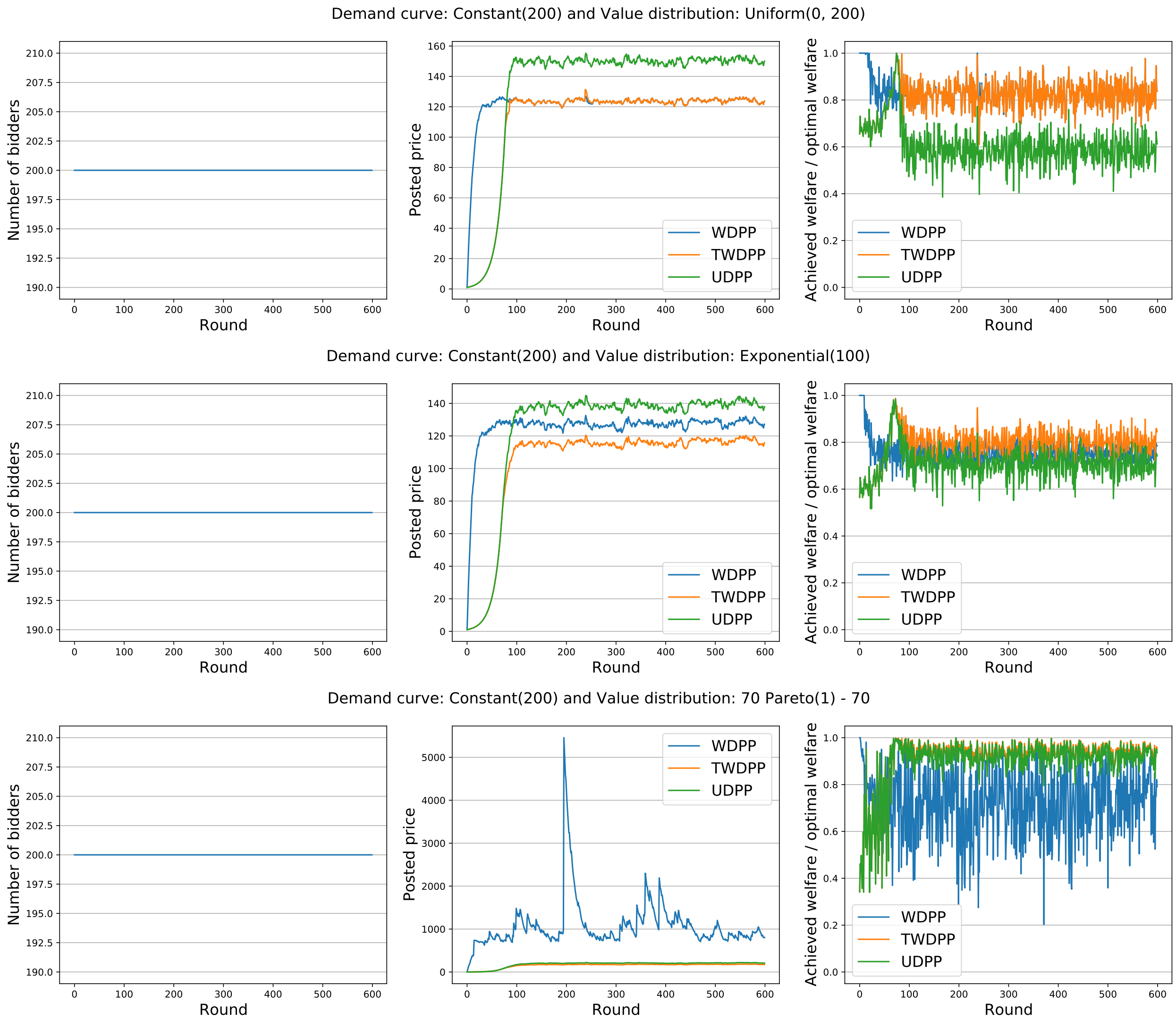


Figure 1: Constant demand $n_t = 200$ for all $t$, constant supply $m = 100$, and uniform, exponential, and Pareto distributions.

## 7.2 Under demand

Here we replicate the experiments from Section 7.1 but with demand $n_t = 67$ smaller than the supply $m = 100$. When the demand is lower than the supply, the market-clearing price is 0. In general, we cannot expect our mechanisms to converge to a posted-price of 0, but we can hope the mechanisms to converge to a price that sells to all almost all bidders. We give the results in Figure 2.

Unfortunately, the WDPP mechanism continues to have high price volatility, which contributes to low welfare on average. Both the UDPP and the TWDPP mechanisms sell to almost all bidders, with the TWDPP having slightly higher welfare because it converges to a lower average price.

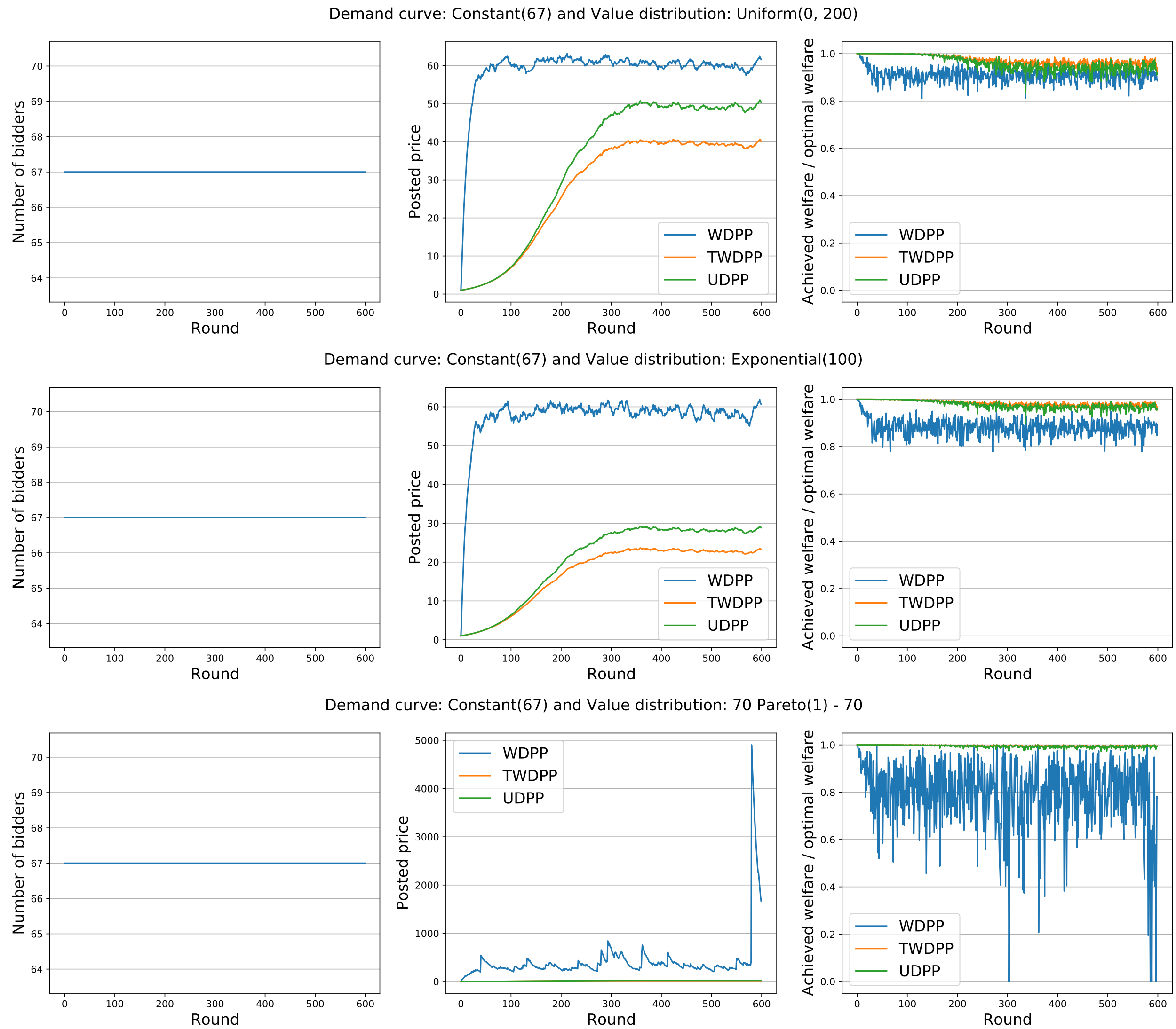


Figure 2: Constant demand $n_t = 67$ for all $t$, constant supply $m = 100$, and uniform, exponential, and Pareto distributions.

## 7.3 Demand shocks

We repeat the experiments from Section 7.1 with a demand shock: initially, the demand is of 200 transactions, jumps to 600, and returns to 200 transactions per time step. The results are given in Figure 3.

We observe all mechanisms converge quickly to an price equilibrium under demand shock. During demand shock, the WDPP mechanism's instability increases for distributions with high variance (e.g., Pareto distribution). The TWDPP has strictly higher welfare for all value distributions because it converges to an average price closer to the market-clearing price.

We observe that the TWDPP mechanism can have price volatility when values a drawn from the uniform distribution over $[0, 200]$. That happens because whenever a block is full, the TWDPP mechanism uses the utilization-based update rule. Thus when the TWDPP reaches a price $q$ close to 175, there is a high probability at least $m$ bidders with values above $q$ causing the subsequent to increase to $q(1+\alpha)$. However, this instability is unpredictable (differently from the instability we will observe in Section 7.4) and even under instability, the TWDPP mechanism extracts higher welfare than the UDPP mechanism.

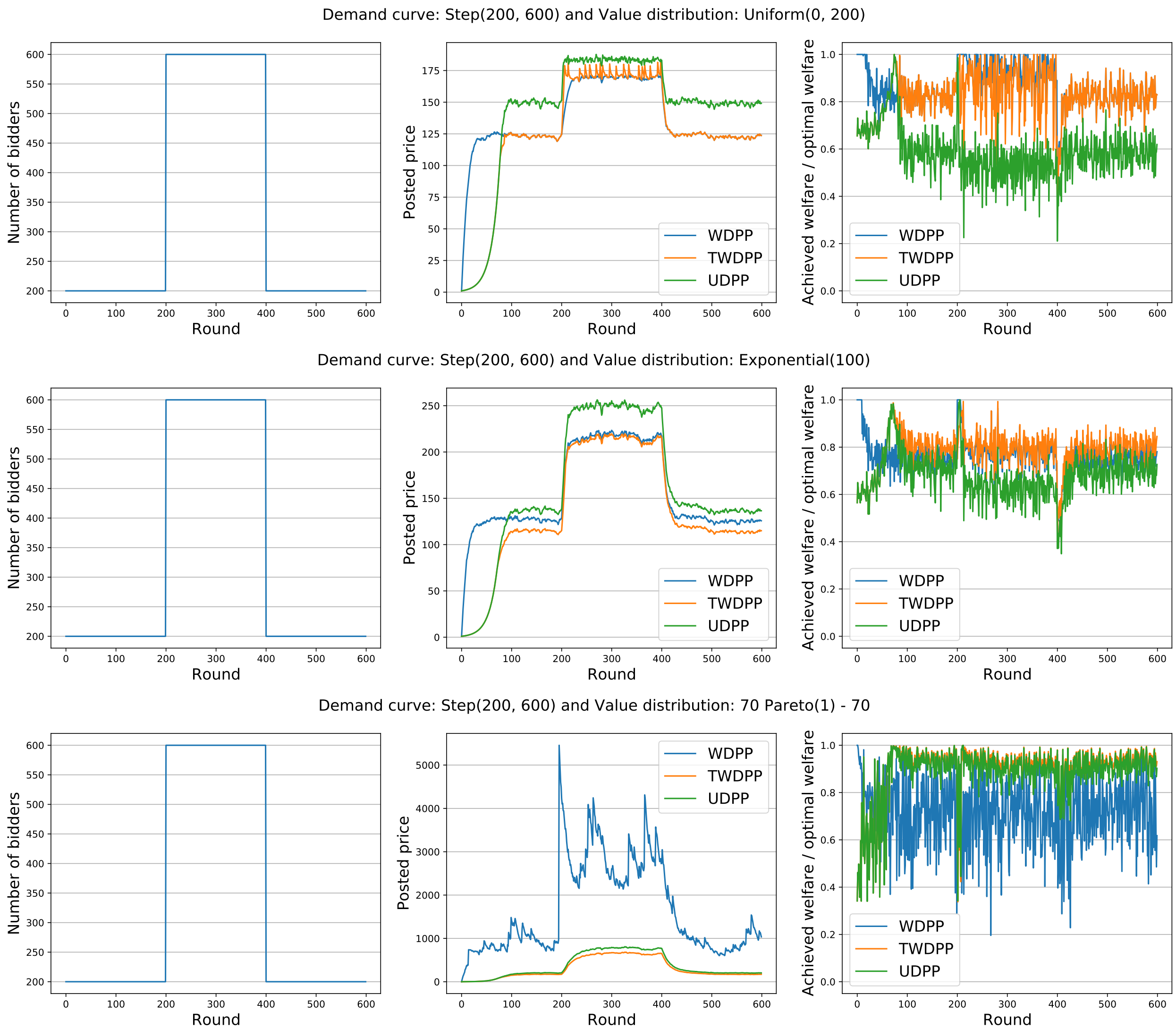


Figure 3: The demand follows a step function with initial demand at 200, then jumping to 600. Fixed supply of $m = 100$ slots per time period, and uniform, exponential, and Pareto value distributions.

## 7.4 Instability of EIP-1559 utilization-based update rule

This section considers the case where all bidders have a deterministic value of 100. The experiment in Figure 4 serves as empirical support for Proposition 5.5. It provides an example of a distribution where the WDPP mechanism is asymptotically stable, but the utilization-based update rule from EIP-1559 is unstable (the UDPP mechanism).

From the experiment, we observe the WDPP converges to a stable price at 100 while the UDPP mechanism oscillates around 100. The price oscillation weakens the bidder's myopic assumption. In particular, a patient bidder would wait to enter a bid only when the price is below 100. For this example, one can check the TWDPP mechanism is also unstable because the truncated welfare-based update rule reduces to the welfare-based update rule.

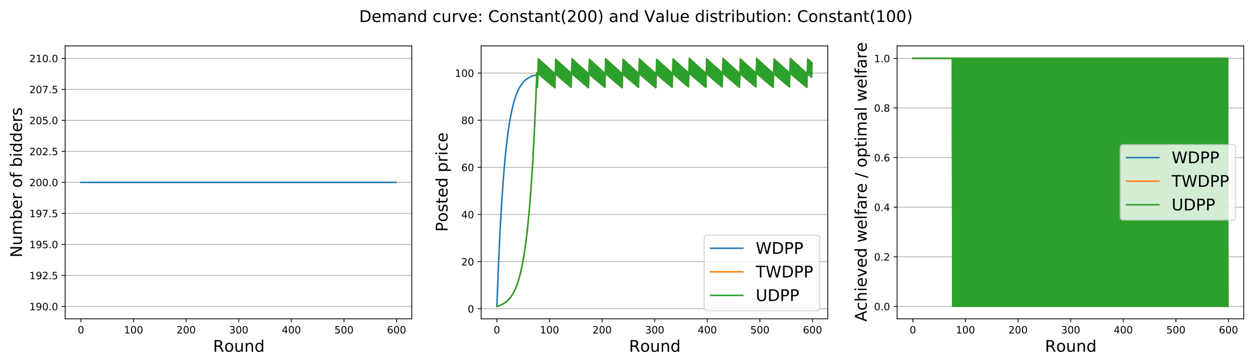


Figure 4: Simulation with constant demand $n = 200$, constant supply $m = 100$, and all bidders have value $v = 100$.

Next, we modify the example in Figure 4 and consider the case where the demand is smaller than the supply. The experiment in Figure 5 serves as an empirical support for Proposition 6.3. It provides an example of a distribution where the WDPP and the TWDPP mechanism are asymptotically stable, but the UDPP is unstable even when demand is lower than the supply.

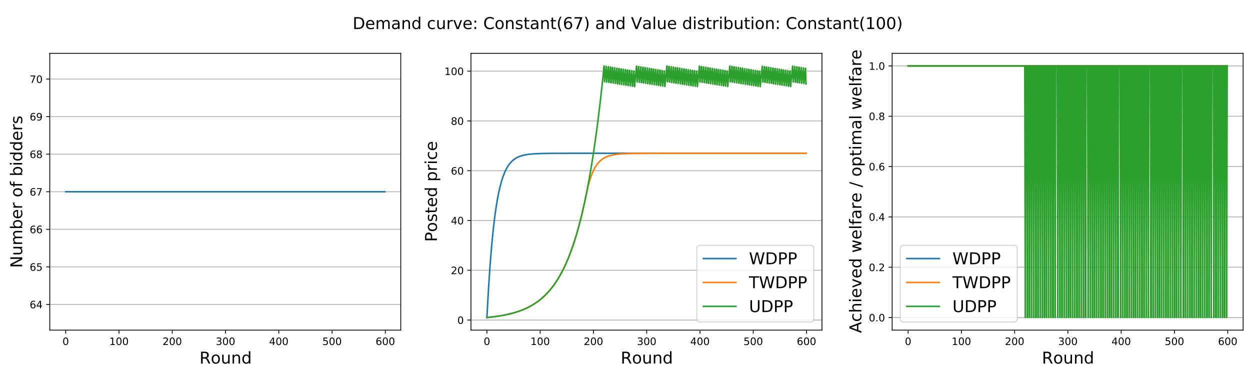


Figure 5: Simulation with constant demand $m = 67$, constant supply $m = 100$, and all bidders have value $v = 100$.

# 8 Conclusion

First-price auctions have been the standard transaction-fee mechanisms for blockchains since Bitcoin's inception. While incentive compatible for miners, first-price auctions provide a bad user experience, with bidders often finding it difficult to estimate how much they need to bid to get their transactions accepted. Typical alternatives from mechanism design theory do not work in the decentralized setting because miners cannot commit to implement the intended auction.

The question, then, is how to design decentralized transaction-fee mechanisms that provide a good user experience and are at the same time robust to manipulation by miners. The Ethereum community has proposed EIP-1559, which reduces to a first-price auction whenever the demand at the current posted-price exceeds the supply. However, whenever demand is lower than the supply, EIP-1559 reduces to a dynamic posted-price mechanism similar to those we study.

We have proposed the *Truncated Welfare-based Dynamic Posted-Price (TWDDP) mechanism*. The TWDDP mechanism satisfies a series of desirable properties. Unlike other proposals, the mechanism is incentive compatible for myopic bidders and dominant strategy incentive compatible for myopic miners even under market instability. It also converges to an equilibrium price under a general assumption. At this equilibrium, the mechanism is approximately welfare optimal. Our experimental results confirm our theoretical findings even for the setting where demand changes over time.

## 8.1 Future work

This line of work leaves many relevant open questions. As with previous work, we study transaction-fee mechanisms under the assumption that miners are myopic because mining is decentralized. However, as blockchain mining becomes centralized through mining pools, miners might be motivated to take on non-myopic strategies. Thus it is relevant to understand *how much revenue non-myopic strategies can improve miner's revenue?* Miners are more likely to deviate from the intended mechanism if deviations are both easy to implement and sufficiently profitable. Showing that miners cannot significantly boost revenue through deviations is evidence miners would not deviate in practice.

For example, miners could collude with impatient bidders whenever there is excess demand and circumvent our randomized allocation by coordinating payments outside the blockchain. If *all miners* and *all bidders* collude in this fashion, our dynamic posted-price mechanism will reduce to EIP-1559. However, if a dynamic-posted mechanism already converges to a posted-price mechanism that is approximately revenue optimal and collusion is costly[14], miners might be less motivated to collude.[15] On the other hand, a mechanism (like

[14]An example of costly deviation is when active miners must construct an infrastructure to collect payments outside the blockchain from a significant fraction of bidders. Additionally, miners might be inclined against publicly announcing they are deviating from the intended mechanism.

[15]It is known posted-price mechanisms can provide 1/2 approximation of the optimal revenue [15]. In this work, we give no revenue guarantees for dynamic posted-price mechanisms. Instead, we focus on providing welfare guarantees, but providing revenue guarantees at equilibrium is a relevant question for future work related to the likelihood o miner deviation.

EIP-1559) that awards miners a negligible fraction of the auction's revenue, miners might be motivated to deviate from the intended mechanism, with nonadoption being the most immediate deviation.

Selfish mining is another example of non-myopic miner's behavior [9]. In this work, we assume there are no forks in the blockchains. Because the number of blocks that one can include in the longest path up to time $T$ is finite, a non-myopic miner might have as objective maximizing their fraction of all revenue over the long time horizon under the assumption blocks provide uniform revenue. For example, miners can improve their fraction of the revenue by forking the blockchain and forcing other miners to lose revenue [21, 11]. As miners' revenue from transaction fees increases, revenue is poised not to be uniform across blocks. One relevant question is to understand *how the transaction fee mechanism modifies optimal strategies when miners are maximizing their fraction of the revenue?*[16]

Beyond transaction fee mechanisms for blockchains, credibility in auctions are a topic of increasing concern. Akbarpour and Li [2] shows credible auctions for multi-item auctions satisfying matroid constraints and for common value auctions. However, it is unknown how to implement incentive-compatible multi-item auctions in more general settings. In particular, developing credible knapsack auctions finds applications in the design of transaction fee mechanisms. In this work, we assume all transactions take the same space in blocks. However, blockchains that support smart contracts allow transactions of arbitrary size. Thus one relevant direction is to design transaction fee mechanisms with knapsack constraints.

# References


[1] 2020. EIP-1559 Community Outreach Report. `https://medium.com/ethereum-cat-herders/eip-1559-community-outreach-report-aa18be0666b5/`. Accessed: 2021-02-11.

[2] Mohammad Akbarpour and Shengwu Li. 2020. Credible auctions: A trilemma. *Econometrica* 88, 2 (2020), 425–467.

[3] Soumya Basu, David Easley, Maureen O'Hara, and Emin Sirer. 2019. Towards a functional fee market for cryptocurrencies. *Available at SSRN 3318327* (2019).

[4] Vitalik Buterin, Eric Conner, Rick Dudley, Matthew Slipper, and Ian Norden. [n.d.]. Ethereum Improvement Proposal 1559: Fee market change for ETH 1.0 chain. `https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1559.md`.

[5] Miles Carlsten, Harry Kalodner, S Matthew Weinberg, and Arvind Narayanan. 2016. On the instability of bitcoin without the block reward. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. 154–167.

[6] Lothar Collatz. 2014. *Functional analysis and numerical mathematics.* Academic Press.


[16] Carlsten et al. [5] considers the case where: miners receive revenue exclusively from transaction fees, and the demand for block space is smaller than the supply. In this setting, even myopic miners might prefer to fork the blockchain to maximize revenue.

[7] Benjamin Edelman and Michael Ostrovsky. 2007. Strategic bidder behavior in sponsored search auctions. *Decision support systems* 43, 1 (2007), 192–198.

[8] Benjamin Edelman, Michael Ostrovsky, and Michael Schwarz. 2007. Internet advertising and the generalized second-price auction: Selling billions of dollars worth of keywords. *American economic review* 97, 1 (2007), 242–259.

[9] Ittay Eyal and Emin Gün Sirer. 2014. Majority is not enough: Bitcoin mining is vulnerable. In *International conference on financial cryptography and data security*. Springer, 436–454.

[10] Matheus VX Ferreira and S Matthew Weinberg. 2020. Credible, Truthful, and Two-Round (Optimal) Auctions via Cryptographic Commitments. In *Proceedings of the 21st ACM Conference on Economics and Computation*. 683–712.

[11] Matheus VX Ferreira and S Matthew Weinberg. 2021. Proof-of-stake Mining Games with Perfect Randomness. In *Manuscript submitted for publication*.

[12] Andrew V Goldberg, Jason D Hartline, Anna R Karlin, Michael Saks, and Andrew Wright. 2006. Competitive auctions. *Games and Economic Behavior* 55, 2 (2006), 242–269.

[13] Gerd Herzog and Peer Chr Kunstmann. 2013. A fixed point theorem for decreasing functions. *Numerical Functional Analysis and Optimization* 34, 5 (2013), 530–538.

[14] John Kennan. 2001. Uniqueness of positive fixed points for increasing concave functions on Rn: An elementary result. *Review of Economic Dynamics* 4, 4 (2001), 893–899.

[15] Robert Kleinberg and S Matthew Weinberg. 2012. Matroid prophet inequalities. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*. 123–136.

[16] Ron Lavi, Or Sattath, and Aviv Zohar. 2019. Redesigning Bitcoin's fee market. In *The World Wide Web Conference*. 2950–2956.

[17] Roger B Myerson. 1981. Optimal auction design. *Mathematics of operations research* 6, 1 (1981), 58–73.

[18] Satoshi Nakamoto. 2009. Bitcoin: A peer-to-peer electronic cash system. `http://www.bitcoin.org/bitcoin.pdf`

[19] Tim Roughgarden. 2020. Transaction Fee Mechanism Design for the Ethereum Blockchain: An Economic Analysis of EIP-1559. *arXiv preprint arXiv:2012.00854* (2020).

[20] Halsey Lawrence Royden and Patrick Fitzpatrick. 1988. *Real analysis*. Vol. 32. Macmillan New York.

[21] Ayelet Sapirshtein, Yonatan Sompolinsky, and Aviv Zohar. 2016. Optimal selfish mining strategies in bitcoin. In *International Conference on Financial Cryptography and Data Security*. Springer, 515–532.

[22] Andrew Chi-Chih Yao. 2020. An Incentive Analysis of Some Bitcoin Fee Designs. In *47th International Colloquium on Automata, Languages, and Programming, ICALP* (Saarbruecken). 1:1–1:12.

# A Existing Proposals of Blockchain Transaction Fee Mechanisms

## A.1 EIP-1559

First-price auctions (Definition 2.11) have been the standard transaction fee mechanism since it was first proposed by Nakamoto [18] as the transaction fee mechanism for Bitcoin. Buterin et al. [4]'s proposal is closest to ours since their mechanism is endowed with an update rule for their posted-price. However, their proposal contains a first-price auction component and a posted-price component, and here we study purely dynamic posted-price mechanisms.

**Definition A.1** (EIP-1559 [4])**.** The EIP-1559 is a dynamic mechanism $\left(\vec{x}, \vec{p}, \mathrm{T}_{\mathrm{U}}^{\alpha,\delta}\right)$ endowed with the utilization-based update rule $\mathrm{T}_{\mathrm{U}}^{\alpha,\delta}$ (Definition 5.1) and a initial posted-price $q_0$. Each bidder submits a tuple $(b_i, c_i)$ where $b_i$ is the bid and $c_i$ is a bid cap. Given history $B_1, B_2, \dots, B_{t-1}$ and active bidders $M_t$, the mechanism computes the posted-price $q_t = T(q_{t-1}, B_{t-1})$ for time step $t$. The intended allocation rule allocates slots to the top $m$ bids $b_i$ with $b_i + q_t \leq c_i$. For all bidders that receive a slot, the intended payment rule charges $b_i + q_t$, but miners are paid only $b_i$. Thus the utility of the active miner is

$$u_0^{EIP-1559}(q_t, B_t) := \sum_{i \in B_t} (p_i(B_1, \dots B_t) - q_t).$$

For EIP-1559, Buterin et al. [4] proposes setting $\delta = 1$ in the hope the mechanism converges to an equilibrium that sells $m/2$ of the slots. Formally studying the stability of EIP-1559 is more challenging since truthful bidding is not an *ex post* Nash equilibrium, and any formal analysis would likely require analyzing bidders participating in a Bayesian Nash equilibrium. An alternative approach, is to study EIP-1559 without the first-price auction component. The resulting mechanism is equivalent to the UDPP mechanism we study in Section 5.

## A.2 Monopolistic price auction

We study mechanisms that sell a fixed supply of block slots. Nevertheless, since blockchain space is a digital good [12], it is not obvious why the supply must be fixed a priori. With that in mind, Lavi et al. [16] propose using the *monopolistic price auction* as a transaction fee mechanism, allowing miners to sell an unlimited supply of block slots. They showed the monopolistic price auction is DSIC for myopic miners and approximately IC for myopic bidders when values a drawn i.i.d. from bounded distribution $F = [\bar{a}, \underline{a}]$ and demand $n$ gets large – i.e., $n \to \infty$.

**Definition A.2** (Monopolistic price auction [16])**.** The *monopolistic price auction* is a static mechanism where the allocation rule allows an unlimited supply of slots to be allocated. First, the mechanism order the active bids in increasing order $b_1 < b_2, \dots, < b_\ell$ and let

$$k = \arg\max_i i \cdot b_i.$$

Then, allocate slots to bidders 1 to $k$. All bidders that receive a slot pay $b_k$ to the active miner.

The monopolistic price is DSIC for myopic miners, and Yao [22] showed it is also approximately IC for myopic bidders for any distribution $F$ when the demand $n \to \infty$. Unfortunately, there is an inherent trade-off between having larger blocks and loss in social welfare.[17] Large block sizes result in a more considerable network propagation delay, which increases the chance of forks. As a result, an unlimited supply of slots opens the margin for new denial of service attacks.

## A.3 Random sampling optimal price

Goldberg et al. [12] proposed the *random sampling optimal price* (RSOP) as a randomized truthful mechanism for selling an unlimited supply of items. RSOP mechanism randomly partitions all bids into two groups and runs the monopolistic price auction in each. Lavi et al. [16] propose using RSOP as a transaction fee mechanism but recognizes that it has undesirable properties. Crucially, RSOP has communication complexity $\Omega(n)$ since it requires all bids to be stored on the blockchain.

## A.4 Generalized second-price auction

The *generalized second-price* (GSP) auction [8] orders the bids in increasing order $b_1 > b_2 > \ldots > b_n$ and allocate slots to the top $m$ bidders and bidder $i \in [m]$ pays $b_{i+1}$ (assuming $n \geq m+1$). In the context of transaction fee mechanisms, Basu et al. [3] proposed a modified generalized second-price auction where bidder $i \in [m]$ pays $b_m$. Note their payment rule is identical to the monopolistic price auction but with a fixed supply. To incentivize miners to not include fake bids and inflate the $m$-th highest bid, the mechanism split the revenue for block $B_t$ among the creators of future blocks $B_{t+1}, B_{t+2}, \ldots, B_{t+k}$. As demand and the number of miners increase, the mechanism is approximately incentive compatible for myopic bidders and myopic miners.

An out-of-model consideration pointed-out by Lavi et al. [16] is collusion between an active miner with bidders where both agree to execute payments outside the blockchain. For example, bidder bids $b_i = 0$ but agrees to pay the intended bid outside the blockchain.[18] To motivate bidders to accept the collusion, the miner might divide the revenue with bidders. Moreover, even without colluding with bidders, a miner could create blocks with $m$ fake bids equal to 0 and share the revenue of blocks $B_{t-k}, B_{t-k+1}, \ldots, B_{t-1}$ for free. The active miner loses $1/k$ of the revenue they could obtain by honestly creating block $B_t$. Thus including only fake transactions in blocks is an approximate equilibrium.

[17] Ethereum allows the blockchain protocol to converge to a fixed supply $m$ that is agreed by the majority of miners by allowing each active miner votes to upvote or downvote the supply by 0.1%. Thus one might expect $m$ converges to a block size that balances the trade-offs between latency and supply.

[18] For simplicity, we consider the case where the auction has no reserve price.

# B Omitted Proofs from Section 4

*Proof of Theorem 1.* Recall $x_i(q)$ is the indicator random variable for bidder $i \in [n] = \{1, \ldots, n\}$ with value $v_i$ receiving a slot when the posted-price is $q$. For fixed $\vec{v}$, $x_i(q)$ is nonincreasing function of $q$ because the mechanism always allocates slots to the highest bidders. Assuming truthful bidding, the expected value of $\mathrm{T}^{\alpha}_{\mathrm{W}}(q, B)$ is

$$E_{\mathrm{T}^{\alpha}_{\mathrm{W}}}(q) := \alpha \underbrace{\frac{1}{m}\mathbb{E}\left[\sum_{i=1}^{n} v_i \cdot x_i(q)\right]}_{\text{Kernel } \mathrm{K}_{\mathrm{W}}(q)} + (1-\alpha)q, \tag{15}$$

where the expectation is taken over $\vec{v}$ drawn from $F^n$. From the proof outline in Section 3.1, we first check $E_{\mathrm{T}^{\alpha}_{\mathrm{W}}}$ is a monotone mixture. Note $\mathrm{K}_{\mathrm{W}}(q) = \textsc{Welfare}(\vec{x}(q))/m$ and $\textsc{Welfare}(\vec{x}(q))$ is nonincreasing function of $q$ since $x_i(q) = 1$ to the top $m$ bids with $v_i \geq q$. Thus $E_{\mathrm{T}^{\alpha}_{\mathrm{W}}}$ is a monotone mixture. Next, we prove the kernel $\mathrm{K}_{\mathrm{W}}$ is Lipschitz continuous under the assumption $\textsc{Rev}$ is Lipschitz continuous.

**Claim B.1.** *If* $\textsc{Rev}$ *is* $L$*-Lipschitz, then kernel* $\mathrm{K}_{\mathrm{W}}$ *is* $(L/m + 1)$*-Lipschitz.*

*Proof.* We decompose the welfare as the revenue plus the surplus. Since the revenue is $L$-Lipschitz, it suffices to show the surplus is $m$-Lipschitz. Fix any positive $q < q'$ and because the welfare is decreasing, we have $\mathrm{K}_{\mathrm{W}}(q) \geq \mathrm{K}_{\mathrm{W}}(q')$. Thus,

$$\begin{aligned}
0 &\leq m \cdot (\mathrm{K}_{\mathrm{W}}(q) - \mathrm{K}_{\mathrm{W}}(q')) \\
&= \underbrace{\mathbb{E}\left[\sum_{i=1}^{n}(v_i - q)\cdot x_i(q)\right]}_{\text{Expected surplus at price } q} - \underbrace{\mathbb{E}\left[\sum_{i=1}^{n}(v_i - q')\cdot x_i(q')\right]}_{\text{Expected surplus at price } q'} + \textsc{Rev}(q) - \textsc{Rev}(q') \\
&= \mathbb{E}\left[\sum_{i=1}^{n}(v_i - q)\cdot (x_i(q) - x_i(q')) - (v_i - q' - v_i + q)\cdot x_i(q')\right] + \textsc{Rev}(q) - \textsc{Rev}(q').
\end{aligned}$$

Observe $x_i(q') \leq x_i(q)$, and whenever $x_i(q) - x_i(q') = 1$, bidder $i$ has value $v_i \leq q'$. Thus the difference between the expected surplus at price $q$ and $q'$ is at most

$$(q'-q)\mathbb{E}\left[\sum_{i=1}^{n} x_i(q) - x_i(q')\right] + (q'-q)\mathbb{E}\left[\sum_{i=1}^{n} x_i(q')\right] = (q'-q)\mathbb{E}\left[\sum_{i=1}^{n} x_i(q)\right] \leq (q'-q)\cdot m.$$

From the assumption $\textsc{Rev}$ is $L$-Lipschitz, we have

$$0 \leq \mathrm{K}_{\mathrm{W}}(q) - \mathrm{K}_{\mathrm{W}}(q') \leq (q'-q)(L/m + 1).$$

This proves $\mathrm{K}_{\mathrm{W}}$ is $(L/m+1)$-Lipschitz. □

From Lemma 3.10 and setting $\alpha \leq 1/(L/m+1)$, we get $E_{\mathrm{T}^{\alpha}_{\mathrm{W}}}(q)$ is a contractive mapping with Lipschitz constant $1-\alpha < 1$. From Banach Contraction Principle, Lemma 3.11, for any initial positive price $q_0$, the iteration $q_0, E_{\mathrm{T}^{\alpha}_{\mathrm{W}}}(q_0), E^2_{\mathrm{T}^{\alpha}_{\mathrm{W}}}(q_0), \ldots$ converges to a unique fixed point $q^*$. From Observation 3.9, $q^*$ is also a unique fixed point for the kernel $\mathrm{K}_{\mathrm{W}}$. This proves the intended mechanism is asymptotically stable with respect to distribution $F^n$.

**Claim B.2.** *If $q$ is a fixed point for* $\mathrm{K_W}$*, then* $\textsc{Welfare}(\vec{x}(q)) \geq \frac{1}{2}OPT$*.*

*Proof.* Observe $q \cdot m$ is the expected welfare of the WDPP mechanism at equilibrium price $q$ since $q$ is a fixed point for $\mathrm{K_W}$. That is,

$$\textsc{Welfare}(\vec{x}(q)) = \mathbb{E}\left[\sum_{i=1}^{n} v_i \cdot x_i(q)\right] = m \cdot \mathrm{K_W}(q) = q \cdot m,$$

where the second equality is simply the definition of $\mathrm{K_W}$ and the third equality follows from the fact $q = \mathrm{K_W}(q)$ is a fixed point of $\mathrm{K_W}$. Assume for contradiction $q \cdot m \leq \frac{1}{2}OPT$, then the optimal welfare

$$\begin{aligned}
OPT = \mathbb{E}\left[\sum_{i=1}^{n} v_i \cdot x_i^*(\vec{v})\right] &= \mathbb{E}\left[\sum_{i=1}^{n} v_i(x_i^*(\vec{v}) - x_i(q))\right] + \mathbb{E}\left[\sum_{i=1}^{n} v_i \cdot x_i(q)\right] \\
&< q\mathbb{E}\left[\sum_{i=1}^{n}(x_i^*(\vec{v}) - x_i(q))\right] + \textsc{Welfare}(\vec{x}(q)) \quad \text{Because } x_i^*(\vec{v}) - x_i(q) = 1 \text{ only if } v_i < q. \\
&\leq \frac{OPT}{2} + \textsc{Welfare}(\vec{x}(q)) \quad \text{Because } q \leq \frac{OPT}{2m} \text{ and } \sum_{i=1}^{n} x_i^*(\vec{v}) - x_i(q) \leq m. \\
&= \frac{OPT}{2} + \textsc{Welfare}(\vec{x}(q)).
\end{aligned}$$

Rearranging the inequality gives $q \cdot m = \textsc{Welfare}(\vec{x}(q)) > \frac{OPT}{2}$, a contradiction. Thus $\textsc{Welfare}(\vec{x}(q)) = q \cdot m \geq \frac{1}{2}OPT$. □

This proves Theorem 1. □

# C Omitted Proofs from Section 6

*Proof of Proposition 6.3.* For any positive value $v$, $\delta$, $\alpha$ and supply $m \geq 4(1+\delta)/\delta$, assume in each time step, there is $n = \lfloor m\frac{1+\delta/2}{1+\delta} \rfloor \leq m - 1$ bidders with value $v$. For the UDPP mechanism $\left(\vec{x}, \vec{p}, \mathrm{T_U^{\alpha,\delta}}\right)$, if the current price $q_t \leq v$, the subsequent price increases to

$$q_{t+1} = q_t\left(1 + \alpha\left(\frac{n}{m}(1+\delta) - 1\right)\right) \geq q_t\left(1 + \alpha\left(1 + \frac{\delta}{2} - \frac{1+\delta}{m} - 1\right)\right) \geq q_t\left(1 + \frac{\alpha\delta}{4}\right).$$

It the current price $q_t > v$, no bidder purchases, and the subsequent price decreases to

$$q_{t+1} = q_t(1 - \alpha).$$

This repeats *ad infinitum*, and the allocation-based update rule is unstable with respect to distribution $F^n$.

For the TWDPP mechanism $\left(\vec{x}, \vec{p}, \mathrm{T_{TW}^{\alpha,\delta}}\right)$, if the current price $q_t > v$, no bidder purchases, and the subsequent price decreases to

$$q_{t+1} = q_t(1 - \alpha).$$

If the current price $q_t < \frac{v}{1+\delta}$, all $n$ bidders purchase, and the subsequent price increases to

$$q_{t+1} = \alpha\frac{n}{m}\min\{v, (1+\delta)q_t\} + (1-\alpha)q_t \le q_t(\alpha(1+\delta)+1-\alpha) = q_t(1+\alpha\delta) < v.$$

Thus eventually, the mechanism reaches a price $q_t \in \left[\frac{v}{1+\delta}, v\right] = X$. If the current price $q_t \in X$, all $n$ bidders purchase, and the subsequent price is

$$q_{t+1} = \mathrm{T}_{\mathrm{TW}}^{\alpha,\delta}(q_t) = \alpha\frac{n}{m}\min\{v, (1+\delta)q_t\} + (1-\alpha)q_t = \alpha\frac{n}{m}v + (1-\alpha)q_t \le v.$$

Additionally,

$$\begin{aligned}
\mathrm{T}_{\mathrm{TW}}^{\alpha,\delta}(q_t) &= \alpha\frac{n}{m}v + (1-\alpha)q_t \\
&\ge \alpha v\left(\frac{1+\delta/2}{1+\delta} - \frac{1}{m}\right) + (1-\alpha)\frac{v}{1+\delta} \quad \text{Because } n \ge m\frac{1+\delta/2}{1+\delta} - 1, \\
&= \alpha v\left(\frac{1}{1+\delta} + \frac{\delta/2}{1+\delta} - \frac{1}{m}\right) + (1-\alpha)\frac{v}{1+\delta} \\
&\ge \alpha v\left(\frac{1}{1+\delta} + \frac{\delta}{4(1+\delta)}\right) + (1-\alpha)\frac{v}{1+\delta} \quad \text{Because } m \ge 4(1+\delta)/\delta, \\
&\ge \frac{v}{1+\delta}.
\end{aligned}$$

Thus $\mathrm{T}_{\mathrm{TW}}^{\alpha,\delta}$ maps $X$ to itself. For all $q, q' \in X$, we have

$$|\,\mathrm{T}_{\mathrm{TW}}^{\alpha,\delta}(q) - \mathrm{T}_{\mathrm{TW}}^{\alpha,\delta}(q')| = (1-\alpha)|q-q'|.$$

Thus the restriction of $\mathrm{T}_{\mathrm{TW}}^{\alpha,\delta}$ to $X$ is a contractive mapping (Definition 3.7). From Banach contraction principle, Lemma 3.11, for all $q_t \in X$, the fixed point iteration

$$q_t, \mathrm{T}_{\mathrm{TW}}^{\alpha,\delta}(q_t), \mathrm{T}_{\mathrm{TW}}^{\alpha,\delta}(\mathrm{T}_{\mathrm{TW}}^{\alpha,\delta}(q_t)), \ldots$$

converges to a unique fixed point $z \in X$. This proves the TWDPP mechanism is asymptotically stable with respect to distribution $F^n$. See Figure 5 for an empirical example of this behavior. ☐

## C.1 Omitted Proofs From Section 6.1

The following is a well-known fact about concave functions.

**Proposition C.1.** *If $f$ and $g$ are (strictly) concave functions:*

*(i) $f+g$ is (strictly) concave.*

We will require the following fact:

**Lemma C.2** (Theorem 3.1 in [14])**.** *If $f$ is strictly concave and $f(0) \ge 0$, then $f$ has at most one positive fixed point.*

Lemma C.2 guarantees a concave function $f$ satisfying Assumption 2 has at most one positive fixed point but it does not guarantee existence. For the one-dimensional case, uniqueness will follow directly from the intermediate value theorem.

*Proof of Lemma 6.5.* First, we show $f : X \to X$ with $X = [0, \bar{a}]$ has at least one nonnegative fixed point.

**Claim C.3.** *There is a positive $a \in X$ such that $f(a) > a$ if and only if $f$ has a unique positive fixed point $x^*$.*

*Proof.* We first prove that if there is a positive $a \in X$ such that $f(a) > a$, then $f$ has a unique positive fixed point.
$\Rightarrow$ From (iv), there is a positive $b \in X$ such that $f(b) < b$. Let

$$g(x) = f(x) - x, \tag{16}$$

and observe $g$ is continuous (because $f$ is continuous) and $x$ is a fixed point for $f$ if and only if $g(x) = 0$. The fact $g$ is continuous, $g(a) > 0$, and $g(b) < 0$ allow us to use the intermediate value theorem to conclude there is a $x^* \in [\min\{a, b\}, \max\{a, b\}] \subseteq X$ such that $g(x^*) = 0$. Thus $x^* > 0$ is a positive fixed point for $f$. From Lemma C.2, $x^*$ is the unique positive fixed point of $f$.

Next, we prove that if $f$ has a unique positive fixed point, then there is a positive $a \in X$ such that $f(a) > a$.
$\Leftarrow$ Let $z \in X$ be a positive fixed point of $f$. For some $\alpha \in (0, 1)$, let $a = \alpha \cdot z > 0$ and note $a \in X$. From strict concavity of $f$,

$$\begin{aligned}
f(\alpha z) &= f(\alpha z + (1 - \alpha) \cdot 0) & \\
&> \alpha f(z) + (1 - \alpha) f(0) & \text{From strict concavity of } f, \\
&\geq \alpha f(z) & \text{From (ii), } f(0) \geq 0, \\
&= \alpha z & \text{Because } z = f(z) \text{ is a fixed point of } f.
\end{aligned}$$

The chain of inequalities witnesses $f(a) = f(\alpha z) > \alpha \cdot z = a > 0$. Thus there is a positive $a \in X$ such that $f(a) > a$. $\square$

**Claim C.4.** *$f$ has at least one nonnegative fixed point and at most one positive fixed point*

*Proof.* Let's first consider the case where $f$ has no positive fixed point. From Claim C.3, if $f$ has no positive fixed point, then $0 \leq f(x) \leq x$ for all positive $x \in X$. Then the sequence

$$f(\bar{a}), f\left(\frac{\bar{a}}{2}\right), f\left(\frac{\bar{a}}{3}\right), \ldots$$

converges to 0. From continuity of $f$, $0 = f(0)$ is a fixed point of $f$ and 0 is a nonnegative fixed point of $f$ whenever $f$ has no positive fixed point. Second, consider the case $f$ has a positive fixed point. From Lemma C.2, this fixed point is unique. $\square$

Let $x^*$ be the largest nonnegative fixed point of $f$. Define the partition of $X$ into the sets

$$A := \{x \in X : f(x) \geq x\}, \tag{17}$$

$$L := \{x \in X : f(x) < x\}. \tag{18}$$

**Claim C.5.** $A = [\inf X, x^*]$ *and* $L = (x^*, \sup X]$.

*Proof.* Observe $x^* \in A$ because $f(x^*) = x^*$. Suppose for contradiction there is $x \in A$ and $y \in L$ such that $x > y$. Because $0 < y < x$, there is $\alpha \in (0,1)$ such that $y = (1-\alpha)x$. From strict concavity of $f$

$$\begin{aligned} f(y) &= f(0 \cdot \alpha + x(1-\alpha)) \\ &> \alpha f(0) + (1-\alpha) f(x) && \text{From strict concavity of } f, \\ &\geq (1-\alpha)x = y && \text{Because } f(0) \geq 0 \text{ and } f(x) \geq x \text{ since } 0, x \in A. \end{aligned}$$

The chain of inequalities witnesses $y \in A$, a contradiction to $y \in L = X \setminus A$. □

We are ready to show that iterating $f$ starting from a positive $x_0$ converges to $x^*$. Define $x_t = f(x_{t-1})$ for $t = 1, 2, \ldots$. It suffices to show the sequence $x_0, x_1, \ldots$ converges to a limit point $z$ since the continuity of $f$ implies $z$ is a fixed point of $f$. When $z$ is positive and $f$ has a unique positive fixed point, we will have $z = x^*$. First, let's consider the case $f$ has no positive fixed point.

**Claim C.6.** *If $f$ has no positive fixed point, the sequence $x_0, x_1, \ldots$ converges to* $0$.

*Proof.* From Claim C.4, 0 is the unique nonnegative fixed point of $f$ and $L = X \setminus \{0\}$. If $x_0 = 0$, then $f(x_0) = 0$. If $x_0 \in L$, from (18) and (ii), $0 \leq x_1 = f(x_0) < x_0$. By induction, the sequence

$$x_0 > x_1 > x_2 > \ldots \geq 0.$$

is decreasing and lower bounded by 0.

**Claim C.7.** *If the sequence $x_0, x_1, \ldots$ is monotone and bounded, the sequence $x_0, x_1, \ldots$ converges to a limit point $z$. Moreover, $z$ is a fixed point of $f$.*

*Proof.* Since the Euclidean space is a complete metric space, the sequence $x_0, x_1, \ldots$ converges to a limit point $z$. From continuity of $f$, $z$ is a fixed point of $f$. □

Thus when $f$ has no positive fixed point, the nonincreasing sequence $x_0, x_1, \ldots$ converges to 0, the unique nonnegative fixed point of $f$. □

For the case $f$ has a positive fixed point, from Lemma C.2, $f$ has a unique positive fixed point $x^*$. Next, we divide the proof into the case $x^* < \bar{x} = \sup_{x \in X} f(x)$ and the case where $x^* \geq \bar{x}$.

**Claim C.8.** *If $f$ has a positive fixed point and $x^* < \bar{x}$, the sequence $x_t, x_{t+1}, \ldots$ converges to $x^*$ .*

*Proof.* Observe $[\inf X, x^*] = A \subseteq I = [\inf X, \bar{x})$. We consider separately the case where $x_t \in A$ and the case $x_t \in L$.

**Case 1:** For the case $x_t \in A$,

$$\begin{aligned}
x_t \le x_{t+1} = f(x_t) & \qquad \text{Because } x_t \in A, \\
\le f(x^*) & \qquad \text{Because } f \text{ is increasing on } I \ni x_t, x^* \text{ and } x_t \le x^*, \\
= x^* & \qquad \text{Because } x^* = f(x^*) \text{ is a fixed point.}
\end{aligned}$$

Thus $x_{t+1} \in A$. By induction, $x_{t+i} \in A$ for all $i \ge 0$. Thus the sequence

$$x_t \le x_{t+1} \le \ldots \le x^*$$

is nondecreasing and upper bounded by $x^*$. From Claim C.7, the sequence $x_t, x_{t+1}, \ldots$ converges to $x^*$.

**Case 2:** For the case $x_t \in L$, we divide the proof into two subcases. First, for the case $x_{t+i} \in L = (x^*, \sup X]$ for all $i \ge 0$, the sequence

$$x_t > x_{t+1} > x_{t+2} > \ldots > x^*$$

is decreasing and lower bounded by $x^*$. From Claim C.7, the sequence $x_t, x_{t+1}, \ldots$ converges to $x^*$.

Second, for the case $x_{t+i} \notin L$ for some $i \ge 0$, $x_{t+i} \in A = X \setminus L$. Thus invoke Case 1 to conclude the sequence $x_{t+i}, x_{t+i+1}, x_{t+i+2}, \ldots$ converges to $x^*$. This proves the sequence $x_t, x_{t+1}, \ldots$ converges to $x^*$ whenever $f$ has a positive fixed point and $x^* < \bar{x}$. $\square$

**Claim C.9.** *If $f$ has a positive fixed point and $\bar{x} \le x^*$, the sequence $x_t, x_{t+1}, \ldots$ converges to $x^*$.*

*Proof.* We first show the restriction of $f$ to $[\bar{x}, f(\bar{x})]$ is a contractive mapping — i.e., $f$ maps $[\bar{x}, f(\bar{x})]$ to itself and the restriction of $f$ to $[\bar{x}, f(\bar{x})]$ is $L$-Lipschitz with $L < 1$.

**Claim C.10.** *The restriction of $f$ to $[\bar{x}, f(\bar{x})]$ is a contractive mapping.*

*Proof.* From assumption (iii), the restriction of $f$ to the rectangle $[\bar{x}, f(\bar{x})] \subseteq D$ is $L$-Lipschitz with $L < 1$. Thus it suffices to show that $f$ maps $[\bar{x}, f(\bar{x})]$ to itself. Let $x \in [\bar{x}, f(\bar{x})]$, then $f(x) \le f(\bar{x})$ since $\bar{x} \le x$ and the restriction of $f$ to $D$ is decreasing. Suppose for contradiction $f(x) < \bar{x}$, then

$$\begin{aligned}
|f(x) - f(\bar{x})| &= f(\bar{x}) - f(x) \\
&> f(\bar{x}) - \bar{x} && \text{From the assumption } f(x) < \bar{x}, \\
&\ge x - \bar{x} \Rightarrow\Leftarrow && \text{Observe } x \le f(\bar{x}) \text{ since } x \in [\bar{x}, f(\bar{x})].
\end{aligned}$$

We reach a contradiction to the fact that the restriction of $f$ to $D$ is $L$-Lipschitz with $L < 1$. Thus $\bar{x} \le f(x) \le f(\bar{x})$ and proves $f$ maps $[\bar{x}, f(\bar{x})]$ to itself. This proves the restriction of $f$ to $[\bar{x}, f(\bar{x})]$ is a contractive mapping. $\square$

It follows that if $x_t \in [\bar{x}, f(\bar{x})]$, the sequence $x_t, x_{t+1}, \ldots$ will converge to a limit point.

**Claim C.11.** *For any $x_t \in [\bar{x}, f(\bar{x})]$, the sequence $x_t, x_{t+1}, x_{t+1}, \dots$ converges to $x^*$.*

*Proof.* Follows from Banach contraction principle, Lemma 3.11, and the fact the restriction of $f$ to $[\bar{x}, f(\bar{x})]$ is a contractive map, Claim C.10. □

Recall from Assumption 2, $I = [\inf X, \bar{x})$ is the interval where $f$ is nondecreasing and $D = [\bar{x}, \sup X]$ is the interval $f$ is nonincreasing. Next, we consider separately the case where $x_t \in I$ and the case $x_t \in D$.

**Case 1:** For the case $x_t \in I$, observe

$$I = [\inf X, \bar{x}) \subset [\inf X, x^*] = A,$$

from the assumption $\bar{x} \leq x^*$. Thus $x_t \in A$. Let's consider two distinct cases depending if $x_{t+i} \in A$ for all $i \geq 0$ or $x_{t+i} \notin A$ for some $i \geq 0$. For the case $x_{t+i} \in A$ for all $i \geq 0$, the sequence

$$x_t \leq x_{t+1} \leq x_{t+2} \leq \ldots \leq \sup_{x \in X} f(x) = f(\bar{x})$$

is nondecreasing and upper bounded by $f(\bar{x}) < \infty$ (because $f$ is Lipschitz continuous):

**Claim C.12.** $\sup_{x \in X} f(x) < \infty$

*Proof.* From (iv), there is a $b \in X$ such that $f(b) < b$. Because $f$ is $L$-Lipschitz,

$$\sup_{x \in X} f(x) - f(b) = |f(\bar{x}) - f(b)| \leq L|\bar{x} - b| \leq L \sup X.$$

Thus $\sup_{x \in X} f(x) \leq L \sup X + f(b) < L \sup X + b < (L+1) \sup X < \infty$. □

From Claim C.7, the nondecreasing sequence $x_t, x_{t+1}, \dots$ converges to $x^*$. For the case $x_{t+i} \notin A$ for some $i$, let $i \geq 1$ be the first element that satisfy this condition — that is, $x_{t+i} \notin A$ while $x_{t+i-j} \in A$ for all $1 \leq j \leq i$. Observe

$$x_{t+i} = f(x_{t+i-1}) \leq \sup_{x \in X} f(x) = f(\bar{x}),$$

and the fact $x_{t+i} \notin A$ implies $x_{t+i} \in X \setminus A = L = (x^*, \sup X]$. Thus $x_{t+i} > x^* \geq \bar{x}$. Thus

$$\bar{x} \leq x^* < x_{t+i} = f(x_{t+i-1}) \leq f(\bar{x}).$$

The chain of inequalities witnesses $x_{t+i} \in [\bar{x}, f(\bar{x})]$ and from Claim C.11, the sequence $x_{t+i}, x_{t+i+1}, x_{t+i+2}, \dots$ converges to $x^*$.

**Case 2:** For the case $x_t \in D = [\bar{x}, \sup X]$, observe $x_t \geq \bar{x} > 0$. We consider separately the case where $x_{t+i} \in D$ for all $i \geq 0$ and $x_{t+i} \notin D$ for some $i \geq 0$.

For the case $x_{t+i} \in D$ for all $i \geq 0$, from Banach contraction principle, the sequence $x_t, x_{t+1}, \dots$ converges to $x^* \geq \bar{x}$ since the restriction of $f$ to $D$ is $L$-Lipschitz with $L < 1$ (iv).

For the case $x_{t+i} \notin D$ for some $i \geq 0$, $x_{t+i} \in X \setminus D = I$. From Case 1, the sequence $x_{t+i}, x_{t+i+1}, \dots$ converges to $x^*$. Case 1 and 2 proves the sequence $x_t, x_{t+1}, \dots$ converges to $x^*$ whenever $\bar{x} \leq x^*$ and $f$ has a positive fixed point. □

Claims C.6, C.8, and C.9 proves the sequence $x_0, x_1, \ldots$ converges to a fixed point of $f$. $\square$

*Proof of Lemma 6.6.* Recall $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is $L$-Lipschitz, the restriction of $f$ to $X = [0, \bar{x}]$ is strictly concave, and $f(x) = 0$ for all $x \geq \bar{a}$. For positive $\alpha \leq \frac{1}{L+1}$, define

$$g(x) = \alpha f(x) + (1-\alpha)x.$$

First, we show the restriction of $g : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ to $X$ maps $X$ to itself and satisfy Assumption 2.

For (i), observe $g$ is the convex combination of $x$ and $f(x)$. From Proposition C.1, $g$ restricted to $X$ is strictly concave (because $f$ restrict to $X$ is strictly concave).

For (ii), from the assumption $f$ is nonnegative, $g$ is also nonnegative.

For (iii), for all $x \in X$,

$$\begin{aligned}
0 \leq g(x) &= \alpha f(x) + (1-\alpha)x \\
&= \alpha(f(x) - f(\bar{a})) + (1-\alpha)x && \text{From (iii), } f(\bar{a}) = 0, \\
&\leq \alpha(\bar{a} - x)L + (1-\alpha)x && \text{From the fact } f \text{ is } L\text{-Lipschitz}, \\
&\leq \bar{a} - x + x - \alpha x && \text{From the fact } \alpha \leq 1/L, \\
&\leq \bar{a}.
\end{aligned}$$

Thus $g$ maps $X$ to itself. Let $I \subseteq X$ be the interval where $f$ is increasing and let $D \subseteq X$ be the interval where $f$ is decreasing. Then the restriction of $g$ to $D$ is a monotone mixture (Definition 3.8) with kernel $f$. From Lemma 3.10, the restriction of $g$ to $D$ is $(1-\alpha)$-Lipschitz for $\alpha \leq \frac{1}{L+1}$. This proves the restriction of $g$ to $X$ satisfy (iii).

For (iv), let $b = \bar{a} > 0$ and from the assumption $f(b) = 0 < b$,

$$g(b) = \alpha f(b) + (1-\alpha)b < b.$$

The work above proves the restriction of $g$ to $X$ satisfy Assumption 2. Consider the fixed point iterating of $g$ starting from a positive $x_0$. Let $x_{t+1} = g(x_t)$ for $t \geq 0$. If $x_t \geq \bar{a}$, then

$$g(x_t) = (1-\alpha)x_t.$$

Let $x_t$ be the first element in the sequence $x_0, x_1, \ldots$ such that $x_t \leq \bar{a}$. From Lemma 6.5, the fixed point iteration of $g$ restricted to $X$ starting from $x_t \in X$ converges to a nonnegative fixed point of $g$. Finally, observe that a fixed point of $g$ is also a fixed point of $f$. $\square$

**Example C.13.** Consider strictly concave functions $f_1(x) = (4 - (x-2)^2)$ and $f_2(x) = \frac{f(x)}{2}$ and for $\alpha = 0.4$, define functions $g_1(x) = \alpha f_1(x) + (1-\alpha)x$, $g_2(x) = \alpha f_2(x) + (1-\alpha)x$. In Figure 6, we plot the fixed point iteration of $g_1$, respectively $g_2$, demonstrating that for a function satisfying Assumption 1 (e.g., $f_1$ and $f_2$), we can construct a function satisfying Assumption 2 (e.g., $g_1$ and $g_2$). Then the fixed-point iteration of $g_1$ (resp. $g_2$) converges to a fixed for $f_1$ (resp. $f_2$).

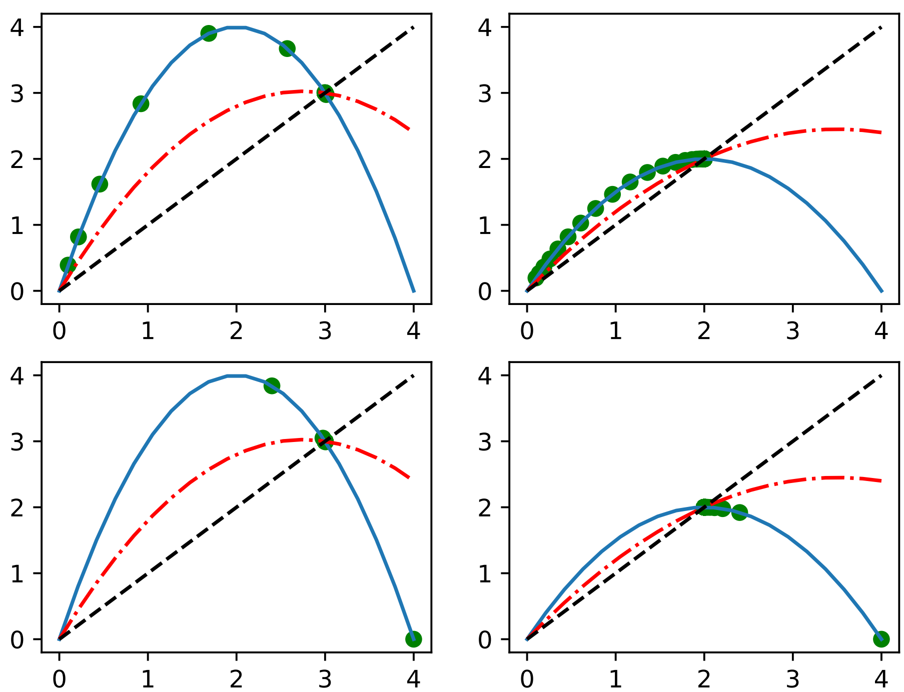


Figure 6: (Top-left) $g_1$ with initial point $q_0 = 0.1$; (Top-right) $g_2$ with initial point $q_0 = 0.1$; (Bottom-left) $g_1$ with initial point $q_0 = 4$; (Bottom-right) $g_2$ with initial point $q_0 = 4$. The solid line (blue) denotes function $f_1$ or $f_2$. The dashed-dot line (red) denotes function $g_1$ or $g_2$. The dashed line (black) is the function $y(x) = x$. Dots (green) denote the sequence of points in $\mathbb{R}^2$: $(q_0, f(q_0)), (f(q_0), f^2(q_0)), (f^2(q_0), f^3(q_0)), \ldots$

## C.2 Omitted Proofs from Section 6.2

**Proposition C.14.** *Consider the RDPP mechanism $(\vec{x}, \vec{p}, T)$ with equilibrium price $q$. If* $\textsc{Welfare}(\vec{x}(q)) \geq \frac{q \cdot m}{1+\delta}$ *and* $Pr[N(q) < m] \geq \frac{\delta}{1+\delta}$*, then*

$$\textsc{Welfare}(\vec{x}(q)) \geq \frac{OPT}{2(1+\delta)} \min\{1, \delta\}.$$

*Proof.* Let $c$ be a positive constant. First, we consider two cases:
**Case 1.** For the case $q \geq \frac{c}{m} OPT$, from the assumption $\textsc{Welfare}(\vec{x}(q)) \geq \frac{q \cdot m}{1+\delta}$, we have

$$\textsc{Welfare}(\vec{x}(q)) \geq \frac{q \cdot m}{1+\delta} \geq \frac{c}{1+\delta} OPT. \tag{19}$$

**Case 2.** Next, consider the case $q < \frac{c}{m} OPT$. From the assumption $Pr\left[N(q) < m\right] \geq \frac{\delta}{1+\delta}$, we might hope to not lose too much welfare in the event $\{N(q) \geq m\}$ since this event is correlated with bidders having smaller values. Moreover, it is easy to estimate the welfare whenever $N(q) \leq m$ — it is simply the sum of all $v_i \geq q$. Since $q < \frac{c}{m} OPT$, we can upper bound the welfare loss from the top $N(q) - m$ bidders with values $v_i < q$. Let $N_{-i}(q) := \sum_{j \neq i} \mathbb{1}_{v_j \geq q}$ and let $\vec{v}_{-i} = (v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n)$ be the vector $\vec{v}$ excluding the $i$-th entry. Then,

$$\begin{aligned}
\textsc{Welfare}(\vec{x}(q)) &= \mathbb{E}\left[\sum_{i=1}^{n} v_i \cdot x_i(q) \cdot \mathbb{1}_{N(q) \leq m}\right] + \mathbb{E}\left[\sum_{i=1}^{n} v_i \cdot x_i(q) \cdot \mathbb{1}_{N(q) < m}\right] \\
&\geq \mathbb{E}\left[\sum_{i=1}^{n} v_i \cdot x_i(q) \cdot \mathbb{1}_{N(q) \leq m}\right] \\
&= \mathbb{E}\left[\sum_{i=1}^{n} v_i \cdot x_i^*(\vec{v}) \cdot \mathbb{1}_{v_i \geq q} \cdot \mathbb{1}_{N(q) \leq m}\right] \\
&= \mathbb{E}\left[\sum_{i=1}^{n} v_i \cdot x_i^*(\vec{v}) \cdot \mathbb{1}_{v_i \geq q} \cdot \mathbb{1}_{N_{-i}(q) \leq m-1}\right] \\
&= \sum_{i=1}^{n} \mathbb{E}_{\vec{v}_{-i} \sim F^{n-1}}\left[\mathbb{1}_{N_{-i}(q) \leq m-1} \cdot \mathbb{E}_{v_i \sim F}\left[v_i \cdot x_i^*(\vec{v}) \cdot \mathbb{1}_{v_i \geq q} \cdot \mathbb{1}_{N_{-i}(q) \leq m-1} | \vec{v}_{-i}\right]\right].
\end{aligned}$$

The third line observes given $N(q) \leq m$, then $x_i(q)$ if and only if bidder $i$ is one of the top $m$ bidders with value $v_i \geq q$. The fourth line observes that the following events are equivalent:

- Bidder $i$ with value $v_i \geq q$ is one of the top $m$ bidders when there is at most $m$ bidders with value at least $q$.
- Bidder $i$ with value $v_i \geq q$ is one of the top $m$ bidders when among bidders $[n] \setminus \{i\}$ there is at most $m - 1$ bidders with value at least $q$.

The fifth line is from linearity of expectation and the law of total expectation by observing that $\vec{v}$ is drawn from product distribution $F^n = \underbrace{F \times \ldots \times F}_{n \text{ times}}$. Next, observe that if among bidders $[n] \setminus \{i\}$ there are at most $m-1$ bidders with value at least $q$, then the event bidder $i$ has value at least $q$ implies bidder $i$ is one of the top $m$ bidders. Thus $\textsc{Welfare}(\vec{x}(q))$ is at least

$$\geq \sum_{i=1}^{n} \mathbb{E}_{\vec{v}_{-i}\sim F^{n-1}} \left[\mathbb{1}_{N_{-i}(q)\leq m-1} \cdot \mathbb{E}_{v_i\sim F}\left[v_i \cdot \mathbb{1}_{v_i\geq q} | \vec{v}_{-i}\right]\right]$$

$$= \sum_{i=1}^{n} Pr\left[N_{-i}(q) \leq m-1\right] \mathbb{E}\left[v_i \cdot \mathbb{1}_{v_i\geq q}\right] \quad \text{From independence between } v_i \text{ and } \vec{v}_{-i},$$

$$\geq Pr\left[N(q) < m\right] \mathbb{E}\left[\sum_{i=1}^{n} v_i \cdot \mathbb{1}_{v_i\geq q}\right] \quad N(q) < m \text{ implies } N_{-i}(q) \leq m-1,$$

$$\geq \frac{\delta}{1+\delta} \mathbb{E}\left[\sum_{i=1}^{n} v_i \cdot \mathbb{1}_{v_i\geq q}\right] \quad \text{From the assumption } N(q) < m \text{ with probability at least } \delta/(1+\delta),$$

$$= \frac{\delta}{1+\delta}\left(\mathbb{E}\left[\sum_{i=1}^{n} v_i \cdot x_i^*(\vec{v})\right] + \mathbb{E}\left[\sum_{i=1}^{n} v_i(\mathbb{1}_{v_i\geq q} - x_i^*(\vec{v}))\right]\right)$$

$$\geq \frac{\delta}{1+\delta}\left(\mathbb{E}\left[\sum_{i=1}^{n} v_i \cdot x_i^*(\vec{v})\right] - \mathbb{E}\left[\sum_{i=1}^{n} v_i \cdot x_i^*(\vec{v}) \cdot \mathbb{1}_{v_i<q}\right]\right)$$

$$> \frac{\delta}{1+\delta}\left(OPT - q\cdot m\right) \quad \text{From the fact } v_i \cdot \mathbb{1}_{v_i<q} < q \text{ and } \sum_{i=1}^{n} x_i^*(\vec{v}) \leq m,$$

$$\geq \frac{\delta}{1+\delta}(1-c)OPT \quad \text{From the assumption } q\cdot m < c\cdot OPT.$$

The second line observes that for independent random variables $X$ and $Y$, $\mathbb{E}[X \cdot Y] = \mathbb{E}[X]\,\mathbb{E}[Y]$. The chain of inequalities proves that for Case 2,

$$\textsc{Welfare}(\vec{x}(q)) \geq \frac{\delta}{1+\delta}(1-c)OPT.$$

Combining Case 1 and 2, we get that

$$\textsc{Welfare}(\vec{x}(q)) \geq \frac{OPT}{1+\delta}\min\{c, (1-c)\delta\}.$$

Setting $c = 1/2$ proves Proposition C.14. □

*Proof of Theorem 4.* Let $N_{-i}(q) = \sum_{j\neq i} \mathbb{1}_{v_j\geq q}$ be the number of bidders that would purchase a slot at price $q$ excluding bidder $i$. Recall the value profile $\vec{v}$ is drawn from product distribution $F^n$ and whenever the demand $N(q) > m$, the active miner selects $m$ random bidders with values at least $q$. Recall the expected value of the random operator $\mathrm{T}_{\mathrm{TW}}^{\alpha,\delta}(q, B)$ is

$$E_{\mathrm{T}_{\mathrm{TW}}^{\alpha,\delta}}(q) = \alpha\, \mathrm{K}_{\mathrm{TW}}(q) + (1-\alpha)q,$$

and if $q$ is an equilibrium price, $q = E_{\mathrm{T}_{\mathrm{TW}}^{\alpha,\delta}}(q)$ is a fixed point of $E_{\mathrm{T}_{\mathrm{TW}}^{\alpha,\delta}}$. From the expression for $E_{\mathrm{T}_{\mathrm{TW}}^{\alpha,\delta}}$, we get that $q = \mathrm{K}_{\mathrm{TW}}(q)$ is also a fixed point of $\mathrm{K}_{\mathrm{TW}}$. By definition of $\mathrm{K}_{\mathrm{TW}}$, Equation 14, if $q$ is a fixed point of $\mathrm{K}_{\mathrm{TW}}$, we have

$$q = \mathrm{K}_{\mathrm{TW}}(q) \geq (1+\delta)qPr[N(q) \geq m]. \tag{20}$$

Thus, the probability that at price $q$, the demand is at most $m-1$ is

$$Pr\left[N(q) < m\right] = 1 - Pr\left[N(q) \geq m\right] \geq \frac{\delta}{1+\delta}. \tag{21}$$

Next, we lower bound $\textsc{Welfare}(\vec{x}(q))$ in terms of $q$ and $\delta$. Because $q$ is a fixed point of $\mathrm{K}_{\mathrm{TW}}$, we have

$$\begin{aligned}
q \cdot m = \mathrm{K}_{\mathrm{TW}}(q) \cdot m &= \mathbb{E}\left[\sum_{i=1}^{n} \min\{v_i, (1+\delta)q\} \cdot x_i(q) \cdot \mathbb{1}_{N(q)<m} + (1+\delta) \cdot q \cdot \mathbb{1}_{N(q)\geq m}\right] \\
&\leq \mathbb{E}\left[\sum_{i=1}^{n} v_i \cdot x_i(q) \cdot \mathbb{1}_{N(q)<m} + (1+\delta) \cdot q \cdot \mathbb{1}_{N(q)\geq m}\right] \\
&= \textsc{Welfare}(\vec{x}(q)) + \mathbb{E}\left[\sum_{i=1}^{n} ((1+\delta) \cdot q - v_i) \cdot x_i(q) \cdot \mathbb{1}_{N(q)\geq m}\right] \\
&\leq \textsc{Welfare}(\vec{x}(q)) + \delta \cdot q \cdot \mathbb{E}\left[\sum_{i=1}^{n} x_i(q) \cdot \mathbb{1}_{N(q)\geq m}\right] \quad \text{Observing } x_i(q) = 1 \text{ only if } v_i \geq q. \\
&= \textsc{Welfare}(\vec{x}(q)) + \delta \cdot q \cdot m \cdot Pr\left[N(q) \geq m\right] \\
&\leq \textsc{Welfare}(\vec{x}(q)) + \frac{\delta \cdot q \cdot m}{1+\delta} \quad \text{From (20).}
\end{aligned}$$

Rearranging the inequality, we get

$$\textsc{Welfare}(\vec{x}(q)) \geq \frac{q \cdot m}{1+\delta}. \tag{22}$$

From (21), (22), Proposition C.14, we establish

$$\textsc{Welfare}(\vec{x}(q)) \geq \frac{OPT}{2(1+\delta)} \min\{1, \delta\}.$$

$\square$