Credible, Optimal Auctions via Blockchains

Tarun Chitra [*] Matheus V. X. Ferreira [†] Kshitij Kulkarni [‡]

January 30, 2023

Abstract

Akbarpour and Li [1] formalized credibility as an auction desideratum where the auctioneer cannot benefit by implementing undetectable deviations from the promised auction and showed that, in the plain model, the ascending price auction with reserves is the only credible, strategyproof, revenue-optimal auction. Ferreira and Weinberg [10] proposed the Deferred Revelation Auction (DRA) as a communication efficient auction that avoids the uniqueness results from [1] assuming the existence of cryptographic commitments and as long as bidder valuations are MHR. They also showed DRA is not credible in settings where bidder valuations are α-strongly regular unless $\alpha > 1$. In this paper, we ask if blockchains allow us to design a larger class of credible auctions. We answer this question positively, by showing that DRA is credible even for α-strongly regular distributions for all $\alpha > 0$ if implemented over a secure and censorship-resistant blockchain. We argue ledgers provide two properties that limit deviations from a self-interested auctioneer. First, the existence of smart contracts allows one to extend the concept of credibility to settings where the auctioneer does not have a reputation—one of the main limitations for the definition of credibility from Akbarpour and Li [1]. Second, blockchains allow us to implement mechanisms over a public broadcast channel, removing the adaptive undetectable deviations driving the negative results of Ferreira and Weinberg [10].

1 Introduction

Incentive compatibility for auctioneers has become a topic of interest to mechanism designers of auctions within digital marketplaces. In online settings, it is hard to verify the identity and strategy of an auctioneer who can simultaneously act as a buyer and can deviate from expected honest strategies. As such, auctioneers can manipulate the prices and guarantees of an auction in ways that distort an auction's clearing price and potentially reduce buyer welfare. The concept of *credibility*, a strong form of incentive compatibility for auctioneers, has been stated as a desired goal of auctions that range from basic transactions in blockchains and NFTs to online ad auctions. The US Department of Justice's 2023 antitrust suit against

[*]Gauntlet (tarun@gauntlet.network)
[†]SEAS, Harvard University (matheus@seas.harvard.edu)
[‡]UC Berkeley (ksk@eecs.berkeley.edu)

Google [25] effectively argues that Google's manipulation of ad auctions from the privileged position of auctioneer caused both buyers and users harm. In particular, the government alleges that the lack of credibility in the auction afforded Google "power to manipulate the quantity of ad inventory and auction dynamics in ways that allow it to charge advertisers more than it could in a competitive market."

Recent work has highlighted challenges in designing mechanisms that are simultaneously incentive compatible for both auctioneers and buyers. The pioneering work of Akbarpour and Li [1] considered a model that the auctioneer can modulate their communication with buyers to increase their revenue and potentially reduce buyer welfare. In their terminology, a *safe deviation* is any non-truthful communication from the auctioneer to buyers that is not detectable by any buyer alone. An auction is credible if safe deviations cannot increase the auctioneer's revenue. Akbarpour and Li [1] demonstrated that credibility cannot coexist simultaneously in an auction with truthfulness and bounded communication complexity.

On the other hand, if one is willing to assume that the auctioneer and buyers are computationally bounded in the sense that they cannot break known cryptographic assumptions, one can get around this so-called trilemma. Ferreira and Weinberg [10] demonstrated that, even if buyers can only communicate over a private channel with the auctioneer, there are cryptographic auctions that can achieve credibility, truthfulness, and bounded communication complexity if buyer valuations satisfy a regularity condition. The main mechanism involves buyers sending cryptographic commitments to their bid and collateral (such as a cryptocurrency) to the auctioneer over a private channel. The cryptographic commitments ensure that the auctioneer cannot decipher the bid from the encrypted commitment unless they break cryptographic assumptions. Moreover, the collateral requirements ensure that an auctioneer cannot add and refuse to reveal fake bids for free (which is akin to what Google is accused of doing). We call such mechanisms credible in a sense to be made precise in §2.

In the same line as Ferreira and Weinberg [10], Essaidi et al. [8] proposes the Ascending Deferred Revelation Auction (ADRA) that is credible without requiring a regularity condition on the distribution. ADRA is similar to an ascending price auction but prices increase exponentially from one round to the next. If done naively, their auction would not be revenue optimal. However, by requiring bidders to cryptographically commit to their bids at the beginning of the auction, they ensure the auction is strategyproof and revenue optimal. As a limitation, ADRA has a constant expected round complexity; however, in the worst case, the round complexity is still unbounded. In this paper, we focus on auctions with constant communication complexity in the worst case.

All aforementioned results consider a definition of credibility that assumes the auctioneer has a publicly known reputation in order to restrict the auctioneer to actions that do not damage said reputation. In both the online ad auction and blockchain scenarios, the reputation of the auctioneer cannot be relied on. For online ad auctions, the auctioneer is a monopolist who can adjust reserve prices ex-post at will (as the DoJ accuses Google of doing [25]). For blockchains, an auctioneer selling non-fungible tokens (NFTs) [22] or block space [13, 24] can easily forge multiple pseudonymous identities.

Moreover, prior work has investigated how credibility and audibility are closely related [17]. However, all aforementioned results assume that buyers and the auctioneer are communicating over private channels. To be precise, if only a private channel is available, then a buyer Alice can only communicate with another buyer Bob by sending a message to the auctioneer and the auctioneer is responsible for forwarding this message to Bob. This allows the auctioneer to launch a man-in-the-middle attack by censoring and injecting messages. On the other hand, if a censorship-resistant public channel is available (like the one enabled by public blockchains), then (1) any message Alice sends over the public channel reaches all other players, and (2) any message Alice receives over the public channel was also received by all other players. This presents the following question: what if the auction took place over public channels, such as a blockchain? Would it then be possible to achieve a credible, truthful, and bounded communication auction for a large class of valuation distributions? We summarize our findings as follows:

- Theorem 4.1: if one implements the Deferred Revelation Auction (DRA) of Ferreira and Weinberg [10] over a secure, censorship-resistant ledger, then DRA is credible for α-strongly distribution valuations as long as $\alpha > 0$. On the other hand, Ferreira and Weinberg [10] showed that DRA is not credible for these valuations if buyers and the auctioneer communicate over private channels. This shows that implementing auctions over public channels can expand the domains for which these auctions are credible.

- Theorem 5.1: DRA over a ledger is not necessarily credible if buyer valuations are regular—or equivalently α-strongly regular for $\alpha = 0$. Thus although blockchains increase the class of credible auctions, it is not a magic bullet that applies to all settings.

1.1 Technical overview

It is believed that blockchains can increase market transparency although little is known about the theory of what can or cannot be accomplished with a blockchain. In this paper, we study the problem of designing credible optimal single-item auctions n buyer auctions with independent valuations and show that it is possible to deploy blockchains in the design of so-called credible auctions. We model a secure, censorship-resistant blockchain as a public functionality that allows anyone to: write immutable data to a ledger, i.e, once data is written it cannot be erased; read previously written data; and execute algorithms on previously written data. Thus a blockchain provides the abstraction of a censorship-resistant public channel where agents can not only communicate, but also execute trusted computations.

A public channel is non-existent in the credibility framework of Akbarpour and Li [1] because they envision auctions executing over the Internet where communication often takes place over a private channel. There, the auctioneer promises to implement an auction and is the nexus of communication with buyers. Each buyer privately sends their actions to the auctioneer and rely on the same to report the action of other buyers. They showed a striking negative result: no communication-efficient auction exists if one aims to design an optimal, strategyproof, and credible auction.

Ferreira and Weinberg [10] showed that standard cryptographic assumptions can avoid the negative result above by proposing the Deferred Revelation Auction (DRA), a two-round auction that is optimal, strategyproof, and credible for certain buyer valuations. They consider classes of valuations known as α-strongly regular parameterized by $\alpha \geq 0$ and showed DRA is credible if and only if $\alpha \geq 1$ [10]. As our main contribution, we show DRA is credible for all $\alpha > 0$ if implemented over a blockchain.

Informally, DRA is a two-phase auction consisting of a commitment and a revelation phase (see §3). During the commitment phase, each buyer sends a cryptographic commitment to a bid to the auctioneer. The auctioneer is responsible for sharing the cryptographic commitment with all other buyers. During the revelation phase, each buyer reveals their bid. Finally, the auctioneer implements the second-price auction with reserves with the revealed bids. To punish a buyer that refuses to reveal their bid, each buyer must also deposit collateral during the commitment phase which is refunded only if their bid is revealed.

To show DRA is not credible for $\alpha \in (0, 1)$, Ferreira and Weinberg [10] used an adaptive strategy that, at a high level, partitions the buyers into two sets A_1 and A_2 where A_2 contains a single buyer. By adaptive strategy, we mean that the auctioneer's actions with one buyer might depend on the actions of other buyers. The auctioneer implements the auction honestly with buyers in the first group. After learning the highest bid b in A_1, the auctioneer raises the reserve price for buyer A_2 by committing to a fake bid of $b + \Delta$ if b is sufficiently large. During the revelation phase, the auctioneer refuses to reveal the fake bid $b + \Delta$ if the buyer in A_2 bids more than b and less than $b + \Delta$. This deviation is possible because, at a particular point in time, buyers in A_1 believe the auction is in the revelation phase while the buyer in A_2 believes the auction is in the commitment phase. Since buyers cannot communicate, they cannot detect this deviation.

Intuitively, to see why the deviation above is profitable, consider the following cases. For the case where the highest bidder is in A_1, the auctioneer receives the same payment as if he was honest since the auctioneer did not cheat these bidders. For the case where the highest bidder is in A_2, we can argue that it is worth it for the auctioneer to increase the reserve price to $b + \Delta$ as long as $\alpha < 1$. If DRA was implemented over a public channel, then this deviation would not be possible because all buyers would be synchronized in the same phase of the auction, i.e., any fake bids the auctioneer sends to buyer A_2 must be independent of b. Hence, our positive shows that adaptive deviations are the only deviations driving this negative result of Ferreira and Weinberg [10].

For the case where valuations are regular (α-strongly regular with $\alpha = 0$), Ferreira and Weinberg [10] gives a non-adaptive strategy to show DRA is not credible. Because this strategy is non-adaptive, we argue the same strategy can be used to show that even if DRA was implemented over a blockchain, then it might not be a credible auction.

1.2 Applications of Credible Auctions and Related Work

While the natural application for a credible auction might seem like a monopolist controlled ad auction, like that of Google, there are a number of other contexts where auctions such as the DRA are applicable. These auctions take place on and/or are settled on blockchains which are natural users of the DRA. The three major auctions we will discuss are non-fungible token (NFT) auctions, maximal extractable value (MEV) auctions, and proposer-builder separation. The latter two auctions are related to the integrity and security of a blockchain itself whereas the former can be viewed as a smart contract that runs on a blockchain and is used to perform price discovery of digital goods.

NFTs. Non-fungible tokens (NFTs) are data structure that can be used to represent a unique, non-divisible asset. Commonly, NFTs are used to represent art and/or collectibles and users purchase NFTs with fungible tokens such as Ethereum and/or stablecoins—tokenized representations of currencies such as dollars. The majority of NFTs are transferred via auctions on platforms such as OpenSea, which has had tens of billions of dollars of auction volume since 2020. NFT auctions have been studied formally and it has been demonstrated that they cannot achieve incentive compatibility and collusion resistance in [22]. One natural question is if one can achieve a credible auction in this setting, extending the weaker equilibrium notion that can be found in [22] for strongly regular distributions. The DRA defined in §3 extends the results of [22] to a broader class of distributions and an improved equilibrium condition.

Miner Extractable Value. Maximal extractable value (MEV) refers to any excess value that validators of a blockchain can extract for themselves by reordering, adding, or removing transactions to a blockchain. Since 2020, the majority of MEV has been extracted via coordinated auctions run by validators, with the most popular auction being the Flashbots auction [16]. Flashbots, in particular, has generated billions of dollars of auction revenue for validators (participants that validate transactions and add blocks to a blockchain). Bidders in these auctions, known as MEV searchers, bid on transaction priority for sequences of transactions. For instance, a bidder who sees a publicly posted Ethereum transaction for a trade may enter the auction with a bundle consisting of a front-run transaction plus the public user transaction. If a bidder wins an auction, they are guaranteed that their bundle of transactions is included in the block and the auction revenue is distributed to the validator who proposed that successful block. These auctions and MEV have been studied in a number of works that analyzed empirical auction performance [7, 26], theoretical properties such as the price of anarchy [20], optimal bidding strategies [3], and mechanisms for reducing auction revenue [9, 21, 18, 6].

Currently, these auctions are run as sealed-bid, first-price auctions[1] run by a monopolist. However, there has been a desire to decentralize this auction and have no single entity control it, as this has been a source of centralization in blockchains [15]. Part of the reason for this is that such auctions can be used to censor particular transactions and/or delay confirmation of time-sensitive transactions. The act of decentralizing such auctions such that there is no single auctioneer who can manipulate the outcome is tantamount to having a credible and truthful auction. Moreover, to ensure the liveness of the underlying blockchain—its ability to continue to accept transactions—, one needs bounded communication complexity.

Flashbots explicitly asks for this in their early design of their decentralized auction [19]:

> If inclusion is not monopolized [...] it might be the case that the sequence of auctions is important in determining where value flows [...] the designs explored in this article feature two auctions, with the first executed without "full information". Is it possible to design a single incentive-compatible, credible auction that takes into account more information?

[1]We note that there are side-channels for reading auction bids that often render these auctions not sealed-bid in practice, as adversaries with enough resources, can learn your bids. However, the majority of the documentation on these auctions describes them as 'sealed-bid' in that the auctioneer does not share the bids with other bidders, even after an auction has been completed.

The DRA presented in §3 is, to the authors' best knowledge, the first auction to meet these requirements in the blockchain setting with independent private valuations. We motivate our consideration of α-strongly regular distributions in Appendix A in blockchains by giving examples of value distributions in MEV auctions that are naturally strongly regular, but not monotone hazard. We show that in a class of decentralized exchanges popular in blockchains called constant function market makers (CFMMs) [2], valuations are generically strongly regular but may not be monotone hazard. Further, most MEV auctions that run on blockchains occur in transactions originating from CFMMs [16]. We further introduce transaction types called liquidations (which occur on most blockchains) whose values are not even regular, and demonstrate that DRA is not credible for these tranasctions which have non-trivial revenue within MEV auctions.

Proposer-Builder Separation. While an MEV auction is often defined as a combinatorial auction where bidders have valuations for distinct transaction bundles, there exist other blockchain auctions that involve selling a single item. MEV auctions are primarily run outside of the consensus mechanism of a blockchain that determines the validity of a new sequence of transactions. This is because it is impossible for a decentralized network to come to an agreement on particular orderings (i.e., it reduces to ranked voting, and Arrow's impossibility theorem applies [18]).

On the other hand, new consensus mechanisms enable a validator to delegate block building to another party allowing the validator to auction an entire block. For example, Proof-of-Work requires the block to be determined before validator selection. On the other hand, Proof-of-Stake allows the block content to be determined after the validator is selected [11, 12]. Thus the validator selected can auction away the privilege to build the next block by receiving offers (b, B) where $b \in \mathbb{R}_+$ is a bid and B is a valid block. These are single-item auctions, where the auctioneer is selling the right for B to become the next block. This separation between the proposer (the winner of the lottery to become the next block proposer) and the builder (the bidder submitting valid blocks) is meant to increase the decentralization of block production in blockchains.

Until now, it has not been formally known if such a scheme can be made incentive compatible. Prior heuristic analysis by Buterin [5] demonstrates that the cost of censorship (e.g., forcing a particular bid to not win in spite of being the highest bid) decreases in the PBS model. However, this model did not account for the auctioneer (the proposer) also participating in the auction and adding fake bids. The collateral requirements for the DRA of §3 can be used to formally realize the censorship-resistant bounds of Buterin [5]. Moreover, the credibility of this auction ensures that even if the auctioneer deviates, provided that the PBS auction follows a DRA and user valuations are α-strongly regular, private, and independent, then censorship in PBS incentive is incompatible.

1.3 Paper organization

We provide optimal auction theory background and formalize the concept of credibility at §2. We define the implementation of the deferred revelation auction over a ledger at §3. We prove our main result, Theorem 4.1, at §4 and our negative result, Theorem 5.1, at §5. We conclude at §6 and include future directions.

2 Preliminaries

We consider a single item, n buyers auction. Buyer $i \in [n] = \{1, \dots, n\}$ has private value $v_i \in \mathbb{R}^+$ and derives quasilinear utility: if they receive the item and pay p_i, then their utility is $v_i - p_i$; if they do not receive the item, then their utility is 0. We assume v_i is drawn independently from distribution D_i with CDF F_i and PDF f_i. The auctioneer knows D_i, but not v_i. Moreover v_i is independent of v_j for all $i \neq j$. We define the product distribution $D = \times_{i=1}^{n} D_i$. We focus on the i.i.d. case where there is a distribution D_0 and $D_i = D_0$ for all i. The auction that allocates the item and charges payments is a game in extended form as follows.

Extended-form game. An auction as an *extended-form game* consists of a tree (H, E) where H represent the set of histories. The game starts at the root of (H, E), has a set of players $\{1, \dots, n\}$ and a collection of actions $A(h)$ available at each history $h \in H$. We refer to player 0 as the auctioneer and player $i \in [n]$ as buyer i. Each history $h \in V$ has one owner $P(h) \in [n]$ responsible for taking the next action. After taking action $a \in A(h)$, the game moves to another history h' where $(h, h') \in E$. We consider games of incomplete information. Formally, a game is of *incomplete information* if only agent $P(h)$ observes the action $A(h)$ taken at h.

A strategy s_i for agent i is a function that takes any history $h \in H$ where $i \in P(h)$ and outputs the agent's action $s_i(h) \in A(h)$. Consider a strategy profile $\vec{s} = (s_1, \dots, s_n)$. Then, the outcome of the auction game is $(\vec{x}(\vec{s}), \vec{p}(\vec{s}))$ where $x_i(\vec{s})$ and $p_i(\vec{s})$ denotes the probability that agent i receives the item and their payment respectively. We write the outcome as $(\vec{x}(\vec{b}), \vec{p}(\vec{b}))$ when the buyer's strategy consists of submitting bids.

Definition 2.1 (Ex post Nash/Strategyproof/Individually Rational)**.** A strategy profile $\vec{s}$ forms an *ex post Nash equilibrium*, if for all buyers i, strategy s_i is a best response to $\vec{s}_{-i}$. An auction is *strategyproof* if there is a strategy profile $\vec{s}$ that forms an ex post Nash equilibrium. An auction is *individually rational* if for all buyers there is a strategy that ensures that buyer receives non-negative utility.

Next, we define the concept of credibility. Informally, it states that the auctioneer promises to implement a game G; however, the auctioneer can implement a game $G' \neq G$ where no buyer, by observing only their own actions, can distinguish G' from G. Then, the auction G is credible, if the auctioneer cannot benefit from deviating and implementing a game $G' \neq G$.

Definition 2.2 (Safe Deviation/Credible Auction)**.** The auctioneer implements a *safe deviation* from the promised game (H, E), if for all buyers $i \in [n]$, their communication and and resulting allocation/payments is consistent with some strategy profile $\vec{s}^{\,i}_{-i} = (s^i_1, s^i_2, \dots, s^i_{n_i})$ for the game (H, E) where bidder i believes there is n_i bidders in the auction. The auction is *credible* if over all safe deviations, implementing the promised auction maximizes the auctioneer's expected revenue.

We extend the model above by assuming players have actions consisting of writing and reading messages from a public ledger. Once a message is written it cannot be erased and anyone can read previously written messages and execute programs/smart contracts that have access to previously written information. As a result, writing a message or executing a smart contract in the ledger is an action that is observed by all other players.

Definition 2.3 (Ledger/Smart Contracts)**.** A ledger provides $\textsc{write}(\cdot)$, $\textsc{read}()$, and a contract execution functionality $\textsc{execute}(\cdot)$. The functionality $\textsc{write}(\cdot)$ takes a message m and writes it to the ledger. The functionality $\textsc{read}()$ outputs all messages previously written to the ledger. A smart contract A is an algorithm that takes previously written information and writes the output to the ledger. The functionality $\textsc{execute}(\cdot)$ takes a smart contract A and executes it in the ledger.

2.1 Virtual values

The formalism for optimal auctions is closely related with the concept of virtual valuations. The *virtual value function* associated with continuous CDF F and PDF f is $\varphi^F(x) = x - \frac{1-F(x)}{f(x)}$. We write $\varphi^F(\cdot)$, omitting the superscript F, when the distribution is clear from the context. We refer to $\bar{\varphi}(\cdot)$ as *Myerson's ironed virtual value* [23] which is a montone increasing function. A distribution F is *α-strongly regular* for $\alpha \geq 0$ if for all $x' \geq x$,

$$\varphi(x') - \varphi(x) \geq \alpha(x' - x).$$

A distribution F has *Monotone Hazard Rate (MHR)*, if F is 1-strongly regular. A distribution is *regular* if F is 0-strongly regular.

Theorem 2.1 (Myerson's Theorem [23])**.** Consider an strategyproof auction that awards the item to bidder i with probability $x_i(\vec{b})$ and charges $p_i(\vec{b})$ on bids $\vec{b}$. Suppose bidder i bids $b_i = v_i$. Then expected revenue is

$$\mathbb{E}_{\vec{v} \leftarrow D}\left[\sum_{i=1}^{n} p_i(\vec{v})\right] = \mathbb{E}_{\vec{v} \leftarrow D}\left[\sum_{i=1}^{n} \bar{\varphi}_i(v_i) \cdot x_i(\vec{v})\right]$$

where $\bar{\varphi}_i(\cdot)$ is the ironed virtual value function of D_i. We refer to the right-hand side as the expected *virtual welfare*. Since $\bar{\varphi}$ is non-decreasing, the optimal auction maximizes expected virtual welfare.

We define the inverse of a monotone function $g(\cdot)$ to be $g^{-1}(y) = \inf_x\{x \mid g(x) \geq y\}$. We define to $r(D_0) := (\bar{\varphi}^{F_0})^{-1}(0)$ as *Myerson's reserve price*. From Myerson's theorem, the optimal auction only sells the item to buyers with value $v_i \geq r(D_0)$. We define $\textsc{Rev}(D)$ as the revenue of the optimal auction when bidder valuations are drawn from D.

Lemma 2.1 (Lemma 7.2 in [10])**.** Let D_0 be α-strongly regular. Then for all $p \geq r(D_0)$,

$$p \cdot Pr_{\vec{v} \leftarrow D_0}\left[v \geq p\right] \leq r(D_0) \cdot Pr_{\vec{v} \leftarrow D_0}\left[v \geq r(D_0)\right](1-\alpha)^{-1/(1-\alpha)}\left(\frac{r}{p}\right)^{\frac{\alpha}{1-\alpha}}.$$

Corollary 2.1. Let D_0 be α-strongly regular. Then for all $p \geq r(D_0)$,

$$\mathbb{E}_{\vec{v} \leftarrow D_0}\left[\varphi(v) \cdot \mathbb{1}(v \geq p)\right] \leq \mathbb{E}_{\vec{v} \leftarrow D_0}\left[\varphi(v) \cdot \mathbb{1}(v \geq r(D_0))\right](1-\alpha)^{-1/(1-\alpha)}\left(\frac{r}{p}\right)^{\frac{\alpha}{1-\alpha}}.$$

Proof. Consider a single item, single bidder posted-price mechanism that offers the item at price p. The bidder value is drawn from D_0. The revenue is $pPr_{\vec{v}\leftarrow D_0}[v \geq p]$ because the bidder purchase whenever their value is bigger than p. From Myerson's theorem, $pPr_{\vec{v}\leftarrow D_0}[v \geq p] = \mathbb{E}_{\vec{v}\leftarrow D_0}[\varphi(v) \cdot \mathbb{1}(v \geq p)]$. The result follows directly by applying Lemma 2.1 to the left-hand side of the inequality. $\square$

3 The Deferred Revelation Auction (DRA) over a Ledger

In this section, we define the deferred revelation auction over a ledger and discuss how it differs from implementing the deferred revelation auction over private channels. The main ingredient are the existence of a ledger (Definition 2.3) and a cryptographic commitment scheme that is perfectly hiding and computationally hiding commitment.

Definition 3.1 (Commitment Scheme)**.** A *commitment scheme* is a function $\textsc{Commit}(\cdot,\cdot)$ that takes a message $m \in \{0,1\}^*$, a random string $r \in \{0,1\}^\lambda$ and outputs a commitment $c \in \{0,1\}^{\textsc{Poly}(\lambda)}$ where $\lambda \in \mathbb{N}$ is the *security parameter.* A commitment scheme is *perfectly hiding* if, for all $m \neq m'$, $\textsc{Commit}(m, r)$ is identically distributed to $\textsc{Commit}(m', r)$ provided that r is uniformly random. A commitment scheme is *perfectly binding* if, for all $(m, r) \neq (m', r')$, $\textsc{Commit}(m, r) \neq \textsc{Commit}(m', r')$. Informally, a commitment scheme is *non-malleable* if by observing a commitment $c = \textsc{Commit}(m, r)$, no adversary can generate a commitment $c' = \textsc{Commit}(f(m), g(r))$ related to c.

For simplicity, we assume commitment schemes are perfectly hiding and perfect binding because the distinction between a perfect binding (resp. hiding) versus a computationally binding (resp. hiding) commitment scheme is not relevant to our results. In practice, one can show no commitment scheme is both perfect hiding and binding, and one must weaken the binding or hiding property to hold only under cryptographic assumptions such as Pedersen's commitment [14].

It will be important for our results that one uses a commitment scheme that is non-malleable. A malleable commitment scheme could allow an adversary to generate a commitment $\textsc{Commit}(m+1, g(r))$ by observing $\textsc{Commit}(m, r)$. Note this does not violate the hiding property if the adversary does not learn m. Formal definitions of non-malleability are quite involved and we refer to [14]. We note, however, malleable commitment schemes can easily be transformed into non-malleable ones if combined with a digital signature scheme. For our purposes, it suffices to assume that if an agent generates a commitment $\textsc{Commit}(b, r)$, then any commitment an adversary can generate before that agent reveals (b, r) must be independent of (b, r).

Definition 3.2 (Deferred Revelation Auction over a Ledger)**.** Let $\textsc{Commit}(\cdot,\cdot)$ be a perfectly hiding, perfectly binding, and non-malleable commitment scheme satisfying Definition 3.1. A *collateral function* $f(\cdot,\cdot)$ takes a distribution D and the number of buyers n and outputs a collateral required from each buyer to bid in the auction. For a collateral function f, $DRA(f)$ is the following auction:

Commitment Phase (1^{st} Round):

- The auctioneer writes into the ledger an announcement for the beginning of the commitment phase.
- Each buyer $i \in [n]$ picks a bid, b_i, draws r_i uniformly at random, and writes $(i, c_i := \textsc{Commit}(b_i, r_i))$ in the ledger.
- All buyers observe (c_i, D_i, i). Let n be the number of buyers that execute the previous bullet.
- Each buyer $i \in [n]$ aborts or deposits collateral $f(n, D_i)$ in the ledger.
- The auctioneer writes into the ledger an announcement for the end of the commitment phase.

Revelation Phase (2^{nd} Round):

- Each buyer i writes (i, b_i, r_i) in the ledger.
- All buyers observe (i, b_i, r_i).
- The auctioneer invokes a smart contract to execute the contract resolution as follows.

Smart Contract Resolution:

- Let S denote the set of buyers that deposited the collateral and for which $c_i = \textsc{Commit}(b_i, r_i)$, and let $b'_i := b_i \cdot I(i \in S)$. Let $i^* := \arg\max_{i \in S}\{\bar{\varphi}_i(b_i)\}$.
- If $\bar{\varphi}_{i^*}(b_{i^*}) > 0$, award buyer i^* the item. Charge them $\bar{\varphi}_{i^*}^{-1}(\max\{0, \max_{i \in S \setminus \{i^*\}}\{\bar{\varphi}_i(b_i)\}\})$.
- The smart contract transfers the collateral $f(n, D_i)$ to buyer $i \in S$. All buyers $i \notin S$ loses their collateral.

Tie-breaking:

- All ties are broken lexicographically, with the auctioneer treated as "buyer zero". With this, we will write all inequalities as $>$ or $<$, taking this tie-breaking already into account.

We briefly discuss how our construction of DRA over private channels [10] differs from DRA over a ledger. Informally, over a public ledger, if a real buyer i receives a message m, then all buyers $j \neq i$ also receive a message m. Moreover, buyers do not rely on the reputation of the auctioneer for receiving the item if they are the highest bidder or receiving back their collateral if they correctly reveal their commitment because these functionalities are implemented by the auction smart contract. We give concrete examples bellow:

1. During the first round, the auctioneer was responsible for sharing (c_i, D_i, i) with buyer $j \neq i$. For the new construction, buyer i writes (c_i, D_i, i) in the ledger so all buyer $j \neq i$ can read (c_i, D_i, i) without having the auctioneer as an intermediary. As a result, this removes deviations where the auctioneer shares (c_i, D_i, i) with only a subset of buyers.

2. The auctioneer was responsible for announcing the end of the commitment phase to buyers. In the new construction, the auctioneer announces the end of the commitment phase in the ledger. As a result, the auctioneer cannot request a buyer to reveal (b_i, r_i) if another buyer believes the auction is still in the commitment phase. Therefore, any fake bids the auctioneer sends to a buyer must be independent of not only b_i but also $\vec{b}_{-i}$ because the commitment scheme is perfectly hiding.

3. During the second round, the auctioneer was responsible for sharing (b_i, r_i) with buyer $j \neq i$. Here, buyer i writes (b_i, r_i) in the ledger and buyer j can read (b_i, r_i) without having the auctioneer as an intermediary.

4. Buyer i transfers the collateral $f(n, D_i)$ to the auctioneer and the auctioneer refunds $f(n, D_i)$ once a bidder reveals (b_i, r_i). With a ledger, the bidder can directly deposits $f(n, D_i)$ in a smart contract that refunds $f(n, D_i)$ once a bidder reveals a (b_i, r_i) such that $c_i = \textsc{Commit}(b_i, r_i)$. This point is not relevant for the proof of credibility since the auctioneer is always restricted to safe deviations; however, it shows our framework can be applied to settings where the auctioneer does not have a reputation.

It is useful to remind that there are still safe deviations that are still possible for a self-interested auction which makes arguing about the credibility of DRA non-trivial. They are as follows:

- Write in the ledger commitments $\hat{c} = \textsc{Commit}(\hat{b}, \hat{r})$ during the commitment phase. Note that $\hat{b}$ must be independent of real bids $\vec{b}$.

- Refuse to reveal $(\hat{b}, \hat{r})$ during the revelation phase with knowledge about $\vec{b}$.

Ferreira and Weinberg [10] uses the following strategy (Definition 3.3) to show that $DRA(f)$ is not credible for any f when buyer valuations are α-strongly regular. Note this strategy is not possible when implementing DRA over a ledger because the auctioneer sends a commitment $\hat{c} = \textsc{Commit}(\hat{b}, \hat{r})$ to buyer n where $\hat{b}$ depends on b_{-i}.

Definition 3.3 (Adaptive Reserve Price Deviation)**.** Assume $n \geq 2$ buyers. The *adaptive reserve price deviation* is a safe deviation for the deferred revelation auction (over private channels) that proceeds as follows:

- For buyer $i \in [n-1]$, the auctioneer announces $n-1$ competing bidders and shares the commitment (c_j, D_j, j) for all $j \in [n] \setminus \{i\}$. Note the auctioneer is being honest with these bidders.

- The auctioneer request buyer $i \in [n-1]$ to reveal (b_i, r_i). Buyer i complies by revealing (b_i, r_i) such that $c_i = \textsc{Commit}(b_i, r_i)$. Let $i^* \in \arg\max_{i \in [n-1]} v_i$.

- The auctioneer picks a large threshold of $T > r(D_0)$. If $b_{i^*} < T$, the auctioneer behaves honestly with buyer n for the rest of the auction.

- If $b_{i^*} \geq T$, the auctioneer announces two competing bidders. The auctioneer sends commitments to bids b_{i^*} and $\hat{b} = b_{i^*} + f(n, D_0)$ to buyer n.

- The auctioneer request buyer n to reveal (b_n, r_n). Buyer n complies and reveals (b_n, r_n) such that $c_n = \textsc{Commit}(b_n, r_n)$. Proceed as follows depending on b_n:
  - If $b_n < b_{i^*}$, the auctioneer reveals $\hat{b}$. Allocates the item to buyer i^* if $b_{i^*} \geq r(D_0)$.
  - If $b_n \in [b_{i^*}, \hat{b}]$, the auctioneer withholds $\hat{b}$ and reveals b_{i^*}. The auctioneer allocates the item to buyer n who pays b_{i^*}.
  - If $b_n > \hat{b}$, the auctioneer reveals all bids. The auctioneer allocates the item to buyer n who pays $\hat{b}$.

Next, we highlight a few relevant facts about DRA over a public ledger. For buyer $i \in [n]$, define $\beta_i(\vec{b})$ as the highest bid the ledger receives not including b_i. Note that it is possible $\beta_i(\vec{b}) > b_i$ if the highest bid is from a fake bidder. Let $\beta(\vec{b}) := \max_{i\in[n]} \beta_i(\vec{b})$.

Observation 3.1. For all bidding profiles $\vec{b}$, $b_i > \beta_i(\vec{b})$ for at most one buyer.

Ferreira and Weinberg [10] proves a similar result for DRA over private channels by observing that if $b_i > \beta_i(\vec{b})$ and $b_j > \beta_j(\vec{b})$ for buyers $i \neq j$, then both buyers intend to receive the item. Since there is a single item for sale, the auctioneer is unable to satisfy both buyers harming the auctioneer's reputation. Over a public ledger, the proof of Lemma 3.1 does not need to appeal for the auctioneer's reputation.

Proof of Observation 3.1. Clearly $\beta_i(\vec{b}) \geq b_j$ for all i and $j \neq i$. If $b_i > \beta_j(\vec{b})$ and $b_j > \beta_j(\vec{b})$ for two distinct buyers i and j, then $b_i > \beta_j(\vec{b}) \geq b_j$ and $b_j > \beta_j(\vec{b}) \geq b_i$, a contradiction. □

Observation 3.2. If $b_i > \beta_i(\vec{b})$, then buyer i is the highest bid in $\vec{b}$. That is, $b_i > b_j$ for all $j \neq i$.

Proof. Clearly $\beta_i(\vec{b}) \geq b_j$ for all $j \neq i$. Then $b_i > \beta_i(\vec{b}) \geq b_j$ as desired. □

Lemma 3.1. Consider an optimal safe deviation where there is a bidding profile $\vec{b}$ where the collateral is at least $\beta(\vec{b})$. Then there is an optimal safe deviation with no history where the auctioneer withholds a fake bid.

Lemma 3.1 will be important when showing that DRA over a ledger is credible for α-strongly regular distribution. Informally, it states that if DRA is not credible, then the auctioneer must *always* commit to a fake bid that is larger than the collateral. Note Lemma 3.1 is not true for DRA implemented over private channels which is witnessed by the adaptive strategy in Definition 3.3 since it is possible $\beta(\vec{b})$ is smaller than the collateral whenever $b_{i^*} \leq T$.

Proof of Lemma 3.1. Let k be the collateral the auctioneer deposits for each fake bid. If the auctioneer cryptographically commits to any fake bids, they must all be independent of $\vec{b}$ because the commitment scheme is perfectly hiding and non-malleable. Thus if the auctioneer commits to any fake bids, they are all smaller than k. To see, observe that if any fake bid $\hat{b}$ is strictly bigger than k, then we must have that $\beta(\vec{b}) \geq \hat{b} > k$ for all $\vec{b}$, a contradiction. This proves that if $\hat{b}$ is a fake bid, then $\hat{b} < k$

Next, suppose for contradiction, the auctioneer withholds a fake bid $\hat{b} < k$. Then there is a real bidder i that wins the item; otherwise, the auctioneer would be indifferent between revealing $\hat{b}$ or not, i.e., the revenue is zero regardless of the auctioneer withholding $\hat{b}$ or not. Given bidder i wins the item, we argue their bid $b_i \leq \hat{b}$. To see, suppose $b_i > \hat{b}$, then the auctioneer could only improve their revenue by revealing $\hat{b}$, i.e., by revealing $\hat{b}$, the auctioneer does not pay any penalty and the price paid by bidder i can only improve. This proves $b_i \leq \hat{b} < k$. Thus to allocate the item to bidder i, the auctioneer withholds fake bid $\hat{b}$ and pays the penalty k strictly bigger than the payment $p_i(\vec{b})$. Clearly $p_i(\vec{b}) \leq b_i < k$ since bidder i pays at most their bid. Thus the auctioneer obtains negative revenue. This contradicts the assumption the auctioneer is following an optimal safe deviation. □

4 DRA over a Ledger is credible for α-strongly regular distributions

We will require Lemma 4.1 from [10] which we prove for completeness.

Lemma 4.1 (Lemma 7.1 in [10])**.** Let D be α-strongly regular. Let E be an event such that $v \geq r(D)$ with probability 1 conditioned on E. Then

$$\mathbb{E}\left[v|E\right] \leq \frac{1}{\alpha}\mathbb{E}\left[\varphi^D(v)|E\right] + r(D).$$

Proof. Because D is α-strongly regular, for all $x' > x$,

$$\varphi^D(x') - \varphi^D(x) \geq \alpha(x' - x)$$

Then for any $x' \geq r(D)$, $x' \leq \frac{1}{\alpha}(\varphi^D(v) - \varphi^D(r(D))) + r(D)$. By definition $\varphi^D(r(D)) = 0$. Conditioned on event E, we have that $v \geq r(D)$ for all v. We conclude $\mathbb{E}_{\vec{v} \leftarrow D}\left[v|E\right] \leq \frac{1}{\alpha}\mathbb{E}\left[\varphi^D(v)|E\right] + r(D)$ as desired. □

Theorem 4.1. Assume all bidder valuations are α-strongly regular distribution for $\alpha > 0$. Then, there is an f such that $DRA(f)$ with access to a public ledger is credible.

Proof. Consider an optimal safe deviation. Because DRA is a truthful auction, we assume buyer i bids $b_i = v_i$. Note all bidders deposit the same collateral k that is independent of $\vec{v}$ since $f(n, D_0)$ is determined during the first round. The proof divides into the case where $k \geq \beta(\vec{v})$ for some bids $\vec{v}$ and the case where $k < \beta(\vec{v})$ for all bids $\vec{v}$.

Case 1. First, consider the case where $k \geq \beta(\vec{v})$ for some bids $\vec{v}$. From Lemma 3.1, the auctioneer never withholds any fake bid. We argue the revenue for this safe deviation is at most the revenue of the second-price auction with an optimal reserve price. To see, suppose the reserve price is r and let $\hat{r}$ be the maximum among the reserve price and the highest fake bid the auctioneer commits to. Note $\hat{r}$ is independent of $\vec{v}$ because the commitment scheme is perfectly hiding and the auctioneer must commit to fake bids before $\vec{v}$ is revealed. Thus the outcome for this auction is equivalent to the outcome of DRA with a reserve price of $\hat{r}$ where the auctioneer implements the auction faithfully, i.e., the auctioneer does not commit to any fake bids. Since DRA with a reserve price of $\hat{r}$ is a strategyproof mechanism, we use Myerson's theorem to conclude the revenue is at most

$$\mathbb{E}_{v \leftarrow D}\left[\sum_{i=1}^{n} p_i(\vec{v})\right] = \mathbb{E}_{v \leftarrow D}\left[\sum_{i=1}^{n} \varphi(v_i) \cdot x_i(\vec{v})\right] \leq \mathbb{E}\left[\max_{i=1}^{n}\{\max\{0, \varphi(v_i)\}\}\right].$$

The inequality witnesses that the revenue of this safe deviation is at most the revenue of the optimal strategyproof auction. This proves that if $k \geq \beta(\vec{v})$ for some $\vec{v}$, then the revenue of $DRA(f)$ is at most the revenue of the optimal strategyproof auction.

Case 2. Next, consider the case where $k < \beta(\vec{b})$ for all bids $\vec{b}$. To bound the expected revenue, we consider separately the case where there is a bidder j where $v_j > \beta_j(\vec{v})$ and the case where $v_j \leq \beta_j(\vec{v})$ for all j. The case where $v_j > \beta_j(\vec{v})$ follows a similar approach as in [10] and uses Observation 3.1 that states that $v_j > \beta_j(\vec{v})$ for at most one bidder.

Claim 4.1. If the collateral is at least $r(D_0)$, then

$$\mathbb{E}_{\vec{v} \leftarrow D}\left[\sum_{i=1}^{n} p_i(\vec{v}) \cdot \mathbb{1}(\exists j, v_j > \beta_j(\vec{v}))\right] \leq \mathbb{E}_{\vec{v} \leftarrow D}\left[\sum_{i=1}^{n} \varphi(v_i) \cdot x_i(\vec{v}) \cdot \mathbb{1}(v_i > \beta_i(\vec{v})) \cdot \mathbb{1}(\forall j \neq i, v_j \leq \beta_j(\vec{v}))\right]$$

Proof. From Observation 3.1, there is at most one bidder i such that $v_i > \beta_i(\vec{v})$ for all $\vec{v}$. Moreover, when $v_i > \beta_i(\vec{v})$, bidder i wins the item and pay $\beta_i(\vec{v})$. Moreover, $\beta_i(\vec{v})$ is independent of v_i. Thus the revenue is equal to the revenue of the posted-price mechanism with reserve price of $\beta_i(\vec{v})$ which from Myerson's theorem is $\mathbb{E}\left[\varphi(v_i) \cdot \mathbb{1}(v_i > \beta_i(\vec{v}))\right]$. Therefore,

$$\begin{aligned}
\mathbb{E}_{\vec{v} \leftarrow D}\left[\sum_{i=1}^{n} p_i(\vec{v}) \cdot \mathbb{1}(\exists j, v_j > \beta_j(\vec{v}))\right] &= \mathbb{E}_{\vec{v} \leftarrow D}\left[\sum_{i=1}^{n} \beta_i(\vec{v}) \cdot \mathbb{1}(v_i > \beta_i(\vec{v}))\right] \\
&= \mathbb{E}_{\vec{v} \leftarrow D}\left[\sum_{i=1}^{n} \varphi(v_i) \cdot \mathbb{1}(v_i > \beta_i(\vec{v}))\right] \qquad \{\text{By Theorem 2.1}\} \\
&= \mathbb{E}_{\vec{v} \leftarrow D}\left[\sum_{i=1}^{n} \varphi(v_i) \cdot \mathbb{1}(v_i > \beta_i(\vec{v})) \cdot \mathbb{1}(\forall j \neq i, v_j \leq \beta_j(\vec{v}))\right] \\
&= \mathbb{E}_{\vec{v} \leftarrow D}\left[\sum_{i=1}^{n} \varphi(v_i) \cdot x_i(\vec{v}) \cdot \mathbb{1}(v_i > \beta_i(\vec{v})) \cdot \mathbb{1}(\forall j \neq i, v_j \leq \beta_j(\vec{v}))\right]
\end{aligned}$$

The second line is Myerson's theorem. The third line observes that $v_i > \beta_i(\vec{v})$ for at most one buyer. The last line observes that the reserve price of the auction is $r(D_0)$ and $\beta(\vec{v}) \geq r(D_0)$. Since $\beta(\vec{v}) = \max\{\beta_i(\vec{v})\}$, $v_i > \beta_i(\vec{v})$, $v_j \leq \beta_j(\vec{v})$ for all $j \neq i$, we conclude that $v_i > \beta(\vec{v}) \geq r(D_0)$. Since buyer i has value $v_i > \beta(\vec{v}) \geq r(D_0)$, then buyer i must receive the receive whenever $v_i > \beta_i(\vec{v})$. □

To bound the expected revenue for the case where $v_j \leq \beta_j(\vec{v})$ for all j, we consider separately the case where $\alpha \geq 1$ and the case where $\alpha \in (0, 1)$.

Case 2.1. Consider the case where $\alpha \geq 1$. We will set $f(n, D_0) = r(D_0)$. This case follows from a similar argument by Ferreira and Weinberg [10] when showing DRA over private channels is credible for MHR distribution.

Claim 4.2. If $r(D_0) \le k < \beta(\vec{v})$ for all $\vec{v}$ and $\alpha \ge 1$, then

$$\mathbb{E}_{\vec{v} \leftarrow D}\left[\sum_{i=1}^{n} p_i(\vec{v}) \cdot \mathbb{1}(\forall j, v_j \le \beta_j(\vec{v}))\right] \le \mathbb{E}_{\vec{v} \leftarrow D}\left[\sum_{i=1}^{n} \varphi(v_i) \cdot x_i(\vec{v}) \cdot \mathbb{1}(\forall j, v_j \le \beta_j(\vec{v}))\right]$$

Proof. When $v_i < \beta_i(\vec{v})$ for all buyers i, any buyer can the item as long as the auctioneer withholds at least one bid and pays a penalty of k. Since buyer i pays at most v_i and the safe deviation is optimal, the auctioneer only allocates the item to buyer i if $v_i \ge k \ge r(D_0)$. We conclude

$$\begin{aligned}
\mathbb{E}_{\vec{v} \leftarrow D}\left[\sum_{i=1}^{n} p_i(\vec{v}) \cdot x_i(\vec{v}) \cdot \mathbb{1}(\forall j, v_j \le \beta_j(\vec{v}))\right] &\le \mathbb{E}_{v \leftarrow D}\left[\sum_{i=1}^{n} (v_i - k) \cdot x_i(\vec{v}) \cdot \mathbb{1}(\forall j, v_j \le \beta_j(\vec{v})) \cdot \mathbb{1}(v_i \ge k)\right] \\
&\le \mathbb{E}_{\vec{v} \leftarrow D}\left[\sum_{i=1}^{n} \left(\frac{1}{\alpha}\varphi(v_i) + r(D) - k\right) \cdot x_i(\vec{v}) \cdot \mathbb{1}(\forall j, v_j \le \beta_j(\vec{v})) \cdot \mathbb{1}(v_i \ge k)\right] \qquad \{\text{By Lemma 4.1}\} \\
&\le \mathbb{E}_{\vec{v} \leftarrow D}\left[\sum_{i=1}^{n} \varphi(v_i) \cdot x_i(\vec{v}) \cdot \mathbb{1}(\forall j, v_j \le \beta_j(\vec{v}))\right]
\end{aligned}$$

The first line observes that if buyer i receives the item, they pay at most v_i and the auctioneer loses a collateral of k by withholding at least one bid. We also use the fact that $v_i \ge k$; otherwise, the auctioneer receives negative revenue by allocating the item to buyer i. The third lines observes that $\alpha \ge 1$ and $r(D_0) \le k$. □

From Claims 4.1 and 4.2, we obtain

$$\begin{aligned}
\mathbb{E}_{\vec{v} \leftarrow D}\left[\sum_{i=1}^{n} p_i(\vec{v})\right] &= \mathbb{E}_{\vec{v} \leftarrow D}\left[\sum_{i=1}^{n} p_i(\vec{v}) \cdot \mathbb{1}(\exists j, v_j > \beta_j(\vec{v}))\right] + \mathbb{E}_{\vec{v} \leftarrow D}\left[\sum_{i=1}^{n} p_i(\vec{v}) \cdot \mathbb{1}(\forall j, v_j \le \beta_j(\vec{v}))\right] \\
&\le \mathbb{E}_{\vec{v} \leftarrow D}\left[\sum_{i=1}^{n} \varphi(v_i) \cdot x_i(\vec{v}) \cdot \mathbb{1}(v_i > \beta_i(\vec{v}))\right] + \mathbb{E}_{\vec{v} \leftarrow D}\left[\sum_{i=1}^{n} \varphi(v_i) \cdot x_i(\vec{v}) \cdot \mathbb{1}(\forall j, v_j \le \beta_j(\vec{v}))\right] \\
&= \mathbb{E}_{\vec{v} \leftarrow D}\left[\sum_{i=1}^{n} \varphi(v_i) \cdot x_i(\vec{v})\right]
\end{aligned}$$

The first line is from linearity of exepectaiton and by observing the events $\{\exists j, v_j > \beta_j(\vec{v})\}$ and $\{\forall j, v_j \le \beta_j(\vec{v})\}$ partition the probability space since one is the complement of the other. The second line is due to Claims 4.1 and 4.2. The third observes that events $\{v_i > \beta_i(\vec{v})\}$ and $\{v_j > \beta_j(\vec{v})\}$ for $j \ne i$ are disjoint (By Observation 3.1). The chain of inequalities witnesses that for the case where $\alpha \ge 1$, the revenue of the safe deviation is upper bounded by the expected virtual welfare which is bounded by the revenue of the optimal auction (By Theorem 2.1).

Case 2.2. Next, we consider the case where $\alpha \in (0, 1)$. We will set

$$f(n, D_0) = r(D_0)\left(\frac{n}{\alpha}\right)^{\alpha/(1-\alpha)} (1-\alpha)^{-(1+\alpha)/(1-\alpha)}.$$

Note $f(n, D_0) \ge r(D_0)$ for all $n \ge 1$ and $\alpha \in (0, 1)$.

Claim 4.3. Assume $k < \beta(\vec{b})$ fora all $\vec{b}$, $\alpha \in (0,1)$ and $k = r(D_0)\left(\frac{n}{\alpha}\right)^{\alpha/(1-\alpha)}(1-\alpha)^{-(1+\alpha)/(1-\alpha)}$. Then

$$\begin{aligned}\mathbb{E}_{v\leftarrow D}\left[\sum_{i=1}^{n} p_i(\vec{v})\cdot x_i(\vec{v})\cdot \mathbb{1}(\forall j, v_j \leq \beta_j(\vec{v}))\right] &\leq \textsc{Rev}(D)\\ &- \mathbb{E}_{v\leftarrow D}\left[\sum_{i=1}^{n}\varphi(v_i)\cdot x_i(\vec{v})\cdot \mathbb{1}(v_i > \beta_i(\vec{v}))\cdot \mathbb{1}(\forall j\neq i, v_j \leq \beta_j(\vec{v}))\right]\end{aligned}$$

Proof. When all buyers i have a value smaller than $\beta_i(\vec{v})$, any buyer can receive the item as long as the auctioneer withholds at least one bid and pays a penalty of k. Since buyer i pays at most v_i and the safe deviation is optimal, the auctioneer only allocates the item to bidder i if $v_i \geq k \geq r(D_0)$. We conclude

$$\begin{aligned}
&\mathbb{E}_{\vec{v}\leftarrow D}\left[p_i(\vec{v})\cdot x_i(\vec{v})\cdot \mathbb{1}(\forall j, v_j \leq \beta_j(\vec{v}))\right] \leq \mathbb{E}\left[(v_i - k)\cdot x_i(\vec{v})\cdot \mathbb{1}(\forall j, v_j\leq \beta_j(\vec{v}))\cdot \mathbb{1}(v_i \geq k)\right]\\
&\quad\leq \mathbb{E}_{\vec{v}\leftarrow D}\left[\left(\frac{1}{\alpha}\varphi(v_i) + r(D) - k\right)\cdot x_i(\vec{v})\cdot \mathbb{1}(\forall j, v_j \leq \beta_j(\vec{v}))\cdot \mathbb{1}(v_i\geq k)\right] \qquad \{\text{By Lemma 4.1}\}\\
&\quad\leq \mathbb{E}_{\vec{v}\leftarrow D}\left[\frac{1}{\alpha}\varphi(v_i)\cdot x_i(\vec{v})\cdot \mathbb{1}(\forall j, v_j\leq \beta_j(\vec{v}))\cdot \mathbb{1}(v_i \geq k)\right]\\
&\quad= \mathbb{E}_{\vec{v}\leftarrow D}\left[\frac{1}{\alpha}\varphi(v_i)\cdot x_i(\vec{v})\cdot \mathbb{1}(\forall j\neq i, v_j \leq \beta_j(\vec{v}))\cdot \mathbb{1}(k\leq v_i < \beta_j(\vec{v}))\right]\\
&\quad= \mathbb{E}_{\vec{v}\leftarrow D}\left[\varphi(v_i)\cdot x_i(\vec{v})\cdot \mathbb{1}(\forall j\neq i, v_j\leq \beta_j(\vec{v}))\cdot\left(\frac{\mathbb{1}(v_i\geq k)}{\alpha} - \frac{\mathbb{1}(v_i > \beta_i(\vec{v}))}{\alpha}\right)\right]\\
&\quad\leq \mathbb{E}_{\vec{v}\leftarrow D}\left[\varphi(v_i)\cdot x_i(\vec{v})\cdot \mathbb{1}(\forall j\neq i, v_j\leq \beta_j(\vec{v}))\cdot\left(\frac{\mathbb{1}(v_i\geq k)}{\alpha} - \mathbb{1}(v_i > \beta_i(\vec{v}))\right)\right]\\
&\quad= \mathbb{E}_{\vec{v}\leftarrow D}\left[\varphi(v_i)\cdot x_i(\vec{v})\cdot \mathbb{1}(\forall j\neq i, v_j\leq \beta_j(\vec{v}))\cdot\frac{\mathbb{1}(v_i\geq k)}{\alpha}\right]\\
&\qquad - \mathbb{E}_{\vec{v}\leftarrow D}\left[\varphi(v_i)\cdot x_i(\vec{v})\cdot \mathbb{1}(\forall j\neq i, v_j\leq \beta_j(\vec{v}))\cdot \mathbb{1}(v_i > \beta_i(\vec{v}))\right]
\end{aligned}$$

The first line observes that if buyer i receives the item, they pay at most v_i and the auctioneer pays at least k for withholding one bid. The second line uses the fact $k \geq r(D_0)$ and $v_i \geq k$ which allows us to apply Lemma 4.1. The third line uses the fact $k \geq r(D_0)$. The sixth line observes $\alpha < 1$. The last line is by the linearity of expectation. By linearity of expectation.

To bound the first expected value, we use the fact $k \geq r(D_0)$ in Corollary 2.1 to obtain

$$\begin{aligned}
&\mathbb{E}_{\vec{v}\leftarrow D}\left[\sum_{i=1}^{n} \varphi(v_i)\cdot x_i(\vec{v})\cdot \mathbb{1}(\forall j\neq i, v_j \leq \beta_j(\vec{v}))\cdot \frac{\mathbb{1}(v_i\geq k)}{\alpha}\right] \leq \frac{1}{\alpha}\mathbb{E}_{\vec{v}\leftarrow D}\left[\sum_{i=1}^{n}\varphi(v_i)\cdot \mathbb{1}(v_i\geq k)\right]\\
&= \frac{1}{\alpha}(1-\alpha)^{-1/(1-\alpha)}\left(\frac{r(D_0)}{k}\right)^{\frac{\alpha}{1-\alpha}}\mathbb{E}_{\vec{v}\leftarrow D}\left[\sum_{i=1}^{n}\varphi(v_i)\cdot\mathbb{1}(v_i\geq r(D_0))\right] \qquad \{\text{By Corollary 2.1}\}\\
&= \frac{\alpha}{\alpha n}\mathbb{E}_{\vec{v}\leftarrow D}\left[\sum_{i=1}^{n}\varphi(v_i)\cdot\mathbb{1}(v_i\geq r(D_0))\right]\\
&= \frac{\alpha n}{\alpha n}\mathbb{E}_{v_1\leftarrow D_0}\left[\varphi(v_1)\cdot\mathbb{1}(v_1\geq r(D_0))\right]\\
&= \textsc{Rev}(D_0)\\
&\leq \textsc{Rev}(D)
\end{aligned}$$

The first line observes $x_i(\vec{v})\cdot\mathbb{1}(\forall j\neq i, v_j\leq\beta_j(\vec{v}))\leq 1$. The second line is Corollary 2.1. The third line substitute $k = \left(\frac{n}{\alpha}\right)^{\alpha/(1-\alpha)}(1-\alpha)^{-(1+\alpha)/(1-\alpha)}$. The fourth line observes $\varphi(v_1),\ldots,\varphi(v_n)$ are i.i.d.. The fifth line observes $r(D_0)$ is the optimal reserve price, then $\mathbb{E}_{v_1\leftarrow D_0}[\varphi(v_1)\cdot\mathbb{1}(v_1\geq r(D_0))]$ is the optimal revenue for the single bidder auction (Theorem 2.1). The last line observes the revenue increases with the number of bidders. This proves the claim. □

From Claims 4.1 and 4.3,

$$\begin{aligned}
&\mathbb{E}_{v\leftarrow D}\left[\sum_{i=1}^{n}p_i(\vec{v})\right] = \mathbb{E}_{v\leftarrow D}\left[\sum_{i=1}^{n}p_i(\vec{v})\cdot\mathbb{1}(\exists j, v_j\geq\beta_j(\vec{v}))\right] + \mathbb{E}_{v\leftarrow D}\left[\sum_{i=1}^{n}p_i(\vec{v})\cdot\mathbb{1}(\forall j, v_j\leq\beta_j(\vec{v}))\right]\\
&= \mathbb{E}_{v\leftarrow D}\left[\sum_{i=1}^{n}\varphi(v_i)\cdot x_i(\vec{v})\cdot\mathbb{1}(v_i>\beta_i(\vec{v})))\cdot\mathbb{1}(\forall j\neq i, v_j\leq\beta_j(\vec{v}))\right] + \textsc{Rev}(D)\\
&\quad - \mathbb{E}_{v\leftarrow D}\left[\sum_{i=1}^{n}\varphi(v_i)\cdot x_i(\vec{v})\cdot\mathbb{1}(v_i>\beta_i(\vec{v}))\cdot\mathbb{1}(\forall j\neq i, v_j\leq\beta_j(\vec{v}))\right] \{\text{By Claims 4.1 and 4.3}\}\\
&= \textsc{Rev}(D)
\end{aligned}$$

This proves that if $k < \beta(\vec{b})$ for all bids $\vec{b}$ and $\alpha\in(0,1)$, then the revenue of the optimal safe deviation is at most $\textsc{Rev}(D)$ for our choice of $f(n,D)$ as desired. These cover all the cases and prove $DRA(f)$ is credible for our choice of f. □

5 DRA for regular distributions

Although implementing DRA over a ledger extends the class of distributions where it is credible, it is not a magic bullet. Indeed, Theorem 5.1 states that there is a regular distribution where if a single buyer valuation is drawn from that distribution, then the auctioneer can profit from cheating. The proof of Theorem 5.1 is the same regardless if one implements DRA over private channels or over a ledger.

Theorem 5.1. There is a regular distribution D_0 such that for all f, $DRA(f)$ over a ledger is not credible even for a single buyer drawn from D_0.

We omit the proof because it is identical to the proof of Theorem 4.4 in [10]. At a high level, the counter-example considers a single buyer drawn from the equal revenue distribution where $F(x) = 1 - \frac{1}{x}$ for all $x \geq 1$ and $F(x) = 0$ for $x < 1$. Then the auctioneer sends m sufficiently large fake bids $b_1, \ldots, b_m$. We omit the precise details about $b_1, \ldots, b_m$ and refer the reader to [10]. After the real buyer reveals their bid v, the auctioneer withholds all fake bids bigger than v if v is larger than a threshold T. By carefully setting the fake bids and T, one can show this deviation obtains revenue that grows linearly with m. Although this deviation was designed for the case where one implements DRA over private channels, it is still a feasible deviation when DRA is implemented over a ledger because the auctioneer sets the fake bids before observing v and decides which fake bids to reveal after observing v.

6 Conclusion and Future Work

The lack of transparency and fairness from Internet platforms is attracting the attention of regulators as observed by the US Department of Justice lawsuit against Google [25]. It is unlikely that customers could unilaterally detect and, more importantly, prove the sophisticated market manipulations alleged in the complaint. Not surprisingly, the report was only possible due to the long and extensive investigation from the DoJ. Moreover, blockchain networks inherently require credible auctions to ensure fair inclusion and censorship resistance given their permissionless nature. This motivates the design of mechanisms that can easily be audited by market participants. In this work, we show that blockchains can be a useful tool for this task by allowing mechanisms to execute over a public channel. Concretely, we show that if implemented over a blockchain the Deferred Revelation Auction of Ferreira and Weinberg [10] is credible for more settings than it would otherwise. Blockchains are not a magic bullet since DRA remains not credible for all regular distributions; therefore, it remains an open question to expand the design of credible mechanisms for other settings including regular distributions and for multi-item auctions.

References

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

[2] G. Angeris, A. Agrawal, A. Evans, T. Chitra, and S. Boyd. Constant function market makers: Multi-asset trades via convex optimization. 2021.

[3] G. Angeris, A. Evans, and T. Chitra. A note on bundle profit maximization, 2021.

[4] G. Angeris, T. Chitra, and A. Evans. When Does The Tail Wag The Dog? Curvature and Market Making. *Cryptoeconomic Systems*, 2(1), June 2022. https://cryptoeconomicsystems.pubpub.org/pub/angeris-curvature-market-making.

[5] V. Buterin. State of research: Increasing censorship resistance of transactions under proposer/builder separation (pbs), Nov 2021. URL `https://notes.ethereum.org/@vbuterin/pbs_censorship_resistance`.

[6] C. Cachin, J. Mićić, N. Steinhauer, and L. Zanolini. Quick order fairness. In *Financial Cryptography and Data Security: 26th International Conference, FC 2022, Grenada, May 2–6, 2022, Revised Selected Papers*, pages 316–333. Springer, 2022.

[7] P. Daian, S. Goldfeder, T. Kell, Y. Li, X. Zhao, I. Bentov, L. Breidenbach, and A. Juels. Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 910–927. IEEE, 2020.

[8] M. Essaidi, M. V. Ferreira, and S. M. Weinberg. Credible, strategyproof, optimal, and bounded expected-round single-item auctions for all distributions. In *13th Innovations in Theoretical Computer Science Conference (ITCS 2022)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2022.

[9] M. V. Ferreira and D. C. Parkes. Credible decentralized exchange design via verifiable sequencing rules. *arXiv preprint arXiv:2209.15569*, 2022.

[10] M. V. Ferreira and S. M. Weinberg. Credible, truthful, and two-round (optimal) auctions via cryptographic commitments. In *Proceedings of the 21st ACM Conference on Economics and Computation*, pages 683–712, 2020.

[11] M. V. Ferreira and S. M. Weinberg. Proof-of-stake mining games with perfect randomness. In *Proceedings of the 22nd ACM Conference on Economics and Computation*, pages 433–453, 2021.

[12] M. V. Ferreira, Y. L. S. Hahn, S. M. Weinberg, and C. Yu. Optimal strategic mining against cryptographic self-selection in proof-of-stake. In *Proceedings of the 23rd ACM Conference on Economics and Computation*, pages 89–114, 2022.

[13] M. V. X. Ferreira, D. J. Moroz, D. C. Parkes, and M. Stern. Dynamic posted-price mechanisms for the blockchain transaction-fee market. In *Proceedings of the 3rd ACM conference on Advances in Financial Technologies*, AFT '21, New York, NY, USA, 2021. Association for Computing Machinery.

[14] M. Fischlin and R. Fischlin. Efficient non-malleable commitment schemes. In *Advances in Cryptology—CRYPTO 2000: 20th Annual International Cryptology Conference Santa Barbara, California, USA, August 20–24, 2000 Proceedings 20*, pages 413–431. Springer, 2000.

[15] Flashbots. The future of mev is suave: Flashbots, Nov 2022. URL `https://writings.flashbots.net/the-future-of-mev-is-suave/`.

[16] Flashbots Team. Mev explore, 2022. URL `https://explore.flashbots.net/`.

[17] A. Grigoryan and M. Moller. A theory of auditability for allocation and social choice mechanisms. *Working Paper*, 2023.

[18] M. Kelkar, S. Deb, and S. Kannan. Order-fair consensus in the permissionless setting. In *Proceedings of the 9th ACM on ASIA Public-Key Cryptography Workshop*, pages 3–14, 2022.

[19] Q. Kilbourn. Order flow, auctions and centralisation ii — order flow auctions: Flashbots, Sep 2022. URL `https://writings.flashbots.net/order-flow-auctions-and-centralisation-II`.

[20] K. Kulkarni, T. Diamandis, and T. Chitra. Towards a theory of maximal extractable value i: Constant function market makers. *arXiv preprint arXiv:2207.11835*, 2022.

[21] C. McMenamin, V. Daza, M. Fitzi, and P. O'Donoghue. Fairtradex: A decentralised exchange preventing value extraction. In *Proceedings of the 2022 ACM CCS Workshop on Decentralized Finance and Security*, pages 39–46, 2022.

[22] J. Milionis, D. Hirsch, A. Arditi, and P. Garimidi. A framework for single-item nft auction mechanism design. In *Proceedings of the 2022 ACM CCS Workshop on Decentralized Finance and Security*, pages 31–38, 2022.

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

[24] T. Roughgarden. Transaction fee mechanism design. *arXiv preprint arXiv:2106.01340*, 2021.

[25] US Department of Justice. Justice department sues google for monopolizing digital advertising technologies. *https://www.justice.gov/opa/pr/justice-department-sues-google-monopolizing-digital-advertising-technologies*, 2023.

[26] B. Weintraub, C. F. Torres, C. Nita-Rotaru, and R. State. A flash (bot) in the pan: measuring maximal extractable value in private pools. In *Proceedings of the 22nd ACM Internet Measurement Conference*, pages 458–471, 2022.

A Value Distributions in Blockchains

We now demonstrate the necessity of considering α-strongly regular distributions in blockchains, as opposed to simply MHR distributions. We further provide counterexamples of items in blockchains in which the valuations of bidders are not even regular. Together, these examples allow us to situate the study of α-strongly regular distributions that we consider in this paper. In the subsequent, we consider that the single item for sale is a *block*. A block is a set of user transactions and the auction utilized is the proposer-builder separation defined in §1.

A.1 Constant Function Market Makers

We now generalize sandwich attacks to more general contracts called *constant function market makers*, which hold some amount of *reserves* $R, R' \geq 0$ of two assets and have a *trading function* $\psi : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$. Traders can then submit a *trade* (Δ, Δ') denoting the amount they wish to tender (if negative) or receive (if positive) from the contract. The contract then accepts the trade if $\psi(R, R', \Delta, \Delta') = \psi(R, R', 0, 0)$, and pays out (Δ, Δ') to the trader.

Curvature. We briefly summarize the main definitions and results of [4] here. Suppose that the trading function ψ is differentiable (as most trading functions in practice are), then the marginal price for a trade of size Δ is $g(\Delta) = \frac{\partial_3 \psi(R,R',\Delta,\Delta')}{\partial_4 \psi(R,R',\Delta,\Delta')}$.. Here ∂_i denotes the partial derivative with respect to the ith argument, while Δ' is specified by the implicit condition $\psi(R, R', \Delta, \Delta') = \psi(R, R', 0, 0)$; i.e., the trade (Δ, Δ') is assumed to be valid. Additionally, the reserves R, R' are assumed to be fixed. Matching the notation of Section **??**, the function g is known as the *price impact* function as it represents the final marginal price of a positive-sized trade. When there are fees, one can show that $g^{fee}(\Delta) = \gamma g(\gamma \Delta)$ where $1 - \gamma$ denotes the percentage fee. We say that a CFMM is *α-stable* if it satisfies $g(0) - g(-\Delta) \leq \alpha \Delta$ for all $\Delta \in [0, M]$ for some positive M. This is a linear upper bound on the maximum price impact that a bounded trade (bounded by M) can have. Similarly, we say that a CFMM is β-liquid if it satisfies $g(0) - g(-\Delta) \geq \beta \Delta$ for all $\Delta \in [0, K]$ for some positive K. One important property of g is that it can be used to compute Δ' [4, §2.1]:

$$\Delta' = \int_0^{-\Delta} g(t) dt \tag{1}$$

Simple methods for computing α and β in common CFMMs are presented in [4, §1.1] and [2, §4]. We define $G(\Delta)$ to be the *forward exchange function*, which is equivalently the amount of output token received for an input of size Δ. Whenever we reference the function $G(\Delta)$ for a given CFMM we always make clear the reserves associated with that function. Further, $G(\Delta)$ was shown to be concave and increasing in [2].

Slippage Limits. Analogously to the case of Uniswap, when a user submits an order to a CFMM, they submit two parameters: a trade size $\Delta \in \mathbb{R}$ and a *slippage limit* $\eta \in (0, 1)$. The slippage is interpreted as the minimum output amount that the user is willing to accept as a fraction of $G(\Delta)$. That is, the trade is accepted if the amount in output token the user receives is larger than or equal to $(1 - \eta)G(\Delta)$. However, the majority of this paper will focus on representing slippage limits in quantity space (e.g. in terms of $G(\Delta)$ not $g(\Delta)$).

Valuations in CFMMs In Flashbots' MEV auction, decentralized exchange arbitrage transactions are amongst the most bid upon transactions with over $1 billion of MEV profits generated [16]. One particular type of transaction, the sandwich attack, has been formally studied and generic bounds of profitability have been constructed [20]. We can use these bounds on profitability to construct a valuation for sandwich attacks. Kulkarni et al. [20] shows the following bound for the profit of sandwiching a single trade Δ with slippage limit η:

$$\mathsf{PNL}(\Delta, \eta) \leq (O(\eta) + \gamma - 1)\,\Delta - \frac{\mu\gamma}{\beta} \leq C\max(\eta, \sqrt{1+\eta})\Delta - \frac{\mu\gamma}{\beta}$$

As such, if we receive a sequence of trades $(\Delta_1, \eta_1), \dots, (\Delta_n, \eta_n)$, we can write a user's valuation ν_i for the sequence of trades as

$$\nu_i((\Delta_1, \eta_1), \dots, (\Delta_n, \eta_n)) = \sum_{i=1}^{n} \mathsf{PNL}(\Delta_i, \eta_i)$$

Assuming that the trades (Δ_i, η_i) are drawn jointly from a distribution P, given a total trade volume V, we define the valuation for an MEV searcher (who is an auction bidder) for a given volume as

$$v_i(V) = \mathop{\mathbf{E}}_{(\Delta_i,\eta_i)\sim P}\left[\nu_i((\Delta_1, \eta_1), \dots, (\Delta_n, \eta_n)) | \sum_i \Delta_i = V\right]$$

Values for CFMMs are generically strongly regular We now demonstrate that for a sequence of CFMM trades, with total trade volume V, $v(V)$ is generically strongly regular given that the trades are sampled iid from a strongly regular distribution. Further, we assume that there exist constants μ, γ, β corresponding to a CFMM. We make the following assumption on the trade-generating distribution P: the trades $\Delta \in \mathbf{R}^n$ drawn jointly from P can be written as:

$$\Delta = D_1\mathbf{e_1} + \cdots + D_n\mathbf{e_n}$$

where D_i are sampled iid from a strongly regular distribution, $\mathbf{e_i}$ are the basis vectors in $\mathbf{R}^n$, and the slippage limits η_i are chosen deterministically. By noting that the value $\nu_i((\Delta_1, \eta_1), \dots, (\Delta_n, \eta_n)) = \sum_{i=1}^n \mathsf{PNL}(\Delta_i, \eta_i)$, we therefore have that:

$$\sum_{i=1}^{n} \mathsf{PNL}(\Delta_i, \eta_i) \leq C\max(\eta_i, \sqrt{1+\eta_i}\sum_{i=1}^{n}\Delta_i - \frac{n\mu\gamma}{\beta}$$

Noting that $\sum_{i=1}^n \Delta_i$ is also strongly regular, and that scaled and shifted strongly regular distributions are also strongly regular, we have that $v_i(V)$ is strongly regular.

Example of non-MHR Distribution in CFMMs We now construct an explicit example of a value distribution in CFMMs that is regular but not MHR. Intuitively, this occurs when the distribution of trades is 'heavy tailed', which occurs in decentralized exchanges on blockchains, especially in times of high market volatility. We assume that blocks of size 1, in which a user's trade Δ_1 is drawn from a distribution F with density $f(x) = \frac{1}{(1+x)^2}$ and the slippage η_1 is deterministic and known. Then, we have that the valuation for the MEV searcher is given by:

$$\begin{aligned} v(V) &= \mathop{\mathbf{E}}_{\Delta_1\sim F}[\mathsf{PNL}(\Delta_1, \eta_1) | \Delta_1 = V] \\ &\leq C\max(\eta, \sqrt{1+\eta})\mathop{\mathbf{E}}_{\Delta_1\sim F}[\Delta_1] - \frac{\mu\gamma}{\beta} \end{aligned}$$

Defining the constants $a = C\max(\eta, \sqrt{1+\eta})$ and $b = \frac{\mu\gamma}{\beta}$, we therefore want to show that $\mathsf{PNL}(\Delta_1, \eta_1)$ is not distributed according to an MHR distribution. To do this, we first show that $a\Delta_1 - b$ is not MHR. This follows from standard results on scaling and shifting non-MHR distributions. The key step is showing that $f(x) = \frac{1}{(1+x)^2}$ is not MHR. Computing the virtual value, $\varphi(x)$, and noting that F has CDF $F(x) = 1 - \frac{1}{1+x}$, we have:

$$
\begin{aligned}
\varphi(x) &= x - \frac{1 - F(x)}{f(x)} \\
&= x - \frac{1 - \left(1 - \frac{1}{1+x}\right)}{(1+x)^2} \\
&= x - (1+x) \\
&= -1
\end{aligned}
$$

This clearly does not satisfy the condition for being MHR.

A.2 Liquidations

A liquidation is a transaction that is specified by two assets, called the *collateral* (C) and *debt* (D). We denote the current price of the two assets as p_C and p_D, where we normalize $p_C = 1$, and therefore p_D is the price of the debt asset in units of collateral. A smart contract on a blockchain such as Ethereum has lent out some amount of D in exchange for holding C as collateral for the debt. Let x_C denote the amount of collateral and x_D the amount of debt. As a result of price change of the debt asset relative to the collateral, the debt may become *liquidatable*. In particular, if the debt-to-collateral ratio $\frac{x_D p_D}{x_C}$ is less than 1, the debt is called healthy. Otherwise, the debt is called liquidatable. We denote the tuple $L = (p_D, x_C, x_D)$ as a liquidation. The prices p_C and p_D are random variables that we describe in more detail subsequently. We write $\mathbb{1}_L \in \{0, 1\}$ to denote the liquidatability of the debt. If $\mathbb{1}_L = 0$, then the debt is healthy, and else it is liquidatable.

Liquidations are not regular We now demonstrate that the valuations for liquidations are not regular. Recall that liquidations have value functions $v(L) = \mathbb{1}_L$ where $\mathbb{1}_L = 1$ if $x_D p_D / x_C > 1$ and 0 otherwise. Assume without loss of generality that $x_D = x_C = 1$, and that $p_D \sim \mathcal{N}(1, 1)$. We therefore see that $\mathbb{1}_L = 1$ with probability 0.5 and $\mathbb{1}_L = 0$ with probability 0.5. This value distribution is not even regular, because $f(x) = 0.5\delta(x) + 0.5\delta(x-1)$, which gives us:

$$
F(x) = \begin{cases} 0.5 \text{ if } 1 > x \geq 0 \\ 1 \text{ if } x \geq 1 \end{cases}
$$

Consider $x, x' = 0, 0.5$. Then, we have $\phi(0) = \frac{1-0.5}{0.5}$ and $\phi(0.5) = 0.5 - \frac{1-0.5}{0} = -\infty$. Therefore, we clearly do not have $\phi(0.5) - \phi(0) \geq 0$.