





# Credible, Optimal Auctions via Public Broadcast

Tarun Chitra  

Gauntlet, New York, NY, USA

Matheus V. X. Ferreira   

University of Virginia, Charlottesville, VA, USA

Kshitij Kulkarni  

UC Berkeley, CA, USA

---

## Abstract

We study auction design in a setting where agents can communicate over a censorship-resistant broadcast channel like the ones we can implement over a public blockchain. We seek to design credible, strategyproof auctions in a model that differs from the traditional mechanism design framework because communication is not centralized via the auctioneer. We prove this allows us to design a larger class of credible auctions where the auctioneer has no incentive to be strategic. Intuitively, a decentralized communication model weakens the auctioneer’s adversarial capabilities because they can only inject messages into the communication channel but not delete, delay, or modify the messages from legitimate buyers. Our main result is a separation in the following sense: we give the first instance of an auction that is credible only if communication is decentralized. Moreover, we construct the first two-round auction that is credible, strategyproof, and optimal when bidder valuations are  $\alpha$ -strongly regular, for  $\alpha > 0$ . Our result relies on mild assumptions – namely, the existence of a broadcast channel and cryptographic commitments.

**2012 ACM Subject Classification** Applied computing → Online auctions; Security and privacy → Formal security models; Theory of computation → Algorithmic mechanism design

**Keywords and phrases** credible auctions, blockchains, cryptographic auctions, optimal auction design, mechanism design with imperfect commitment

**Digital Object Identifier** 10.4230/LIPIcs.AFT.2024.19

**Related Version** *Full Version:* <https://arxiv.org/pdf/2301.12532> [3]

**Funding** *Matheus V. X. Ferreira:* Research was performed while author was at Harvard University.

## 1 Introduction

Incentive compatibility for buyers is desirable in auctions due to improvements in user experience. For example, in a second-price auction, if the highest bidder bids \$10 and the second highest bidder bids \$5, the highest bidder wins and pays \$5. Thus, for any buyer, bidding the maximum they are willing to pay is an optimal strategy, independently of the strategy of others. This differs from non-incentive compatible auctions, such as first-price auctions, where optimal strategies are a complex balance between demand and the strategy of competing buyers.

Extending incentive compatibility to auctioneers is increasingly becoming a topic of interest in designing auctions within digital marketplaces. In online settings, it is challenging to audit auctions and verify the identity of participants. Thus, a strategic auctioneer can act simultaneously as the seller and a buyer to deviate from the promised auction. For example, in the second-price auction above, buyers must trust the auctioneer can commit to implementing the promised auction. Otherwise, a strategic auctioneer impersonating a buyer can easily leverage their privileged position to submit a bid of \$9, increasing revenue and reducing the buyer’s welfare.



© Tarun Chitra, Matheus V. X. Ferreira, and Kshitij Kulkarni;  
licensed under Creative Commons License CC-BY 4.0

6th Conference on Advances in Financial Technologies (AFT 2024).

Editors: Rainer Böhme and Lucianna Kiffer; Article No. 19; pp. 19:1–19:16

Leibniz International Proceedings in Informatics



LIPIC Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

*Credibility* is a form of incentive compatibility for auctioneers that formalizes the incentives for an auctioneer to follow their promised specifications. It is desirable for auctioning objects ranging from Non-Fungible Tokens (NFTs) to online advertising because it ensures auction outcomes are auditable. The US Department of Justice’s 2023 antitrust suit against Google [17] effectively argues that Google’s manipulation of ad auctions from the privileged position of auctioneer caused both buyers and users harm. Allegedly, the lack of market transparency afforded Google “power to manipulate the quantity of ad inventory and auction dynamics in ways that allowed it to charge advertisers more than it could in a competitive market”. Thus, credibility is not only a compelling objective for regulators, but also for sellers that wish to prove their auctions are fair.

Unfortunately, recent work has highlighted challenges in designing mechanisms that are simultaneously incentive-compatible for both sellers and buyers. The pioneering work of [1] considered a model where the auctioneer can modulate their private communication with buyers to increase their revenue and potentially reduce buyer welfare via a safe deviation from a promised auction. Informally, a *safe deviation* is any auctioneer deviation that passes undetectable by any buyer alone. An auction is *credible* if safe deviations cannot increase the auctioneer’s expected revenue. For example, an auctioneer waiting for the highest bidder to bid \$10 and impersonating a false buyer that bids \$9 is a profitable, safe deviation from a second-price auction. Unfortunately, [1] demonstrated that auctioneer credibility could not coexist with buyer incentive compatibility unless the communication complexity is unbounded: they showed that an ascending price auction is the only credible, strategyproof optimal auction.

On the other hand, if one is willing to assume that the auctioneer and buyers are computationally bounded – and thus cannot break known cryptographic assumptions – one can get around the theoretical barriers of [1]. Concretely, [6] demonstrated that there are cryptographic auctions that are credible, incentive compatible, and have bounded communication complexity if buyer valuations satisfy a regularity condition. They proposed the (centralized) *Deferred Revelation Auctions (DRA)*, a two-round auction that is optimal, strategyproof, and credible under the assumption buyer valuations are  $\alpha$ -strongly regular for any  $\alpha \geq 1$ . They also show their auction is not always credible if  $\alpha < 1$  and valuations have unbounded support. This challenges adopting these auctions because they are only credible if the buyer valuations have tails not heavier than the exponential distribution, i.e.,  $\alpha$ -strongly regular for  $\alpha \geq 1$  does not contain the Pareto distribution, for example.

In the same line as [6], [4] proposed the Ascending Deferred Revelation Auction (ADRA), which is strategyproof and credible without requiring any assumption on the distributions. However, ADRA communication complexity is constant on expectation and unbounded in the worst case. In contrast, we study auctions with bounded communication in the worst case.

All results above consider a centralized communication model where buyers can only exchange messages with the auctioneer. This assumption is motivated by the scenario where one buyer does not have prior knowledge of the identity of a second buyer. Unfortunately, if the communication is centralized, the auctioneer can launch a man-in-the-middle-like attack by censoring, injecting, and modifying messages they were supposed to forward to other participants. In contrast, our work explores the design of credible auctions when agents can access a broadcast channel where any buyer can broadcast messages to all participants. This assumption is well-motivated in an auction in a physical environment like a traditional auction house. Further, this assumption has also become realistic for auctions implemented over a communication network like the Internet due to the proliferation of censorship-resistant public blockchains. Our main contribution shows a simple change in the communication model (centralized vs. distributed) affects the design of credible auctions.

We summarize our findings as follows:

- **Theorem 21.** Assume buyer values are drawn independently from an  $\alpha$ -strongly regular distribution for  $\alpha > 0$ . Then, the deferred revelation auction with public broadcast is credible, strategyproof, and revenue optimal. Moreover, modifying the auction so buyers can only communicate privately with the auctioneer makes the resulting auction not credible.
- **Theorem 25.** There is a 0-strongly regular buyer valuation that witnesses that deferred revelation auction with public broadcast is not credible.

## 1.1 Related Work

We have already reviewed the most relevant prior work in our earlier discussion. Our model is similar to [1] under the additional assumption of cryptographic primitives plus a public broadcast channel.

The security of auctions using cryptography has been extensively studied in the literature [15, 2]. Notably, Yao’s seminal work on multi-party computation [19] was initially motivated by economic applications. Recent research has revisited the problem of secure auction design, incorporating novel cryptographic tools such as homomorphic encryption and timed encryption techniques [16] [9].

However, these approaches come with stronger trust assumptions. For instance, multi-party computation assumes that a majority of participants are honest. In contrast, our setting allows the auctioneer to create multiple identities. Furthermore, timed encryption, although an intriguing concept, has seen limited practical applications due to its reliance on stronger cryptographic assumptions. Importantly, our goal of reducing the number of auction rounds aims to enhance auction speed, whereas timed encryption would counter this objective by increasing the auction duration.

Credible mechanism design has applications beyond auctions such as in the design of manipulation-resistant decentralized exchanges [18], blockchain transaction fee mechanisms [8, 5], and in Bayesian persuasion [12].

## 1.2 Technical overview

[1] does not consider the existence of a broadcast channel in their framework because they envision auctions executing over the Internet (or over the telephone) and assume buyers do not know the identity of each other beforehand. Implementing a broadcast channel in this scenario is challenging and draws from years of research in consensus and cryptography, starting from the Byzantine general’s problem of [11]. This line of research culminated with the Bitcoin blockchain, which provides censorship-resistant consensus at large scale [14]. In the framework of [1], the auctioneer promises to implement an auction and is the nexus of communication with buyers. A buyer privately sends messages to the auctioneer and trusts that the auctioneer will forward those messages to other buyers.

We propose a simple modification to this framework that, surprisingly, increases the incentive for the auctioneer to commit to a promised auction. Concretely, rather than sending messages privately to the auctioneer, we assume any agent can broadcast messages. Once an agent broadcasts a message  $m$ , all other participants simultaneously learn about message  $m$ .

Under the new framework, our main contribution is the *deferred revelation auction with public broadcast*. It is similar to the centralized deferred revelation auction of [6] with the main difference that buyers can now broadcast messages. Our main result shows *DRA* with public broadcast is a credible auction, assuming buyer valuations are  $\alpha$ -strongly regular for

## 19:4 Credible, Optimal Auctions via Public Broadcast

all  $\alpha > 0$ . Recall [6] showed centralized *DRA* is not credible for these buyer valuations. This has significant practical implications because it provides the first design of a communication-efficient, credible, strategyproof, optimal auction when buyer value distributions have tails as heavy as Pareto distributions.

Informally, the deferred revelation auction with public broadcast is a two-phase auction (see §3) as follows:

1. In the *bidding phase*, each buyer broadcasts a cryptographic commitment of their bid and deposits a collateral.
2. The auctioneer broadcasts the end of the commitment phase and the start of the revelation phase.
3. In the *revelation phase*, each buyer broadcasts the opening of their commitment (e.g., their bid and the random seed used to generate the commitment).
4. The auctioneer marks a bid as revealed if the second phase message opens the cryptographic commitment received in the first phase. Then, the auctioneer implements the second-price auction with reserves using the revealed bids.
5. The auctioneer refunds the collateral if, and only if, a buyer reveals their bid. The confiscated collateral is given to the winner of the auction.

As in [6], we consider a threat model where the auctioneer can shill bid (i.e., impersonate false buyers that submit false bids). To argue the credibility of our auction, we must show that under certain conditions, sufficiently large collateral incentivizes the auctioneer not to impersonate false buyers. Central to our argument is observing that the security of our cryptographic commitment scheme (see Definition 5) together with a broadcast channel ensures the auctioneer cannot commit to a bid that depends on the bids of other buyers. This is not the case for the centralized deferred revelation auction. To see, consider modifying the auction above so that whenever a buyer broadcasts a message, the buyer sends that message to the auctioneer, who “promises” to forward it to all other buyers. The following is a safe deviation to centralized *DRA* where shill bids depends on bids from genuine buyers.

► **Example 1.** Suppose there are genuine buyers  $A$  and  $B$  as well as a false buyer  $C$ . Any message the auctioneer receives from  $B$ , the auctioneer forwards to  $A$ . The auctioneer does not forward any message from  $A$  to  $B$  which makes buyer  $B$  unaware that  $A$  exists. The auctioneer asks buyer  $A$  to open their bid and after learning the bid  $b_A$  of  $A$ , the auctioneer impersonates a false buyer  $C$  that commits to bid  $b_A + \Delta$  to buyer  $B$ . This deviation is undetectable because buyer  $A$  believes only  $A$  and  $B$  participate in the auction. Moreover,  $A$  cannot detect their messages were censored. On the other hand,  $B$  believes only  $B$  and  $C$  participate in the auction. Moreover,  $B$  cannot detect that  $A$ ’s messages were censored (in fact,  $B$  is unaware of  $A$ ). Finally, observe that  $B$  receives a bid from a false buyer correlated with the bid of  $A$ .

This might seem like an innocent deviation, but Section 5 shows centralized *DRA* is not credible for  $\alpha$ -strongly regular valuations for any  $\alpha \in [0, 1)$  if we adapt this strategy and allow the auctioneer to submit shill bids that depend on genuine bids. Clearly this deviation is not possible if a broadcast channel is available since the auctioneer cannot choose who gets to observe  $A$ ’s messages and the auctioneer cannot commit to shill bids after starting the revelation phase. Our main technical contribution shows that safe deviations that leverage shill bids correlated to genuine bids were the only strategies that prevented centralized *DRA* from being a credible auction when buyer valuations are  $\alpha$ -strongly regular for  $\alpha > 0$ .

### 1.3 Paper organization

We provide the necessary background in optimal auction theory in §2. We define the implementation of the deferred revelation auction with public broadcasts in §3. We prove our main result, Theorem 21, in §4 and our negative result, Theorem 25, in §6. §5 shows that a broadcast channel is necessary for Theorem 21. We conclude in §7 and include future directions.

## 2 Preliminaries

We consider a single item,  $n$  buyer auction. Buyer  $i \in [n] = \{1, \dots, n\}$  has private value  $v_i \in \mathbb{R}^+$  and has 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 a distribution  $D$  with CDF  $F$  and PDF  $f$ . The auctioneer knows the distribution  $D$ , but not the values  $\{v_i\}_{i=1}^n$ . We refer to  $\vec{v} = (v_1, \dots, v_n)$  as a *value profile*. We write the value profile of all buyers except buyer  $i$  as  $\vec{v}_{-i} = (v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n)$ .

**Communication model.** Agents can communicate on a *private channel* or a *broadcast channel*. If agent  $i$  sends a message  $m$  in a broadcast channel, then the message is immediately received by all other agents. If agent  $i$  sends a message  $m$  to agent  $j \neq i$  in a private channel, only agent  $j$  observes  $m$ .

**Extensive-form game.** An extensive-form game  $G$  consists of a tree  $(H, E)$  where the nodes  $H$  are the set of histories and edges  $E \subseteq H \times H$  are state transitions. The game starts at the root of  $(H, E)$ , has a set of players  $\{0, 1, \dots, n\}$ , 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  $h \in H$  has one owner  $P(h) \in \{0, \dots, n\}$  responsible for taking the next action when the game is at state  $h$ . 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 where only agent  $P(h)$  observes the action  $A(h)$  taken at  $h$ .

A strategy  $s_i$  for buyer  $i \in [n]$  on game  $G$  is a function that takes buyer  $i$ 's private type  $v_i$  and any history  $h \in H$  where  $i \in P(h)$  and outputs the agent's action  $s_i(v_i, h) \in A(h)$  at  $h$ . Consider a strategy profile  $\vec{s} = (s_1, \dots, s_n)$ . An *auction game*  $(G, \vec{s})$  is a communication game on  $G$  when buyers follow strategy  $\vec{s}$  that allocates the item and charges payments.

The outcome of auction game  $(G, \vec{s})$  is a tuple  $(\vec{x}^{(G, \vec{s})}(\vec{v}), \vec{p}^{(G, \vec{s})}(\vec{v}))$  where  $x_i^{(G, \vec{s})}(v)$  and  $p_i^{(G, \vec{s})}(\vec{v})$  denotes the probability that agent  $i$  receives the item and their payment respectively. A strategy  $s_i$  is a best response to  $\vec{s}_{-i}$  if for any strategy  $s'_i$  for buyer  $i$ , for any  $\vec{v}$ ,

$$v_i \cdot x_i^{(G, \vec{s})}(\vec{v}) - p_i^{(G, \vec{s})}(\vec{v}) \geq v_i \cdot x_i^{(G, s'_i, \vec{s}_{-i})}(\vec{v}) - p_i^{(G, s'_i, \vec{s}_{-i})}(\vec{v}).$$

► **Definition 2** (Ex-post Nash/Strategyproof/Individually Rational). *Consider an auction  $(G, \vec{s})$ . A strategy profile  $\vec{s}$  forms an ex-post Nash equilibrium, if for any buyer  $i$ , strategy  $s_i$  is the best response to  $\vec{s}_{-i}$ . An auction is strategyproof if some strategy profile  $\vec{s}$  forms an ex-post Nash equilibrium. An auction is individually rational (IR) if there is a strategy for any buyer that ensures such buyer receives non-negative utility.*

The auctioneer's *expected revenue* on auction game  $(G, \vec{s})$  is  $\text{REV}(G, \vec{s}) := \mathbb{E}_{\vec{v}} \left[ \sum_{i=1}^n p_i^{(G, \vec{s})}(\vec{v}) \right]$ .

## 19:6 Credible, Optimal Auctions via Public Broadcast

We assume the auctioneer can deviate from implementing  $(G, \vec{s})$  as long as any buyer cannot detect a deviation. These are a *safe deviation* from the promised auction  $(G, \vec{s})$ . Formally,  $(G', s)$  is a *safe deviation* from  $(G, \vec{s})$  if for any buyer  $i \in [n]$ , there is a strategy profile  $s_{-i}^i = (s_1^i, \dots, s_{i-1}^i, s_{i+1}^i, \dots, s_{n_i}^i)$  for  $n_i$  buyers where buyer  $i$  observes the same messages in communication games  $(G', \vec{s})$  and  $(G, s_i, s_{-i}^i)$ .

► **Definition 3** (Credible Auction). *An auction game  $(G, \vec{s})$  is credible if for any safe deviation  $(G', \vec{s})$  of  $(G, \vec{s})$ ,  $REV(G, \vec{s}) \geq REV(G', \vec{s})$ .*

### Virtual values

Virtual values functions allow us to formalize optimal auctions. 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  $\varphi(\cdot)$ , omitting the superscript  $F$ , when the distribution is clear from the context. We write  $\varphi^+(x) = \max\{0, \varphi(x)\}$ . A distribution  $F$  is  $\alpha$ -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. Note that MHR distributions have exponentially decaying tails, whereas distributions with  $\alpha \in (0, 1)$  have polynomially decaying tails.

► **Theorem 4** (Myerson's Theorem [13]). *Consider a strategyproof auction that awards the item to buyer  $i$  with probability  $x_i(\vec{v})$  and charges  $p_i(\vec{v})$  on bids  $\vec{v}$ . Then, the expected revenue is*

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

We refer to the right-hand side as the *expected virtual welfare*. For cases where  $D$  is regular,  $\varphi$  is non-decreasing, and 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  $r(D) := (\varphi^D)^{-1}(0)$  as *Myerson's reserve price*. From Myerson's theorem, the optimal auction only sells the item to buyers with the value  $v_i \geq r(D)$ . We define  $REV(D^n)$  as the expected revenue of the optimal auction with  $n$  buyers with valuations drawn i.i.d. from  $D$ . We provide facts about  $\alpha$ -strongly regular distributions in Appendix A.

## 3 Deferred Revelation Auction (DRA) with Public Broadcast

This section defines the deferred revelation auction with public broadcast. The central assumption is the existence of a perfectly hiding, computationally binding, and non-malleable cryptographic commitment scheme as follows.

► **Definition 5** (Commitment Scheme). *A commitment scheme is a function  $COMMIT(\cdot, \cdot)$  that takes a message  $m \in \{0, 1\}^*$ , a random string  $r \in \{0, 1\}^\lambda$  where  $\lambda \in \mathbb{N}$  is the security parameter and outputs a commitment  $c \in \{0, 1\}^{POLY(\lambda)}$  where  $POLY(\lambda)$  is a polynomial with variable  $\lambda$ .*

**Perfectly hiding.** *A commitment scheme is perfectly hiding if, for all  $m \neq m'$ ,  $COMMIT(m, r)$  is identically distributed to  $COMMIT(m', r')$  provided that  $r$  and  $r'$  are uniformly random.*

**Computationally binding.** A commitment scheme is computationally binding if for any probabilistic polynomial time algorithm that takes the security parameter  $\lambda$  and terminates in expected time  $\text{POLY}(\lambda)$ , then the probability the algorithm outputs  $(m, r) \neq (m', r')$  such that  $\text{COMMIT}(m, r) = \text{COMMIT}(m', r')$  is at most  $2^{-\lambda}$ .

**Non-malleable.** Consider any communication game where a probabilistic polynomial time adversary receives  $c = \text{COMMIT}(m, r)$  where  $m$  is drawn from a known distribution and  $r$  is uniformly random. In the first round, the adversary must output some commitment  $c' \neq c$ . In the second round, the attacker learns  $(m, r)$  and outputs  $(m', r')$  such that  $\text{COMMIT}(m', r') = c$ . We say the commitment scheme is non-malleable if, for any such game, the random variable  $(m', r')$  is independent of  $(m, r)$ .

Some commitment schemes are malleable; for example, they allow a receiver that observes  $\text{COMMIT}(b, r)$  to compute  $\text{COMMIT}(b - 1, r)$ . This does not violate secrecy since the receiver does not learn  $b$  or can open  $\text{COMMIT}(b - 1, r)$  before the sender opens  $(b, r)$ . Yet, this malleability would pose serious security vulnerabilities in an auction. If a bidder commits to bid  $b$  with  $\text{COMMIT}(b, r)$ , the auctioneer can shill bid and commit to bidding  $b - 1$  by computing  $\text{COMMIT}(b - 1, r)$ . Constructions of non-malleable commitment schemes are involved and outside the scope of this work (see [10, 7] for a more general definition and practical constructions).

► **Definition 6** (Deferred Revelation Auction with Public Broadcast). Let  $\text{COMMIT}(\cdot, \cdot)$  be a perfectly hiding, perfectly binding, and non-malleable commitment scheme satisfying Definition 5. A collateral function  $f(\cdot, \cdot)$  takes the number of buyers  $n$  and a distribution  $D$  and outputs a collateral required from each buyer to bid in the auction. For a collateral function  $f$ ,  $\text{DRA}(f)$  with public broadcast is the following auction:

**Commitment phase (1<sup>st</sup> round):**

- Each buyer  $i \in [n]$  picks a bid  $b_i = v_i$ , draws  $r_i$  uniformly at random, and broadcast  $(i, \text{COMMIT}(b_i, r_i))$ . Moreover, buyer  $i$  sends collateral  $f(n, D)$  to the auctioneer.
- The auctioneer broadcasts “End of Commitment Phase”.

**Revelation phase (2<sup>nd</sup> round):**

- Each buyer  $i$  broadcasts  $(i, b'_i, r'_i)$  where  $b'_i = b_i$  and  $r'_i = r_i$ .
- The auctioneer broadcasts “End of Revelation Phase”.

**Resolution phase:**

- Let  $S$  denote the set of buyers for which  $\text{COMMIT}(b_i, r_i) = \text{COMMIT}(b'_i, r'_i)$ . Let  $b'_i := b_i \cdot \mathbf{1}(i \in S)$ . Let  $i^* := \arg \max_{i \in S} b_i$ .
- If  $b_{i^*} > r(D)$ , award buyer  $i^*$  the item. Charge them

$$\max\{r(D), \max_{i \in S \setminus \{i^*\}} b_i\}.$$

- The auctioneer refunds the collateral of buyer  $i \in S$ .
- The auctioneer transfers the collateral of each buyer  $i \notin S$  to buyer  $i^*$ .

**Tie-breaking:**

- All ties are broken lexicographically, with the auctioneer treated as “buyer zero”.

Before discussing how our auction differs from centralized  $\text{DRA}(f)$ , we quickly observe that  $\text{DRA}(f)$  with public broadcast is indeed strategyproof and revenue optimal.

► **Theorem 7.** For all  $f$ ,  $\text{DRA}(f)$  with public broadcast is a strategyproof optimal auction.



**Proof.** The definition for  $DRA(f)$  instructs each buyer  $i \in [n]$  to follow the strategy where buyer  $i$  sets  $b_i = v_i$ ; in the commitment phase, buyer  $i$  picks a uniformly random  $r_i$  and broadcasts a commitment  $\text{COMMIT}(v_i, r_i)$ ; and in the revelation phase, buyer  $i$  reveals  $(v_i, r_i)$ . Since  $DRA(f)$  implements the same outcome as a second-price auction, it follows this strategy profile and is an ex-post Nash equilibrium, which proves the auction is strategyproof. Moreover, because the auction maximizes expected virtual welfare, Theorem 4 (Myerson’s Theorem) implies the auction is revenue optimal. ◀

Definition 8 provides a definition for centralized  $DRA(f)$  [6]. Lemma 9 shows that centralized  $DRA(f)$  has strategy space for the auctioneer at least as ample as  $DRA(f)$  with public broadcast. To be concrete, the lemma shows that any safe deviation to  $DRA(f)$  with public broadcast maps to a safe deviation to centralized  $DRA(f)$ .

► **Definition 8** (Centralized Deferred Revelation Auction). *The centralized  $DRA(f)$  is identical to  $DRA(f)$  with public broadcast except under the following cases:*

- *In  $DRA(f)$  with public broadcast, consider a history  $h$  where buyer  $i$  broadcasts a message  $m$ . In centralized  $DRA(f)$ , instead of broadcasting  $m$ , buyer  $i$  sends  $m$  to the auctioneer in a private channel. Then, the auctioneer sends  $m$  to each buyer  $j \neq i$  in a private channel.*
- *In  $DRA(f)$  with public broadcast, consider a history  $h$  where the auctioneer broadcasts a message  $m$ . In centralized  $DRA(f)$ , instead of broadcasting  $m$ , the auctioneer sends  $m$  to each buyer  $i \in [n]$  in a private channel.*

► **Lemma 9.** *Let  $(G, \vec{s})$  be a safe deviation to  $DRA(f)$  with public broadcast, then there is a safe deviation  $(G', \vec{s}')$  to centralized  $DRA(f)$  where  $\text{REV}(G', \vec{s}') = \text{REV}(G, \vec{s})$*

**Proof.** Let  $(G', \vec{s}')$  be a communication game identical to  $(G, \vec{s})$  except on the following scenario:

- Whenever buyer  $i \in [n]$  broadcasts message  $m$  in  $(G, \vec{s})$ , in  $(G', \vec{s}')$ , buyer  $i$  sends  $m$  to the auctioneer. After receiving  $m$ , the auctioneer sends  $m$  to each buyer  $j \neq i$ .
- Whenever the auctioneer broadcasts message  $m$  in  $(G, \vec{s})$ , in  $(G', \vec{s}')$ , the auctioneer sends  $m$  to each buyer  $i \in [n]$ .

The deviation  $(G', \vec{s}')$  is safe assuming  $(G, \vec{s})$  is safe. Moreover, it induces the same allocation/payment rules, meaning it obtains the same revenue as  $(G, \vec{s})$ . This concludes the proof. ◀

Unfortunately, the converse of Lemma 9 is untrue. There are safe deviations to centralized  $DRA(f)$  that do not map to any safe deviation in  $DRA(f)$  with public broadcast. We give the following examples to illustrate this fact.

► **Example 10.** In  $DRA(f)$  with public broadcast, buyer  $i$  sends  $(i, c_i)$  to all buyers. On the other hand, in centralized  $DRA(f)$ , buyer  $i$  must send  $(i, c_i)$  to the auctioneer, and the auctioneer “promises” to forward  $(i, c_i)$  to all buyers  $j \neq i$ . Unfortunately, buyer  $i$  cannot verify whether the auctioneer forwards their message to any buyer  $j \neq i$ . This allows the auctioneer to share  $(i, c_i)$  with a strict subset of buyers.

► **Example 11.** In  $DRA(f)$  with public broadcast, the auctioneer broadcasts the end of the commitment phase to all buyers. On the other hand, on centralized  $DRA(f)$ , the auctioneer “promises” to simultaneously announce the end of the commitment for each buyer. Suppose the auctioneer announces the end of the commitment phase to buyer  $i$  at 10:00 p.m. but only sends this announcement to buyer  $j$  at 11:00 p.m. This deviation is safe because buyer



$i$  does not know which messages buyer  $j$  received and vice-versa. Thus, at 10:10 p.m., the auctioneer requests buyer  $i$  to reveal  $(b_i, r_i)$ . Then, the auctioneer impersonates a false buyer  $z$  that bids  $b_z(b_i)$  that might depend on  $b_i$ . Buyer  $z$  sends  $\text{COMMIT}(b_z(b_i), r_z)$  only to buyer  $j$  at 10:20 p.m.

These examples do not prove there are safe deviations to centralized  $DRA(f)$  that are more profitable than any safe deviation to  $DRA(f)$  with public broadcast. They aim to showcase additional manipulations the auctioneer can perform that they cannot perform when a broadcast channel is present. Our main result will formally prove that these manipulations strictly improve the auctioneer's revenue relative to deviations that do not manipulate the order and time of messages.

Note some deviations are still possible even when buyers communicate in a broadcast channel, which makes arguing about the credibility of  $DRA(f)$  with public broadcast non-trivial – namely, the addition of false bids and the refusal to reveal false bids.

**Broadcasting false bids.** In the commitment phase, the auctioneer can impersonate a *false buyer* – agents that submit bids not coming from any *real buyer*  $i \in [n]$  – which broadcast a *false bid*  $\text{COMMIT}(\hat{b}, \hat{r})$  where  $\hat{r}$  is uniformly random. We refer to  $\tilde{b}(n, D)$  as the highest bid among all false buyers. Set  $\tilde{b}(n, D) = 0$  if the auctioneer does not impersonate any false buyer.

► **Lemma 12.** *Assume the auctioneer follows a safe deviation to  $DRA(f)$  with public broadcast. If, during the commitment phase, a false buyer broadcasts  $\text{COMMIT}(b, r)$ , and, in the revelation phase, the false buyer reveals  $(b, r)$ , then  $b$  is a random variable independent of  $\vec{v}$ .*

**Proof.** Suppose for contradiction the false buyer broadcasts  $\text{COMMIT}(b, r)$  and later reveals  $(b, r)$  where  $b$  is not independent of  $\vec{v}$ . Use this auction to construct an adversary that outputs  $\text{COMMIT}(b, r)$  whenever the false buyer does. Once the false buyer reveals  $(b, r)$ , the adversary reveals  $(b, r)$ . Because  $b$  is correlated to  $\vec{v}$ , this implies the commitment scheme is malleable, a contradiction. ◀

**Withhold false bids.** In the revelation phase, the auctioneer can refuse to reveal any bid  $\hat{b}$  submitted from a false buyer. The decision to reveal or withhold a bid from a false buyer might depend on the real bids  $\vec{b}$ .

Next, we highlight a few relevant facts about our protocol. In the commitment phase, buyer  $i$  observes commitments  $\{\text{COMMIT}(d_j^i, r_j^i)\}_j$  from both real buyers and false buyers (excluding their bid  $b_i$ ). That is,  $d_j^i$  is the  $j$ -th bid buyer  $i$  observes excluding their own bid. Let  $\beta_i(\vec{b}) = \max\{r(D), \max_j\{d_j^i\}\}$  be the highest bid buyer  $i$  observed in the commitment phase (including the reserve price  $r(D)$  and excluding their bid  $b_i$ ) when real buyers bid  $\vec{b}$ . It is possible  $\max_{i \in [n]} \beta_i(\vec{b}) > \max\{r(D), \max_{i \in [n]} \{b_i\}\}$  if the highest bid is from a false buyer.

► **Observation 13.** *Assume the auctioneer follows a safe deviation to  $DRA(f)$  with public broadcast. Then for all value profiles  $\vec{b}$ ,  $b_i > \beta_i(\vec{b})$  for at most one buyer  $i \in [n]$ .*

**Proof.** Suppose for contradiction there are distinct buyers  $i$  and  $j$  such that  $b_i > \beta_i(\vec{b})$  and  $b_j > \beta_j(\vec{b})$ . Observe that buyer  $i$  receives the bid of buyer  $j$  and buyer  $j$  receives the bid of buyer  $i$  which implies  $\beta_i(\vec{b}) \geq b_j$  and  $\beta_j(\vec{b}) \geq b_i$ . The inequalities implies  $b_i > b_j$  and  $b_j > b_i$ , a contradiction. This proves there is at most one buyer  $i$  such that  $b_i > \beta_i(\vec{b})$ . ◀

## 19:10 Credible, Optimal Auctions via Public Broadcast

► **Observation 14.** *Suppose the auctioneer follows a safe deviation to  $DRA(f)$  with public broadcast. If  $b_i > \beta_i(\vec{b})$ , then buyer  $i$  receives the item and pays  $\beta_i(\vec{b})$ .*

**Proof.** Buyer  $i$  can observe that their bid is above the reserve price and they are the highest bidder in the auction. If the auctioneer's deviation is safe, it must allocate the item to  $b_i$  and charge  $\beta_i(\vec{b})$ . ◀

The following Lemma 15 shows that under certain conditions, it is optimal for the auctioneer to reveal any bids from false buyers.

► **Lemma 15.** *Consider any safe deviation  $(G, \vec{s})$  of  $DRA(f)$  where, in the commitment phase, the auctioneer impersonates a false buyer that bids  $0 < b \leq f(n, D)$ , and, in the revelation phase, the auctioneer withholds  $b$ . Let  $h$  be the history where the auctioneer reveals or withholds  $b$ . Let  $(G', \vec{s}')$  be a new deviation identical to  $(G, \vec{s})$  except at history  $h$  the auctioneer reveals  $b$ . Then  $G'$  is a safe deviation and  $REV(G', \vec{s}') \geq REV(G, \vec{s})$ .*

**Proof.** The fact  $(G', \vec{s}')$  is a safe deviation follows directly from the fact  $(G, \vec{s})$  is a safe deviation. Next, we argue  $REV(G', \vec{s}') \geq REV(G, \vec{s})$ .

First, consider the case where no real buyer receives the item at  $(G, \vec{s})$ . Then, no real buyer will receive the item at  $(G', \vec{s}')$ . Moreover,  $(G', \vec{s}')$  improves the auctioneer's revenue relative to  $(G, \vec{s})$  because the auctioneer receives no payments but pays fewer penalties for revealing  $b$ .

Next, consider the case where some buyer  $i \in [n]$  receives the item and pays  $p$  at  $(G, \vec{s})$ . For the case where  $b \leq p$ , buyer  $i$  remains the highest bidder and pays  $p$  while the auctioneer pays fewer penalties for revealing  $b$  at  $(G', \vec{s}')$ . For the case where  $b > p$ , by assumption  $f(n, D) \geq b$ . Then, the auctioneer receives negative profits at  $(G, \vec{s})$  since the penalty for withholding  $b$  is higher than the payment they receive from buyer  $i$ . On the other hand, at  $(G', \vec{s}')$ , the revenue loss for revealing  $b$  is lower than the penalties for withholding  $b$ . ◀

### 4 DRA with Public Broadcast is Credible for $\alpha$ -Strongly Regular Distributions

In this section, we show that for any  $\alpha$ -strongly regular distributions for  $\alpha > 0$ , there is a  $f(\cdot, \cdot)$  that makes  $DRA(f)$  with public broadcast credible. Recall that  $\tilde{b}(n, D)$  is the most significant bid from a false buyer. From Lemma 12  $\tilde{b}(n, D)$  is independent of  $\vec{v}$ .

For the case where  $\alpha \geq 1$ , [6] proved Theorem 16 stating centralized  $DRA(f)$  is a credible auction if we set the collateral to be at least the optimal reserve price. Extending their result for our auction is a simple observation that any safe deviation for  $DRA(f)$  with public broadcast is also a safe deviation for centralized  $DRA(f)$ .

► **Theorem 16** (Theorem 4.1 in [6]). *Assume buyer valuations are  $\alpha$ -strongly regular for any  $\alpha \geq 1$ . If  $f(n, D) \geq r(D)$ , then centralized  $DRA(f)$  is a credible auction.*

► **Theorem 17.** *Assume buyer valuations are  $\alpha$ -strongly regular for any  $\alpha \geq 1$ . If  $f(n, D) \geq r(D)$ , then  $DRA(f)$  with public broadcast is a credible auction.*

**Proof.** Suppose for contradiction  $DRA(f)$  with public broadcast is not a credible auction when  $f(n, D) \geq r(D)$ . There is a safe deviation  $(G, \vec{s})$  to  $DRA(f)$  with public broadcast where  $REV(G, \vec{s}) > REV(D^n)$ . From Lemma 9, there is a safe deviation  $(G', \vec{s}')$  to centralized  $DRA(f)$  where  $REV(G', \vec{s}') = REV(G, \vec{s}) > REV(D^n)$ . Thus, centralized  $DRA(f)$  is not a credible auction, a contradiction to Theorem 16. ◀

The challenging case is to argue  $DRA(f)$  with public broadcast is credible for some  $f(n, D)$  for the case where  $\alpha \in (0, 1)$ . We first show that any safe deviation where false buyers only broadcast bids smaller than the collateral cannot improve the auctioneer's revenue.

► **Lemma 18.** *Assume the auctioneer follows a safe deviation to  $DRA(f)$  with public broadcast. Let  $\tilde{b}(n, D)$  be the highest bid from a false buyer (or zero if there are no false buyers). If  $f(n, D) \geq \tilde{b}(n, D)$ , the auctioneer's revenue is at most  $REV(D^n)$ .*

**Proof.** From Lemma 15 and the fact the highest false buyer bids  $k$ , it is without loss of generality to assume the auctioneer always will reveal  $\tilde{b}(n, D)$ .

Suppose the reserve price is  $r$  and let  $\hat{r} = \max\{r(D), \tilde{b}(n, D)\}$ . Note that  $\hat{r}$  is independent of  $\vec{v}$  because  $r(D)$  depends only on  $D$  and  $\tilde{b}(n, D)$  depends only on  $n$  and  $D$ . Thus, the allocation/payment rule is equivalent to a second-price auction with reserve  $\hat{r}$ . Since the second-price auction with reserve  $\hat{r}$  is a strategyproof auction, Myerson's theorem implies the revenue is at most:

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

The first equality is Theorem 4. The second inequality observes  $\sum_{i=1}^n x_i(\vec{v}) \leq 1$ . From Myerson's theorem, the optimal auction maximizes virtual surplus or equivalently,  $REV(D^n) = \mathbb{E} [\max_i \varphi(v_i)]$ . This concludes the proof. ◀

Next, we consider the case where false buyers might broadcast bids higher than the collateral. Our first Lemma will bound the revenue for events where  $v_j > \beta_j(\vec{v})$  for some buyer  $j$ . The second Lemma bounds the revenue for events where  $v_j < \beta_j(\vec{v})$  for all buyers.

► **Lemma 19.** *Assume the auctioneer follows a safe deviation to  $DRA(f)$  with public broadcast. Let  $R(\vec{v})$  be the auctioneer's revenue when buyers have value profile  $\vec{v}$ . Then*

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

**Proof.** From Observation 13, there is at most one buyer  $i$  such that  $v_i > \beta_i(\vec{v})$  for any  $\vec{v}$ . Moreover, when  $v_i > \beta_i(\vec{v})$ , buyer  $i$  wins the item and pay  $\beta_i(\vec{v})$ . Since  $\beta_i(\vec{v})$  is independent of  $v_i$ , this payment/allocation rule is strategyproof. From Myerson's theorem, the revenue is the expected virtual surplus  $\mathbb{E}_{\vec{v} \leftarrow D} [\varphi(v_i) \cdot \mathbf{1}(v_i > \beta_i(\vec{v}))]$ . We obtain

$$\begin{aligned} \mathbb{E}_{\vec{v} \leftarrow D} [R(\vec{v}) \cdot \mathbf{1}(\exists j, v_j > \beta_j(\vec{v}))] &= \mathbb{E}_{\vec{v} \leftarrow D} \left[ \sum_{i=1}^n \beta_i(\vec{v}) \cdot \mathbf{1}(v_i > \beta_i(\vec{v})) \right] \\ &= \mathbb{E}_{\vec{v} \leftarrow D} \left[ \sum_{i=1}^n \varphi(v_i) \cdot \mathbf{1}(v_i > \beta_i(\vec{v})) \right] \quad \{\text{By Theorem 4}\} \end{aligned}$$

as desired. ◀

► **Lemma 20.** *Assume the auctioneer follows a safe deviation to  $DRA(f)$  with public broadcast. Assume  $D$  is  $\alpha$ -strongly regular for  $\alpha \in (0, 1)$ . Let  $\tilde{b}(n, D)$  be the highest bid from a false buyer (or zero if there are no false buyers). Assume  $f(n, D) \geq r(D) \left(\frac{n}{\alpha}\right)^{\frac{1-\alpha}{\alpha}} \left(\frac{1}{1-\alpha}\right)^{\frac{1}{\alpha}}$  and  $\tilde{b}(n, D) > f(n, D)$ . Let  $R(\vec{v})$  be the auctioneer's revenue when buyers have value profile  $\vec{v}$ . Then, the auctioneer's expected revenue is at most*

$$\mathbb{E}_{\vec{v} \leftarrow D} [R(\vec{v}) \cdot \mathbf{1}(\forall j, v_j < \beta_j)] \leq REV(D^n) - \mathbb{E}_{\vec{v} \leftarrow D} \left[ \sum_{i=1}^n \varphi(v_i) \cdot \mathbf{1}(v_i > \beta_i(\vec{v})) \right].$$

## 19:12 Credible, Optimal Auctions via Public Broadcast

**Proof.** When  $v_j < \beta_j(\vec{v})$  for all buyers, a false buyer is the highest bidder. Therefore,  $\max_j \beta_j(\vec{v}) = \tilde{b}(n, D) > f(n, D)$  where the inequality is a statement assumption. In this case, any buyer  $j$  can receive the item as long as the auctioneer withholds at least one bid. Because buyer  $j$  pays at most  $v_j$ , the auctioneer receives negative revenue if  $v_j < f(n, D)$ . Recall  $x_i(\vec{v})$  is an indicator variable taking value 1 if and only if buyer  $i$  receives the item. This gives

$$\begin{aligned}
& \mathbb{E}_{\vec{v} \leftarrow D} [R(\vec{v}) \cdot \mathbf{1}(\forall j, v_j < \beta_j(\vec{v}))] \\
& \leq \mathbb{E}_{\vec{v} \leftarrow D} \left[ \sum_{i=1}^n (v_i - f(n, D)) \cdot x_i(\vec{v}) \cdot \mathbf{1}(\forall j, v_j < \beta_j(\vec{v})) \cdot \mathbf{1}(v_i \geq f(n, D)) \right] \\
& \leq \mathbb{E}_{\vec{v} \leftarrow D} \left[ \sum_{i=1}^n \left( \frac{1}{\alpha} \varphi(v_i) + r(D) - f(n, D) \right) \cdot x_i(\vec{v}) \cdot \mathbf{1}(\forall j, v_j < \beta_j(\vec{v})) \cdot \mathbf{1}(v_i \geq f(n, D)) \right] \\
& \leq \mathbb{E}_{\vec{v} \leftarrow D} \left[ \sum_{i=1}^n \frac{1}{\alpha} \varphi(v_i) \cdot x_i(\vec{v}) \cdot \mathbf{1}(\forall j, v_j < \beta_j(\vec{v})) \cdot \mathbf{1}(v_i \geq f(n, D)) \right] \\
& = \mathbb{E}_{\vec{v} \leftarrow D} \left[ \sum_{i=1}^n \frac{1}{\alpha} \varphi(v_i) \cdot x_i(\vec{v}) \cdot \mathbf{1}(\forall j \neq i, v_j < \beta_j(\vec{v})) \cdot \mathbf{1}(f(n, D) \leq v_i < \beta_i(\vec{v})) \right] \\
& = \mathbb{E}_{\vec{v} \leftarrow D} \left[ \sum_{i=1}^n \frac{\varphi(v_i)}{\alpha} \cdot x_i(\vec{v}) \cdot \mathbf{1}(\forall j \neq i, v_j < \beta_j(\vec{v})) \cdot (\mathbf{1}(v_i \geq f(n, D)) - \mathbf{1}(v_i > \beta_i(\vec{v}))) \right] \\
& < \mathbb{E}_{\vec{v} \leftarrow D} \left[ \sum_{i=1}^n \frac{\varphi(v_i)}{\alpha} \cdot \mathbf{1}(v_i \geq f(n, D)) \right] - \mathbb{E}_{\vec{v} \leftarrow D} \left[ \sum_{i=1}^n \varphi(v_i) \cdot \mathbf{1}(v_i > \beta_i(\vec{v})) \right]
\end{aligned}$$

The second line observes that if buyer  $i$  receives the item, they pay at most  $v_i$ , and the auctioneer loses a collateral of  $f(n, D)$  by withholding at least one bid. The third line invokes Lemma 26. To see that the assumptions for the Lemma are satisfied, let  $E$  be the event where  $v_i \geq f(n, D)$  and observe that  $f(n, D) \geq r(D)$  for all  $n \geq 1$  and  $\alpha \in (0, 1)$ . The fourth line observes  $f(n, D) \geq r(D)$ . The fifth line observes the event  $\{\forall j, v_j < \beta_j(\vec{v})\}$  implies  $\{v_i < \beta_i(\vec{v})\}$  and uses the fact  $\beta_i(\vec{v}) > f(n, D)$ . The sixth line uses the fact  $\mathbf{1}(a \leq X < b) = \mathbf{1}(X \geq a) - \mathbf{1}(X \geq b)$  for any random variable  $X$  and constants  $a > b$ . The seventh line uses the fact  $\alpha > 1$  and Observation 13 which states the event  $\{v_i > \beta_i\}$  implies  $x_i(\vec{v})$  and  $v_j < \beta_j(\vec{v})$  for all  $j \neq i$  since  $v_i$  expects to win the item. Moreover, we use the fact

$$x_i(\vec{v}) \cdot \mathbf{1}(\forall j \neq i, v_j < \beta_j(\vec{v})) \cdot \mathbf{1}(v_i \geq f(n, D)) \leq \mathbf{1}(v_i \geq f(n, D)).$$

To conclude, we must show that

$$\mathbb{E}_{\vec{v} \leftarrow D} \left[ \sum_{i=1}^n \frac{\varphi(v_i)}{\alpha} \cdot \mathbf{1}(v_i \geq f(n, D)) \right] \leq \text{REV}(D^n).$$

From Lemma 28,

$$\begin{aligned}
& \mathbb{E}_{\vec{v} \leftarrow D} \left[ \sum_{i=1}^n \frac{\varphi(v_i)}{\alpha} \cdot \mathbf{1}(v_i \geq f(n, D)) \right] \\
& = \frac{1}{\alpha} \left( \frac{1}{1-\alpha} \right)^{\frac{1}{1-\alpha}} \left( \frac{r(D)}{f(n, D)} \right)^{\frac{\alpha}{1-\alpha}} \mathbb{E}_{\vec{v} \leftarrow D} \left[ \sum_{i=1}^n \varphi(v_i) \cdot \mathbf{1}(v_i \geq r(D)) \right] \\
& \leq \frac{\alpha}{\alpha n} \mathbb{E}_{\vec{v} \leftarrow D} \left[ \sum_{i=1}^n \varphi(v_i) \cdot \mathbf{1}(v_i \geq r(D)) \right]
\end{aligned}$$

$$\begin{aligned}
&= \frac{\alpha n}{\alpha n} \mathbb{E}_{v_1 \leftarrow D} [\varphi(v_1) \cdot \mathbf{1}(v_1 \geq r(D))] \\
&= \text{REV}(D) \\
&\leq \text{REV}(D^n)
\end{aligned}$$

The second line observes  $f(n, D) \geq r(D)$  and applies Lemma 28. The third line uses the assumption  $f(n, D) \geq r(D) \left(\frac{n}{\alpha}\right)^{\frac{1-\alpha}{\alpha}} \left(\frac{1}{1-\alpha}\right)^{\frac{1}{\alpha}}$ . The fourth line observes  $\varphi(v_1), \dots, \varphi(v_n)$  are i.i.d.. The fifth line observes  $r(D)$  is the optimal reserve price, and so  $\mathbb{E}_{v_1 \leftarrow D} [\varphi(v_1) \cdot \mathbf{1}(v_1 \geq r(D))]$  is the optimal revenue for the single buyer auction (Theorem 4). The last line observes the revenue is non-decreasing in the number of buyers. ◀

Next, we prove our main result.

► **Theorem 21.** *Assume the auctioneer follows a safe deviation to  $\text{DRA}(f)$  with public broadcast and assume all buyer valuations are  $\alpha$ -strongly regular for  $\alpha > 0$ . Then, there is an  $f$  such that  $\text{DRA}(f)$  with public broadcast is a credible auction.*

**Proof.** Set  $f(n, D) = r(D) \left(\frac{n}{\alpha}\right)^{\frac{1-\alpha}{\alpha}} \left(\frac{1}{1-\alpha}\right)^{\frac{1}{\alpha}}$ . Observe for all  $n \geq 1$  and  $\alpha > 0$ ,  $f(n, D) \geq r(D)$ . For the case where  $\alpha \geq 1$ , the proof follows directly from Theorem 17 because  $f(n, D) \geq r(D)$ . Next, consider the case where  $\alpha \in (0, 1)$ . Recall  $\tilde{b}(n, D)$  refers to the highest bid among false buyers (or zero if no false buyer exists).  $R(\vec{v})$  refers to the auctioneer's revenue when buyers have value  $\vec{v}$ . For the case where  $f(n, D) \geq \tilde{b}(n, D)$ , Lemma 18 states the auctioneer's revenue is at most  $\text{REV}(D^n)$ . Next, consider the case where  $f(n, D) < \tilde{b}(n, D)$ . We can write the revenue as

$$\begin{aligned}
\mathbb{E}_{\vec{v} \leftarrow D} [R(\vec{v})] &= \mathbb{E}_{\vec{v} \leftarrow D} [R(\vec{v}) \cdot \mathbf{1}(\exists j, v_j > \beta_j(\vec{v}))] + \mathbb{E}_{\vec{v} \leftarrow D} [R(\vec{v}) \cdot \mathbf{1}(\forall j, v_j < \beta_j(\vec{v}))] \\
&\leq \mathbb{E}_{\vec{v} \leftarrow D} \left[ \sum_{i=1}^n \varphi(v_i) \cdot \mathbf{1}(v_i > \beta_i(\vec{v})) \right] + \text{REV}(D^n) - \mathbb{E}_{\vec{v} \leftarrow D} \left[ \sum_{i=1}^n \varphi(v_i) \cdot \mathbf{1}(v_i > \beta_i(\vec{v})) \right] \\
&= \text{REV}(D^n)
\end{aligned}$$

The second line is due to Lemma 20 and Lemma 19. This shows the auctioneer's revenue is at most  $\text{REV}(D^n)$  and proves there is a  $f$  such that  $\text{DRA}(f)$  is a credible auction. ◀

## 5 Public Broadcast is Necessary

This section revisits the fact centralized  $\text{DRA}(f)$  is not a credible auction for certain  $\alpha$ -strongly regular valuations when  $\alpha \in (0, 1)$ .

► **Theorem 22** (Theorem 4.4 in [6]). *For all  $f$ ,  $\alpha \in (0, 1)$ , there exists a  $D^n$  that is  $\alpha$ -strongly regular such that centralized  $\text{DRA}(f)$  is not credible for instance  $D^n$ .*

The following is a special case for the instance given in the proof of Theorem 22. By inspection, this strategy is a safe deviation for centralized  $\text{DRA}(f)$  since, in the view of each buyer, the strategy is indistinguishable from the promised auction. In this strategy the auctioneer only sends a shill bids to buyer  $B$  that depend on the bid of buyer  $A$ . This would not be possible if, rather than relying on the auctioneer to forward messages, messages were sent in a broadcast channel because any message one buyer receives is also received by other buyers.

► **Definition 23** (Adaptive Reserve Price). *Consider an auctioneer who promises to implement centralized  $\text{DRA}(f)$  on an instance with two buyers  $A$  and  $B$ . The adaptive reserve price deviation is the following deviation:*

## 19:14 Credible, Optimal Auctions via Public Broadcast

- $A$  sends  $(A, c_A)$  to the auctioneer.
- $B$  sends  $(B, c_B)$  to the auctioneer.
- The auctioneer sends  $(B, c_B)$  to  $A$  and  $(A, c_A)$  to  $B$ .
- The auctioneer sends “End of the Commitment Phase” to buyer  $A$ , then requests  $A$  to reveal their bid.  $A$  complies and reveals  $(b_A, r_A)$  such that  $c_A = \text{COMMIT}(b_A, r_A)$ .
- The auctioneer picks a large threshold  $T$ :
  - If  $b_A < T$ , the auctioneer sends “End of Commitment Phase” to buyer  $B$ , then requests  $B$  to reveal their bid (who complies by revealing  $(b_B, r_B)$  such that  $c_B = \text{COMMIT}(b_B, r_B)$ ). The auctioneer implements the allocation/payment rule for the second-price auction with reserve  $r(D)$  on bids  $\{b_A, b_B\}$ .
  - If  $b_A \geq T$ , the auctioneer impersonates a false buyer  $C$ . Let  $r_C$  be uniformly random and  $b_C = b_A + f(2, D)$ . Then, the auctioneer sends  $(C, \text{COMMIT}(b_C, r_C))$  to  $B$ . The auctioneer sends “End of Commitment Phase” to buyer  $B$ , then request  $B$  to reveal their bid.  $B$  complies and reveal  $(b_B, r_B)$  such that  $c_B = \text{COMMIT}(b_B, r_B)$ . Next, the auctioneer proceeds as follows:
    - \* If  $r(D) \geq \max\{b_A, b_B\}$ , the auctioneer reveals all bids. No one receives the item.
    - \* If  $b_B < b_A$  and  $b_A > r(D)$ , the auctioneer reveals all bids and allocates the item to  $A$  and charges  $\max\{r(D), b_B\}$ .
    - \* If  $b_B \in [b_A, b_C]$  and  $b_B > r(D)$ , the auctioneer reveals  $b_A$  and hides  $b_C$  from  $B$ . Then, the auctioneer allocates the item to  $B$  and charges  $\max\{b_A, r(D)\}$ .
    - \* If  $b_B > b_C$ , the auctioneer reveals all bids and allocates the item to  $B$  who pays  $b_C$ .

### 6 DRA over Public Broadcast for Regular Distributions

Although *DRA* with public broadcast extends the class of distributions where it is credible, it is not a magic bullet. Indeed, Theorem 25 states there is an instance with a single buyer drawn from a regular distribution that witnesses *DRA*( $f$ ) with public broadcast is not credible. The proof relies on a similar negative result in [6].

► **Theorem 24** (Theorem 4.4 in [6]). *There is a regular distribution  $D$  such that for all  $f(\cdot, \cdot)$ , centralized *DRA*( $f$ ) is not credible even when there is a single buyer with valuation drawn from  $D$ .*

► **Theorem 25.** *There is a regular distribution  $D$  such that for all  $f(\cdot, \cdot)$ , *DRA*( $f$ ) over public broadcast is not credible even when there is a single buyer with a valuation drawn from  $D$ .*

**Proof.** We will argue for any instance with a single buyer, any safe deviation to centralized *DRA*( $f$ ) maps to a safe deviation to *DRA*( $f$ ) over public broadcast. To see, let  $(G, \vec{s})$  be a safe deviation to centralized *DRA*( $f$ ). Let  $(G', \vec{s}')$  be a deviation to *DRA*( $f$ ) with public broadcast identical to  $(G, \vec{s})$  except on the following cases:

- Whenever the buyer sends  $m$  to the auctioneer in  $(G, \vec{s})$ , the buyer broadcast  $m$  in  $(G', \vec{s}')$ .
- Whenever the auctioneer sends  $m$  to the buyer in  $(G, \vec{s})$ , the auctioneer broadcast  $m$  in  $(G', \vec{s}')$ .

$(G', \vec{s}')$  is a safe deviation because  $(G, \vec{s})$  is a safe deviation. Moreover,  $(G', \vec{s}')$  induces the same allocation/payment rule as  $(G, \vec{s})$ ; therefore,  $\text{REV}(G', \vec{s}') = \text{REV}(G, \vec{s})$ .

From Theorem 24, there is a  $D$  such that for all  $f(\cdot, \cdot)$ , there is a safe deviation  $(G, \vec{s})$  to centralized *DRA*( $f$ ) where  $\text{REV}(G, \vec{s}) > \text{REV}(D)$ . The mapping above proves there is a safe deviation  $(G', \vec{s}')$  to *DRA*( $f$ ) with public broadcast where  $\text{REV}(G', \vec{s}') = \text{REV}(G, \vec{s}) > \text{REV}(D)$ . This proves *DRA*( $f$ ) with public broadcast is not a credible auction on instance  $D$  as desired. ◀

## 7 Conclusion

Improving the transparency and fairness in Internet platforms is becoming an essential concern for regulators, as observed by the US Department of Justice lawsuit against Google [17]. It is unlikely that customers could unilaterally detect and, more importantly, prove the sophisticated market manipulations alleged in the complaint. Credible auctions formalize the notion that an auction is “auditable” by its participants: the auctioneer has no incentive to deviate from running the promised mechanism in earnest. However, existing credible auctions suffer from restrictive assumptions on valuation distributions and exclude valuations with tails thicker than the exponential distribution.

This work shows that censorship-resistant broadcast channels like blockchains are helpful to circumvent this problem. We propose the deferred revelation auction with public broadcast, a natural modification of the centralized deferred revelation auction of [6]. Although our auction represents a simple modification of a known auction, the resulting auction is credible in instances where no known communication-efficient auctions were known to be credible. This work builds on the emerging line of research that attempts to improve the performance of economic mechanisms by appending cryptographic primitives to them. The need for large collateral is a limitation of our work. Minimizing collateral is an important objective to make these auctions practical which we leave as future direction.

---

### References

- 1 Mohammad Akbarpour and Shengwu Li. Credible auctions: A trilemma. *Econometrica*, 88(2):425–467, 2020.
- 2 Felix Brandt. Cryptographic protocols for secure second-price auctions. In *International Workshop on Cooperative Information Agents*, pages 154–165. Springer, 2001.
- 3 Tarun Chitra, Matheus VX Ferreira, and Kshitij Kulkarni. Credible, optimal auctions via blockchains. *arXiv preprint*, 2023. [arXiv:2301.12532](https://arxiv.org/abs/2301.12532).
- 4 Meryem Essaidi, Matheus VX Ferreira, and S Matthew 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.
- 5 Matheus VX Ferreira, Daniel J Moroz, David C Parkes, and Mitchell Stern. Dynamic posted-price mechanisms for the blockchain transaction-fee market. In *Proceedings of the 3rd ACM Conference on Advances in Financial Technologies*, pages 86–99, 2021.
- 6 Matheus VX Ferreira and S Matthew Weinberg. Credible, truthful, and two-round (optimal) auctions via cryptographic commitments. In *Proceedings of the 21st ACM Conference on Economics and Computation*, pages 683–712, 2020.
- 7 Marc Fischlin and Roger 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.
- 8 Aadityan Ganesh, Clayton Thomas, and S Matthew Weinberg. Revisiting the primitives of transaction fee mechanism design, 2024.
- 9 Noemi Glaeser, István András Seres, Michael Zhu, and Joseph Bonneau. Cicada: A framework for private non-interactive on-chain auctions and voting. *Cryptology ePrint Archive*, 2023.
- 10 Dakshita Khurana and Amit Sahai. How to achieve non-malleability in one or two rounds. In *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 564–575. IEEE, 2017.
- 11 Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. In *Concurrency: the works of leslie lamport*, pages 203–226. ACM, 2019.



## 19:16 Credible, Optimal Auctions via Public Broadcast

- 12 Xiao Lin and Ce Liu. Credible persuasion. *Journal of Political Economy*, 132(7):000–000, 2024.
- 13 Roger B Myerson. Optimal auction design. *Mathematics of operations research*, 6(1):58–73, 1981.
- 14 Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2009. URL: <http://www.bitcoin.org/bitcoin.pdf>.
- 15 Michael O Rabin and Christopher Thorpe. Time-lapse cryptography. *Harvard University*, 2006.
- 16 Nirvan Tyagi, Arasu Arun, Cody Freitag, Riad Wahby, Joseph Bonneau, and David Mazières. Riggs: Decentralized sealed-bid auctions. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, pages 1227–1241, 2023.
- 17 US Department of Justice. Justice department sues google for monopolizing digital advertising technologies, 2023. URL: <https://www.justice.gov/opa/pr/justice-department-sues-google-monopolizing-digital-advertising-technologies>.
- 18 Matheus Venturyne Xavier Ferreira and David C Parkes. Credible decentralized exchange design via verifiable sequencing rules. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, pages 723–736, 2023.
- 19 Andrew Chi-Chih Yao. Protocols for secure computations. *Mathematics of operations research*, 82(1):160–164, 1982.

### A Mathematical Background

► **Lemma 26** (Lemma 7.1 in [6]). *Let  $D$  be  $\alpha$ -strongly regular for  $\alpha > 0$ . Let  $E$  be an event such that  $v \geq r(D)$  with probability 1 conditioned on  $E$ . Then*

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

**Proof.** Because  $D$  is  $\alpha$ -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  $\mathbb{E}_{\bar{v} \leftarrow D}[v|E] \leq \frac{1}{\alpha} \mathbb{E}[\varphi^D(v)|E] + r(D)$  as desired. ◀

► **Lemma 27** (Lemma 7.2 in [6]). *Let  $D$  be a  $\alpha$ -strongly regular distribution. Then for all  $p \geq r(D)$ ,*

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

► **Lemma 28.** *Let  $D$  be a  $\alpha$ -strongly regular for  $\alpha > 0$ . Then for all  $p \geq r(D)$ ,*

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

**Proof.** Consider a single item, single bidder posted-price mechanism that offers the item at a price  $p$ . The bidder value is drawn from  $D$ . The revenue is  $p Pr_{\bar{v} \leftarrow D}[v \geq p]$  because the buyer purchases whenever their value exceeds  $p$ . From Myerson’s theorem,  $p Pr_{\bar{v} \leftarrow D}[v \geq p] = \mathbb{E}_{\bar{v} \leftarrow D}[\varphi(v) \cdot \mathbf{1}(v \geq p)]$ . The result follows directly by applying Lemma 27 to the left-hand side of the inequality. ◀