

# Noisy Truth Beats Precise Lies: Blockchain-Enabled Information Equilibria\*

**Leo Bao**

Monash University

**Evgeny Lyandres**

Tel Aviv University and Monash University

**Ruize Sun**

Monash University

November 19, 2025

---

\*Leo Bao, leo.bao@monash.edu, Monash University; Evgeny Lyandres, lyandres@tauex.tau.ac.il., Tel Aviv University and Monash University; Ruize Sun, ruize.sun@monash.edu, Monash University. Bao and Sun thank Monash University for financial support. Lyandres thanks the Kassirer Institute at Tel Aviv University for financial support.

# Noisy Truth Beats Precise Lies: Blockchain-Enabled Information Equilibria

## Abstract

Truth-telling is essential to efficient allocation of resources but is often undermined by strategic misreporting. We show how verifiably fair randomness, complemented by other blockchain functionalities, can lead to truth-telling at the cost of introduction of random noise in information transmission. The optimal trade-off between truthfulness and precision yields equilibria that outperform those attainable without randomization in information transmission. We characterize two classes of information equilibria: information designated to directly trigger value transfer via decentralized consensus (“enforcive information”), and strategic information sharing between Bayesian-rational decision makers (“advisive information”). Our findings demonstrate usefulness of randomized transmission in broad financial settings and illustrate the benefits of blockchain technology for optimal mechanism design.

*JEL* Code: D43, D80, G14, L13.

*Keywords*: blockchain; information design; decentralized consensus; Cournot competition.

# 1 Introduction

Truth-telling is fundamental to financial interactions, yet absent sufficient incentives to behave truthfully agents may choose to misreport their private information for personal gain. We propose a novel solution empowered by blockchain technology, featuring verifiably fair randomness embedded into information transmission, which facilitates truthful information sharing and improves equilibrium outcomes. Intuitively, in a binary-state setting where a sender has incentives to mislead others about the actual state of nature, as the probability of message flipping approaches 50%, the expected gain from lying converges to zero because the message conveys diminishing information. On the flip side, of course, injecting noise into messages/reports reduces the precision of information transmitted.

This trade-off between *truthfulness* and *precision* allows us to identify an optimal degree of artificial noise that yields messages more informative about the true state than in the absence of such noise. We develop a theoretical framework that characterizes how orchestrated randomness improves welfare in two broad types of information equilibria, corresponding to central contexts in finance and economics in which information is generated, transmitted, and acted upon.

The first type of information equilibria features *enforcive* information, that is, the designated function of information is to trigger value transfer rather than to change beliefs of decision makers. An example of this type of information is decentralized oracles, whose goal is to aggregate information from multiple decentralized data providers.

Blockchain promises to solve the incomplete contracts problem (i.e., complex contingencies can hardly be written down and verified ex post by a court in case of dispute, see, e.g., [Tirole, 1999](#)) by *smart contracts*, which allow value transfers, in the form of cryptocurrencies, to be automated by tamper-proof computer code. However, oracles powering smart contracts still rely on human truth-telling because the basis upon which oracles aggregate information—in order to produce blockchain consensus on the contingencies written in smart contracts—is reports submitted by data providers fetching information from the off-chain world to the blockchain. Whenever off-chain information is certified to be on-chain consensus, vulnerability to manipulation or strategic misreporting ensues, which is termed as the *oracle problem* (see, e.g., [Cong et al., 2025](#)).

We show that a layer of random noise distancing the data providers from the aggregator of

reports (i.e., a pre-defined function of reports acting as the generator of decentralized consensus) can, if optimally designed, significantly improve the quality of the resulting decentralized consensus. Without artificial noise, the consensus' deviation from truth is systematic and driven by strategic misreporting; with such noise, the systematic part dwindles due to a dampened incentive to lie, while random deviation emerges. Specifically, the pivot is that honesty is judged by—hence the cost of lying is associated to—the message a data provider sends *but not* the version the aggregator receives. Given a fixed cost of lying and an aggregator *not discriminating* the underlying precision of any received report, a protocol designer can always find a transmission precision such that 1) truthful reporting is incentive-compatible to a data provider and 2) the received report carries nonempty information (i.e., it is not pure noise).

We further derive the optimal trade-off between truthfulness and precision in various situations, whereby a protocol designer can orchestrate artificial noise to maximize the quality of decentralized consensus. Depending on the situation, a protocol designer may assign customized transmission precisions to keep all the data providers honest, or make a system-wide choice of randomization when a data provider's type is *ex ante* unknown, balancing data providers' truth-telling probability and the loss of information due to randomization.

Notably, blockchain technology makes randomized transmission of information technically feasible, thanks to its capacity of producing artificial randomness that is unpredictable, tamper-resistant, and most importantly, verifiably fair, different from a variety of off-chain methods such as physically flipping a coin (see, e.g., [Randao, 2017](#)).

The second type of information equilibria features *advisive* information, that is, the only channel via which information impacts outcomes is by changing decision makers' beliefs about the state of nature. To illustrate the effect of randomized transmission of information in this setting, we consider standard sender-receiver interactions with Bayesian rationality, where misreporting gain can only be an off-equilibrium matter, yet a lack of commitment to truth-telling boils down to an inability to credibly signal one's own type *ex post* even though truthful revelation is *ex ante* desirable for both parties.

Specifically, we model communication between two firms in the context of product market oligopoly. Two firms produce substitutable goods and are subject to idiosyncratic demand shocks. Each firm observes a private signal realization that (partially) reveals its own demand and shares

this information with its product market competitor. With updated information sets, the two firms make production decisions noncooperatively. Truthful reporting is not automatically guaranteed, because, for example, a firm may have incentives to overstate its demand to reduce the aggressiveness of its rival’s product market strategy. This renders ex ante desirable information sharing not incentive-compatible, thus disabling communication that would have led to higher expected equilibrium profits for both firms.

The first way blockchain can help with achieving a truthful-information-sharing equilibrium is by enabling a smart contract that requires each firm to post collateral on the blockchain, through which the incentive to misreport can be outweighed by a contingent loss of collateral triggered by delinquency, given the ex post verifiability of the truthfulness of submitted reports.<sup>1</sup> However, the collateral-based mechanism for addressing truth-telling is imperfect, as the amount of collateral required for proper incentivization of truth-telling may be high, rendering this solution impractical for financially constrained firms or for firms with high opportunity costs of capital.

As a countermeasure, access to verifiably fair randomness allows to design a mechanism for truthful (yet noisy) information sharing, which would lead to a second-best equilibrium. Such equilibrium is preferred to the non-information-sharing equilibrium that arises in the absence of randomized transmission when the first-best equilibrium with truthful and precise information sharing is unattainable due to collateral limitations.

In a nutshell, the two types of information equilibria offer an integrated perspective of how verifiably fair randomness, complemented by smart contracts empowered by blockchain consensus, incentivizes agents to behave truthfully, and extends the set of equilibria involving both enforive and advising information.

Our paper contributes to the blockchain mechanism design literature, in which the central problem involves the construction of a consensus protocol that provides decentralized, inherently self-interested data providers with incentives leading to truthful recording (Abadi and Brunnermeier, 2018; Biais et al., 2019; Cong and He, 2019; Chiu and Koepl, 2019; Goldstein, Jiang, and Karolyi, 2019; Leshno and Strack, 2020; Breidenbach et al., 2021; Cong, He, and Li, 2021; Hal-

---

<sup>1</sup>It follows from the discussion above that a fair clearance of collateral must rely on a high-quality decentralized consensus, which we assume when studying the advisable type of information equilibria. Stated differently, while the firms’ reports are directly recorded on the blockchain, oracles are still required to collect and validate off-chain information, such as product prices and quantities sold.

aburda, He, and Li, 2021; Gans and Gandal, 2021; Saleh, 2021; Drakopoulos, Lo, and Mulvany, 2022; Gans and Holden, 2022; Garratt and Monnet, 2022; Benhaim, Falk, and Tsoukalas, 2023; John, Kogan, and Saleh, 2023; Cao, Cong, and Yang, 2025; Cong et al., 2025).

This literature studies trade-offs within various consensus protocols. For example, [Abadi and Brunnermeier \(2018\)](#) demonstrate a blockchain trilemma among fault-tolerance, resource-efficiency, and full transferability; [Leshno and Strack \(2020\)](#) examine a trilemma involving anonymity, lack of consolidation, and Sybil incentives, facing blockchain miners; [Garratt and Monnet \(2022\)](#) show that truthfulness cannot be guaranteed in fully decentralized systems without deontological preferences toward truth-telling; [Cong et al. \(2025\)](#) examine a trilemma involving scalability, decentralization, and truthfulness, facing blockchain oracles.

Other papers in this literature examine specific mechanisms and phenomena related to blockchain consensus. For instance, [Biais et al. \(2019\)](#) study the occurrence of forks (i.e., coexistence of multiple, potentially conflicting sequences of blocks) which can jeopardize consensus quality; [Halaburda, He, and Li \(2021\)](#) investigate Byzantine fault tolerant (BFT) mechanisms on blockchain, with an emphasis on maintaining consensus quality in the presence of malfunctioning nodes and strategic dishonesty; [Saleh \(2021\)](#) compares properties of Proof-of-Work (PoW) consensus mechanism and Proof-of-Stake (PoS) one; [Cong, He, and Li \(2021\)](#) examine the effects on decentralization of consolidation of miners (i.e., “mining pools”); [Benhaim, Falk, and Tsoukalas \(2023\)](#) explore potential benefits of generating consensus through a small committee of elected miners.

Our paper also contributes to the long-established literature on product market competition with private information ([Novshek and Sonnenschein, 1982](#); [Li, 1985](#); [Gal-Or, 1985, 1986](#); [Ziv, 1993](#); [Raith, 1996](#); [Einy, Moreno, and Shitovitz, 2002](#); [Amir, Jin, and Troege, 2010](#); [Jain, Seshadri, and Sohoni, 2011](#); [Goltsman and Pavlov, 2014](#); [He, Chen, and Shen, 2018](#); [Bimpikis, Crapis, and Tahbaz-Salehi, 2019](#); [Argenton, Ivanova-Stenzel, and Müller, 2024](#); [Flor et al., 2025](#)) by analyzing equilibria that are made possible in reality by blockchain technology and, in particular, by verifiably fair randomness. In particular, the information design problem for two competitive firms can be benchmarked against [Gal-Or \(1985, 1986\)](#) and [Raith \(1996\)](#), but a fundamental difference between these papers and ours is that the former ones assume truthful reporting. Existing solutions to potentially dishonest firms include costly messages ([Ziv, 1993](#)) and collateral staking ([Flor et al., 2025](#)). The solution proposed in our paper is a design of information sharing that involves

randomized transmission of reports.

Our paper also relates to the literature on Bayesian persuasion (Kamenica and Gentzkow, 2011) under limited commitment power and/or mediation (Perez-Richet, 2014; Best and Quigley, 2016; Salamanca, 2021; Arieli, Babichenko, and Sandomirskiy, 2022; Drakopoulos, Lo, and Mulvany, 2022; Lipnowski, Ravid, and Shishkin, 2022), in which truthful reporting is generally not ex post optimal for a sender. Best and Quigley (2016) casually point out the potential of blockchain to act as a mediator strengthening commitment in repeated persuasion games. This idea is developed in Drakopoulos, Lo, and Mulvany (2022) which rely on costly messages relayed by blockchain per an information structure specified ex ante. Our paper contributes to this literature in two fundamental ways. First, our framework does not necessarily rely on Bayesian rationality—for example, the aggregator of reports may behave as a mechanical counting machine regardless of the data-generating process behind each report. Second, we model strategic interactions in the two types of information equilibria, in contrast to stylized sender-receiver models in Bayesian persuasion, most of which are effectively nonstrategic.

The remainder of this paper is organized as follows: Section 2 analyzes the enforive information equilibria, in the context of production of decentralized consensus; Section 3 analyzes the advisable information equilibria, through the lens of communication among product market competitors; Section 4 concludes. All mathematical proofs are delegated to the Appendix.

## 2 Information Equilibrium in Decentralized Consensus

One of the fundamental functions of blockchain is producing decentralized consensus that serves as basis for state-contingent value transfer via smart contracts (Cong and He, 2019). However, blockchain is inherently oblivious to events occurring outside of it (i.e., off-chain events). In other words, many contingencies are observable but difficult to verify by an external arbitrator (e.g., a court), which makes contracting on such contingencies feasible in principle yet prohibitively costly in practice (e.g., Hart and Moore, 1988). Blockchain circumvents this problem via oracles, i.e., mechanisms for aggregation of information provided by parties external to the blockchain. Smart contracts powered by these oracles ensure that state-contingent value transfer can be executed in a frictionless way.

However, decentralized consensus does not necessarily reflect the true state of nature. Loosely speaking, a decentralized consensus is a voting outcome. Each member in a designated set of data providers, who can access ground truth, is asked to submit a report on what she observed, e.g., whether a delicate good was successfully delivered, after which a prespecified function maps the set of reports to a consensus on the state of nature. Conceivably, truthful reporting may or may not be in the best interest of a data provider. As a result, incentivizing truth-telling is crucial for the production of reliable decentralized consensus.

We demonstrate that another important function of blockchain, namely producing verifiably fair randomness, offers a promising solution to the truthfulness problem. Intuitively, lying generates both benefits and costs to a data provider. The role of randomness that is artificially added into information transmission is to obfuscate the benefits while leaving the costs unchanged, until the latter outweighs the former. Truthful information sharing achieved by means of introducing noise into information transmission to the blockchain does not come without a cost: randomness can compromise the quality of consensus by reducing its precision. Our model shows that there is an optimal trade-off between truthfulness and precision that maximizes the quality of consensus.

## 2.1 Setup

*Technology.* There are  $n$  data providers, each of which independently observes the same binary state of nature  $\omega \in \{0, 1\}$ , i.e., the ground truth. A generic data provider, denoted by  $i$ , submits a report  $r_i \in \{0, 1\}$  to a transmission technology middleware parameterized by  $\tau_i$ , while the transmission technology sends a randomized report  $\hat{r}_i \in \{0, 1\}$  distributed as

$$\mathbb{P}(\hat{r}_i = r_i) = \tau_i \tag{1}$$

to an *aggregation protocol* deployed on a (decentralized) blockchain. The aggregation protocol produces the decentralized consensus  $\hat{\omega} \in \{0, 1\}$  according to

$$\mathbb{P}(\hat{\omega} = 1) = \sum_{i=1}^n \lambda_i \hat{r}_i \tag{2}$$

where  $\lambda_1, \dots, \lambda_n$  are positive weights summed to one. That is, the probability of generating a particular consensus equals the weighted fraction of received reports of the corresponding state. A data provider is referred to as *truthful* if her submitted report is consistent with the observed ground truth, i.e.,  $r_i = \omega$ . We define a *transmission protocol* as a collection of transmission technologies assigned to the  $n$  data providers,  $\{\tau_1, \dots, \tau_n\}$ , which are assumed to be independent. Without loss of generality, assume  $0.5 \leq \tau_i \leq 1$  so that it admits an interpretation of *transmission precision*. A transmission protocol is referred to as *deterministic* if  $\tau_1 = \dots = \tau_n = 1$ —this is the corner case examined in [Cong and He \(2019\)](#).

*Preference.* A data provider, which is assumed to be risk-neutral, has a von Neumann-Morgenstern utility function<sup>2</sup>

$$u_i(r_i, \omega, \hat{\omega}) = b_i|\omega - \hat{\omega}| - h_i|r_i - \omega|, \quad (3)$$

where  $b_i > 0$  is the benefit (e.g., payment from an on-chain derivatives position or a bet on a prediction market) of reaching a false consensus and  $h_i > 0$  the cost of misreporting—of a report that is at odds with the ground truth, i.e.,  $r_i \neq \omega$ . For example, it is widely accepted that economic agents have a nonpecuniary aversion to lying even in a cheap-talk communication (see, e.g., [Lundquist et al., 2009](#); [Gneezy, Kajackaite, and Sobel, 2018](#); [Bao et al., 2024](#)). More broadly, even in situations in which truthfulness cannot be verified, agents often refrain from lying despite the potential for pecuniary gain, due to for instance reputational concerns<sup>3</sup>. This specification follows [Cong and He \(2019\)](#). We show in [Section 2.5](#) that our results are robust to incorporation of another (parallel, not mutually exclusive) type of cost triggered instead by being inconsistent with the consensus (i.e.,  $r_i \neq \hat{\omega}$ ) and taking the form of collateral forfeited by data providers.

A data provider’s problem then reads as  $\max_{r_i \in \{0,1\}} \mathbb{E}[u_i(r_i, \omega, \hat{\omega})]$ . As a tie-breaking rule, we assume that a data provider reports truthfully in case of indifference, that is,  $r_i^* = \omega$  in case  $\mathbb{E}[u_i(\omega, \omega, \hat{\omega})] = \mathbb{E}[u_i(1 - \omega, \omega, \hat{\omega})]$ , which guarantees a unique optimal choice.

*Quality of Consensus.* The quality of decentralized consensus is proxied by the minus variance  $-\mathbb{V}[\omega - \hat{\omega}]$  evaluated ex ante (i.e., before  $\omega$  is revealed to anyone). We assume for simplicity an

<sup>2</sup>In [Section 2.5](#), we will introduce the generalized utility  $\hat{u}_i(r_i, \omega, \hat{\omega}) = b_i|\omega - \hat{\omega}| - h_i|r_i - \omega| - \eta_i|r_i - \hat{\omega}|$  where  $\eta_i \geq 0$  reflects a sum of collateral forfeited when being at variance with the consensus.

<sup>3</sup>For example, large oracle providers, such as Chainlink and Pyth Network are known to occasionally remove providers of faulty data.

uninformative prior for any potential information user, which may or may not be a data provider at the same time. An uninformative prior guarantees identical ex ante variances as  $\mathbb{V}[\omega] = \mathbb{V}[\hat{\omega}]$ , so that we have the simplification

$$-\mathbb{V}[\omega - \hat{\omega}] = -\mathbb{V}[\omega] - \mathbb{V}[\hat{\omega}] + 2\rho\sqrt{\mathbb{V}[\omega]\mathbb{V}[\hat{\omega}]} = 0.5(\rho - 1) \quad (4)$$

where  $-1 \leq \rho \leq 1$  denotes the Pearson correlation coefficient between  $\omega$  and  $\hat{\omega}$ . Also, as we show in Eq. (A3) in the Appendix,  $-\mathbb{V}[\omega - \hat{\omega}] = \mathbb{P}(\hat{\omega} = \omega) - 1$ . It is therefore evident that  $-\mathbb{V}[\omega - \hat{\omega}] \in [-1, 0]$  measures to what extent the consensus approximates ground truth. In particular,  $-\mathbb{V}[\omega - \hat{\omega}] = 0$  ( $-\mathbb{V}[\omega - \hat{\omega}] = -1$ , respectively) when all data providers report truthfully (untruthfully, respectively)<sup>4</sup>.

## 2.2 A Data Provider's Choice

It is evident from Eq. (3) that while a data provider's utility depends on other data providers' choices, the utility difference of truth-telling and misreporting does not, as the marginal effect of an individual data provider's report,  $r_i$ , on the aggregated consensus,  $\hat{\omega}$ , is constant. As a result, the choice of  $r_i$  involves no strategic consideration<sup>5</sup>. Under a deterministic transmission technology (i.e.,  $\tau_i = 1$ ), the trade-off for a data provider is fairly straightforward: using truthful reporting as a benchmark, misreporting increases the probability of reaching a false consensus by  $\lambda_i$  and therefore increases expected utility by  $\lambda_i b_i$  but incurs a cost of  $h_i$ —hence, the incentive-compatibility constraint for truth-telling is  $\lambda_i b_i \leq h_i$ .

Under randomized transmission, in contrast, with probability  $\tau_i$  ( $1 - \tau_i$ , respectively) misreporting (truthful reporting, respectively) contributes to reaching a false consensus (i.e., ends up with  $\hat{r}_i \neq \omega$ ), while only misreporting incurs the cost  $h_i$ . Put differently, in the state  $\hat{r}_i \neq r_i$ , truthful reporting reaps the benefit  $\lambda_i b_i$  while avoiding the cost  $h_i$  (i.e., double good news), whereas misreporting misses the benefit  $\lambda_i b_i$  while bearing the cost  $h_i$  (i.e., double bad news). As a result, randomized transmission curbs the incentives to misreport, as formalized in the proposition below.

<sup>4</sup>When all data providers report truthfully,  $\hat{\omega} = \omega$  with probability one and hence  $-\mathbb{V}[\omega - \hat{\omega}] = -\mathbb{V}[0] = 0$ . When all data providers report untruthfully,  $\hat{\omega} = 1 - \omega$  with probability one and hence  $-\mathbb{V}[\omega - \hat{\omega}] = -\mathbb{V}[\omega - (1 - \omega)] = -\mathbb{V}[2\omega - 1] = -\mathbb{E}[(2\omega - 1 - \mathbb{E}[2\omega - 1])^2] = -\mathbb{E}[(2\omega - 1 - 0)^2] = -1$ .

<sup>5</sup>Strategic interactions will arise if we introduce an additional penalty triggered by being inconsistent with the consensus, i.e.  $r_i \neq \hat{\omega}$  - we address this matter in Section 2.5.

In the noisiest transmission case,  $\tau_i = 0.5$ ,  $\hat{r}_i$  is independent of  $r_i$  and hence the data provider sees no benefit of lying, while the cost of lying remains unchanged at  $h_i$ .

**Proposition 2.1.** *A data provider's optimal choice is given by*

$$r_i^* = \begin{cases} \omega, & (2\tau_i - 1)\lambda_i b_i \leq h_i \\ 1 - \omega, & (2\tau_i - 1)\lambda_i b_i > h_i \end{cases}. \quad (5)$$

*As a result, one can always find a transmission precision for data provider  $i$ , such that 1) she reports truthfully and 2) the randomized report  $\hat{r}_i$  carries nonempty information to the aggregation protocol, i.e., it is not pure noise.*

Proposition 2.1 highlights a trade-off between truthfulness and precision—using a more precise transmission technology requires more commitment to truth-telling, which is, unfortunately, scarce in many contexts. Whilst it is widely accepted that decentralization increases truth-telling, that is, as  $n \rightarrow \infty$  and hence  $\lambda_i \rightarrow 0$  we always have  $r_i^* = \omega$ , decentralization does not come without a cost—each data provider needs to be compensated. Proposition 2.1 illustrates a new channel to achieve truthfulness without resorting to a large number of data providers—reduction in information transmission precision,  $\tau_i$ . On the flip side, it is perhaps not surprising that randomization has a side effect of introducing noise into aggregated consensus. As a result, randomization should be used as a remedy when the first-best outcome (i.e., truthful and precise information) cannot be achieved within a given network of data providers. We provide a rigorous analysis of the effects of randomized transmission on the overall quality of decentralized consensus—which trades off truthfulness and precision—in the next subsection.

### 2.3 Consensus Quality and Optimal Information Design

The quality of decentralized consensus is jointly determined by the truthfulness and precision of the individual reports collected from the data providers, as characterized in the following proposition.

**Proposition 2.2.** *The quality of decentralized consensus is given by*

$$-\mathbb{V}[\omega - \hat{\omega}] = - \left( 1 - \sum_{i=1}^n \lambda_i \left[ \tau_i \mathbb{I}_{\tau_i \leq \frac{h_i}{2\lambda_i b_i} + \frac{1}{2}} + (1 - \tau_i) \mathbb{I}_{\tau_i > \frac{h_i}{2\lambda_i b_i} + \frac{1}{2}} \right] \right) \quad (6)$$

where  $\mathbb{I}$  denotes the indicator function.

Proposition 2.2 implies that, with truthfulness (i.e.,  $\tau_i \leq \frac{h_i}{2\lambda_i b_i} + \frac{1}{2}$ ) a higher transmission precision enhances consensus quality, whereas without truthfulness (i.e.,  $\tau_i > \frac{h_i}{2\lambda_i b_i} + \frac{1}{2}$ ) a higher transmission precision jeopardizes consensus quality, because a data provider's contribution to  $-\mathbb{V}[\omega - \hat{\omega}]$  is  $\lambda_i \tau_i$  in the former case but  $\lambda_i(1 - \tau_i)$  in the latter case. To design a transmission protocol maximizing the quality of consensus, we should minimize the noise during transmission while keeping the data providers truthful. This logic is captured in the following proposition.

**Proposition 2.3.** *The problem  $\max_{\tau_1, \dots, \tau_n} -\mathbb{V}[\omega - \hat{\omega}]$  has a unique solution*

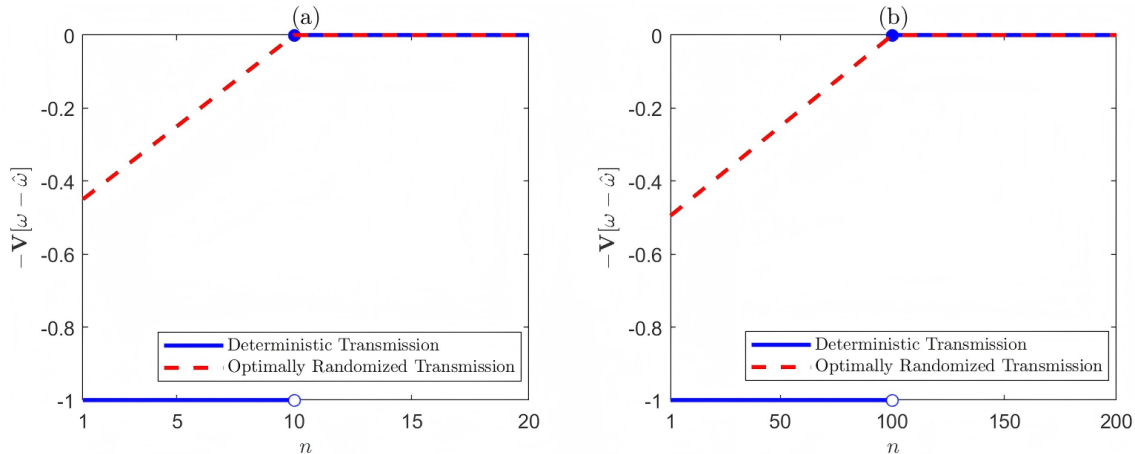
$$\tau_i^* = \min \left\{ 1, \frac{h_i}{2\lambda_i b_i} + \frac{1}{2} \right\}, i = 1, \dots, n \quad (7)$$

under which every data provider reports truthfully. The maximized consensus quality is

$$-\left( 1 - \sum_{i=1}^n \tau_i^* \lambda_i \right), \quad (8)$$

which improves upon the consensus quality under a deterministic transmission protocol by  $\sum_{i=1}^n \tau_i^* \lambda_i \mathbb{I}_{\tau_i^* < 1}$ .

Figure 1 shows the quality-improving effect of optimally randomized transmission, with a set of homogeneous data providers. The two panels differ in the cost of misreporting: the cost (to each data provider) is higher in (a). The consensus quality under a deterministic transmission protocol, illustrated by solid lines in both panels, is a binary-valued function (weakly) increasing in  $n$ —it either achieves the first-best outcome such that the information used to feed the aggregation protocol is both precise and truthful, or degenerates to the worst outcome when the incentive-compatibility constraint for truth-telling is not satisfied: recall that without truthfulness a higher transmission precision is detrimental to consensus quality. In contrast, consensus quality under an optimally randomized transmission protocol is smoothly increasing in  $n$ . The reason is that when the first-best outcome is not feasible due to insufficient truth-telling incentives, randomized transmission allows to achieve the second-best outcome, in which the information is noisy but truthful.



**Figure 1: Quality of Consensus: Deterministic vs. Randomized Transmission.** This figure plots the quality of consensus  $-\mathbb{V}[\omega - \hat{\omega}]$  formed under the deterministic transmission protocol (solid lines) and the optimally randomized transmission protocol (dashed lines) respectively, with parameter values  $b_i = 1$ ,  $\lambda_i = 1/n$ ,  $i = 1, \dots, n$ ,  $h_1 = \dots = h_n = 0.1$  in (a), and  $h_1 = \dots = h_n = 0.01$  in (b).

## 2.4 Cost of Misreporting as Private Information

In practice, it may be infeasible for a protocol designer to observe the misreporting costs  $h_1, \dots, h_n$  ex ante, which makes it difficult to design a customized transmission precision for each data provider. This subsection characterizes a protocol designer's problem in the presence of a set of ex ante homogeneous data providers with the distribution of  $h_i$  known, while the realization of each  $h_i$  is unknown. In the remainder of this subsection we assume:  $\lambda_i = 1/n$ ,  $b_i = \bar{b}$ ,  $h_i \stackrel{i.i.d.}{\sim} F_h$ ,  $i = 1, \dots, n$ ;  $F_h$  is the c.d.f. of a positive, continuous random variable. Given the ex ante homogeneity of data providers, it is without loss of generality that we restrict attention to the choice of a single  $\bar{\tau}$  such that  $\tau_1 = \dots = \tau_n = \bar{\tau}$ <sup>6</sup>.

**Proposition 2.4.** *With ex ante homogeneous data providers whose  $h_i$ 's are unknown and distributed according to  $F_h$ , the quality of decentralized consensus is given by*

$$-\mathbb{V}[\omega - \hat{\omega}] = \bar{\tau} - (2\bar{\tau} - 1)F_h\left(\frac{\bar{b}(2\bar{\tau} - 1)}{n}\right) - 1. \quad (9)$$

Proposition 2.4 offers a revealing factorization of the trade-off between truthfulness and precision.  $F_h\left(\frac{\bar{b}(2\bar{\tau} - 1)}{n}\right)$  is the probability of lying for a generic data provider, which is increasing

<sup>6</sup>See Eq. (A12): maximizing  $-\mathbb{V}[\omega - \hat{\omega}]$  is equivalent to maximizing each data provider's contribution separately.

in the transmission precision  $\bar{\tau}$  and is decreasing in decentralization  $n$ ; moreover, the detrimental effect of lying is amplified by a higher transmission precision, as reflected in the coefficient  $(2\bar{\tau} - 1) \geq 0$  that multiplies  $F_h$ . As  $\bar{\tau}$  increases, the gain term in Eq. (9),  $\bar{\tau}$ , increases yet the loss term  $(2\bar{\tau} - 1)F_h\left(\frac{\bar{b}(2\bar{\tau}-1)}{n}\right)$  also increases, such that the optimal trade-off is determined by the relative magnitude of the two competing forces. In particular,  $\lim_{n \rightarrow \infty} F_h\left(\frac{\bar{b}(2\bar{\tau}-1)}{n}\right) = 0$ , i.e., for a large  $n$ , the loss term vanishes and the optimal transmission precision is simply 1. Put differently, noisy transmission is useful only for a limited number of data providers, similar to the result for known costs of misreporting in Section 2.3, illustrated in Figure 1.

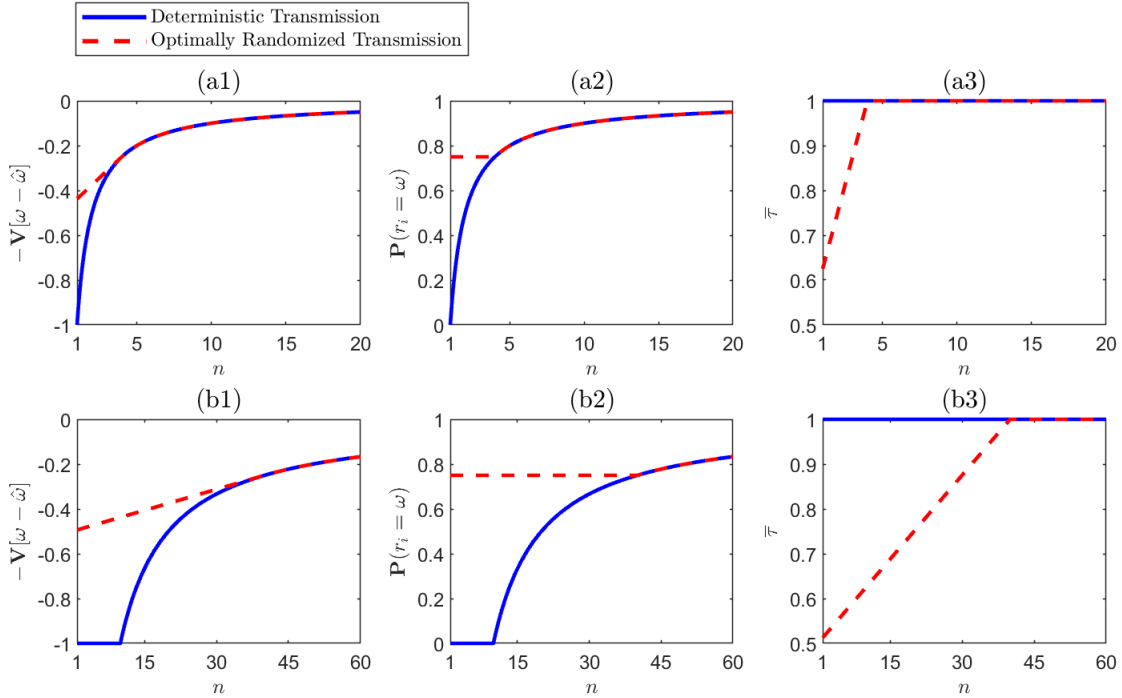
As a concrete example, when  $F_h$  is the uniform distribution over  $[0, \bar{b}]$ , the consensus quality is given by

$$-\mathbb{V}[\omega - \hat{\omega}] = \bar{\tau} - \frac{(2\bar{\tau} - 1)^2}{n} - 1, \quad (10)$$

which features a linear gain and a quadratic loss in  $\bar{\tau}$ ; the benefit of decentralization appears in the denominator of the quadratic term. The optimal design problem  $\max_{\bar{\tau}} \left( \bar{\tau} - \frac{(2\bar{\tau}-1)^2}{n} - 1 \right)$  has a unique solution  $\bar{\tau}^* = \min \left\{ \frac{1}{2} + \frac{n}{8}, 1 \right\}$ , at which from the protocol designer's perspective the truth-telling probability of each data provider is  $\max \left\{ \frac{3}{4}, \frac{n-1}{n} \right\}$ . Interestingly, as  $n$  increases from 1 to 4, the protocol designer has more "resources" to allocate between truthfulness and precision. In this range of  $n$ , the optimal design is one that keeps the truth-telling probability at  $\frac{3}{4}$  while increasing precision as much as possible, until the transmission precision reaches its upper bound of 1 at  $n = 4$ . When  $n > 4$ , the optimal precision is fixed at 1, with a truth-telling probability growing with  $n$ ; since the support of  $F_h$  starts from 0, the truth-telling probability never reaches 1 under a finite  $n$ .

Figure 2 (a1)–(a3) characterize the example discussed above with  $\bar{b} = 1$  and  $F_h = \text{Uniform}(0, 1)$ . As in (a1), the optimally randomized transmission protocol improves consensus quality upon that under the deterministic transmission protocol. The reason is that, as (a2) suggests, randomness brings about a higher chance of having a truthful data provider, since truth-telling is endogenous. The incremental truthfulness comes at a cost of precision, as illustrated in (a3) which plots the respective transmission precisions. Figure 2 (b1)–(b3) depict the case where the cost of misreporting is lower, by adopting  $F_h = \text{Uniform}(0, 0.1)$ . As expected, while the patterns are similar, a lower misreporting cost entails a higher degree of decentralization (i.e., a larger  $n$ ) for a protocol

to attain the same consensus quality. Unlike that in (a1), in (b1) the consensus quality under deterministic transmission remains at its lower bound for small  $n$ 's. This is because, under deterministic transmission, the quality improvement driven by decentralization cannot manifest itself until  $F_h\left(\frac{\bar{b}(2\bar{\tau}-1)}{n}\right) = F_h\left(\frac{\bar{b}}{n}\right) < 1$ ; by contrast, under optimally randomized transmission, the consensus quality is strictly increasing in  $n$ . Overall, the marginal benefit of optimally randomized transmission is especially salient when  $n$  is small.



**Figure 2: Quality of Consensus with Unknown  $h_i$ 's: Deterministic vs. Randomized Transmission.** This figure plots the quality of consensus  $-V[\omega - \hat{\omega}]$  formed under the deterministic transmission protocol and the optimally randomized transmission protocol respectively, with parameter values  $b_i = 1$ ,  $h_i \stackrel{i.i.d.}{\sim} F_h$ ,  $\lambda_i = 1/n$ ,  $i = 1, \dots, n$ ; in particular,  $F_h = \text{Uniform}(0, 1)$  in (a1)–(a3) and  $F_h = \text{Uniform}(0, 0.1)$  in (b1)–(b3).

## 2.5 Collateral and Truth-Telling

As relying on the non-pecuniary aversion to lying may not be sufficient, an oracle provider may incentivize truthful reporting through a contingent forfeiture of a data provider's collateral (i.e., stake). As  $\hat{\omega}$  is the unique enforced consensus on  $\omega$  and hence the unique trigger of value transfer where relevant, a designated penalty on dishonesty can only be contingent upon  $\hat{\omega}$  rather than  $\omega$ .

This motivates a generalized utility function of a data provider:

$$\hat{u}_i(r_i, \omega, \hat{\omega}) = b_i|\omega - \hat{\omega}| - h_i|r_i - \omega| - \eta_i|r_i - \hat{\omega}| \quad (11)$$

where  $\eta_i \geq 0$  is a sum of collateral the data provider posts on the blockchain, which is forfeited when she is judged to be dishonest, i.e.,  $r_i \neq \hat{\omega}$ . Clearly, when  $\eta_i = 0$  Eq. (11) degenerates to Eq. (3).

The following proposition shows, perhaps surprisingly, that the introduction of collateral-based incentives does not really interfere with the role of randomization in eliciting truth-telling.

**Proposition 2.5.** *When the utility includes forfeiture of collateral in case of deviations from consensus, as in Eq. (11), a data provider's optimal choice is given by*

$$r_i^* = \begin{cases} \omega, & (2\tau_i - 1)\lambda_i b_i - (2p_i - 1)\eta_i \leq h_i \\ 1 - \omega, & (2\tau_i - 1)\lambda_i b_i - (2p_i - 1)\eta_i > h_i \end{cases} \quad (12)$$

where  $p_i = \mathbb{P}_i(\hat{\omega} = \omega | r_i = X)$ ,  $X \sim \text{Bernoulli}(0.5)$ , is the probability, evaluated under the data provider's subjective belief, of reaching a true consensus when the data provider herself babbles. With homogeneous data providers, i.e.,  $\lambda_i = 1/n$ ,  $b_i = \bar{b}$ ,  $h_i = \bar{h}$ ,  $\eta_i = \bar{\eta}$ ,  $\tau_i = \bar{\tau}$ ,  $i = 1, \dots, n$ , there exists either a truthful equilibrium or a untruthful equilibrium or both. The region in which the two equilibria coexist is given by  $\bar{h} \in \mathcal{I}$  where

$$\mathcal{I} = \left[ \frac{(2\bar{\tau} - 1)(\bar{b} - \bar{\eta}(n + 1 - 2\bar{\tau}))}{n}, \frac{(2\bar{\tau} - 1)(\bar{b} + \bar{\eta}(n + 1 - 2\bar{\tau}))}{n} \right), \quad (13)$$

such that when  $\bar{h} \geq \sup \mathcal{I}$  ( $\bar{h} < \inf \mathcal{I}$ ) only the truthful (untruthful) equilibrium exists. Focusing on the Pareto-dominant equilibrium within the coexisting region, the equilibrium is truthful (untruthful) if  $\bar{h} \geq \frac{(2\bar{\tau}-1)\bar{b}}{n}$  ( $\bar{h} < \frac{(2\bar{\tau}-1)\bar{b}}{n}$ ), which does not depend on  $\bar{\eta}$ . As a result, the optimal transmission precision is given by  $\bar{\tau}^* = \min \left\{ 1, \frac{\bar{h}}{2n-1\bar{b}} \right\}$ , which is the same as that implied by Proposition 2.3.

Intuitively, the intrinsic value of truth/lie is determined by  $h_i$  and  $b_i$ , while the collateral-based incentives only matter with data providers' subjective beliefs. For example, consider a very large  $\eta_i$  under which the collateral-based incentives dominate. In this case, the game “converges” to a unanimity game as in [Harsanyi and Selten \(1988, p. 213\)](#), such that unanimity is the only

consideration, be it a truthful one or an untruthful one.

Pareto-efficiency is not the only equilibrium selection rule in the coexisting region; there are alternative selection rules (e.g., risk-dominance as in [Harsanyi and Selten \(1988\)](#)). It is difficult, however, to find a selection rule that predisposes the game to either of the two equilibria. One exception is the argument that, in the absence of prior communication, truth is more salient than a lie as a point to be coordinated towards even when the choices have the same intrinsic values, in the spirit of [Schelling \(1960\)](#).

Thus, we may assume that the equilibrium in the coexisting region is truthful (untruthful) if  $\bar{h} \geq \frac{(2\bar{\tau}-1)(\bar{b}-\bar{\eta}(n+1-2\bar{\tau}))}{n}$  ( $\bar{h} < \frac{(2\bar{\tau}-1)(\bar{b}-\bar{\eta}(n+1-2\bar{\tau}))}{n}$ ), instead of focusing on the Pareto-dominant one. In this case randomization still helps to achieve truth-telling, especially when  $\bar{h}$  and  $\bar{\eta}$  are small and  $\bar{b}$  is large, as  $\bar{\tau}$  can be chosen low enough that  $\frac{(2\bar{\tau}-1)(\bar{b}-\bar{\eta}(n+1-2\bar{\tau}))}{n}$  falls below  $\bar{h}$ .

### 3 Information Equilibrium in Product Market Competition

The model in the previous section generalizes the framework of decentralized consensus initiated by [Cong and He \(2019\)](#): in order to elicit truth-telling, we add verifiably fair random noise into the transmission of information from the data providers to the aggregator of reports, which leads to an information design problem trading off truthfulness and precision. In this section we examine another example of benefits of randomized transmission—that of information sharing among product market competitors, modifying established results in that literature.

Unlike the decentralized consensus depicted in [Section 2](#), information equilibrium in product market competition involves multi-faceted strategic considerations. An important distinction between the two settings is that in product market competition, information is *advisive* but not *enforcive*. This implies that no participant can profit from cheating: if truthful reporting is not incentive-compatible for a firm, a rational receiver will treat the firm’s report as cheap talk. A lack of commitment to truth-telling leads to cheap-talking ([Crawford and Sobel, 1982](#)), eliminating information sharing that could make both parties better off.

One solution to the cheap talk problem enabled by the blockchain and smart contracts is staking, as in [Flor et al. \(2025\)](#): a firm posts collateral on the blockchain, which is forfeited if misreporting is detected. However, staking requirement may discourage participation, especially for financially

constrained firms, as liquid assets are scarce.

We demonstrate that adding randomness into the communication between firms enables achieving a truth-telling equilibrium with an infinitesimal participation hurdle. Specifically, given any strictly positive amount of collateral, one can find a maximum truth-telling transmission precision for the firm, in the same vein as the truthfulness-precision trade-off in Section 2. In what follows, we characterize the Nash equilibrium where transmission precisions are endogenously determined and transformed into real impacts through subsequent production decisions.

### 3.1 Setup

Consider two firms  $j$  and  $-j$  in a Cournot duopoly, each of which maximizes its expected profit<sup>7</sup>, with a linear demand curve

$$P_i = \alpha_i - Q_i - Q_{-i}, i \in \{j, -j\}, \quad (14)$$

where  $i$  defines a generic firm. The production quantity  $Q_i$  is the corresponding firm's choice variable, and the unit cost of production is constant and normalized to zero, which implies a profit of  $Q_i(\alpha_i - Q_i - Q_{-i})$ . The demand function in Eq. (14), where the two products are perfect substitutes, is a reduced form derived from the standard full specification (see, e.g., Vives, 1999) of a representative consumer's utility when  $\beta = \gamma = 1$ :

$$U = \alpha_j Q_j + \alpha_{-j} Q_{-j} - \frac{1}{2} (\beta(Q_j^2 + Q_{-j}^2) + 2\gamma Q_j Q_{-j}) - P_j Q_j - P_{-j} Q_{-j} \quad (15)$$

where  $\beta > 0$  measures the rate of getting satiated and  $\gamma \in [-\beta, \beta]$  measures substitutability. Rather than developing a general model of information sharing in the context of product market competition as Raith (1996), our aim is to keep a clean incentive to misreport. Thus, we choose a setting in which a firm has the strongest incentives to overstate (but not understate) demand in communication in order to reduce (but not increase) its rival's output. Moreover, with perfect substitutes, unidirectional information disclosure is ex ante beneficial to a firm, as shown below. This helps to

---

<sup>7</sup>Unlike Section 2, in this section we do not incorporate a nonpecuniary aversion to lying, i.e., we assume profit-maximizing oligopolistic firms not affected by behavioral considerations, in contrast to largely atomistic data providers in decentralized consensus.

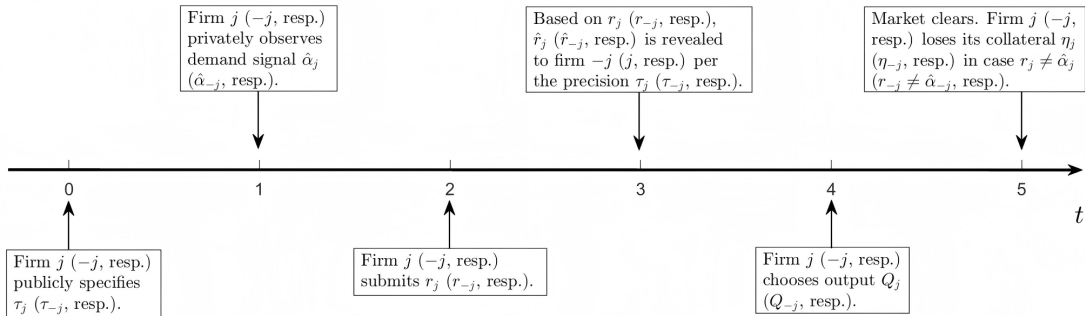
abstract from potential bargaining in which each firm would trade off the loss from information outflow and the gain from information inflow—an effect that is only tangentially relevant to our main argument.

The intercepts of demand for the firms’ products,  $(\alpha_i, \alpha_{-i})$ , are independent random variables, binary-valued in

$$\{\underline{\alpha}, \bar{\alpha}\} = \{\alpha(1 - \epsilon), \alpha(1 + \epsilon)\} \quad (16)$$

with equal probabilities, where  $\alpha > 0$  is the mean and  $\epsilon \in [0, 1/3]$  parameterizes the dispersion—the range of  $\epsilon$  is such that we focus on non-extreme demand fluctuations in which the higher value  $\bar{\alpha}$  is no more than two times of the lower one  $\underline{\alpha}$ <sup>8</sup>.

The two firms are ex ante symmetric except for a potential difference in their respective collaterals  $(\eta_j, \eta_{-j})$  posted on the blockchain, which are predetermined. The timeline of the game is as follows. At  $t = 0$ , firm  $i$  publicly sets up a transmission technology  $0.5 \leq \tau_i \leq 1$ . At  $t = 1$ , firm  $i$  privately observes a noisy signal realization of its own demand,  $\hat{\alpha}_i \in \{\underline{\alpha}, \bar{\alpha}\}$  in which  $\mathbb{P}(\hat{\alpha}_i = \alpha_i) = \phi \geq 0.5$ . At  $t = 2$ , firm  $i$  submits a report  $r_i \in \{\underline{\alpha}, \bar{\alpha}\}$  to its prespecified transmission technology. At  $t = 3$ ,  $\hat{r}_i \in \{\underline{\alpha}, \bar{\alpha}\}$  distributed as  $\mathbb{P}(\hat{r}_i = r_i) = \tau_i$  is revealed to firm  $-i$ . At  $t = 4$ , firm  $i$ , who is equipped with the information set  $(\hat{\alpha}_i, \hat{r}_{-i})$ , chooses its output  $Q_i$ . At  $t = 5$ , the market clears and firm  $i$  forfeits its collateral  $\eta_i$  if it misreported, i.e., submitted  $r_i \neq \hat{\alpha}_i$ <sup>9</sup>. Figure 3 provides an overview of the timeline.



**Figure 3: Timeline.**

As we shall see in Section 3.3, whether truthful reporting is incentive-compatible for firm  $i$

<sup>8</sup>This restriction ensures a nonnegative expected equilibrium price under any realization of the pre-production information set.

<sup>9</sup>This requires ex post verifiability of  $\hat{\alpha}_i$ , which we assume for now but relax in due course.

is determined by its own collateral-precision pair  $(\eta_i, \tau_i)$  but unaffected by the rival firm's profile  $(\eta_{-i}, \tau_{-i})$ . We assume for simplicity that if firm  $i$ 's profile  $(\eta_i, \tau_i)$  fails to prove incentive-compatible truthfulness, it is excluded from sending information immediately after time 0, which gives it a de facto outside option of abstaining from sending information with no penalty. This outside option, by ensuring the ex ante freedom of not committing to sending information, makes the assumption of predetermined collateral innocuous. As in Section 2, we adopt the tie-breaking rule in favor of truthfulness, that is, a firm reports truthfully whenever misreporting yields the same expected payoff.

### 3.2 Production Equilibrium under a Given Information Set

To study the endogenous determination of  $(\tau_j, \tau_{-j})$ , we use backwards induction. We clarify in this subsection the equilibrium production profile  $(Q_j, Q_{-j})$  and the subsequent profit under the assumption that the two firms have performed truthful information sharing via a given  $(\tau_j, \tau_{-j})$ . Importantly, truthful information sharing may not be incentive-compatible; it is an assumption in this subsection which we endogenize later.

The pre-production information set of firm  $i$  is given by  $I_i = (\hat{\alpha}_i, \hat{r}_{-i})$  which consists of its own private information  $\hat{\alpha}_i$  and its rival's randomized report  $\hat{r}_{-i}$ . Denote by  $\{Q_i(\hat{\alpha}_i, \hat{r}_{-i})\}_{i \in \{j, -j\}}$  the Bayesian Nash equilibrium in this subgame—it exists and is unique, as we will show later. Using a standard first-order-condition argument of expected profit maximization, we have

$$Q_i(\hat{\alpha}_i, \hat{r}_{-i}) = \frac{1}{2} \mathbb{E}_i [\alpha_i - Q_{-i}(\hat{\alpha}_{-i}, \hat{r}_i) | \hat{\alpha}_i, \hat{r}_{-i}]. \quad (17)$$

Since each firm's information set has four possible states, condition Eq. (17) yields a system of eight equations, with eight unknowns, namely

$$\{Q_i(\hat{\alpha}_i, \hat{r}_{-i})\}_{i \in \{j, -j\}, \hat{\alpha}_i \in \{\underline{\alpha}, \bar{\alpha}\}, \hat{r}_{-i} \in \{\underline{\alpha}, \bar{\alpha}\}} \quad (18)$$

which, upon solving, provides the unique Bayesian Nash equilibrium given any state of  $(I_j, I_{-j})$ ; though in a closed form, the solution is tedious and delegated to Eqs. (A17)–(A20) in the Appendix.

Firm  $i$ 's expected equilibrium profit evaluated by itself using the information set  $I_i$  is then:<sup>10</sup>

$$\Pi_i(\hat{\alpha}_i, \hat{r}_{-i}) = \mathbb{E}_i [Q_i(\hat{\alpha}_i, \hat{r}_{-i}) (\alpha_i - Q_i(\hat{\alpha}_i, \hat{r}_{-i}) - Q_{-i}(\hat{\alpha}_{-i}, \hat{r}_i)) | \hat{\alpha}_i, \hat{r}_{-i}]. \quad (19)$$

The next proposition characterizes the comparative statics of a firm's production decision with respect to the pre-production information set as well as the transmission technology.

**Proposition 3.1.** *Assume that the two firms have shared information truthfully. A firm produces more (less) when its own demand intercept (its rival's demand intercept) is likely to be high, that is,*

$$Q_i(\bar{\alpha}, \hat{r}_{-i}) - Q_i(\underline{\alpha}, \hat{r}_{-i}) \geq 0, \quad Q_i(\hat{\alpha}_i, \bar{\alpha}) - Q_i(\hat{\alpha}_i, \underline{\alpha}) \leq 0. \quad (20)$$

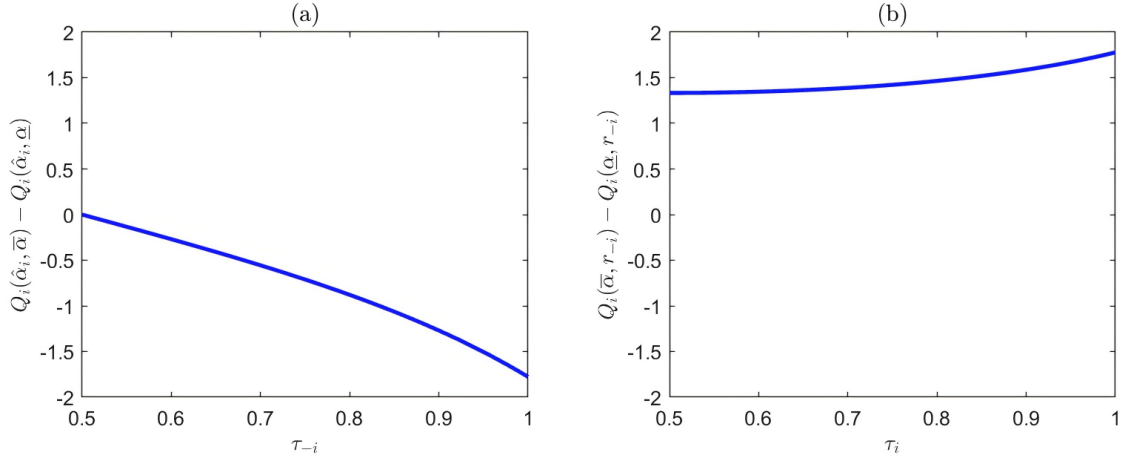
Moreover, a firm's production decision is more sensitive to its pre-production information set under higher transmission precisions, that is,

$$d \frac{Q_i(\bar{\alpha}, \hat{r}_{-i}) - Q_i(\underline{\alpha}, \hat{r}_{-i})}{d\tau_i} \geq 0, \quad d \frac{Q_i(\hat{\alpha}_i, \bar{\alpha}) - Q_i(\hat{\alpha}_i, \underline{\alpha})}{d\tau_{-i}} \leq 0. \quad (21)$$

Communication results in a de facto coordination, as it enables a firm to respond to the rival firm's demand intercept by differentiated production decisions. The second inequality in Eq. (21) shows that a noisier transmission carries less information and therefore flattens the differentiation in the response to the firm's rival's reported demand signal, as illustrated in Figure 4 (a). Relatedly, the first inequality in Eq. (21) is due to the fact that a firm's ability to influence its rival's production is only as good as its ability to signal its demand. A higher signal precision leads to higher (lower) output when firm  $i$ 's own demand intercept is high (low), as it implies a larger impact on the rival's optimal output, leading to a stronger indirect effect on the firm's optimal output. This effect is depicted in Figure 4 (b). Interestingly, the relation between  $Q_i(\bar{\alpha}, \hat{r}_{-i}) - Q_i(\underline{\alpha}, \hat{r}_{-i})$  and  $\tau_i$  is flatter than that between  $Q_i(\hat{\alpha}_i, \bar{\alpha}) - Q_i(\hat{\alpha}_i, \underline{\alpha})$  and  $\tau_{-i}$ , because observing  $\hat{\alpha}_i = \bar{\alpha}$  is itself a sufficient reason for a higher output even if the rival firm is agnostic of this (i.e., even if  $\tau_i = 0.5$ ), which represents the first-order effect, while what Panel (b) captures is the output adjustment attributed

<sup>10</sup>We could have used the notation  $\{Q_i(\hat{\alpha}_i, \hat{r}_{-i}; \tau_i, \tau_{-i})\}_{i \in \{j, -j\}}$  for the equilibrium production as it certainly depends on  $(\tau_i, \tau_{-i})$ , but to economize space we use  $\{Q_i(\hat{\alpha}_i, \hat{r}_{-i})\}_{i \in \{j, -j\}}$  instead, since  $(\tau_j, \tau_{-j})$  can be deemed as exogenous if we start from  $t = 4$ . This is also the case of  $\Pi_i(\hat{\alpha}_i, \hat{r}_{-i})$  which could have been denoted as  $\Pi_i(\hat{\alpha}_i, \hat{r}_{-i}; \tau_i, \tau_{-i})$ .

to signaling, which represents the second-order effect, as it implies both a higher deterring likelihood (i.e.,  $\mathbb{P}(\hat{r}_i = \bar{\alpha})$ ) and a stronger deterring effect (i.e.,  $\mathbb{P}_{-i}(\alpha_i = \bar{\alpha} | \hat{\alpha}_i = \bar{\alpha})$ ).



**Figure 4: Production Responsiveness and Transmission Precisions.** (a) plots  $Q_i(\hat{\alpha}_i, \bar{\alpha}) - Q_i(\hat{\alpha}_i, \underline{\alpha})$  as a function of  $\tau_{-i}$ , and (b) plots  $Q_i(\bar{\alpha}, \hat{r}_{-i}) - Q_i(\underline{\alpha}, \hat{r}_{-i})$  as a function of  $\tau_i$ . The parameter values are  $\alpha = 10$ ,  $\phi = 0.7$ , and  $\epsilon = 1/3$ .

We now characterize the relation between the transmission precisions,  $(\tau_j, \tau_{-j})$ , and a firm's equilibrium profit.

**Proposition 3.2.** *Assume that the two firms have shared information truthfully. Firm  $i$ 's expected equilibrium profit evaluated after the transmission protocol is set but before  $(\hat{\alpha}_i, \hat{r}_{-i})$  is observed, i.e.,  $\mathbb{E}_{\hat{\alpha}_i, \hat{r}_{-i}} [\Pi_i(\hat{\alpha}_i, \hat{r}_{-i})]$ , is increasing in both its own transmission precision  $\tau_i$  and the rival firm's transmission precision  $\tau_{-i}$ .*

If firm  $i$  has sufficient commitment power, i.e., the on-chain collateral  $\eta_i$  is sufficiently large, it will always choose  $\tau_i = 1$  regardless of the rival firm's choice; if both firms have sufficient commitment power, then  $(\tau_j, \tau_{-j}) = (1, 1)$  is the unique Nash equilibrium which is Pareto-optimal. Besides, it implies that even participating in the information sharing agreement as a pure receiver (or pure sender) makes both firms better off. This is important because it challenges the apparently plausible argument that attributes nonparticipation to a firm's inability to post sufficient collateral and hence its inability to credibly send information.

### 3.3 Incentive-Compatible Truth-Telling

The required collateral for truthful reporting equals the maximum incremental expected profit from misreporting. Denote by  $\Delta_i(\hat{\alpha}_i, \hat{r}_{-i}; \tau_i, \tau_{-i})$  the expected profit of firm  $i$  under  $r_i \neq \hat{\alpha}_i$  in excess of  $\Pi_i(\hat{\alpha}_i, \hat{r}_{-i})$ . Put differently,  $\Delta_i(\hat{\alpha}_i, \hat{r}_{-i}; \tau_i, \tau_{-i})$  is the difference between expected profits under two scenarios: 1) firm  $i$  misreporting and 2) firm  $i$  reporting truthfully, assuming that firm  $-i$  always reports truthfully and always trusts firm  $i$ 's report. Since at the time of reporting firm  $i$  has not observed  $\hat{r}_{-i}$ , the necessary collateral to ensure truth-telling after receiving either of the demand signals is

$$C_i(\tau_i) = \max_{\hat{\alpha}_i} \mathbb{E}_{\hat{r}_{-i}} [\Delta_i(\hat{\alpha}_i, \hat{r}_{-i}; \tau_i, \tau_{-i})]. \quad (22)$$

As a result, a transmission protocol  $(\tau_j, \tau_{-j})$  leads to a truthful equilibrium if and only if

$$C_i(\tau_i) \leq \eta_i, \forall i \in \{j, -j\}. \quad (23)$$

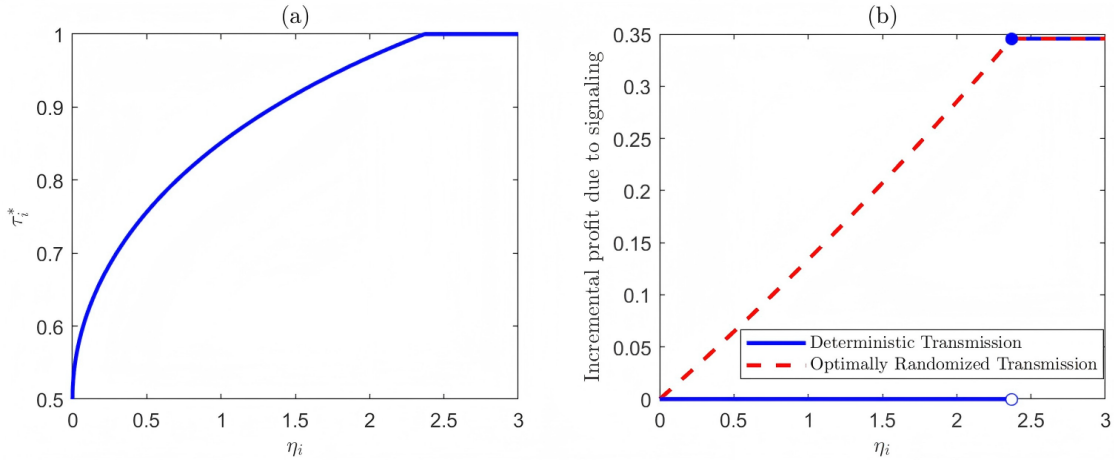
We characterize the comparative statics of the necessary collateral in the proposition below, which, together with Proposition 3.2, highlights a trade-off between the truthfulness and the precision of information sharing given the scarcity of commitment power; fully exploiting the capacity of collateral leads to the Nash equilibrium of  $(\tau_j, \tau_{-j})$ .

**Proposition 3.3.**  *$C_i(\tau_i)$  is continuous and increasing in  $\tau_i$ ,  $\alpha$ ,  $\phi$ , and  $\epsilon$ ; trivially,  $C_i(0.5) = 0$ . Optimal  $\tau_i^* = \max_{C_i(\tau_i) \leq \eta_i} \tau_i$ , which does not depend on the rival firm's choice of  $\tau_{-i}$ , such that the unique Nash equilibrium of the transmission protocol is given by  $(\tau_j^*, \tau_{-j}^*)$ .*

Though obvious, we explicitly state the continuity of  $C_i(\tau_i)$  in  $\tau_i$  (as well as other variables) to stress that there always exists a transmission precision,  $\tau_j$ , that ensures a nonwasteful use of  $\eta_i$ , the highest collateral available, which bears important implications for participation in information sharing. To illustrate, suppose  $0 < \eta_i < C_i(1)$ , that is, firm  $i$  has some collateral but the amount is insufficient for  $\tau_i = 1$  (i.e.,  $\tau_i = 1$  would lead to incentives to misreport being too strong). In other words, under deterministic transmission, firm  $i$  would immediately miss the collateral hurdle required to ensure truth-telling. In contrast, under randomized transmission, firm  $i$  can always

find  $\tau_i^* \in (0.5, 1)$  such that  $C_i(\tau_i^*) = \eta_i$ , which improves both firms' welfare relative to that under deterministic transmission. In sum, randomized transmission enables a firm to attain the second-best outcome, which is between the first-best (but possibly infeasible) one associated with  $\tau_j = 1$  and the worst one associated to abstaining from information sharing, so that the firm's collateral is always productive.

On the other hand,  $\alpha$  and  $\epsilon$  encapsulate the magnitude of exogenous uncertainty of which the fraction a firm privately resolves is  $\phi$ . As a result, the same value of  $\tau_i$  would reveal a larger amount of information when any of  $\alpha$ ,  $\phi$ , and  $\epsilon$  is higher, which renders  $C_i(\tau_i)$  increasing in each of the three variables.



**Figure 5: Collateral, Optimal Transmission Precision, and Incremental Profit.** (a) plots  $\tau_i^*$  as a function of  $\eta_i$ . (b) plots the incremental profit due to information sharing as a function of  $\eta_i$ , under deterministic transmission and optimally randomized transmission, respectively. The parameter values are  $\alpha = 10$ ,  $\phi = 0.7$ , and  $\epsilon = 1/3$ .

Figure 5 shows the maximum transmission precision for incentive-compatible truth-telling as a function of the amount of collateral (Panel (a)) and the incremental profit due to information sharing (Panel (b)) under deterministic transmission (solid line) and randomized transmission (dashed line). As evident from Panel (a), optimal transmission precision is increasing in collateral, up to the point at which collateral is sufficient to support truthful deterministic transmission. As shown in Panel (b), a firm's profit is monotonically increasing in collateral up to the point at which truthful deterministic transmission becomes possible and at which the incremental profit under two transmission mechanisms coincide.

### 3.4 Unverifiable Private Information

We have assumed so far that all relevant quantities  $(\alpha_j, \alpha_{-j}, Q_j, Q_{-j}, P_j, P_{-j}, \hat{\alpha}_j, \hat{\alpha}_{-j}, r_j, r_{-j}, \hat{r}_j, \hat{r}_{-j})$  become public ex post, which allows to base collateral forfeiture on all these quantities. The observability of outputs  $(Q_j, Q_{-j})$  as well as prices  $(P_j, P_{-j})$  is a standard assumption, from which  $(\alpha_j, \alpha_{-j})$  can be inferred, and  $(r_j, r_{-j}, \hat{r}_j, \hat{r}_{-j})$  are quantities directly recorded on the blockchain. In other words, the ex post verifiability assumption is very natural for all elements except for  $(\hat{\alpha}_j, \hat{\alpha}_{-j})$  which could be permanently private information. In this subsection only we assume that  $(\hat{\alpha}_j, \hat{\alpha}_{-j})$  is never observable to outsiders, and demonstrate the validity of the model's qualitative results to ex post unobservable private demand signals.

Can collateral clearance be properly enforced without verifying  $(\hat{\alpha}_j, \hat{\alpha}_{-j})$ ? A naive idea is to infer  $\hat{\alpha}_i$  from  $Q_i$ , that is, to infer private information from its output. However, this reasoning is flawed because a firm can overstate its demand signal and pretend to be honest by choosing the output quantity consistent with its report. Formally, define  $\tilde{\Delta}_i(\hat{\alpha}_i, \hat{r}_{-i}; \tau_i, \tau_{-i})$  as the incremental expected profit firm  $i$  could make from *misreporting and disguising*, in contrast to  $\Delta_i(\hat{\alpha}_i, \hat{r}_{-i}; \tau_i, \tau_{-i})$  which represents the incremental expected profit from *misreporting and optimizing (hence not disguising)*. That is, under both  $\Delta_i(\hat{\alpha}_i, \hat{r}_{-i}; \tau_i, \tau_{-i})$  and  $\tilde{\Delta}_i(\hat{\alpha}_i, \hat{r}_{-i}; \tau_i, \tau_{-i})$ , the firm chooses  $r_i \neq \hat{\alpha}_i$ ; however, under  $\Delta_i(\hat{\alpha}_i, \hat{r}_{-i}; \tau_i, \tau_{-i})$  the firm chooses the profit-maximizing output, whereas under  $\tilde{\Delta}_i(\hat{\alpha}_i, \hat{r}_{-i}; \tau_i, \tau_{-i})$  the firm chooses the the output  $Q_i(r_i, \hat{r}_{-i})$  consistent with its report. The maximum incremental expected profit a firm could make from misreporting and disguising is

$$\tilde{M}_i(\tau_i) = \max \left\{ 0, \max_{\hat{\alpha}_i} \mathbb{E}_{\hat{r}_{-i}} \left[ \tilde{\Delta}_i(\hat{\alpha}_i, \hat{r}_{-i}; \tau_i, \tau_{-i}) \right] \right\}, \quad (24)$$

where, unlike  $\max_{\hat{\alpha}_i} \mathbb{E}_{\hat{r}_{-i}} [\Delta_i(\hat{\alpha}_i, \hat{r}_{-i}; \tau_i, \tau_{-i})]$ ,  $\max_{\hat{\alpha}_i} \mathbb{E}_{\hat{r}_{-i}} [\tilde{\Delta}_i(\hat{\alpha}_i, \hat{r}_{-i}; \tau_i, \tau_{-i})]$  may be negative because the firm is forced to choose a suboptimal output. We show in the Appendix that there indeed exist cases in which  $\tilde{M}_i(\tau_i) > 0$ , so a forfeiture of collateral triggered by  $Q_i \neq Q_i(r_i, \hat{r}_{-i})$  only cannot ensure truth-telling.

The only possibility of properly incentivizing truth-telling is a forfeiture of collateral triggered by  $r_i \neq \alpha_i$  in addition to  $Q_i \neq Q_i(r_i, \hat{r}_{-i})$ . As such, for a collateral of  $x$ , the difference of the expected amount of collateral refund for truth-telling versus misreporting and disguising is  $(2\phi - 1)x$ , which

implies that the necessary collateral for prohibiting misreporting and disguising is  $\tilde{M}_i(\tau_i)/(2\phi - 1)$ .

In sum,  $C_i(\tau_i)$  is the collateral required to prohibit misreporting and optimizing on quantity, while  $\tilde{M}_i(\tau_i)/(2\phi - 1)$  is the collateral required to prohibit misreporting and disguising. Therefore, the necessary collateral to ensure truth-telling is the maximum between the two, as formalized in the proposition below.

**Proposition 3.4.** *Under the mechanism that firm  $i$  loses its collateral if  $r_i \neq \alpha_i$  or  $Q_i \neq Q_i(r_i, \hat{r}_{-i})$  or both, the necessary collateral to ensure truthful reporting is*

$$\tilde{C}_i(\tau_i) = \max \left\{ C_i(\tau_i), \tilde{M}_i(\tau_i)/(2\phi - 1) \right\} \quad (25)$$

where we have  $C_i(\tau_i) \geq \tilde{M}_i(\tau_i)/(2\phi - 1)$  for large  $\phi$  and  $C_i(\tau_i) \leq \tilde{M}_i(\tau_i)/(2\phi - 1)$  for small  $\phi$ ; moreover,  $\tilde{C}_i(\tau_i)$  is continuous and increasing in  $\tau_i$  with  $\tilde{C}_i(0.5) = 0$  so that randomized transmission still helps a financially constrained firm fully exploit its collateral if any.

Intuitively, when the demand signal  $\hat{\alpha}_i$  is itself precise, the manipulation in output for disguising purposes seldom conduces to avoid forfeiture of collateral, because of a big difference in collateral recovery probability of truthful reporting and misreporting followed by disguising,  $\mathbb{P}(r_i = \alpha_i | r_i = \hat{\alpha}_i) - \mathbb{P}(r_i = \alpha_i | r_i \neq \hat{\alpha}_i) = 2\phi - 1$ . Therefore, it suffices to focus on  $C_i(\tau_i)$  when  $\phi$  is large. In contrast, when  $\phi$  is small and hence  $\hat{\alpha}_i$  is itself noisy, discouraging misreporting and disguising becomes very difficult due to a small difference in collateral recovery probability, such that we have to require a large amount of collateral.

Proposition 3.4 shows that, on the one hand, the unverifiability of  $(\hat{\alpha}_j, \hat{\alpha}_{-j})$  does not eliminate the core advantage of randomized transmission because the firms can still credibly share some information so long as  $\max\{\eta_j, \eta_{-j}\} > 0$ ; on the other, when the private information is itself noisy (i.e.,  $\phi$  is small), the maximum transmission precision a financially constrained firm can commit to is further lowered, which quantitatively impairs firms' ability to share information.

## 4 Conclusion

Blockchain disruption reshapes information transmission among economic agents. This paper studies how verifiably fair randomness, complemented by other blockchain functionalities, can dis-

courage strategic information misreporting and improve equilibrium outcomes. We characterize the optimal trade-off between truthfulness and precision across two broad classes of information equilibria—those featuring enforceable and advise information, respectively—with positive effects of orchestrated randomness being present in both. From a broader perspective, the paper advances our understanding of the economics of information in the FinTech era and demonstrates a compelling vision where blockchain technology appeals to a wide range of information users.

There are several promising avenues for future research. The first is incorporation of heterogeneous data providers' individual preferences and optimal design of aggregation of data providers' reports. Second, our binary-state setting downplays the notion that truth is, due to its uniqueness, more salient than lies as a point to be coordinated towards unanimity, which calls for a multi-state modeling. Third, testing the tension between truthfulness and precision using empirical data would be valuable for adapting the theoretical mechanisms to real-world implementations.

## Appendix

**Proof of Proposition 2.1.** The difference in probability of earning  $b_i$  from misreporting and truthful reporting is

$$\begin{aligned}
 & \mathbb{P}(\omega \neq \hat{\omega} | r_i \neq \omega) - \mathbb{P}(\omega \neq \hat{\omega} | r_i = \omega) \\
 &= (\tau_i \mathbb{P}(\omega \neq \hat{\omega} | \hat{r}_i \neq \omega) + (1 - \tau_i) \mathbb{P}(\omega \neq \hat{\omega} | \hat{r}_i = \omega)) - (\tau_i \mathbb{P}(\omega \neq \hat{\omega} | \hat{r}_i = \omega) + (1 - \tau_i) \mathbb{P}(\omega \neq \hat{\omega} | \hat{r}_i \neq \omega)) \\
 &= (2\tau_i - 1) (\mathbb{P}(\omega \neq \hat{\omega} | \hat{r}_i \neq \omega) - \mathbb{P}(\omega \neq \hat{\omega} | \hat{r}_i = \omega)) = (2\tau_i - 1)\lambda_i. \tag{A1}
 \end{aligned}$$

As a result, truthful reporting is optimal if and only if

$$(2\tau_i - 1)\lambda_i b_i \leq h_i, \tag{A2}$$

that is, the incremental probability of earning  $b_i$  does not exceed the cost  $h_i$ . Rearranging Eq. (A2) gives  $\tau_i \leq \underbrace{\frac{h_i}{2\lambda_i b_i}}_{>0} + \frac{1}{2}$  such that any  $\tau_i$  in the interval  $(0.5, 0.5 + h_i/(2\lambda_i b_i)]$  induces truth-telling and carries nonempty information. ■

**Proof of Proposition 2.2.** We have  $\omega \stackrel{d}{=} \hat{\omega}$  as  $\mathbb{P}(\hat{\omega} = 1) = 0.5\mathbb{P}(\hat{\omega} = \omega) + 0.5(1 - \mathbb{P}(\hat{\omega} = \omega)) = 0.5 = \mathbb{P}(\omega = 1)$  given that we have assumed an uninformative prior about  $\omega$ . Note that

$$\begin{aligned}
 -\mathbb{V}[\omega - \hat{\omega}] &= -\mathbb{E}[(\omega - \hat{\omega})^2] = -(\mathbb{P}(\hat{\omega} = \omega)\mathbb{E}[(\omega - \hat{\omega})^2 | \hat{\omega} = \omega] + (1 - \mathbb{P}(\hat{\omega} = \omega))\mathbb{E}[(\omega - \hat{\omega})^2 | \hat{\omega} = 1 - \omega]) \\
 &= -(1 - \mathbb{P}(\hat{\omega} = \omega))\mathbb{E}[(2\omega - 1)^2] = -(1 - \mathbb{P}(\hat{\omega} = \omega)). \tag{A3}
 \end{aligned}$$

The best response of data provider  $i$  as a function of  $\omega$ , that is,

$$r_i(\omega) = \omega \mathbb{I}_{(2\tau_i - 1)\lambda_i b_i \leq h_i} + (1 - \omega) \mathbb{I}_{(2\tau_i - 1)\lambda_i b_i > h_i} = \omega \mathbb{I}_{\tau_i \leq \tau_i^*} + (1 - \omega) \mathbb{I}_{\tau_i > \tau_i^*}, \tag{A4}$$

where  $\tau_i^* = \min \left\{ 1, \frac{h_i}{2\lambda_i b_i} + \frac{1}{2} \right\}$ . Given a realization  $\omega^* \in \{0, 1\}$ ,

$$\begin{aligned}
\mathbb{P}(\hat{\omega} = \omega^* | \omega = \omega^*) &= \mathbb{E} [\mathbb{I}_{\hat{\omega} = \omega^*} | r_i = r_i(\omega), i = 1, \dots, n] \\
&= \mathbb{I}_{\omega^* = 1} \mathbb{E} \left[ \sum_{i=1}^n \lambda_i \hat{r}_i | r_i = r_i(1), i = 1, \dots, n \right] + \mathbb{I}_{\omega^* = 0} \mathbb{E} \left[ 1 - \sum_{i=1}^n \lambda_i \hat{r}_i | r_i = r_i(0), i = 1, \dots, n \right] \\
&= \mathbb{I}_{\omega^* = 1} \sum_{i=1}^n \lambda_i \mathbb{E}[\hat{r}_i | r_i = r_i(1)] + \mathbb{I}_{\omega^* = 0} \left( 1 - \sum_{i=1}^n \lambda_i \mathbb{E}[\hat{r}_i | r_i = r_i(0)] \right) \\
&= \mathbb{I}_{\omega^* = 1} \sum_{i=1}^n \lambda_i [\tau_i \mathbb{I}_{\tau_i \leq \tau_i^*} + (1 - \tau_i) \mathbb{I}_{\tau_i > \tau_i^*}] + \mathbb{I}_{\omega^* = 0} \left( 1 - \sum_{i=1}^n \lambda_i [(1 - \tau_i) \mathbb{I}_{\tau_i \leq \tau_i^*} + \tau_i \mathbb{I}_{\tau_i > \tau_i^*}] \right) \\
&= \mathbb{I}_{\omega^* = 1} \sum_{i=1}^n \lambda_i [\tau_i \mathbb{I}_{\tau_i \leq \tau_i^*} + (1 - \tau_i) \mathbb{I}_{\tau_i > \tau_i^*}] + \mathbb{I}_{\omega^* = 0} \sum_{i=1}^n \lambda_i [1 - (1 - \tau_i) \mathbb{I}_{\tau_i \leq \tau_i^*} + \tau_i \mathbb{I}_{\tau_i > \tau_i^*}] \\
&= \mathbb{I}_{\omega^* = 1} \sum_{i=1}^n \lambda_i [\tau_i \mathbb{I}_{\tau_i \leq \tau_i^*} + (1 - \tau_i) \mathbb{I}_{\tau_i > \tau_i^*}] + \mathbb{I}_{\omega^* = 0} \sum_{i=1}^n \lambda_i [\mathbb{I}_{\tau_i \leq \tau_i^*} + \mathbb{I}_{\tau_i > \tau_i^*} - (1 - \tau_i) \mathbb{I}_{\tau_i \leq \tau_i^*} + \tau_i \mathbb{I}_{\tau_i > \tau_i^*}] \\
&= (\mathbb{I}_{\omega^* = 1} + \mathbb{I}_{\omega^* = 0}) \sum_{i=1}^n \lambda_i [\tau_i \mathbb{I}_{\tau_i \leq \tau_i^*} + (1 - \tau_i) \mathbb{I}_{\tau_i > \tau_i^*}] \\
&= \sum_{i=1}^n \lambda_i [\tau_i \mathbb{I}_{\tau_i \leq \tau_i^*} + (1 - \tau_i) \mathbb{I}_{\tau_i > \tau_i^*}], \tag{A5}
\end{aligned}$$

which implies  $\mathbb{P}(\hat{\omega} = \omega | \omega = 1) = \mathbb{P}(\hat{\omega} = \omega | \omega = 0) = \mathbb{P}(\hat{\omega} = \omega)$  and hence

$$\mathbb{P}(\hat{\omega} = \omega) = \sum_{i=1}^n \lambda_i [\tau_i \mathbb{I}_{\tau_i \leq \tau_i^*} + (1 - \tau_i) \mathbb{I}_{\tau_i > \tau_i^*}]. \tag{A6}$$

Therefore,

$$-\mathbb{V}[\omega - \hat{\omega}] = - \left( 1 - \sum_{i=1}^n \lambda_i [\tau_i \mathbb{I}_{\tau_i \leq \tau_i^*} + (1 - \tau_i) \mathbb{I}_{\tau_i > \tau_i^*}] \right). \tag{A7}$$

■.

**Proof of Proposition 2.3.** Following the proof of Proposition 2.2, maximizing the quality of consensus is equivalent to maximizing  $\mathbb{P}(\hat{\omega} = \omega)$  (see Eq. (A6)). Now the problem becomes

$$\max_{\tau_1, \dots, \tau_n} \sum_{i=1}^n \lambda_i [\tau_i \mathbb{I}_{\tau_i \leq \tau_i^*} + (1 - \tau_i) \mathbb{I}_{\tau_i > \tau_i^*}]. \tag{A8}$$

$\tau_i^*, i = 1, \dots, n$  is the only maximizer of problem Eq. (A8), under which every data provider reports truthfully and the maximized  $\mathbb{P}(\hat{\omega} = \omega)$  is  $\mathbb{P}^*(\hat{\omega} = \omega) = \sum_{i=1}^n \lambda_i \tau_i^*$ , which immediately yields the maximized consensus quality in the proposition. In case of deterministic transmission, plugging  $\tau_1 = \dots = \tau_n = 1$  into the expression of  $\mathbb{P}(\hat{\omega} = \omega)$  gives  $\mathbb{P}^D(\hat{\omega} = \omega) = \sum_{i=1}^n \lambda_i \mathbb{I}_{1 \leq \tau_i^*}$ . Hence,

$$\mathbb{P}^*(\hat{\omega} = \omega) - \mathbb{P}^D(\hat{\omega} = \omega) = \sum_{i=1}^n \lambda_i (\tau_i^* - \mathbb{I}_{1 \leq \tau_i^*}) = \sum_{i=1}^n \tau_i^* \lambda_i \mathbb{I}_{\tau_i^* < 1}, \quad (\text{A9})$$

which completes the proof, provided that the difference between two  $-\mathbb{V}[\omega - \hat{\omega}]$ 's equals the difference between the two corresponding  $\mathbb{P}(\hat{\omega} = \omega)$ 's. ■

**Proof of Proposition 2.4.** Observe that

$$\begin{aligned} \mathbb{P}(\omega = \hat{\omega}) &= \frac{1}{n} \mathbb{E}_{h_1, \dots, h_n} \left[ \sum_{i=1}^n \left( \tau_i \mathbb{I}_{\frac{(2\tau_i-1)\bar{b}}{n} \leq h_i} + (1 - \tau_i) \mathbb{I}_{\frac{(2\tau_i-1)\bar{b}}{n} > h_i} \right) \right] \\ &= \frac{1}{n} \sum_{i=1}^n \left[ \tau_i \left( 1 - F_h \left( \frac{(2\tau_i-1)\bar{b}}{n} \right) \right) + (1 - \tau_i) F_h \left( \frac{(2\tau_i-1)\bar{b}}{n} \right) \right] \\ &= \frac{1}{n} \sum_{i=1}^n \left[ \tau_i - (2\tau_i - 1) F_h \left( \frac{(2\tau_i-1)\bar{b}}{n} \right) \right]. \end{aligned} \quad (\text{A10})$$

Form Eq. (A10) we have

$$-\mathbb{V}[\omega - \hat{\omega}] = -(1 - \mathbb{P}(\omega = \hat{\omega})) = -1 + \frac{1}{n} \sum_{i=1}^n \left[ \tau_i - (2\tau_i - 1) F_h \left( \frac{(2\tau_i-1)\bar{b}}{n} \right) \right], \quad (\text{A11})$$

which implies that

$$\begin{aligned} \max_{\tau_1, \dots, \tau_n} -\mathbb{V}[\omega - \hat{\omega}] &= -1 + \frac{1}{n} \sum_{i=1}^n \max_{\tau_i} \left[ \tau_i - (2\tau_i - 1) F_h \left( \frac{(2\tau_i-1)\bar{b}}{n} \right) \right] \\ &= -1 + \max_{\bar{\tau}} \left[ \bar{\tau} - (2\bar{\tau} - 1) F_h \left( \frac{(2\bar{\tau}-1)\bar{b}}{n} \right) \right] \end{aligned} \quad (\text{A12})$$

such that in maximizing consensus quality it is without loss of generality to assume  $\tau_1 = \dots = \tau_n = \bar{\tau}$ , in which case we have  $-\mathbb{V}[\omega - \hat{\omega}] = \bar{\tau} - (2\bar{\tau} - 1) F_h \left( \frac{(2\bar{\tau}-1)\bar{b}}{n} \right) - 1$ . ■

**Proof of Proposition 2.5.** We first prove Eq. (12). Observe that  $\mathbb{P}_i(\hat{\omega} = \omega | r_i = \omega) = p_i + \lambda_i (\tau_i -$

0.5) and  $\mathbb{P}_i(\hat{\omega} = \omega | r_i = 1 - \omega) = p_i - \lambda_i(\tau_i - 0.5)$ , which are the probabilities of reaching a true consensus when data provider  $i$  itself reports truthfully and untruthfully respectively. As a result, the chance of recovering  $\eta_i$  when it reports truthfully is  $\mathbb{P}_i(\hat{\omega} = \omega | r_i = \omega) = p_i + \lambda_i(\tau_i - 0.5)$ , while the chance of recovering  $\eta_i$  when it reports untruthfully is

$$\mathbb{P}_i(\hat{\omega} = 1 - \omega | r_i = 1 - \omega) = 1 - \mathbb{P}_i(\hat{\omega} = \omega | r_i = 1 - \omega) = 1 - p_i + \lambda_i(\tau_i - 0.5). \quad (\text{A13})$$

The difference in chance of recovering collateral following misreporting and that following truthful reporting is

$$d_i = \mathbb{P}_i(\hat{\omega} = 1 - \omega | r_i = 1 - \omega) - \mathbb{P}_i(\hat{\omega} = \omega | r_i = \omega) = 1 - 2p_i. \quad (\text{A14})$$

Recall from Proposition 2.1 that the utility difference (in the absence of collateral) of misreporting and truthful reporting is  $D_i = (2\tau_i - 1)\lambda_i b_i - h_i$  such that truthful reporting is preferred if and only if  $D_i \leq 0$ . As a result, with the collateral-based incentive, truthful reporting is preferred if and only if  $D_i + d_i \leq 0$ , which establishes Eq. (12).

Now we characterize the equilibrium. An equilibrium is a collection of actions and beliefs  $\{(r_i, p_i)\}_{i=1, \dots, n}$ , where we parameterize the optimal response  $r_i^*$  as a function of  $p_i$ , that is,

$$r_i(p_i) = \begin{cases} \omega, & D_i - (2p_i - 1) \leq 0 \\ 1 - \omega, & D_i - (2p_i - 1) > 0 \end{cases} \quad (\text{A15})$$

such that

$$\begin{aligned} p_i + (\mathbb{I}_{r_i(p_i)=\omega} - \mathbb{I}_{r_i(p_i)=1-\omega}) \lambda_i(\tau_i - 0.5) &= \mathbb{P}(\omega = \hat{\omega}) \\ &= \sum_{i=1}^n \lambda_i (\mathbb{I}_{r_i(p_i)=\omega} \tau_i + \mathbb{I}_{r_i(p_i)=1-\omega} (1 - \tau_i)), \quad i = 1, \dots, n. \end{aligned} \quad (\text{A16})$$

Because of the tie-breaking rule preferring truthful reporting over misreporting in case of identical utility values, no mixed strategy can occur; for the same reason, at equilibrium there must be either  $r_i = \omega, p_i = 1 - \frac{\bar{\tau}-0.5}{n}, i = 1, \dots, n$  (i.e., truthful) or  $r_i = 1 - \omega, p_i = \frac{\bar{\tau}-0.5}{n}, i = 1, \dots, n$  (i.e., untruthful) given the homogeneity of data providers. When  $p_i = 1 - \frac{\bar{\tau}-0.5}{n}$ ,  $r_i(p_i) = \omega$  if

and only if  $\bar{h} \geq \frac{(2\bar{\tau}-1)(\bar{b}-\bar{\eta}(n+1-2\bar{\tau}))}{n}$ ; similarly, when  $p_i = \frac{\bar{\tau}-0.5}{n}$ ,  $r_i(p_i) = 1 - \omega$  if and only if  $\bar{h} < \frac{(2\bar{\tau}-1)(\bar{b}+\bar{\eta}(n+1-2\bar{\tau}))}{n}$ , which establishes the coexisting region  $\mathcal{I}$  as well as the region on which only the truthful (untruthful) equilibrium exists.

At any of the two equilibria, a data provider's collateral is recovered with probability  $\bar{\tau}$ , such that for each data provider the difference of utility at the untruthful equilibrium and utility at the truthful equilibrium simply degenerates to  $D_i$ , which implies that within the coexisting region the Pareto-dominant equilibrium is the one coinciding with the equilibrium in case  $\bar{\eta} = 0$ . ■

**Proof of Proposition 3.1.** We first derive the equilibrium output, which is from solving eight equations for eight unknowns as in Eqs. (17)–(18), which gives,  $\forall i \in \{j, -j\}$ ,

$$Q_i(\bar{\alpha}, \bar{\alpha}) = \frac{\begin{bmatrix} \alpha \left( -4\tau_{-i}^2(-4\tau_i^2 + 4\tau_i + 12\epsilon\phi - 6\epsilon + 3) \right. \\ \left. + 2\tau_{-i}(4\tau_i^2(6\epsilon\phi - 3\epsilon - 2) + \tau_i(-24\epsilon\phi + 12\epsilon + 8) + 6\epsilon\phi - 3\epsilon + 6) \right. \\ \left. - 3(\tau_i^2(8\epsilon\phi - 4\epsilon + 4) + \tau_i(-8\epsilon\phi + 4\epsilon - 4) - 18\epsilon\phi + 9\epsilon - 3) \right) \\ \left. \right]}{3(4\tau_{-i}^2 - 4\tau_{-i} - 3)(4\tau_i^2 - 4\tau_i - 3)}, \quad (\text{A17})$$

$$Q_i(\bar{\alpha}, \underline{\alpha}) = Q_i(\bar{\alpha}, \bar{\alpha}) - \underbrace{\frac{2\alpha\epsilon(2\phi - 1)(2\tau_{-i} - 1)}{4\tau_{-i}^2 - 4\tau_{-i} - 3}}_{\leq 0}, \quad (\text{A18})$$

$$Q_i(\underline{\alpha}, \bar{\alpha}) = Q_i(\bar{\alpha}, \underline{\alpha}) - \underbrace{\frac{4\alpha\epsilon(1 - 2\phi)}{4\tau_i^2 - 4\tau_i - 3}}_{\geq 0}, \quad (\text{A19})$$

$$Q_i(\underline{\alpha}, \underline{\alpha}) = Q_i(\bar{\alpha}, \bar{\alpha}) - \frac{2\alpha\epsilon(2\phi - 1)(2\tau_{-i} - 1)}{4\tau_{-i}^2 - 4\tau_{-i} - 3} - \frac{4\alpha\epsilon(1 - 2\phi)}{4\tau_i^2 - 4\tau_i - 3}. \quad (\text{A20})$$

■

**Proof of Proposition 3.2.** Combining Eq. (17) and Eq. (19), it turns out that  $\Pi_i(\hat{\alpha}_i, \hat{r}_{-i}) = Q_i(\hat{\alpha}_i, \hat{r}_{-i})^2$ . Hence,

$$\mathbb{E}_{\hat{\alpha}_i, \hat{r}_{-i}}[\Pi_i(\hat{\alpha}_i, \hat{r}_{-i})] = \frac{Q_i(\bar{\alpha}, \bar{\alpha})^2 + Q_i(\bar{\alpha}, \underline{\alpha})^2 + Q_i(\underline{\alpha}, \bar{\alpha})^2 + Q_i(\underline{\alpha}, \underline{\alpha})^2}{4}. \quad (\text{A21})$$

The comparative statics are:

$$\frac{\partial \mathbb{E}_{\hat{\alpha}_i, \hat{r}_{-i}}[\Pi_i(\hat{\alpha}_i, \hat{r}_{-i})]}{\partial \tau_i} = \frac{32\alpha^2\epsilon^2(1-2\phi)^2(2\tau_i-1)}{(4\tau_i+3-4\tau_i^2)^3} \geq 0, \quad (\text{A22})$$

$$\frac{\partial \mathbb{E}_{\hat{\alpha}_i, \hat{r}_{-i}}[\Pi_i(\hat{\alpha}_i, \hat{r}_{-i})]}{\partial \tau_{-i}} = -\frac{4\alpha^2\epsilon^2(1-2\phi)^2(8\tau_{-i}^3-12\tau_{-i}^2+14\tau_{-i}-5)}{(4\tau_{-i}^2-4\tau_{-i}-3)^3} \geq 0. \quad (\text{A23})$$

■

**Proof of Proposition 3.3.** As indicated by Eq. (17), firm  $i$ 's optimal output is determined by its expectation about its own demand intercept  $\alpha_i$  and the rival's production  $Q_{-i}(\hat{\alpha}_{-i}, \hat{r}_i)$ . In case firm  $i$  misreports, the distribution of  $Q_{-i}(\hat{\alpha}_{-i}, \hat{r}_i)$  is altered but that of  $\alpha_i$  is not. Hence, in case of misreporting firm  $i$ 's optimal output can be written as  $Q_i(-\hat{\alpha}_i, \hat{r}_{-i})$  plus an adjustment for the expectation of  $\alpha_i$ , as

$$\tilde{Q}_i(\hat{\alpha}_i, \hat{r}_{-i}) = Q_i(-\hat{\alpha}_i, \hat{r}_{-i}) + (2\phi - 1)\alpha\epsilon(\mathbb{I}_{\hat{\alpha}_i=\bar{\alpha}} - \mathbb{I}_{\hat{\alpha}_i=\underline{\alpha}}) \quad (\text{A24})$$

where for a binary-valued variable  $x \in \{x_0, x_1\}$  we define the use of “ $\neg$ ” as  $\neg x_0 = x_1$  and  $\neg x_1 = x_0$ .

The incremental profit from misreporting is therefore

$$\Delta_i(\hat{\alpha}_i, \hat{r}_{-i}; \tau_i, \tau_{-i}) = \tilde{Q}_i(\hat{\alpha}_i, \hat{r}_{-i})^2 - Q_i(\hat{\alpha}_i, \hat{r}_{-i})^2. \quad (\text{A25})$$

As implied by Eqs. (A17)–(A20), we have

$$Q_i(\bar{\alpha}, \hat{r}_{-i}) - Q_i(\underline{\alpha}, \hat{r}_{-i}) = \frac{(2\phi - 1)\alpha\epsilon}{\tau_i + 3/4 - \tau_i^2} \geq (2\phi - 1)\alpha\epsilon \quad (\text{A26})$$

given that  $\tau_i + 3/4 - \tau_i^2 \leq 1$ . Combining Eq. (A24) and Eq. (A26), we have  $\tilde{Q}_i(\bar{\alpha}, \hat{r}_{-i}) \leq Q_i(\bar{\alpha}, \hat{r}_{-i})$ , which implies  $\Delta_i(\bar{\alpha}, \hat{r}_{-i}; \tau_i, \tau_{-i}) \leq 0$ , and  $\tilde{Q}_i(\underline{\alpha}, \hat{r}_{-i}) \geq Q_i(\underline{\alpha}, \hat{r}_{-i})$ , which implies  $\Delta_i(\underline{\alpha}, \hat{r}_{-i}; \tau_i, \tau_{-i}) \geq 0$ . That is, overstating  $\hat{\alpha}_i$  is profitable for firm  $i$  but understating is not. As a result,

$$\begin{aligned} C_i(\tau_i) &= \mathbb{E}_{\hat{r}_{-i}}[\Delta_i(\underline{\alpha}, \hat{r}_{-i}; \tau_i, \tau_{-i})] = \frac{\Delta_i(\underline{\alpha}, \bar{\alpha}; \tau_i, \tau_{-i}) + \Delta_i(\underline{\alpha}, \underline{\alpha}; \tau_i, \tau_{-i})}{2} \\ &= \frac{\alpha^2\epsilon(2\phi - 1)(2\tau_i - 1)^2(2 - 3\epsilon(2\phi - 1))}{3(4\tau_i + 3 - 4\tau_i^2)}. \end{aligned} \quad (\text{A27})$$

It follows from Eq. (A27) that  $C_i(0.5) = 0$ . The comparative statics are:

$$\frac{\partial C_i(\tau_i)}{\partial \tau_i} = \frac{16\alpha^2\epsilon(2\phi - 1)(2\tau_i - 1)(2 - \epsilon(6\phi - 3))}{3(-4\tau_i^2 + 4\tau_i + 3)^2} \geq 0, \quad (\text{A28})$$

$$\frac{\partial C_i(\tau_i)}{\partial \alpha} = \frac{2\alpha\epsilon(2\phi - 1)(2\tau_i - 1)^2(2 - 3\epsilon(2\phi - 1))}{3(4\tau_i + 3 - 4\tau_i^2)} \geq 0, \quad (\text{A29})$$

$$\frac{\partial C_i(\tau_i)}{\partial \phi} = \frac{4\alpha^2\epsilon(1 - 2\tau_i)^2(\epsilon(6\phi - 3) - 1)}{3(4\tau_i^2 - 4\tau_i - 3)} \geq 0, \quad (\text{A30})$$

$$\frac{\partial C_i(\tau_i)}{\partial \epsilon} = \frac{2\alpha^2(2\phi - 1)(1 - 2\tau_i)^2(\epsilon(6\phi - 3) - 1)}{3(4\tau_i^2 - 4\tau_i - 3)} \geq 0. \quad (\text{A31})$$

Since firm  $i$ 's ex ante expected profit  $\mathbb{E}_{\hat{\alpha}_i, \hat{r}_{-i}}[\Pi_i(\hat{\alpha}_i, \hat{r}_{-i})]$  is increasing in  $\tau_i$ , its optimal choice is  $\tau_i^* = \max_{C_i(\tau_i) \leq \eta_i} \tau_i$  regardless of the rival firm's choice. ■

**Proof of Proposition 3.4.** This proof is closely related to the proof of Proposition 3.3 and we follow the notations used therein. If firm  $i$  misreports and disguises, the output is simply given by  $Q_i(-\hat{\alpha}_i, \hat{r}_{-i})$ , while the resultant expected profit can be written as (the trick is to express the expectation of  $\alpha_i - Q_{-i}(\hat{\alpha}_{-i}, \hat{r}_{-i})$  as a suitable member in  $\{Q_i(\hat{\alpha}_i, \hat{r}_{-i}) : (\hat{\alpha}_i, \hat{r}_{-i}) \in \{\underline{\alpha}, \bar{\alpha}\}^2\}$  plus an adjustment)

$$Q_i(-\hat{\alpha}_i, \hat{r}_{-i}) \left( Q_i(-\hat{\alpha}_i, \hat{r}_{-i}) + 2(2\phi - 1)\alpha\epsilon(\mathbb{I}_{\hat{\alpha}_i = \bar{\alpha}} - \mathbb{I}_{\hat{\alpha}_i = \underline{\alpha}}) \right). \quad (\text{A32})$$

Trivially, there must be

$$\mathbb{E}_{\hat{r}_{-i}} \left[ \tilde{\Delta}_i(\bar{\alpha}, \hat{r}_{-i}; \tau_i, \tau_{-i}) \right] \leq \mathbb{E}_{\hat{r}_{-i}} \left[ \Delta_i(\bar{\alpha}, \hat{r}_{-i}; \tau_i, \tau_{-i}) \right] \leq 0 \quad (\text{A33})$$

because  $\mathbb{E}_{\hat{r}_{-i}} [\Delta_i(\bar{\alpha}, \hat{r}_{-i}; \tau_i, \tau_{-i})]$  is maximized but  $\mathbb{E}_{\hat{r}_{-i}} [\tilde{\Delta}_i(\bar{\alpha}, \hat{r}_{-i}; \tau_i, \tau_{-i})]$  is not. Hence, the only possibility of profiting from misreporting and disguising is overstating and disguising, but not understating and disguising, such that

$$\tilde{M}_i(\tau_i) = \max \{0, m_i(\tau_i)\}, \quad (\text{A34})$$

where

$$\begin{aligned}
m_i(\tau_i) &= \mathbb{E}_{\hat{r}_{-i}} \left[ \tilde{\Delta}_i(\underline{\alpha}, \hat{r}_{-i}; \tau_i, \tau_{-i}) \right] \\
&= \mathbb{E}_{\hat{r}_{-i}} \left[ Q_i(\bar{\alpha}, \hat{r}_{-i}) (Q_i(\bar{\alpha}, \hat{r}_{-i}) - 2(2\phi - 1)\alpha\epsilon) - Q_i(\underline{\alpha}, \hat{r}_{-i})^2 \right] \\
&= \frac{2\alpha^2\epsilon(2\phi - 1) (4\tau_i^2 - 4\tau_i - 6\epsilon(2\phi - 1) + 1)}{3 (4\tau_i + 3 - 4\tau_i^2)}. \tag{A35}
\end{aligned}$$

Note that

$$\frac{\partial m_i(\tau_i)/(2\phi - 1)}{\partial \tau_i} = \frac{16\alpha^2\epsilon (2\tau_i - 1) (2 - \epsilon(6\phi - 3))}{3 (-4\tau_i^2 + 4\tau_i + 3)^2} \geq 0 \tag{A36}$$

and hence  $\frac{\partial m_i(\tau_i)}{\partial \tau_i} \geq 0$ , and that

$$\frac{\partial m_i(\tau_i)/(2\phi - 1)}{\partial \phi} = \frac{8\alpha^2\epsilon^2}{4\tau_i^2 - 4\tau_i - 3} \leq 0. \tag{A37}$$

In particular, at  $\phi = 1$ ,

$$m_i(\tau_i)/(2\phi - 1) - C_i(\tau_i) = \alpha^2\epsilon^2 \geq 0, \tag{A38}$$

while

$$\lim_{\phi \downarrow 0.5} (m_i(\tau_i)/(2\phi - 1) - C_i(\tau_i)) = \frac{2\alpha^2\epsilon (2\tau_i - 1)^2}{3 (4\tau_i^2 - 4\tau_i - 3)} \leq 0. \tag{A39}$$

Together with the opposing derivatives of  $m_i(\tau_i)/(2\phi - 1)$  and  $C_i(\tau_i)$  in  $\phi$ , Eqs. (A38)–(A39) imply that  $C_i(\tau_i) \geq \tilde{M}_i(\tau_i)/(2\phi - 1)$  for large  $\phi$  and  $C_i(\tau_i) \leq \tilde{M}_i(\tau_i)/(2\phi - 1)$  for small  $\phi$ . As both  $m_i(\tau_i)/(2\phi - 1)$  and  $C_i(\tau_i)$  are continuous and increasing in  $\tau_i$ ,  $\tilde{C}_i(\tau_i)$  is also continuous and increasing in  $\tau_i$ . Finally, it follows from Eq. (A35) that  $m_i(0.5) \leq 0$ , which implies that  $\tilde{C}_i(\tau_i) = 0$  given that we have shown  $C_i(0.5) = 0$ . ■

## References

- Abadi, J., and M. Brunnermeier. 2018. Blockchain economics. NBER Working Paper No. 25407.
- Amir, R., J. Y. Jin, and M. Troege. 2010. Robust results on the sharing of firm-specific information: Incentives and welfare effects. *Journal of Mathematical Economics* 46:855–66.
- Argenton, C., R. Ivanova-Stenzel, and W. Müller. 2024. Cournot meets Bayes-Nash: A discontinuity in behavior in finitely repeated duopoly games. *Games and Economic Behavior* 144:1–12.
- Arieli, I., Y. Babichenko, and F. Sandomirskiy. 2022. Bayesian persuasion with mediators. Technion Working Paper. Available at: <https://doi.org/10.48550/arXiv.2203.04285>.
- Bao, L., J. Cao, L. Gangadharan, D. Huang, and C. Lin. 2024. Effects of lockdowns in shaping socioeconomic behaviors. *Proceedings of the National Academy of Sciences* 121:e2405934121–.
- Benhaim, A., B. H. Falk, and G. Tsoukalas. 2023. Scaling blockchains: Can committee-based consensus help? *Management Science* 69:6525–39.
- Best, J. W., and D. P. Quigley. 2016. Honestly dishonest: A solution to the commitment problem in bayesian persuasion. University of Oxford Working Paper. Available at: <https://www.nuffield.ox.ac.uk/economics/papers/2016/Repeated%20Persuasion%202016.pdf>.
- Biais, B., C. Bisiere, M. Bouvard, and C. Casamatta. 2019. The blockchain folk theorem. *Review of Financial Studies* 32:1662–715.
- Bimpikis, K., D. Crapis, and A. Tahbaz-Salehi. 2019. Information sale and competition. *Management Science* 65:2646–64.
- Breidenbach, L., C. Cachin, B. Chan, A. Coventry, S. Ellis, A. Juels, F. Koushanfar, A. Miller, B. Magauran, B. Moroz, S. Nazarov, A. Topliceanu, F. Tramer, and F. Zhang. 2021. Chainlink 2.0: Next steps in the evolution of decentralized oracle networks. White Paper. Available at: <https://research.chain.link/whitepaper-v2.pdf>.
- Cao, S. S., L. W. Cong, and B. Yang. 2025. Distributed ledgers and secure multiparty computation for financial reporting and auditing. *Management Science* 71:3852–72.
- Chiu, J., and T. V. Koeppl. 2019. Blockchain-based settlement for asset trading. *Review of Financial Studies* 32:1716–53.
- Cong, L. W., L. Fox, S. Li, and L. Zhou. 2025. A primer on oracle economics. *Journal of Corporate Finance* 94:102800–.
- Cong, L. W., and Z. He. 2019. Blockchain disruption and smart contracts. *Review of Financial Studies* 32:1754–97.

- Cong, L. W., Z. He, and J. Li. 2021. Decentralized mining in centralized pools. *Review of Financial Studies* 34:1191–235.
- Crawford, V. P., and J. Sobel. 1982. Strategic information transmission. *Econometrica* 50:1431–51.
- Drakopoulos, K., I. Lo, and J. Mulvany. 2022. Blockchain mediated persuasion. University of Southern California Working Paper. Available at: <https://ssrn.com/abstract=4300675>.
- Einy, E., D. Moreno, and B. Shitovitz. 2002. Information advantage in cournot oligopoly. *Journal of Economic Theory* 106:151–60.
- Flor, C. R., S. Hirth, E. Lyandres, and A. Schandlbauer. 2025. Information sharing with blockchain. *Research Policy* Forthcoming.
- Gal-Or, E. 1985. Information sharing in oligopoly. *Econometrica* 53:329–43.
- . 1986. Information transmission—Cournot and Bertrand equilibria. *Review of Economic Studies* 53:85–92.
- Gans, J. S., and N. Gandal. 2021. Consensus mechanisms for the blockchain. In R. Rau, R. Wardrop, and L. Zingales, eds., *Palgrave Handbook of Technological Finance*, 269–86. Springer.
- Gans, J. S., and R. T. Holden. 2022. Mechanism design approaches to blockchain consensus. NBER Working Paper No. 30189.
- Garratt, R., and C. Monnet. 2022. An impossibility theorem on truthful reporting in fully decentralized systems. University of California, Santa Barbara Working Paper. Available at: <https://ssrn.com/abstract=4017963>.
- Gneezy, U., A. Kajackaite, and J. Sobel. 2018. Lying aversion and the size of the lie. *American Economic Review* 108:419–53.
- Goldstein, I., W. Jiang, and G. A. Karolyi. 2019. To FinTech and beyond. *Review of Financial Studies* 32:1647–61.
- Goltsman, M., and G. Pavlov. 2014. Communication in Cournot oligopoly. *Journal of Economic Theory* 153:152–76.
- Halaburda, H., Z. He, and J. Li. 2021. An economic model of consensus on distributed ledgers. NBER Working Paper No. 29515.
- Harsanyi, J. C., and R. Selten. 1988. *A general theory of equilibrium selection in games*. MIT Press.
- Hart, O., and J. Moore. 1988. Incomplete contracts and renegotiation. *Econometrica* 56:755–85.

- He, Q. C., Y. J. Chen, and Z. J. Shen. 2018. On the formation of producers' information-sharing coalitions. *Production and Operations Management* 27:917–27.
- Jain, A., S. Seshadri, and M. Sohoni. 2011. Differential pricing for information sharing under competition. *Production and Operations Management* 20:235–52.
- John, K., L. Kogan, and F. Saleh. 2023. Smart contracts and decentralized finance. *Annual Review of Financial Economics* 15:523–42.
- Kamenica, E., and M. Gentzkow. 2011. Bayesian persuasion. *American Economic Review* 101:2590–615.
- Leshno, J. D., and P. Strack. 2020. Bitcoin: An axiomatic approach and an impossibility theorem. *American Economic Review: Insights* 2:269–86.
- Li, L. 1985. Cournot oligopoly with information sharing. *RAND Journal of Economics* 16:521–36.
- Lipnowski, E., D. Ravid, and D. Shishkin. 2022. Persuasion via weak institutions. *Journal of Political Economy* 130:2705–30.
- Lundquist, T., T. Ellingsen, E. Gribbe, and M. Johannesson. 2009. The aversion to lying. *Journal of Economic Behavior & Organization* 70:81–92.
- Novshek, W., and H. Sonnenschein. 1982. Fulfilled expectations cournot duopoly with information acquisition and release. *Bell Journal of Economics* 13:214–8.
- Perez-Richet, E. 2014. Interim bayesian persuasion: First steps. *American Economic Review* 104:469–74.
- Raith, M. 1996. A general model of information sharing in oligopoly. *Journal of Economic Theory* 71:260–88.
- Randao. 2017. Randao: Verifiable random number generation. White Paper. Available at: [https://www.randao.org/whitepaper/Randao\\_v0.85\\_en.pdf](https://www.randao.org/whitepaper/Randao_v0.85_en.pdf).
- Salamanca, A. 2021. The value of mediated communication. *Journal of Economic Theory* 192:105191–.
- Saleh, F. 2021. Blockchain without waste: Proof-of-stake. *Review of Financial Studies* 34:1156–90.
- Schelling, T. C. 1960. *The strategy of conflict*. Harvard University Press.
- Tirole, J. 1999. Incomplete contracts: Where do we stand? *Econometrica* 67:741–81.
- Vives, X. 1999. *Oligopoly pricing: Old ideas and new tools*. MIT Press.
- Ziv, A. 1993. Information sharing in oligopoly: The truth-telling problem. *RAND Journal of Economics* 24:455–65.