Quality Certification and Market Transparency with Decentralized Information Management*

Jun Aoyagi†

Department of Economics, University of California at Berkeley

610 Evans Hall, Berkeley, CA 94720.

Daisuke Adachi

Department of Economics, Yale University

28 Hillhouse Avenue, New Haven, CT 06511

First Draft: February 2018   This Version: March 2020

Abstract

This paper studies how decentralized information management affects asset quality uncertainty and consumer welfare. We show that quality certification improves transparency but has a non-monotonic impact on trading activity and the fee for certification. Thus, if a single agent serves as a centralized quality certifier, she has an incentive to leave the market opaque even if resolution of uncertainty increases consumer welfare. By contrast, if a decentralized system (e.g., blockchain) is adopted, multiple record keepers competitively determine the reliability of quality certification. Each record keeper in the decentralized system does not incorporate the impact of her monitoring on the general equilibrium transparency, as well as the non-monotonic reaction of the fee revenue. Thus, it may outperform the centralized counterpart in terms of consumer welfare. As a leading example, the blockchain economy is analyzed to derive its implications for the cryptocurrency price and the total hash rate.

JEL codes: D47, D51, D53, G10, G20, L10.

Keywords: asymmetric information, quality certification, market transparency, decentralized monitoring, blockchain technology, cryptocurrency.

*This paper was initially circulated under the title "Economic Implications of Blockchain Platforms." Declarations of interest: none.

†Corresponding author. E-mail: jun.aoyagi@berkeley.edu

1 Introduction

Decentralized information management has been popular due to the recent hype about the blockchain technology. Its distributed ledger system (DLS) deals with information asymmetry by exploiting a new type of record-keeping mechanism that potentially involves an infinite number of record keepers. With the increasing consumers' demand to know more about what they are purchasing, the DLS has been widely adopted in supply-chain management and financial transactions in the expectation that it works as a new quality certification and improves transparency.[1]

The existing literature on certification and market transparency has analyzed the information revelation as a strategic decision of a *centralized* certifier (e.g., Stahl and Strausz, 2017). However, the advent of the decentralized information system has changed the landscape. For example, each record keeper in the blockchain network may engage in "mining" to obtain a reward without incorporating the impact of her behavior on the nature of each transaction or traded asset.[2]

In light of this, we propose a stylized model of an exchange economy with asset quality uncertainty where traders have access to quality certification provided by *decentralized* record keepers. We then compare the equilibrium with decentralized information management to that with centralized management. Although the blockchain is a good representation of our model, we keep our discussions as general as possible so that the model's insights have much broader generality.

We show that the reliability of certification and market transparency have a non-monotonic impact on the dollar value of trade and the equilibrium fee for certification. By the definition of decentralized management, no single record keeper exerts monopolistic power to generate certification. Instead, a set of record keepers *competitively* determine it without incorporating the non-monotonic reaction of the economy. In terms of consumer welfare, decentralized information management can outperform the traditional centralized system that involves a single certifier. This is because the centralized certifier intentionally keeps the market opaque knowing about the non-monotonic reaction of the fee revenue, whereas the decentralized record keepers may improve transparency since they do not internalize its non-monotonic impact.

In an exchange economy, price-taking buyers (consumers) and sellers (producers) trade assets,

[1] See Appendix A for examples of blockchain adoption in the real world.

[2] All the record keepers in the blockchain network try to solve a costly cryptographic problem. If, and only if, a record keeper becomes the first agent who finds the solution, she is entitled to record information about a transaction and obtain a reward. This process is called "mining," as they mine new cryptocurrency (e.g., Bitcoin). See Appendix A for more details.

while only the sellers know asset quality (Akerlof, 1970). Assets can be traded with quality certification, but it may falsely declare that a low-quality asset has high quality. We define the likelihood of avoiding this error as the *reliability* of certification, and it works as a proxy for market transparency. The coexistence of certified and uncertified assets triggers trader differentiation between them (Tirole, 1988), leading to endogenous spreads in average asset quality and the asset price (Kurlat, 2013).

A more reliable certification and higher transparency have two competing effects on the dollar value of certified transactions (CTs) and the welfare of consumers who purchase certified assets. On the one hand, a certification mitigates asymmetric information by improving expected quality of certified assets. The consumers face higher *ex-ante* expected quality, which ameliorates their utility. On the other hand, due to a higher expected return, consumers' demand for certified assets rises, thereby increasing their equilibrium price. A higher price for certified assets reduces consumers' trading profit and harms trading volume.

These two competing effects generate a non-monotonic reaction of equilibrium variables in the exchange economy. When certification is not reliable or underlying quality uncertainty is high, the positive effect of higher transparency dominates its negative effect. This is because the consumers facing high uncertainty are eager to resolve it, and the benefit from a decline in uncertainty becomes salient. The opposite holds when certification is reliable, making the impact of higher transparency non-monotonic.

The *decentralized* record keepers determine the reliability of quality certification and transparency. They leverage costly monitoring power and compete against each other to record information about asset quality and obtain a reward. A specific algorithm (e.g., Proof-of-Work; PoW) derives a consensus on asset quality from recorded information, provides it to traders as quality certification, and yields a monetary reward to one of the record keepers who made the largest contribution to the consensus. Since the monetary reword is the certification fee paid by consumers, the more active the CTs become, the higher the reward the record keepers (as a whole) obtain. Due to the non-monotonic reaction of the value of CTs, the fee-maximizing transparency can be *below* the perfect transparency.

In such a situation, if a centralized record keeper is in charge of generating certification, she keeps the market untransparent. The single certifier can exert her monopolistic control of the reliability and intentionally keeps it low to achieve the maximum fee. However, the certification fee only reflects the value of CTs and does not impound consumer welfare associated with *un*certified assets. We show that welfare associated with *un*certified assets is increasing in transparency. Thus, the fee-maximizing reliability set by the centralized certifier tends to be lower than the welfare-maximizing level.

In contrast, each agent in the decentralized record-keeping system behaves competitively. She does not internalize the impact of her monitoring on the equilibrium reliability and transparency, leading to overinvestment in aggregate monitoring compared to the fee-maximizing level. This deviation, however, improves the aggregate consumer welfare by solving the underinvestment problem that the centralized system may suffer.

As one of the most conspicuous examples of our model, we also discuss the blockchain technology in supply-chain management. The non-monotonic behavior of our exchange economy suggests that the cryptocurrency price also exhibits a non-monotonic reaction to the blockchain miners' behavior. Our model also implies that the correlation between the cryptocurrency price and the total hash rate can be both positive and negative, depending on the asymmetric information between traders who use the blockchain as quality certification.

1.1 Literature Review

Quality uncertainty, certification, and transparency A large body of literature has emerged from Akerlof (1970) and examined the adverse selection problem when traders face asymmetric information. Regarding the impact of quality certification and market transparency, Lizzeri (1999), Strausz (2005), Mathis et al. (2009), and Stahl and Strausz (2017) investigate the possibility that a quality certifier does not fully resolve uncertainty to keep a market untransparent. We complement the above literature by showing that opacity arises even in our parsimonious environment with competitive traders and in the absence of their strategic motive (i.e., signaling and inspection motives).

Moreover, the existing models assert that the "information revelation must be treated as a strategic decision" (Lizzeri, 1999; Albano and Lizzeri, 2001) of a quality certifier. Even if there exit multiple certifiers (or middlemen), each of them affects traders' behavior and is aware of it (Biglaiser and Friedman, 1994). However, this statement is not always true in the new markets with the distributed ledger system (e.g., the blockchain), as it involves many agents who behave competitively in determining a single certification that affects market transparency. Our model analyzes such an environment and compares the welfare implications of the decentralized certification to those of the centralized one.[3]

[3]In my companion paper (Aoyagi, 2019), I analyze the general equilibrium model in which a centralized record keeper and decentralized record keepers compete against each other to provide quality certification.

Two-sided markets Also, our model features two-sided markets (Rochet and Tirole, 2003) and trader differentiation (Tirole, 1988), as buyers and sellers decide whether to trade certified or uncertified assets. Hendel and Lizzeri (1999) and Kurlat (2013) consider endogenous asset quality due to the differentiation of competitive agents, and our model generalizes their studies to accommodate quality certification by the decentralized record keepers.[4]

The literature in industrial organization and finance that explores market structures and platform competition includes the studies by Foucault and Parlour (2004), Armstrong (2006), Damiano and Hao (2008), Foucault and Menkveld (2008), Ambrus and Argenziano (2009), Gabszewicz and Wauthy (2014), and Cespa and Vives (2019). However, they do not deal with asymmetric information with asset quality uncertainty, although it is one of the key frictions that the blockchain aims to solve. Yanelle (1997) and Halaburda and Yehezkel (2013) consider competing platforms with asymmetric information between a platform and users (traders), whereas our model analyzes asymmetric information *between traders* to investigate the impacts of the new type of certification.

Blockchain and cryptocurrency The blockchain exemplifies the decentralized information management system, and the research on it (or FinTech, in general) is expanding (see Harvey, 2016, Chen et al., 2019, and Vives, 2019 for comprehensive reviews). Chiu and Koeppl (2017, 2019) analyze the optimal design of the blockchain to guarantee "Delivery vs. Payment." Cong, Li and Wang (2019) consider the demand and price dynamics of tokens (cryptocurrency). Abadi and Brunnermeier (2018) and Pagnotta and Buraschi (2018) consider the network externality in the general equilibrium blockchain economy. Cong and He (2019) argue that the blockchain promotes firms' entrance and improves consumer welfare. Malinova and Park (2017) consider the degree of transparency of the private blockchain with front-running risk. Khapko and Zoican (2017) focus on the optimal duration of the transactions with counterparty risk and search frictions. Tinn (2018) specifies the optimal contract contingent on time-stamped cash flow managed by the blockchain system.[5] We analyze the adoption of the DLS when buyers face *ex-ante* quality uncertainty and show that traders' non-monotonic reaction differentiates the welfare implications of the decentralized system from those of the centralized system.

[4]Authors such as Kim (2012), Guerrieri and Shimer (2014), and Chang (2017) also show that market segmentation leads to quality differences across markets when agents strategically behave.

[5]For the feasibility of the blockchain implementation, seeAune, Krellenstein, O'Hara and Slama (2017) and Biais et al. (2019).

2 Model

Consider a single-period exchange economy inhabited by traders and record keepers. The traders consist of buyers (consumers) and sellers (producers), and they engage in asset trading. At the beginning of the game, each seller is endowed with a single unit of asset. Its quality is either $s = 1$ (high) or $s = 0$ (low) with $\pi \equiv \Pr(s = 1)$ denoting the fraction of high-quality assets. Each seller privately observes the quality of her endowment, whereas buyers cannot observe it (Akerlof, 1970).

Quality certification There exist an endogenous set of *certified assets*. Before the trading game starts, each seller decides whether to send her asset to record keepers to obtain quality certification. If it is certified as a high-quality asset, it obtains a label $q = 1$ and is sold to buyers. If an asset is certified as low-quality $q = 0$, on the other hand, it is sent back to the original seller, and she consumes it by herself.[6] If a seller does not send her asset to the record keepers, it is classified as an *uncertified asset* with no labels ($q = \Phi$).

Regarding quality certification, we define

$$\theta \equiv 1 - \Pr(q = 1|s = 0). \tag{1}$$

Note that $1 - \theta$ represents the probability that a low-quality asset obtains a "high" certification. Thus, the higher the value of θ, the more likely the "high" certification is correct. We call θ the "reliability" of quality certification or "transparency" of the market, as θ measures (inverse) quality uncertainty in our model. Also, assets with a high certification ($q = 1$) are referred to as the "certified assets."[7] In what follows, we analyze the behavior of traders by taking θ as given, while Subsection 2.4 endogenizes θ.

2.1 Traders

There exist a continuum of risk-neutral buyers and sellers, each with a unit mass, and they are characterized by the private value of asset $\alpha \in [0, 1]$ and $\beta \in [0, 1]$, respectively. For simplicity, we

[6] The assumption that assets with low labels $q = 0$ are not sold and must be consumed by the original sellers is for tractability. Instead, we can allow sellers with $q = 0$ to sell their assets as "uncertified" assets by removing the label. This alternative assumption does not change our main results, although the equilibrium conditions are slightly modified. The results are available on request.

[7] For simplicity, we assume that there are no type-I errors, i.e., $\Pr(q = 1|s = 1) = 1$. Subsection 2.4 provides motivations for this setting.

assume $\alpha, \beta \overset{\text{iid}}{\sim} U[0,1]$. The heterogeneous private value motivates asset trading.

For an agent with a private value $x = \alpha, \beta$, the asset yields the following (per capita) utility at the end of the game

$$y(x) = \begin{cases} x & \text{if } s = 1, \\ \phi x & \text{if } s = 0, \end{cases}$$

where $\phi \in (0,1)$ represents the primitive quality difference. If the asset is low-quality, agents obtain only ϕ fraction of the full utility.[8] Following the literature on market microstructure (e.g., Glosten and Milgrom, 1985), agents can trade and hold, at most, one unit of asset and cannot short-sale.

Buyers A buyer is endowed with a certain amount of cash w and uses it to purchase certified assets ($j = c$), uncertified assets ($j = nc$), and to make risk-free savings with a zero interest rate. Specifically, a buyer with type α solves the following problem:

$$\begin{aligned} W(\alpha) = & \max_{k_c, k_{nc} \in [0,1]} \mathbb{E}\left[\sum_{j=c,nc} y_j(\alpha) k_j\right] + a \\ & \text{s.t., } w \geq \sum_{j=c,nc} P_j k_j + a. \end{aligned} \tag{2}$$

k_j and P_j represent the demand and dollar price of asset $j = c$ (certified) and $j = nc$ (uncertified). A risk-free saving is denoted by $a \geq 0$.

We denote the *endogenous* probability of high-quality certified assets as $\pi_c \equiv \Pr(s = 1 | q = 1)$. Similarly, π_{nc} denotes the probability that an uncertified asset is of high quality. Then, for $j \in \{c, nc\}$,

$$\mathbb{E}[y_j(\alpha)] = \underbrace{[\pi_j + (1 - \pi_j)\phi]}_{\equiv \tilde{\pi}_j} \alpha, \tag{3}$$

where $\tilde{\pi}_j$ represents the average quality of assets j.

Because of the risk neutrality, asset demand always hits its upper or lower limit ($k_j = 0, 1$).[9] Therefore, the expected return from purchasing an asset with and without certification (W_c, W_{nc})

[8] As in Rubinstein and Wolinsky (1987), ϕ can be seen as a delay cost, where a low-quality asset suffers from a delay in delivery.

[9] We simplify our discussion by assuming a tie-breaking rule that the indifferent agents use quality certification.

and that from saving all the endowment (W_0) are given by[10]

$$W_j(\alpha) = \begin{cases} \tilde{\pi}_j \alpha - P_j & \text{for } j \in \{c, nc\} \\ 0 & \text{for } j = 0. \end{cases} \tag{4}$$

To solve the problem, we guess the following:[11]

$$\frac{P_c}{\tilde{\pi}_c} > \frac{P_{nc}}{\tilde{\pi}_{nc}}, \pi_c > \pi_{nc}. \tag{5}$$

These conditions guarantee that both types of assets have positive demand. The following sections show that they hold in the equilibrium.

Lemma 1. *The optimal behavior of type α buyers is (i) buying one unit of certified asset if $\alpha \geq \alpha^*$, (ii) buying one unit of uncertified assets if $\alpha \in [\frac{P_{nc}}{\tilde{\pi}_{nc}}, \alpha^*)$, and (iii) saving all the endowment otherwise, where the cutoff is $\alpha^* \equiv \frac{P_c - P_{nc}}{\tilde{\pi}_c - \tilde{\pi}_{nc}}$.*

Proof. Comparing $\{W_j\}_{j=c,nc,0}$ in (4) yields the result. □

A buyer faces a price-quality tradeoff. On the one hand, the certified assets provide higher quality and expected returns. One the other hand, they charge a higher price. The gain from consuming high-quality assets is multiplied by the private value α, while the cost is constant at P_j. Hence, the certified assets are more attractive for high-α buyers, leading to the differentiation in Lemma 1.

By aggregating along α, the total demand for assets j is

$$D_j = \begin{cases} 1 - \alpha^* & \text{for } j = c, \\ \alpha^* - \frac{P_{nc}}{\tilde{\pi}_{nc}} & \text{for } j = nc. \end{cases} \tag{6}$$

Due to the unit demand assumption, D_j also represents the aggregate measure of buyers who demand assets j.

Low-quality sellers A seller with a low-quality asset may try to obtain quality certification, in which case her asset is monitored and labeled by q. In this case, she obtains the following

[10] We subtract the cash endowment w from W_j, as it does not affect the equilibrium behavior.

[11] See Gabszewicz and Wauthy (2014) for a similar structure, in which they state (5) as assumptions, while we derive them endogenously.

expected return:

$$W_c^L(\beta) = (1-\theta)P_c + \theta\phi\beta. \tag{7}$$

With probability $1-\theta$, her low-quality asset obtains a certification $q = 1$ and is sold at price P_c while, with probability θ, the asset obtains a low certification $q = 0$, and she consumes her own asset to get $\phi\beta$. Moreover, she can sell her asset as an uncertified asset ($j = nc$), i.e., without obtaining certification. In this case, the return is $W_{nc}^L(\beta) = P_{nc}$. The last option is not selling her asset, which gives $W_0^L(\beta) = \phi\beta$.

By comparing $\{W_j^L(\beta)\}_{j=c,nc,0}$, we obtain the following:

Lemma 2. *The optimal behavior of a low-type seller is (i) not selling her asset if $\beta > \frac{P_c}{\phi}$, (ii) selling it with a certification if $\beta \in (\beta_L, \frac{P_c}{\phi}]$, and (iii) selling it without certifications if $\beta \leq \beta_L$, where the second cutoff is given by*

$$\beta_L = \max\left\{\frac{P_{nc} - (1-\theta)P_c}{\phi\theta}, 0\right\}. \tag{8}$$

A seller with a high private value β is willing to consume her asset by herself. A seller with an intermediate β still derives relatively high utility from her asset, leading her to "gamble" to get the higher price P_c with certification $q = 1$. However, a low-β seller wants to avoid consuming her asset and tries to sell it as uncertified.

High-quality sellers For a seller with a high-quality asset, the returns from selling her asset as $j = c$, $j = nc$, and not selling it are given by

$$W_j^H(\beta) = \begin{cases} P_j & \text{for } j = c, nc, \\ \beta & \text{if } j = 0. \end{cases}$$

This is because certification does not fail to detect high-quality assets.

Lemma 3. *The optimal behavior of a high-quality seller is (i) not selling her asset if $\beta > P_c$ and (ii) selling it by obtaining $q = 1$ if $\beta \leq P_c$.*

2.1.1 Aggregate supply and endogenous quality

By aggregating sellers' optimal behavior, the supply functions of certified and uncertified assets (S_c, S_{nc}) are given by

$$S_j = \begin{cases} \pi P_c + (1-\pi)(1-\theta)\left(\frac{P_c}{\phi} - \beta_L\right) & \text{for } j = c \\ (1-\pi)\beta_L & \text{for } j = nc. \end{cases} \tag{9}$$

The first term in S_c implies that all of the active high-quality sellers attempt to obtain the certification. On the other hand, low-quality sellers are differentiated between certified transactions (the second term in S_c) and uncertified transactions (the first term in S_{nc}). The second term of S_c is discounted by θ because only $1-\theta$ fraction of low-quality assets are certified with $q = 1$.

The above arguments provide the updated average quality of assets $j \in \{c, nc\}$.

Lemma 4. *The average quality measures of uncertified ($j = nc$) and certified ($j = c$) assets are given by $\pi_{nc} = 0$ and*

$$\pi_c = \frac{\pi P_c}{\pi P_c + (1-\pi)(1-\theta)\left(\frac{P_c}{\phi} - \beta_L\right)}. \tag{10}$$

The endogenous quality is reminiscent of Kurlat (2013). The reliability of certification θ affects the quality of (un)certified assets π_j via its direct effect (i.e., $\frac{\partial \pi_c}{\partial \theta} > 0$) and its indirect effect (via P_c and β_L) caused by the differentiation of asset sellers.[12]

2.2 Traders' partial equilibrium

We define the trader-side partial equilibrium as follows:

Definition 1. *Given θ, the traders' partial equilibrium is defined by the price, quality, and quantity $\{P_j, \pi_j, D_j, S_j\}_{j\in\{c,nc\}}$, such that, (i) S_j and D_j for $j \in \{c, nc\}$ are given by (6) and (9), and (ii) asset prices P_j clear the markets for certified and uncertified assets ($S_j = D_j$).*

Note that this is not the general equilibrium, as it does not capture the record keepers' behavior. Hereafter, let $Vol_j \equiv D_j = S_j$ denote the trading volume of asset $j \in \{c, cn\}$.

2.2.1 Price, quality, and trading volume

The equilibrium price, quality, and trading volume behave as follows.

[12] See the previous version of our paper (Aoyagi and Adachi, 2018) for more general settings that yield $\pi_{nc} > 0$ in the equilibrium.

Lemma 5. *(i) The certified assets obtain higher quality and a higher price than the uncertified assets, i.e., $\pi_c > \pi_{nc}$ and $P_c > P_{nc}$.*
(ii) The price and quality of certified assets are increasing in the reliability, i.e., $\frac{dP_c}{d\theta} > 0$, $\frac{d\pi_c}{d\theta} > 0$.
(iii) The price spread is more responsive than the quality spread, i.e., $\frac{d\log(P_c - P_{nc})}{d\theta} > \frac{d\log(\pi_c - \pi_{nc})}{d\theta} > 0$.
(iv) The trading volume of certified assets is decreasing in θ, i.e., $\frac{dVol_c}{d\theta} < 0$.

Proof. See Appendix B.2. □

Consider an increase in the reliability θ. With the price P_c fixed, it reduces the supply of certified assets S_c by detecting and sweeping out low-quality assets. The average quality of certified assets π_c increases, and consumers are more willing to buy them. Thus, regarding certified assets, supply declines and demand increases, leading to a higher price P_c.

Point (iii) suggests that the asset price reacts to θ more strongly than asset quality. A change in quality π_j is associated with supply-side behavior, which is one of the channels through which θ moves the price P_j. However, π_j not only changes the supply but also affects the demand for assets, thus amplifying the change in the price.

Since the buyers face price-quality tradeoff, and the price increases more than quality does, a part of consumers stop buying the certified assets and switch to the uncertified assets, as point (iv) attests.

No trading of uncertified assets The opposite argument applies to the reaction of the uncertified assets: the price P_{nc} declines more than the quality π_{nc} does. In other words, higher reliability θ not only makes the certified assets less attractive, but it also makes the uncertified ones more attractive. It strengthens consumers' incentive to switch from certified to uncertified assets.

However, the coexistence of two assets ($j = c$ and nc) can collapse endogenously due to the sellers' behavior.[13] To see this, define the following cutoff:

$$\theta_0 = \frac{1}{1-\pi}\left(\frac{1}{2} - \sqrt{\frac{1}{4} - (1-\pi)\pi(1-\phi)}\right).$$

[13]The complete shutdown stems from two simplifying assumptions of our model. Firstly, all the sellers know about the quality of their endowment. This assumption is relaxed by allowing $\omega \in (0,1)$ fraction of sellers to know about asset quality, while leaving $1-\omega$ of them uninformed. Secondly, traders' are not restricted in choosing $j \in \{c, nc\}$. Alternatively, we can assume only γ fraction of traders have access to the certified assets. These generalizations provide richer results, but the model's implications stay the same. The previous version of our model (Aoyagi and Adachi, 2018) analyses these general structures in its appendix.

Lemma 6. *(i) If $\theta > \theta_0$, the trading volume of uncertified assets Vol_{nc} is positive. Otherwise, $Vol_{nc} = 0$.*
(ii) θ_0 is decreasing in ϕ and π.
(iii) The price of uncertified assets is decreasing in the reliability, i.e., $\frac{dP_{nc}}{d\theta} < 0$, when $\theta \geq \theta_0$, while it is increasing in θ when $\theta < \theta_0$.

Proof. See Appendix B.3 for the statements (i) and (iii). Point (ii) comes from the definition of θ_0. □

Lemma 6 implies that the market for uncertified assets can endogenously shut down. Intuitively, a small θ makes it easier for L-type sellers to "gamble," as quality certification tends to commit an error, and L-type sellers can sell her asset at the higher price P_c.[14] As $Vol_{nc} = 0$ is a corner solution, the structural change at $\theta = \theta_0$ contributes to the non-monotonic behavior of the traders' partial equilibrium.

With Lemma 6, the trader-side partial equilibrium is explicitly solved:

Proposition 1. *Given θ, let $u \equiv \frac{P_c - P_{nc}}{P_c}$ be the normalized price spread. Then, the traders' partial equilibrium is characterized by the following:*

$$P_c = \begin{cases} \frac{\pi(1-\phi)\theta\phi}{[\pi\phi\theta+(1-\pi)(1-\theta)u][\pi(1-\phi)+u]} & \text{if } \theta \geq \theta_0 \\ \frac{\phi[\pi+(1-\pi)(1-\theta)]}{[2-\theta(1-\pi)][\phi\pi+(1-\pi)(1-\theta)]} & \text{if } \theta < \theta_0, \end{cases}$$

$$Vol_c = \begin{cases} \frac{\pi(1-\phi)}{\pi(1-\phi)+u} & \text{if } \theta \geq \theta_0 \\ \frac{\pi+(1-\pi)(1-\theta)}{2-\theta(1-\pi)} & \text{if } \theta < \theta_0, \end{cases}$$

$$P_{nc} = \begin{cases} \frac{1-\pi P_c}{2-\pi}\phi & \text{if } \theta \geq \theta_0 \\ \frac{\phi}{2-\theta(1-\pi)} & \text{if } \theta < \theta_0, \end{cases} \tag{11}$$

$$Vol_{nc} = \begin{cases} \frac{\phi-[\phi\pi+(1-\theta)(2-\pi)]P_c}{\phi\theta(2-\pi)} & \text{if } \theta \geq \theta_0 \\ 0 & \text{if } \theta < \theta_0, \end{cases} \tag{12}$$

$$u = \begin{cases} u^* & \text{if } \theta \geq \theta_0 \\ \frac{\pi(1-\phi)}{\pi+(1-\pi)(1-\theta)} & \text{if } \theta < \theta_0, \end{cases} \tag{13}$$

[14] We can reconcile the no-trading result to the study by Hendel and Lizzeri (1999), where they show that the market for lemons (e.g., used cars) never shuts down due to the existence of the market for peaches (e.g., new cars), because the market for new cars is transparent and corresponds to the case with $\theta = 1$ in our model.

where u^* is a unique positive solution of $\Psi(u) = 0$ with

$$\Psi(u) = (1-\pi)(1-\theta)u^2 + \pi[\theta + (1-\pi)(1-\phi)]u - \theta\pi(1-\phi)(2-\pi).$$

Proof. See Appendix B.1. □

2.2.2 Non-monotonic effect of quality certification

In a transparent market First, we analyze the case with relatively high reliability and transparency $\theta \geq \theta_0$. Let

$$V_j \equiv P_j \times Vol_j$$

represent the trading value of assets j. With two thresholds regarding the measure of asset quality, $\phi_1 = \frac{2-\pi}{3-\pi}$ and ϕ_0 given by Appendix B.4, we obtain the following.

Proposition 2. *(i) If $\phi < \phi_0$, the trading value of certified assets V_c is monotonically increasing in the reliability θ.*
(ii) If $\phi_0 \leq \phi < \phi_1$, V_c is U-shaped. There exists a tipping point θ^* s.t. $\frac{dV_c}{d\theta} \lesseqgtr 0 \Leftrightarrow \theta \lesseqgtr \theta^*$.
(iii) If $\phi_1 \leq \phi \leq 1$, V_c is monotonically decreasing in θ.
(iv) θ^* is increasing in ϕ and π.

Proof. See Appendix B.4. □

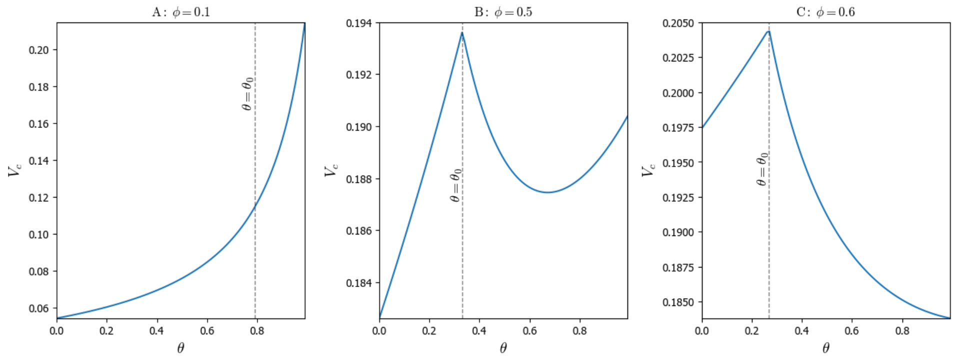
The proposition indicates that the trading value of certified assets exhibits a non-monotonic reaction to the reliability θ. A higher θ increases the price of certified assets P_c but reduces trading volume Vol_c (Lemma 5). Whether a decline in Vol_c outweighs an increase in P_c depends on ϕ and θ.

Rewriting the derivative of the trading value V_c by using elasticity makes intuition clearer:

$$\frac{dV_c}{d\theta} = (1-\varepsilon_{PV})Vol_c\frac{dP_c}{d\theta} \text{ with } \varepsilon_{PV} \equiv -\left(\frac{d\log Vol_c}{d\log P_c}\right).$$

ε_{PV} is the price elasticity of the certified transaction volume. It measures how easily buyers can switch from certified assets to uncertified assets to save the price difference $P_c - P_{nc} > 0$. When the utility from consuming low-quality assets ($\phi\alpha$) is sufficiently large, the buyers are not eager to have certified assets. Thus, a marginal increase in the price of certified assets P_c leads to a large decline in the trading volume V_c, which reduces the transaction value V_c. A small-ϕ region gives the opposite result.

Figure I: Market transparency and trading value of certified assets



If ϕ is intermediate, the reliability and transparency θ matter because they determine the quality difference between two assets, $\Delta\pi \equiv \pi_c - \pi_{nc}$. When θ is small, so is $\Delta\pi$. Then, buying a certified asset is slightly different from buying an uncertified asset in terms of the probability of purchasing low-quality assets. This facilitates the outflow of certified consumers, Vol_c declines more than P_c rises, and the transaction value V_c shrinks. The opposite argument holds for a high-reliability case, generating the non-monotonic behavior of V_c.

In an opaque market Now, we focus on relatively unreliable certifications, $\theta < \theta_0$.

Corollary 1. *If $\theta < \theta_0$, then the trading value of certified assets V_c is monotonically increasing in the reliability of certifications θ.*

Proof. See Appendix B.3 □

This result highlights the importance of the market for uncertified assets because, if there is no trade of uncertified assets, the reaction of trading value V_c to θ is always positive. When $\theta < \theta_0$, if a consumer decides not to buy certified assets, she does not have uncertified assets as her alternative option and must put all of her money into zero-return savings. This weakens her switching incentive, and she tends to stick to the certified assets. Thus, even if the asset price P_c increases, the trading volume Vol_c declines slightly, leading to a higher V_c.

Figure I illustrates the reaction of the transaction value of certified assets V_c to the reliability θ with different values of ϕ. It can be non-monotonic due to its ambiguous reaction in $\theta \geq \theta_0$ (Proposition 2), as well as due to the switch of the structure at $\theta = \theta_0$.

2.3 Consumer welfare

We define consumer welfare W as the buyers' trading surplus (see Appendix C.2 for sellers' trading surplus):

$$W = \int_{\frac{p_{nc}}{\bar{\pi}_{nc}}}^{\alpha^*} W_{nc}(\alpha) d\alpha + \int_{\alpha^*}^{1} W_c(\alpha) d\alpha \tag{14}$$

where $W_j(\alpha)$ is given by (4) and represents a trading surplus for a buyer with private value α consuming asset j. W is rewritten by using *reservation welfare* W_{res} and *welfare gain* ΔW:

$$W = \underbrace{\int_{\frac{p_{nc}}{\bar{\pi}_{nc}}}^{1} W_{nc}(\alpha) d\alpha}_{\equiv W_{res}} + \underbrace{\int_{\alpha^*}^{1} \left(W_c(\alpha) - W_{nc}(\alpha)\right) d\alpha.}_{\equiv \Delta W} \tag{15}$$

W_{res} in (15) represents the welfare of active buyers when they can trade only uncertified assets. ΔW is the extra value in welfare that stems from the introduction of quality certification, which only buyers with $\alpha \geq \alpha^*$ attempt to exploit.

Lemma 7. *The welfare gain is proportional to the dollar value of certified transactions, i.e.,*

$$\Delta W = \frac{\phi(1-\pi)}{2} V_c.$$

Proof. See Appendix C.1. □

Intuitively, V_c is the extra trading *value* stemming from the intermediation by quality certification, and it corresponds to the extra trading surplus created by switching from the world with no certification to the one with quality certification.

As $W = W_{res} + \Delta W$, Lemma 7 suggests that W can be non-monotonic. With ϕ_2 defined in Appendix C.1, we obtain the following results:

Proposition 3. *The reliability of certifications has the following impact on welfare:*
(i) The behavior of welfare gain ΔW is the same as that of V_c in Proposition 2.
(ii) The reservation welfare W_{res} is monotonically increasing in θ, i.e., $\frac{dW_{res}}{d\theta} > 0$.
(iii) The aggregate consumer welfare W is
—(a) monotonically increasing in θ if $\pi > 1/2$ or $\pi \leq 1/2$ and $\phi < \phi_2$.
—(b) Otherwise, it takes a U-shaped curve. A unique $\theta^{**} \in (\theta_0, 1]$ characterizes a tipping point, i.e., $\frac{dW}{d\theta} \gtrless 0 \Leftrightarrow \theta \gtrless \theta^{**}$.

Proof. See Appendix C.1. □

Firstly, the non-monotonicity of ΔW has the same intuition as the behavior of V_c. Secondly, the reservation welfare W_{res} is monotonically increasing in transparency θ. Higher reliability and transparency reduce the price of uncertified assets P_{nc} more than the decline in their quality $\pi_{nc}(= 0)$. Thus, it makes uncertified assets more profitable for consumers, and their welfare in the absence of certification increases.

Moreover, the total consumer welfare can *decrease* with θ due to the decreasing welfare gain ΔW. If the initial fraction of high-quality assets π is small, a marginal increase in θ rejects a large number of lemons, magnifying its impact. Also, if low-quality assets are not bad (ϕ is high), consumers can easily switch from certified to uncertified assets, leading to a decline in the value of certified transactions V_c and consumer welfare W.

2.4 Quality certification

In this subsection, we analyze how the *decentralized* record keepers determine the reliability of quality certification. In line with the blockchain technology, we suppose that the record keepers do not generate new information. Rather, they keep track of recorded information to avoid manipulations by some malicious agents, e.g., cyber-attacks.

The original information about assets is generated by some devices, such as Internet-of-Things (IoT), that acquire information about assets' condition.[15] We abstract away from noise stemming from these devices by assuming that they work perfectly and detect true conditions s, whereas the recorded data is exposed to the risk of manipulation. The original information about s is stored in the record keepers' computer, and they monitor it to avoid manipulation and to generate a quality certification.

Consider an infinite number of risk-neutral potential record keepers. Their decision involves the following steps.

Participation decision A potential record keeper pays a fixed cost z to participate in the record-keeping task. By paying it, she obtains true information about each asset s provided by the IoT. This cost can be thought of as the price of a specific computer to read IoT information. Once z is paid, she becomes an *active* record keeper and engages in monitoring.

Monitoring and manipulation risk Suppose that N record keepers become active as the result of the first step. We index them by $i \in \mathcal{A} = \{1, \cdots, N\}$. They decide how intensively monitor information

[15] We can also think of it as the original quality certifiers, such as auction houses for art works, Gemological Institute of America and the American Gem Society for diamond, and the Certified Specialist of Wine Exam for wine.

s provided by the IoT to avoid manipulation. We denote the monitoring intensity by $\lambda_i \geq 0$.

Given $\{\lambda_i\}_{i \in \mathcal{A}}$, a certain algorithm (e.g., PoW) picks one of the active record keepers as a winner $i = i^*$, rewards her by a fee F, and declares information recorded by the winner's computer as quality certification. N and F are endogenously determined in the general equilibrium.

During this process, measure $\rho(s)$ of malicious record keepers (MRCs) try to forge recorded information about low-quality assets ($s = 0$). They participate as active record keepers and leverage (exogenous) monitoring power, anticipating that the consensus algorithm may select them as the winner. If this attempt is fulfilled, the low-quality asset with $s = 0$ obtains a high-quality certification $q = 1$, i.e., it fails to reject lemons. They can be thought of as noise or an informational shock that stems from low-quality sellers trying to counterfeit their assets.

Since producers of high-quality assets have no incentive to "downgrade" their assets, we define $\rho(1) \equiv 0$, while we set $\rho(0) = \rho > 0$. Assume that each MRC has a unit monitoring level, i.e., $\lambda = 1$, and their utility and participation decision (ρ) are exogenous, as the noise traders in the literature on market microstructure.

Consensus algorithm Given the monitoring intensity (λ_i, ρ), the consensus algorithm picks record keeper i as the winner i^* with probability γ_i that is proportional to her monitoring share:

$$\gamma_i \equiv \Pr(i = i^*) = \frac{\lambda_i}{\sum_{j=1}^{N} \lambda_i + \rho}. \tag{16}$$

We denote the aggregate monitoring power of record keepers by $\Lambda = \sum_i^N \lambda_i$ and analyze the symmetric equilibrium ($\lambda_i = \lambda_{-i} = \lambda$).

2.4.1 Optimal behavior of record keepers

We focus on the behavior of record keepers when they monitor low-quality assets ($s = 0$).[16] The expected return for record keeper i is given by

$$U_i = \max_{\lambda_i \geq 0} \gamma_i(\lambda_i, \Lambda)F - C(\lambda_i) - z \tag{17}$$

where $C(\lambda)$ is a variable monitoring cost, such as an electricity cost, and given by $C(\lambda) = \tau\lambda$ with a cost parameter τ.[17] We solve this problem by backward induction.

[16]Their behavior for high-quality assets with $s = 1$ does not matter to the reliability of the certification by the definition of θ and $\rho(1) = 0$.

[17]A quadratic cost function $C = \frac{\tau}{2}\lambda^2$ does not change qualitative results.

Firstly, (17) provides the following optimal monitoring intensity:

$$\lambda_i^* = \lambda^* = \frac{1}{N}\left(\frac{F}{\tau} - \rho\right). \tag{18}$$

Due to the non-negativity constraint, we focus on the equilibrium with $F > \tau\rho$.

To solve the participation problem, we adopt a free-entry condition which captures a public blockchain's mining sector in the real world (Budish, 2018; Easley et al., 2019). This makes all the record keepers indifferent between participating and not *ex-ante*, i.e., $U_i = 0$, leading to

$$N^* = \frac{\tau}{zF}\left(\frac{F}{\tau} - \rho\right). \tag{19}$$

2.4.2 Reliability of quality certification

The reliability of certification θ is characterized by the probability of selecting normal record keepers $\sum_i^N \gamma_i$, i.e., the consensus succeeds at detecting a low-quality asset by $q = 0$. From the definition of θ in (1), we obtain the following:

$$\theta = \sum_{i=1}^{N} \gamma_i = \frac{\Lambda^*}{\Lambda^* + \rho}, \tag{20}$$

with $\Lambda^* \equiv N^*\lambda^*$. The optimal λ^* and N^* ([18] and [19]) yield $\Lambda^* = \frac{F}{\tau} - \rho$ or, equivalently,

$$\theta = 1 - \frac{\rho\tau}{F}. \tag{21}$$

Lemma 8. *The reliability of the quality certification θ is monotonically increasing in the fee F and decreasing in the risk of cyber attack ρ and the cost of monitoring τ.*

Equation (20) suggests that a larger set of active record keepers (N) diversify away the risk of manipulation (ρ). This is one of the most frequently cited benefits of distributing information to a large set of nodes in the network rather than keeping it in one place. Even if a cyber attack manipulates one of the records, it does not affect the resulting consensus. Thus, a higher N makes the certifications more reliable. In turn, N^* in equation (19) implies that more record keepers are willing to participate when the fee F is high and the monitoring cost τ is small.[18]

We define the partial equilibrium of the record-keeping system.

[18] The equilibrium reliability θ is independent of the participation cost z because what matters for θ is the total monitoring power $\Lambda^* = N^*\lambda^*$. Even though z affects the number of active record keepers N^*, each of them optimally chooses the intensity λ^* that is inversely proportional to N, thereby making $N\lambda$ unaffected by z at the optimal level.

Definition 2. *Given the fee F from consumers, the record keepers' partial equilibrium is defined by the monitoring intensity λ^*, the number of active record keepers N^*, and the reliability of the certifications θ^* that solve the record keepers' optimization problem and satisfy the break-even condition for record keepers, i.e., they are given by (18), (19), and (21).*

2.4.3 Certification fee

We close the model by describing the fee F for quality certification. For tractability, we assume that the record-keeping system charges buyers the certification fee, whereas sellers do not pay it. Appendix C.2 shows the robustness of our results: imposing an additional fee F_S on the producer side does not change the model's implications.

Before the private value α is realized, each buyer decides whether to pay an *ex-ante* fee F to record keepers (as a whole) to gain access to quality certification or certified assets. A buyer does not anticipate the impact of her decision on the general equilibrium variables because her measure is zero. Thus, she compares the expected value functions at the trading stage with and without access to the certified assets.

If she pays the fee, her expected utility at the trading stage is given by W in (14). By contrast, if she does not pay the fee, her expected utility stays at the reservation level W_{res} in (15) because she ends up trading uncertified assets regardless of the private value α.

Therefore, buyers pay the fee F if $W - F \geq W_{res}$, whereas the record keepers have an incentive to impose a higher fee as long as each buyer is willing to pay. Thus, the equilibrium fee is given by

$$F^* = W - W_{res} = \Delta W. \tag{22}$$

We set a tie-breaking rule that a buyer pays the fee if she is indifferent. Hence, as a result of (22), all consumers get access to a set of certified assets, making the trading stage equilibrium consistent with Definition 1. Moreover, the aggregate fee that the record-keeping system collects is equal to $\int_0^1 F d\alpha = F$. Lemma 7 and (22) imply the following results:

Lemma 9. *(i) The equilibrium fee is linear in the trading value of certified assets, i.e.,*

$$F^* = \Delta W = \frac{\phi(1-\pi)}{2} V_c.$$

(ii) The reaction of the equilibrium fee F^* to the reliability θ is given by Proposition 2.

3 General equilibrium

Now, we can define the general equilibrium (GE) of the economy.

Definition 3. *The general equilibrium is defined by the set of prices, quantity, and quality,* $\{P_j, Vol_j, \pi_j\}_{j=c,nc}$*, the transaction value,* $\{V_j\}_{j=c,nc}$*, the number of active record keepers* N*, the monitoring intensity* λ*, and the reliability of the certifications* θ *that satisfy (i) the traders' partial equilibrium in Definition 1 and the record keepers' partial equilibrium in Definition 2.*

By substituting V_c for F (Lemma 9), the GE is characterized by the following:

Proposition 4. *The GE is summarized by* (θ, V_c) *that solve the following two equations:*

$$V_c^{tr}(\theta) \equiv V_c(\theta) = \begin{cases} \frac{1-\phi}{\pi(1-\phi)+u(\theta)} \frac{\phi\pi}{(2-\pi)(1-p)+\pi\phi} & \text{for } \theta \geq \theta_0 \\ \phi\left[\pi\phi + (1-\pi)(1-\theta)\right]^{-1}\left[1 + \frac{1}{1-(1-\pi)\theta}\right]^{-2} & \text{for } \theta < \theta_0, \end{cases} \tag{23}$$

$$\theta(V_c) = 1 - \frac{2\rho\tau}{\phi(1-\pi)V_c}, \tag{24}$$

where $u(\theta)$ *is given by (13) in Proposition 1.*

The GE simultaneously determines θ and V_c. On the one hand, (23) and Lemma 9 indicate that the value of certified transactions V_c corresponds to the consumers' willingness to pay for certification with the reliability θ. On the other hand, $\theta(V_c)$ in (24) represents the optimal response of the record keepers to the consumers' willingness to pay V_c. Also, by inverting (24),

$$V_c^{rc}(\theta) = \frac{2\rho\tau}{\phi(1-\pi)(1-\theta)} \tag{25}$$

represents the required amount of reward V_c that the record keepers would demand when they competitively achieve a certain level of reliability θ.

To make the following discussions clear, we add superscript "*rc*" in (25), indicating that it is derived from the record keepers' partial equilibrium, while we write $V_c(\theta)$ in (23) as $V_c^{tr}(\theta)$ to show that it is traders' valuation of θ.

3.1 Equilibrium transparency

The GE transparency is determined by the fixed point problem, $V_c^{rc}(\theta) = V_c^{tr}(\theta)$. If $V_c^{rc} > V_c^{tr}$, the consumers cannot pay a sufficient reward to sustain the reliability θ, and θ declines until it achieves $V_c^{rc} \leq V_c^{tr}$. However, if $V_c^{rc} \geq V_c^{tr}$, the consumers are willing to pay more than required by the record keepers, and they obtain a strictly positive profit. Thus, additional record keepers flow into the record-keeping system and dilute the expected revenue U_i to sustain the zero-profit condition. Then, θ increases until $V_c^{rc} > V_c^{tr}$ holds. Therefore, if the curve V_c^{rc} crosses V_c^{tr} from below, the intersection θ^* is a stable solution, while if it crosses from above, θ^* is unstable. Following the literature (e.g., Hendershott and Mendelson, 2000; Zhu, 2014), we adopt the stability as the equilibrium selection criteria because the unstable equilibrium is not robust and cannot withstand a small perturbation in parameters.

As for the existence of the solution, the non-negativity constraint, $\lambda^* > 0$ in (18), implies $V_c^{tr}(0) > V_c^{rc}(0)$. Also, $\lim_{\theta\to 1} V_c^{tr} < \infty = \lim_{\theta\to 1} V_c^{rc}$, meaning that there exists at least one stable equilibrium. In the following, we denote the general equilibrium reliability by

$$\theta^* \equiv \left\{ \theta \in [0,1] \,\middle|\, V_c^{tr}(\theta) = V_c^{rc}(\theta), \lim_{\tilde{\theta}\to\theta-0} V_c^{rc} < \lim_{\tilde{\theta}\to\theta-0} V_c^{tr} \right\},$$

where the second condition represents the stability of the fixed point.

As for the uniqueness, Appendix D shows that the fixed point problem has a unique stable solution for most parameter values (π, ϕ, τ, ρ) by conducting exhaustive numerical experiments. However, note that the discussions in the following sections do not hinge on the uniqueness of the solution: even if multiple solutions exist, the same discussions apply as long as they are stable.

3.2 Fee-maximizing reliability

For later use, we first characterize the level of reliability/transparency θ that maximizes the fee F, the value of certified transactions V_c^{tr}, and the consumer welfare gain ΔW. Note that all of them are maximized by the same θ, and candidates for the maximizer are $\theta = 1$ and $\theta = \theta_0$ due to the shape of V_c^{tr} (Proposition 2 and Figure I).

Lemma 10. *The perfect quality certification ($\theta = 1$) maximizes $(F, V_c^{tr}, \Delta W)$ if and only if the following condition is satisfied:*

$$\theta_0 < (1-\phi)(1-\pi)\frac{\left[\frac{(2-\pi)^2}{1-\pi} + \phi\pi\right] - \frac{\phi}{\pi}\left(1 + \frac{1}{1+(1-\pi)(1-\phi)}\right)^2}{1+(1-\phi)(1-\pi)(3-\pi)}. \tag{26}$$

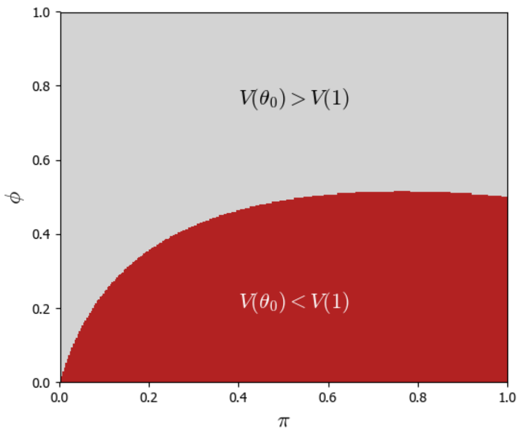
Otherwise, $V_c^{tr}(1) < V_c^{tr}(\theta_0)$, and θ_0 is the maximizer of F, V_r^{tr}, and ΔW.

Proof. See Appendix B.5. □

Figure II illustrates the region of (π, ϕ) that satisfies condition (26), and we denote it as $\mathcal{P}$:

$$\mathcal{P} \equiv \left\{ (\pi, \phi) \in [0,1] \times [0,1] \mid \text{condition (26) holds} \right\}.$$

Figure II: Region for $V_c^{tr}(1) \gtrless V_c^{tr}(\theta_0)$



Firstly, a higher return from low-quality assets (ϕ) tends to make the intermediate transparency θ_0 the maximizer of V_c^{tr}. When low-quality assets provide high utility (i.e., ϕ is high), consumers are not attracted to high-quality assets and the certified transactions. Thus, it is easy to give up certified assets to buy uncertified ones, and a marginal increase in the reliability θ, as well as a higher price P_c, tends to lower the transaction value of certified assets. Due to this negative impact of increasing θ, a low θ achieves higher trading activity than a high θ, leading to $V_c^{tr}(1) < V_c^{tr}(\theta_0)$.

One the other hand, a large fraction of high-quality assets (π) tend to make $V_c^{tr}(1) > V_c^{tr}(\theta_0)$, meaning that the positive impact of increasing θ is stronger than its negative impact. A high π means that the low-quality assets are scares at the beginning. This reduces uncertainty in certified transactions that stems from the risk of buying low-quality but certified assets. The return from certified transactions becomes substantially higher than that from uncertified transactions. Therefore, consumers are attracted to the certified assets, V_c^{tr} tends to be upward-sloping, and higher reliability ($\theta = 1$) attains the maximum value of certified transactions.

3.3 General equilibrium with centralized record keeper

In preparation for the next section, we define the GE with a *centralized* record keeper (CRK), in which the CRK replaces the decentralized record keepers to monopolistically provide quality certification. This equilibrium represents the traditional world before the advent of the blockchain. Although this paper compares two different general equilibria, the companion paper by Aoyagi (2019) considers the coexistence of decentralized and centralized systems: they engage in the Bertrand-type competition to provide certification, while one of them is managed by the decentralized agents.

The CRK solves the same objective function as the decentralized record keepers.[19]

$$\theta_C^* = \arg\max_{\theta} F(\theta) - C(\lambda(\theta))$$
$$\text{s.t., } F(\theta) = \frac{\phi(1-\pi)}{2} V_c^{tr}(\theta), \; \theta = \frac{\lambda(\theta)}{\lambda(\theta)+\rho}. \tag{27}$$

Since the traders' partial equilibrium stays the same as previously defined, we define the GE as follows:

Definition 4. *The general equilibrium with the centralized record keeper is defined by the price, quality, quantity, the trading value of assets, and the fee for quality certification* $(\{P_j, \pi_j, Vol_j, V_j\}_{j=c,nc}, F)$, *which satisfy the traders' partial equilibrium in Definition 1, and the certification reliability* θ *that maximizes the CRK's problem in (27).*

The GE with the CRK differs from the decentralized management because the CRK incorporates the impact of her monitoring λ on the equilibrium reliability θ and the reaction of traders' partial equilibrium (i.e., V_c^{tr}, F) to θ.

Moreover, if there is no monitoring cost ($\tau = 0$), the CRK's problem reduces to

$$\theta_C^* = \arg\max_{\theta\in[0,1]} F(\theta). \tag{28}$$

Namely, she chooses

$$\theta_C^* = \mathbb{I}_{\{(\pi,\phi)\in\mathcal{P}\}} + \theta_0 \mathbb{I}_{\{(\pi,\phi)\notin\mathcal{P}\}},$$

where $\mathbb{I}_X$ is the indicator function of event X. Thus, the optimal reliability achieves the maximum in the value of certified transactions V_c and consumer welfare gain ΔW. Adding $\tau > 0$ has a negative impact on θ_C^*.

4 Analysis

This section considers which one of the record-keeping systems performs better in terms of the fee revenue, trading activity, and consumer welfare.

[19] Since the CRK is the monopolist, we ignore the participation decision of the CRK (i.e, the participation cost z is sunk), and she obtains the fee revenue for sure.

4.1 Equilibrium fee revenue

Regarding the fee revenue, the decentralized record-keeping system may provide suboptimal transparency compared to the fee-maximizing level. We first consider the case with a positive monitoring cost ($\tau > 0$) but even $\tau = 0$ generates a suboptimal fee revenue in some parameter regions.

Proposition 5. *If $\tau > 0$, the general equilibrium reliability θ^* cannot achieve the maximum in the fee (F), the value of certified transactions (V_c^{tr}), and the consumer welfare gain (ΔW) almost surely.*

Case with $(\pi, \phi) \in \mathcal{P}$ If $(\pi, \phi) \in \mathcal{P}$, then $\theta = 1$ is the maximizer of $(V_c^{tr}, F, \Delta W)$, as Lemma 10 attests. However, the general equilibrium cannot achieve the perfect quality certification if $\tau > 0$. To achieve $\theta = 1$, the risk of manipulation ρ must be perfectly diversified, and it requires each record keeper to provide unbounded monitoring (i.e., $\lambda \to \infty$), which is not attained in the equilibrium, as long as the monitoring cost is strictly positive.

If there are no monitoring costs, the decentralized monitoring can achieve the maximum in the above variables:

Corollary 2. *In the absence of the monitoring costs ($\tau = 0$), the record keepers provide $\theta^* = 1$, at which $(V_c^{tr}, F, \Delta W)$ are all maximized.*

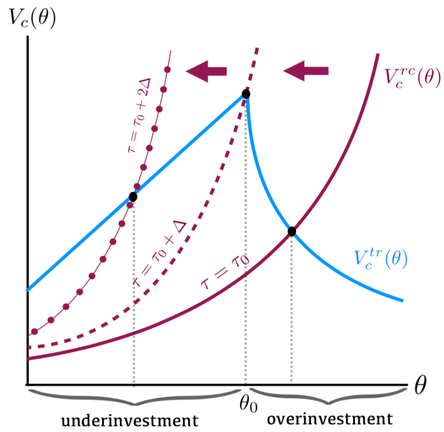
Proof. $\lim_{\tau=0} \lambda^* = \infty$, and θ in (24) is $\theta = 1$ regardless of V_c^{tr}. □

Case with $(\pi, \phi) \notin \mathcal{P}$ In contrast, if $(\pi, \phi) \notin \mathcal{P}$, even a zero monitoring cost ($\tau = 0$) cannot achieve the maximum fee. In this case, the transaction value of certified assets V_c^{tr} does not require high reliability θ to attain its maximum, as $\theta = \theta_0 < 1$ is the maximizer. However, the general equilibrium θ^* can achieve the fee-maximizing transparency θ_0 only in a knife-edge case, because the measure of a parameter set $\boldsymbol{p} = (\pi, \phi, \tau, \rho)$ such that $\theta^*(\boldsymbol{p}) = \theta_0(\boldsymbol{p})$ is zero.

If the monitoring cost is zero ($\tau = 0$), we always have $\theta^* = 1$, which is an overinvestment from the perspective of the value of certified transactions V_c^{tr} and the fee F. As τ increases, θ^* declines and achieves $\theta^* = \theta_0$ only with zero probability. If τ rises even more, θ^* dips into $\theta^* < \theta_0$, meaning that record keepers underinvest. Figure III illustrates this comparative statics.

Therefore, we have established that the trading activity of certified assets (V_c), as well as the fee for the record keepers (F), cannot attain its maximum with decentralized monitoring if it is costly ($\tau > 0$). Even if the monitoring cost can be ignored ($\tau = 0$), there is a certain parameter region ($\mathcal{P}^c$) in which the maximum in V_c and F is unattainable. This is because the decentralized

Figure III: Impact of τ on general equilibrium θ



Note: This figure illustrates the behavior of the fixed point problem when the monitoring cost $C = \tau\lambda$ experiences an increase in τ from $\tau = \tau_0$ to $\tau = \tau_0 + \Delta\tau$

.

record keepers behave competitively and do not internalize the behavior of the trader-side partial equilibrium.

4.1.1 Centralized monitoring

Regarding the fee F and the activity of certified transactions V_c, problem (28) implies that the CRK performs better than the decentralized record keepers when $(\pi, \phi) \notin \mathcal{P}$ and $\tau = 0$. The CRK knows that higher transparency reduces the trading activity of certified assets and the fee revenue. Thus, in the absence of the monitoring cost, she keeps the transparency at $\theta_C^* = \theta_0$, thereby obtaining a higher fee revenue than the decentralized system (with $\theta^* = 1$). In contrast, both of them can achieve the maximum V_c and F if the monitoring is free $\tau = 0$ and $(\pi, \phi) \in \mathcal{P}$ because they set $\theta_C^* = \theta^* = 1$, which is the fee-maximizing transparency.

Therefore, the decentralized record keepers cannot perform better than the centralized system in terms of these variables if there is no monitoring cost. This is because the centralized agency internalizes the non-monotonic impact of her behavior on the economy, while the decentralized record keepers do not. Also, Figure XI in Appendix E illustrates the case with a positive monitoring cost ($\tau > 0$) and shows that the above result for $(\pi, \phi) \notin \mathcal{P}$ survives with a relatively small τ.

4.2 Welfare implication

Although the decentralized system may not earn more than the CRK does, they can outperform the CRK in terms of the total consumer welfare. Firstly, we have the following lemma:

Lemma 11. *(i) The consumer welfare W is monotonically increasing in θ for $\theta \le \theta_0$.*

(ii) W is convex in $\theta \ge \theta_0$.

(iii) If $(\pi, \phi) \in \mathcal{P}$, W is maximized by the perfect quality certification with $\theta = 1$.

Proof. Points (i) and (iii) are obvious from Proposition 3. See Appendix C.1 for point (ii). □

Even though the welfare-maximizing θ is not analytically solved when $(\pi, \phi) \notin \mathcal{P}$, the convexity of W allows us to focus on $\theta = \theta_0$ or $\theta = 1$ as the maximizer of W. Appendix E employs an exhaustive numerical analysis covering the entire parameter space $(\pi, \phi) \in [0, 1] \times [0, 1]$ and shows that $\theta = 1$ maximizes W (see Figure X in Appendix E for the result of the numerical analysis).

Remark *The perfect quality certification with $\theta = 1$ maximizes consumer welfare W.*

Therefore, the consumers in aggregate prefer quality certification that perfectly resolves quality uncertainty so that they enjoy the perfect-information world.

4.2.1 Decentralized versus centralized certification

Now, we analyze which one of the record-keeping systems (centralized or decentralized) becomes closer to the perfect transparency ($\theta = 1$). In the following, we focus on the case with $(\pi, \phi) \notin \mathcal{P}$ and $V_c^{tr}(1) < V_c^{tr}(\theta_0)$, as it makes the difference between these two systems salient.[20]

Proposition 6. *When $\tau = 0$ and $(\pi, \phi) \notin \mathcal{P}$,*

(i) the general equilibrium with the CRK exhibits underinvestment in terms of consumer welfare W, i.e., $\theta_C^* = \theta_0 < 1$ and $W(\theta_C^*) < W(1)$.

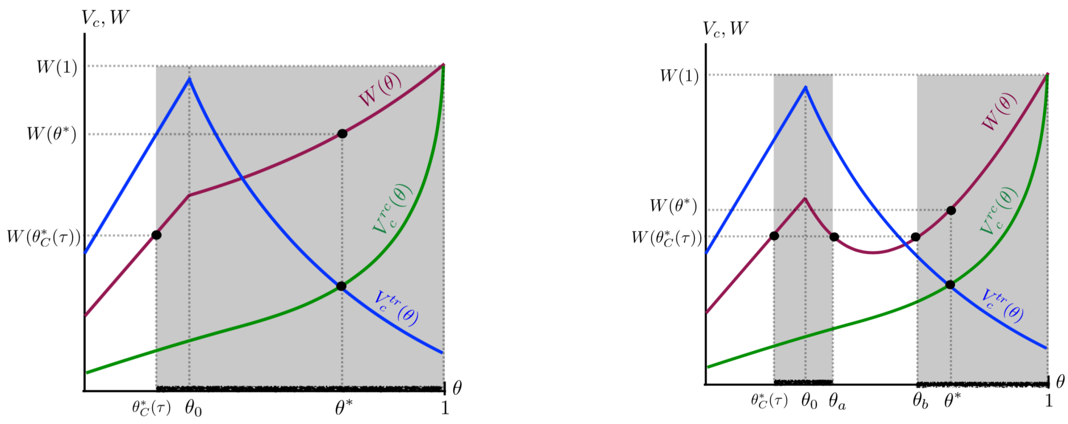
(ii) The general equilibrium with decentralized record keepers achieves the maximum consumer welfare, i.e., $\theta_0 = \theta_C^* < \theta^* = 1$ and $W(\theta_C^*) < W(1) = W(\theta^*)$.

Proof. $\theta_0 = \theta_C^*$ comes from $\tau = 0$ and $(\pi, \phi) \notin \mathcal{P}$. Corollary 2 implies point (ii). □

If there is no monitoring cost, the CRK tries to maximize the fee revenue or, equivalently, the value of certified transactions $V_c^{tr}(\theta)$. When $(\pi, \phi) \notin \mathcal{P}$, improving transparency can reduce the trading activity of certified assets V_c^{tr}. Thus, even if the total consumer welfare W attains its maximum with perfect transparency ($\theta = 1$), the centralized record keeper has an incentive to keep the market opaque ($\theta_C^* = \theta_0$). Even though higher reliability is always beneficial for consumers of uncertified assets (i.e., the reservation welfare W_{res} in point [ii] of Proposition 3), the CRK cares only about the trading activity of certified assets (V_c^{tr}), leading to insufficient transparency compared to the welfare-maximizing level.

[20] For the case with $(\pi, \phi) \in \mathcal{P}$ and $\tau > 0$, see Appendix E.

Figure IV: General equilibrium θ and welfare



A: Monotonic W

B: Non-monotonic W

In contrast, the decentralized record keepers can solve this problem. Since they are competitive and do not have direct control of the equilibrium transparency (and the fee F), they do not incorporate the negative impact of higher transparency θ on the fee and the value of certified transactions. Even though this causes the overinvestment from the perspective of the fee revenue, it mitigates the underinvestment problem measured by the consumer welfare that the equilibrium with the CRK suffers. Therefore, the competitive nature of the decentralized record-keeping system can be the solution to the distortion generated by the centralized information management.

The above results survive even if the monitoring cost is positive.

Corollary 3. *Suppose that $(\pi, \phi) \notin \mathcal{P}$ and $\tau > 0$. Regarding the total consumer welfare W,*
(i) the general equilibrium with the CRK exhibits underinvestment, i.e., $\theta_C^* < \theta_0 < 1$ and $W(\theta_C^*) < W(\theta_0) < W(1)$.
(ii) The general equilibrium with the decentralized record keepers outperforms the CRK, as $\theta_C^* < \theta_0 < \theta^* < 1$ and $W(\theta_C^*) < W(\theta^*) < W(1)$, if and only if the monitoring cost and the manipulation risk (τ, ρ) fall in some parameter regions.

The first statement is obvious because the positive monitoring cost τ always reduces the optimal reliability for the CRK, i.e., $\frac{d\theta_C^*}{d\tau} < 0$. The second statement is understood in Figure IV. By the same logic as the case with $\tau = 0$, the decentralized record keepers can overinvest compared to the fee-maximizing θ (i.e., $\theta = \theta_0$) when parameters (τ, ρ) are small. Although this overinvestment does not attain the first-best level ($\theta = 1$), it is superior to the certification by the CRK.

Both τ and ρ increase the required amount of reward for the record keepers $V_c^{rc}(\theta)$. The continuity of the fixed point problem (and its solution θ^*) implies the existence of a parameter region (τ, ρ), such that the general equilibrium with decentralized monitoring outperforms the centralized monitoring in terms of consumer welfare.

Figure IV illustrates such a situation. Panel A shows the case with a monotonically increasing W (point [iii-a] in Proposition 3). In this case, the CRK sets $\theta^*_C < \theta_0$, and the decentralized record keepers can outperform the CRK if the general equilibrium achieves $\theta^* > \theta^*_C$. This region is highlighted by the shaded area in the figure. Regardless of (τ, ρ), the CRK's reliability does not exceed θ_0, while θ^* is likely to be higher than θ_0 when parameters (τ, ρ) are sufficiently small, as they shift down the required amount of reward for record keepers V^{rc}_c.

Panel B shows the case with non-monotonic W (point [iii-b] in Proposition 3). Due to the U-shaped W, the shaded area that gives $W(\theta^*) > W(\theta^*_C)$ is divided into two intervals. There exist θ_a and $\theta_b (> \theta_a)$, such that the decentralized record keepers outperform the CRK when $\theta \in [\theta_0, \theta_a] \cup [\theta_b, 1]$. To be in the first region $[\theta_b, 1]$, the cost and the risk of attack (τ, ρ) must be sufficiently small so that θ^* achieves high θ, as in Panel A. Interestingly, however, intermediate (τ, ρ) can also generate θ^* that outperforms the CRK because of the non-monotonic W. That is, lowering θ can increase the transaction value V^{tr}_c and consumer welfare gain ΔW, which drives up the total welfare W.

Therefore, our model attests that a centralized record keeper provides suboptimal certification and transparency from the perspective of consumer welfare because she is aware of the non-monotonic reaction of the traders' partial equilibrium. This result is reminiscent of the existing models of transparency (Lizzeri, 1999; Strausz, 2005; Stahl and Strausz, 2017), while we do not rely on the strategic motives of traders.

Moreover, we have characterized when and why the decentralized record-keeping system outperforms (or underperforms) the traditional centralized information management in terms of consumer welfare. It depends on the nature of traded assets (the quality difference ϕ and fraction of high-quality assets π), as well as on the environment in which the record keepers operate (the monitoring cost τ and risk of manipulation ρ).

The ongoing discussions about the blockchain technology have emphasized that the benefit of decentralizing information comes from the robustness of the network to the single-point failure. We show that it is more than that. The competitive nature of the decentralized record-keeping system prevents record keepers from internalizing the non-monotonic impact of their behavior on the traders' equilibrium, thereby mitigating the welfare cost that stems from the strategic behavior of the traditional record keeper.

5 Discussion

In this section, we briefly discuss how to translate our model into the blockchain economy, which is the most prominent example of the decentralized information management system in the real world. Afterward, we propose some testable implications of our theoretical model.

5.1 Application to the blockchain economy

As elaborated in Appendix A, the blockchain technology exploits the decentralized record-keeping system. At its core, the record keepers called *miners* monitor information brought into the blockchain system by leveraging computing power measured by the *hash rate*. There are several consensus-generating algorithms but we focus on the PoW, as it is adopted in the Bitcoin and Ethereum, the two largest blockchains as of October 2019.[21]

Many institutions have adopted the blockchain to mitigate asymmetric information in supply-chain management and financial transactions. Various types of assets are traded with information monitoring by the blockchain, such as diamond, wine, meat, artwork, photography, security, financial value, and information itself. Traditionally, recorded information about asset quality (e.g., wine vintage, diamond mines, the provenance of artwork) is maintained by a centralized authority, making it vulnerable to information manipulation. The blockchain technology tackles this issue by exploiting the distributed ledger system (see Appendix A).

5.1.1 Traders' behavior

The quality certification in this extension is achieved by the public information on the blockchain system. For example, when a consumer buys a bottle of wine, she can purchase a bottle with information tracked by the blockchain and decentralized miners.

Since most blockchains (e.g., Ethereum) require traders to hold cryptocurrency as a means of transaction, we introduce the cryptocurrency with dollar price p. Appendix A.3 provides a formal model and shows that the traders' partial equilibrium provides exactly the same results as the main model (Definition 1 and Proposition 1) with one additional variable, i.e., the cryptocurrency price.

A consumer holds a sufficient amount of cryptocurrency as a means of transaction of certified assets, and the demand for cryptocurrency, denoted by b_d, satisfies $pb_d \geq P_c k_c$ with equality. In aggregate, the demand for cryptocurrency in the equilibrium amounts to $B_d = \int_0^1 b_d d\alpha = \frac{P_c D_c}{p} = \frac{V_c^{tr}}{p}$. On the other hand, to capture the supply-side of the cryptocurrency in the real world (see

[21] For example, Saleh (2018) analyzes other algorithms, such as the Proof-of-Stake.

Appendix A.3), we assume its supply, denoted by B_s, is fixed ($B_s = 1$ with normalization). Thus, the market clearing condition for the cryptocurrency ($1 = B_d$) makes its price equal to the value of certified transactions:

$$p = p^{tr}(\theta) = V_c^{tr}(\theta). \tag{29}$$

We use superscript "tr" to show that equation (29) represents the cryptocurrency price derived from the traders' partial equilibrium. Since we have shown that the fee for the certifications is linear in V_c^{tr}, the cryptocurrency price in (29) can be thought of as the consumers' willingness to pay for the certified transactions.

Proposition 2 implies the following:

Corollary 4. *The cryptocurrency price p is non-monotonic in the reliability of information (θ) tracked by the blockchain.*

Intuition follows the main model. It implies that more transparent information on the blockchain can reduce the value of certified transactions and the cryptocurrency price p.

5.1.2 Miners' behavior

Although the miners' behavior is the same as that of record keepers' in the main model, we reinterpret some variables. Firstly, miners try to solve a cryptographic problem to be the winner $i = i^*$, i.e., to record information and obtain the reward F. Solving the problem involves large hash power, and the winning probability γ_i is proportional to her hash share. Thus, the monitoring intensity λ_i corresponds to the hash rate and the aggregate intensity $\Lambda + \rho$ is the total hash rate of the blockchain network.

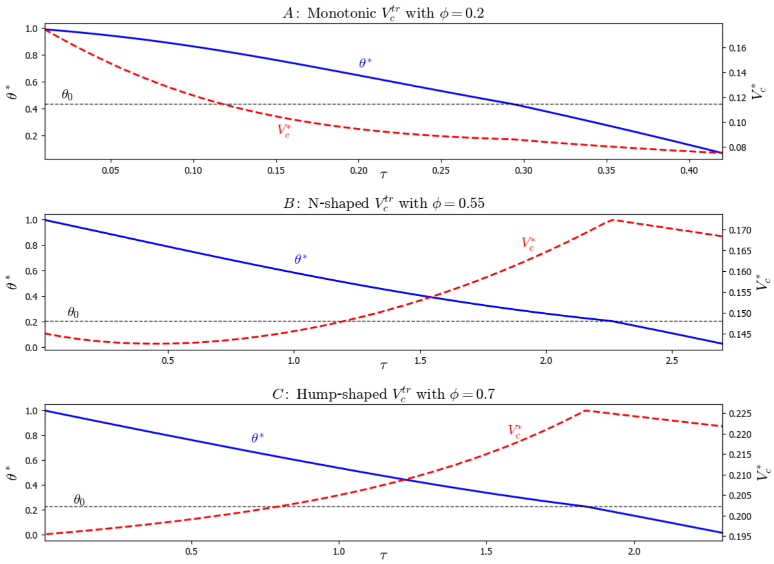
Secondly, the winning miner is rewarded in cryptocurrency, and its amount is fixed.[22] Therefore, by normalizing the amount of the reward, the cryptocurrency price p represents the value of the reward. Thus, we have $p = F$, and Lemma 9 and (25) yield

$$p = p^m(\theta) = \frac{2\rho\tau}{\phi(1-\pi)(1-\theta)}, \tag{30}$$

where the superscript "m" stands for the variables in the miners' partial equilibrium. Thus, the cryptocurrency price in (30) can be seen as the required price of a reward for miners to sustain a

[22] When a miner wins the mining game, the blockchain system generates a certain amount (say, X) of new cryptocurrency to provide her with a reward with value pX. This newly created digital token works as the supply side of the cryptocurrency. In the real world, the growth rate of X is constant in the short or medium-run, while it decays in the long-run, making the total supply of the cryptocurrency constant over time.

Figure V: Behavior of the reliability and trading value



certain level of θ.

5.1.3 General equilibrium

The general equilibrium is defined in the same manner as Definition 3, while it is now characterized by the fixed point problem of (29) and (30), i.e., $p^m(\theta) = p^{tr}(\theta)$.

The behavior of the general equilibrium is the same as the main model. It implies that the cryptocurrency price p and the reliability of blockchain information θ must be simultaneously determined and linked by the non-monotonic relationship. We discuss the implications of the model in the following.

5.2 Empirical implication

Impact of monitoring cost Consider an increase in the monitoring cost τ, e.g., an electricity price, a cost of information devise, and hiring costs. Due to the non-monotonic curve of the certified transaction value V_c^{tr}, the general equilibrium reliability θ^* and the trading activity of certified assets $V_c^* = V_c(\theta^*)$ exhibit a non-monotonic relationship when τ fluctuates.

Obviously, when V_c^{tr} is monotonically increasing in θ, a higher cost τ lowers θ^* and V_c^*. However, if V_c^{tr} is hump-shaped or N-shaped, θ^* and V_c^* can negatively correlate. For example, Figure V shows the response of these variables to a change in τ when V_c^{tr} is monotonically increasing (Panel A), N-shaped (Panel B), and hump-shaped (Panel C). For all τ, the equilibrium reliability θ^* negatively react to τ because a higher monitoring cost reduces the monitoring intensity of each record keeper, thereby pushing up the required amount of reward $F \sim V_c^{rc}$ without affecting the traders' partial equilibrium V_c^{tr}. In a high-τ (or a low-θ) region, an increase in τ and a decline in θ^* weaken the trading activity V_c^*, generating positive comovement between θ^* and V_c^*. However, if θ^* exceeds θ_0 in a low-τ region, the transaction value of certified assets V_c^{tr} slopes downward at the fixed point. Then, an increase in τ yields negative comovement between these variables (Panels B and C). Note that the same argument can be applied to the risk of information manipulation ρ.

Cryptocurrency price The above discussion on the impact of τ and ρ generates clear implications for the blockchain economy. Note that the cryptocurrency price p is proportional to the trading value of the certified assets V_c^*. Since we can use the total hash rate Λ as the proxy of the reliability θ, the above arguments imply that the relationship between the cryptocurrency price p and the total hash rate Λ is ambiguous, as Figure V shows.

For example, an increase in the mining cost τ (e.g., electricity price) has a robust negative impact on the miners' activity Λ. However, it can both increase and decrease the cryptocurrency price depending on the level of the cost τ and the total hash power Λ.

Note that the total hash power (Λ), the electricity price (τ), the economy-wide fraction of high-quality assets (π), and the probability of cyber attack (ρ) are observable.[23] Thus, if we have an appropriate measure of the utility difference between low and high-quality assets (ϕ),[24] we can test the ambiguous comovement between p and V_c^* when τ exogenously changes. On the other hand, analyzing the comovement between these observable variables provides a measure of the consumer utility difference (ϕ) between high-quality and low-quality goods.

Moreover, our model shows that the cryptocurrency price and the total hash rate are simultaneously determined. Therefore, as already noted by cryptocurrency investors, the hash rate may be a good predictor for the cryptocurrency price in the long run. However, the simultaneous equations imply that analyzing these variables by simple regressions may suffer from the endogeneity problem. It also indicates that, in the long-run, these two variables may have cointegration relationship, meaning that the total hash rate can be seen as a fundamental factor in determining the cryptocurrency price (Aoyagi and Hattori, 2019; Bhambhwani et al., 2019). This goes counter to the real-world discussions that argue that the cryptocurrency is a bubble.

[23] As for the fraction of high-quality assets π, we can measure the total value of counterfeiting, e.g., economic value of fake wine and conflicting diamonds.

[24] For some assets, ϕ can be easily measured by comparing the monetary value of authentic assets to that of forged assets.

6 Conclusion

This paper studies the impact of decentralized information management on an exchange economy with asymmetric information regarding asset quality. We consider a competitive environment, and traders can mitigate uncertainty by using quality certification provided and managed by the decentralized record keepers. In contrast to the existing models, we show that the trading activity has a non-monotonic reaction to the reliability of quality certification. Since decentralized record keepers competitively behave without internalizing the non-monotonicity, they may improve consumer welfare compared to the case with a centralized record keeper.

Although our competitive model is a good starting point to analyze decentralized information management, a couple of important forces are missing. Firstly, we do not model traders' strategic motives, such as a signaling incentive via quality certification. We believe our results are robust to this generalization, as it may strengthen the differentiation of sellers and the economy's non-monotonic reaction. Moreover, this paper compares two general equilibria, one with a centralized record keeper and the other with decentralized record keepers. These two record-keeping systems coexist in the real world and should compete against each other in a single equilibrium framework. The companion paper by Aoyagi (2019) provides a similar model to this paper to analyze the competition between them. It shows how the Bertrand-type competition may change when one of the competitors is managed by decentralized agents.

As one of the examples of the decentralized system, we adopt our baseline model to the blockchain economy. Even though the blockchain technology and cryptocurrency are still in their nascent and pivot around speculation, their influence is growing, and their potential applications are vigorously sought. Therefore, we believe that the analyses of their fundamental effects in our theoretical model will have important implications not only for financial markets but also for the entire economy.

Acknowledgement

We gratefully acknowledge that Christine Parlour gave us invaluable guidance. We also appreciate the constructive comments from Kosuke Aoki, Michael Brolley, Gadi Barlevy, Will Cong, Shin-ichi Fukuda, Nicolae Garleanu, Wei Jiang, Xuelin Li (discussant), Katya Malinova (discussant), Giuseppe Perrone, Fahad Saleh, Susumu Sato, Naga Sethuraman, Yoko Shibuya, Katrin Tinn (discussant), Cristian Ugarte, Harald Uhlig, Noriyuki Yanagawa, Yingge Yan, and Marius Zoican, and from the seminar participants at the 2019 NFA Conference, the Southampton CRC, GSU/RFS FinTech Conference, SWET at Hokkaido, UC Berkeley, University of Tokyo, and WINDS at Wharton School. This research was financially supported by the Berkeley Blockchain Initiative Fund by Ripple.

References

Abadi, Joseph and Markus Brunnermeier, "Blockchain economics," Technical Report, mimeo Princeton University 2018.

Akerlof, George, "The market for lemons," *Quarterly Journal of Economics*, 1970, *84* (3), 488–500.

Albano, Gian Luigi and Alessandro Lizzeri, "Strategic certification and provision of quality," *International Economic Review*, 2001, *42* (1), 267–283.

Ambrus, Attila and Rossella Argenziano, "Asymmetric networks in two-sided markets," *American Economic Journal: Microeconomics*, 2009, *1* (1), 17–52.

Antonopoulos, Andreas M, *Mastering Bitcoin: unlocking digital cryptocurrencies*, O'Reilly Media, Inc., 2014.

Aoyagi, Jun, "Industry Competition: The Blockchain versus Centralized Authority," *Available at SSRN 3426895*, 2019.

— **and Daisuke Adachi**, "Economic Implications of Blockchain Platforms," *Available at SSRN 3132235*, 2018.

— **and Takahiro Hattori**, "The empirical analysis of Bitcoin market in the general equilibrium framework," *Working Paper*, 2019, *SSRN 3433833.*

Armstrong, Mark, "Competition in two-sided markets," *The RAND Journal of Economics*, 2006, *37* (3), 668–691.

Aune, Rune Tevasvold, Adam Krellenstein, Maureen O'Hara, and Ouziel Slama, "Footprints on a blockchain: Trading and information leakage in distributed ledgers," *The Journal of Trading*, 2017, *12* (3), 5–13.

Bhambhwani, Siddharth, Stefanos Delikouras, and George M Korniotis, "Do Fundamentals Drive Cryptocurrency Prices?," *Available at SSRN 3342842*, 2019.

Biais, Bruno, Christophe Bisiere, Matthieu Bouvard, and Catherine Casamatta, "The blockchain folk theorem," *The Review of Financial Studies*, 2019, *32* (5), 1662–1715.

Biglaiser, Gary and James W Friedman, "Middlemen as guarantors of quality," *International Journal of Industrial Organization*, 1994, *12* (4), 509–531.

Biswas, Kamanashis, Vallipuram Muthukkumarasamy, and Wee Lum Tan, "Blockchain Based Wine Supply Chain Traceability System," in "Future Technologies Conference" 2017.

Budish, Eric, "The economic limits of bitcoin and the blockchain," Technical Report, National Bureau of Economic Research 2018.

Cespa, Giovanni and Xavier Vives, "Exchange Competition, Entry, and Welfare," *Working Paper*, 2019.

Chang, Briana, "Adverse selection and liquidity distortion," *The Review of Economic Studies*, 2017, *85* (1), 275–306.

Chen, Long, Lin William Cong, and Yizhou Xiao, "A Brief Introduction to Blockchain Economics," *Available at SSRN*, 2019.

Chiu, Jonathan and Thorsten V Koeppl, "The economics of cryptocurrencies–bitcoin and beyond," *Available at SSRN 3048124*, 2017.

— **and** — , "Blockchain-based settlement for asset trading," *The Review of Financial Studies*, 2019, *32* (5), 1716–1753.

Cong, Lin William and Zhiguo He, "Blockchain disruption and smart contracts," *The Review of Financial Studies*, 2019, *32* (5), 1754–1797.

— **, Ye Li, and Neng Wang**, "Tokenomics: Dynamic adoption and valuation," *Becker Friedman Institute for Research in Economics Working Paper*, 2019, (2018-49), 2018–15.

Damiano, Ettore and Li Hao, "Competing matchmaking," *Journal of the European Economic Association*, 2008, *6* (4), 789–818.

Easley, David, Maureen O'Hara, and Soumya Basu, "From mining to markets: The evolution of bitcoin transaction fees," *Journal of Financial Economics*, 2019.

Foucault, Thierry and Albert J Menkveld, "Competition for order flow and smart order routing systems," *The Journal of Finance*, 2008, *63* (1), 119–158.

— **and Christine A Parlour**, "Competition for listings," *The RAND Journal of Economics*, 2004, pp. 329–355.

Gabszewicz, Jean J and Xavier Y Wauthy, "Vertical product differentiation and two-sided markets," *Economics Letters*, 2014, *123* (1), 58–61.

Glosten, Lawrence R and Paul R Milgrom, "Bid, ask and transaction prices in a specialist market with heterogeneously informed traders," *Journal of Financial Economics*, 1985, *14* (1), 71–100.

Guerrieri, Veronica and Robert Shimer, "Dynamic adverse selection: A theory of illiquidity, fire sales, and flight to quality," *American Economic Review*, 2014, *104* (7), 1875–1908.

Halaburda, Hanna and Yaron Yehezkel, "Platform competition under asymmetric information," *American Economic Journal: Microeconomics*, 2013, *5* (3), 22–68.

Harvey, Campbell, "Cryptofinance," *Available at SSRN 2438299*, 2016.

Hendel, Igal and Alessandro Lizzeri, "Adverse selection in durable goods markets," *American Economic Review*, 1999, *89* (5), 1097–1115.

Hendershott, Terrence and Haim Mendelson, "Crossing networks and dealer markets: Competition and performance," *The Journal of Finance*, 2000, *55* (5), 2071–2115.

Khapko, Mariana and Marius Zoican, "Smart settlement," Technical Report, Working paper 2017.

Kim, Kyungmin, "Endogenous market segmentation for lemons," *The RAND Journal of Economics*, 2012, *43* (3), 562–576.

Kurlat, Pablo, "Lemons markets and the transmission of aggregate shocks," *American Economic Review*, 2013, *103* (4), 1463–89.

Lizzeri, Alessandro, "Information revelation and certification intermediaries," *The RAND Journal of Economics*, 1999, pp. 214–231.

Malinova, Katya and Andreas Park, "Market Design with Blockchain Technology," *Available at SSRN 2785626*, 2017.

Mathis, Jerome, James McAndrews, and Jean-Charles Rochet, "Rating the raters: are reputation concerns powerful enough to discipline rating agencies?," *Journal of Monetary Economics*, 2009, *56* (5), 657–674.

Pagnotta, Emiliano and Andrea Buraschi, "An equilibrium valuation of bitcoin and decentralized network assets," *Available at SSRN 3142022*, 2018.

Rochet, Jean-Charles and Jean Tirole, "Platform competition in two-sided markets," *Journal of the European Economic Association*, 2003, *1* (4), 990–1029.

Rubinstein, Ariel and Asher Wolinsky, "Middlemen," *The Quarterly Journal of Economics*, 1987, *102* (3), 581–593.

Saleh, Fahad, "Blockchain without waste: Proof-of-stake," 2018.

Schilling, Linda and Harald Uhlig, "Some simple bitcoin economics," *Journal of Monetary Economics*, 2019.

Stahl, Konrad and Roland Strausz, "Certification and market transparency," *The Review of Economic Studies*, 2017, *84* (4), 1842–1868.

Strausz, Roland, "Honest certification and the threat of capture," *International Journal of Industrial Organization*, 2005, *23* (1-2), 45–62.

Tinn, Katrin, "Smart Contracts and External Financing," *Available at SSRN 3072854*, 2018.

Tirole, Jean, *The theory of industrial organization*, MIT press, 1988.

Vives, Xavier, "Digital Disruption in Banking," *Annual Review of Financial Economics*, 2019, *11*, 243–272.

Yanelle, Marie Odile, "Banking competition and market efficiency," *The Review of Economic Studies*, 1997, *64* (2), 215–239.

Zhu, Haoxiang, "Do dark pools harm price discovery?," *The Review of Financial Studies*, 2014, *27* (3), 747–789.

Appendix

Table I: Blockchain use case

	Date	Traded goods	Blockchain
EY Ops Chain	Octber 2017	Wine	Ethereum
ADNOC	December 2018	Oil	IBM Blockchain
De Beers	January 2018	Diamond	Ethereum
EverLedger	May 2018	Diamond	IBM Blockchain
LDC	January 2018	Food	Ethereum
Walmart	July 2018	Food	IBM Blockchain
OriginTrail	May 2018	Food	Ethereum, ODN
Martine Jarlgaard	May 2017	Fashion	Ethereum
Kahawa 1893	March 2018	Coffee	Bext 360
Overstock	January 2018	Security	tZero
Kodak	June 2019	Document	Ethereum
Propy	March 2019	Real estate	Ethereum
Civil	Novemver 2018	Journalism	Ethereum
Ujo	June 2018	Music	Ethereum
Maersk	August 2018	Shipping	IBM Blockchain
AIG	June 2017	Insurance	IBM Blockchain
uPort	January 2018	ID	Ethereum

Note: This table shows the real-world use cases of the blockchain in supply-chain and other industries.

A Example of the blockchain adoption

Asset quality depends on its provenance and transaction history but information is hard to track. The blockchain is one of the solutions for the difficulty, which is built on the decentralized record keeping system. As Table I shows, the blockchain technology is penetrating into many industries, such as food and asset supply chain, information management, art, and security trading. Table I covers only the tip of the iceberg, and the use cases of the blockchain are expanding. In the following, we take food supply chain (wine blockchain) as an example and present details of its implementation.

A.1 Wine supply chain

In the wine industry, counterfeiting accounts for roughly 5% of the secondary market ($15 billion). One of the most prevalent types of fraud is relabeling cheap wine as expensive ones. Wine provenance can be opaque, as the wine supply chain involves many intermediaries (e.g., vineyard, wine producers, distributers, transit cellars, fillers/packers, wholesalers, retailers), and product quality depends on many factors (e.g., brand, blending, weather, storage condition, vintage). Traditionally, information about products is (sometimes manually) managed by a centralized record keeper, and tracking all the records is difficult because data can easily be forged and reproduced (see Biswas et al., 2017 for more details).

The Wine Blockchain (WB) by EY is an application of Ops Chain for Food Traceability (OCFT), which uses Ethereum public blockchain to notarize data and tokenize batch and products. On the supply chain, fields and particles of cultivation, steps of transformation, and numbers of bottles are recorded by the blockchain with time stamps. As the next subsection shows, information on the blockchain is almost immutable and difficult to manipulate. The smart contract is written so that transaction of a bottle is executed contingent on some conditions regarding the bottle's quality.

A.2 Overview of the blockchain technology

Environment The blockchain can be seen as a novel way of managing and tracking transaction information. On the blockchain, the ledger is not held by a particular entity, but is distributed across all participants in the network (i.e., record keepers). The *distributed ledger system* (DLS) requires the information about the state of the blockchain users to be a consensus among all record keepers. A consensus mechanism determines what data should be recorded as the truth and as fraudulent information. This highlights its first difference from traditional record-keeping systems, in which only a centralized authority keeps track of state information.

For example, in the Bitcoin blockchain, each record keeper called "miner" in the network maintains a temporary list of unconfirmed transactions called a *transaction pool*. It contains transactions that are known to the network but not recorded on the blockchain yet. All asset transactions between buyers and sellers are stored in the pool and wait for validation by the blockchain miners before they are consummated. A miner picks one of the transactions in the pool and tries to validate it following a certain algorithm (see below).

Moreover, Ethereum allows users to impound a complex script that describes conditions that transactions must satisfy. In other words, a transaction of goods is validated, executed, and recorded on the blockchain if, and only if, the conditions on Ethereum scripts are satisfied. This implies that a transaction is state contingent.

Information management In general, it is extremely difficult for one record keeper in the network to overturn the consensus. In the case of Bitcoin, for example, record keepers called miners leverage their computing power to solve a time-consuming cryptographic problem. This process is called proof of work (PoW), and the miner who performs it fastest is entitled to write transaction information in the pool on a new block and add it to a chain to generate the blockchain. Therefore, if a malicious agent attempts to add fraudulent information to the transaction history, she must outpace all miners in the network, which requires prohibitively high computing power.[25]

Once a set of transaction information forms a block, it is encrypted by a hash function and passed to the next block to create a chain. The output of the hash function becomes different if one piece of input changes. Thus, revising a piece of information in a chain requires the revision of all of the subsequent data. Consequently, any attempt to benefit from modifying the existing information is virtually impossible. That is to say, only relevant information can be added to the blockchain, and it is free from tampering. See Antonopoulos (2014) for more details on Bitcoin and blockchain implementation.

A.3 Extension of the main model

To translate the main model into the blockchain economy with cryptocurrency (or digital token), we consider the following modifications of the traders' partial equilibrium in Section 2.

First, to obtain the access to the assets tracked by the blockchain, a buyer must hold a certain amount of cryptocurrency. This is because the cryptocurrency serves as a means of transaction on the blockchain system. For example, on the EY's OpsChain for wine trade, users can buy and sell a bottle by using a digital token (ERC-721 on Ethereum). In the case of Bitcoin, if a consumer wants to buy a cup of coffee by using the Bitcoin, she must exchange her cash to the Bitcoin before she executes her transaction.

[25] There are several ways to reach a consensus, and different blockchains adopt different processes. Saleh (2018) analyzes the viability of the proof of stake (PoS).

In light of this, we adopt the "cryptocurrency in advance" (CCIA) constraint, as in Schilling and Uhlig (2019). If a buyer wants to buy $P_c k_c$ of certified assets tracked by the blockchain, she must hold at least $pb_d \geq P_c k_c$ of cryptocurrency. Thus, a consumer with type α solves the following:

$$W(\alpha) = \max_{k_j, b_d} \mathbb{E}\left[\sum_j y_j(\alpha) k_j\right] + a,$$
$$\text{s.t., } w \geq P_{nc}k_{nc} + pb_d + a, pb_d \geq P_c k_c.$$

Due to the linear utility, the budget constraint, the unit-trading constraint on k_j, and the CCIA constraint bind, leading to $b_d(\alpha) = \frac{P_c k_c(\alpha)}{p}$. As the optimal behavior of the buyers stays the same as the main model, the aggregate demand for the cryptocurrency is given by

$$B_d = \frac{P_c}{p}\int_0^1 k_c(\alpha) d\alpha = \frac{P_c}{p} D_c.$$

As in the real-world cryptocurrency, we adopt fixed supply assumption, and normalize the supply of cryptocurrency by $B_s = 1$. Thus, in the equilibrium, the market clearing condition for the cryptocurrency implies

$$p = P_c D_c = V_c.$$

Note that the rest of the model is exactly the same as the main model, leading to the discussion in Subsection 5.1.

B Proof

B.1 Proof of Proposition 1

Case with $\theta \geq \theta_0$ Let $u = \frac{P_c - P_{nc}}{P_c}$. Then, demand for certified assets is rewritten as

$$D_c = 1 - \frac{P_c - P_{nc}}{(1-\phi)\frac{\pi P_c}{S_c}} = 1 - \frac{S_c}{\pi(1-\phi)} u.$$

By the clearing condition for the certified market ($S_c = D_c$), we have

$$S_c = \left(1 + \frac{u}{\pi(1-\phi)}\right)^{-1}.$$

Next, the supply equation implies that

$$\frac{1}{1 + \frac{u}{\pi(1-\phi)}} = P_c\left[\pi + (1-\pi)(1-\theta)\frac{u}{\phi\theta}\right].$$

$$\therefore P_c = \frac{\pi(1-\phi)\theta\phi}{[\pi\phi\theta + (1-\pi)(1-\theta)u]\,[\pi(1-\phi) + u]}.$$

Thus, by exploiting $Vol_c = S_c$, the equilibrium trading value of certified assets is

$$V_c = P_c S_c = \left[\pi + (1-\pi)(1-\theta)\frac{u}{\phi\theta}\right]^{-1}\left[1 + \frac{u}{\pi(1-\phi)}\right]^{-2}. \quad \text{(B.1)}$$

Regarding u, the market clearing condition implies $D_c + D_{nc} = S_c + S_{nc}$, leading to

$$P_{nc} = \frac{1 - \pi P_c}{2 - \pi}\phi. \tag{B.2}$$

By substituting prices in the market clearing conditions, we obtain

$$\left[\pi + (1-\pi)(1-\theta)\frac{u}{\phi\theta}\right]\left[1 + \frac{u}{\pi(1-\phi)}\right] = \frac{2-\pi}{\phi}\left[\left(1 + \frac{\pi\phi}{2-\pi}\right) - u\right].$$

Rearranging this yields the quadratic equation for u:

$$\Psi(u) \equiv (1-\pi)(1-\theta)u^2 + \pi[\theta + (1-\pi)(1-\phi)]u - \theta\pi(1-\phi)(2-\pi) = 0.$$

This has a unique positive solution, as $\Psi(0) < 0$. By applying $\Psi(u) = 0$ to (B.1), it reduces to

$$V_c = \frac{1-\phi}{\pi(1-\phi) + u}\frac{\phi\pi}{(2-\pi)(1-u) + \pi\phi}.$$

Case with $\theta < \theta_0$ In this case, the total market clearing, $D_c + D_{nc} = S_c + S_{nc}$, reduces to

$$1 - \frac{P_{nc}}{\phi} = \left(\pi + \frac{(1-\pi)(1-\theta)}{\phi}\right)P_c.$$

$$\therefore P_{nc} = \phi - [\pi\phi + (1-\pi)(1-\theta)]\,P_c.$$

Thus, by the definition of u,

$$u = \frac{\pi(1-\phi)}{1-(1-\pi)\theta}.$$

Then, we obtain

$$V_c = \phi\,[\pi\phi + (1-\pi)(1-\theta)]^{-1}\left[1 + \frac{1}{1-(1-\pi)\theta}\right]^{-2}.$$

B.2 Proof of Lemma 5

Our arguments start from two conditions:

$$P_c\tilde{\pi}_{nc} > P_{nc}\tilde{\pi}_c \tag{B.3}$$

and

$$\pi_c > \pi_{nc}. \tag{B.4}$$

Given these, the buyers' partial equilibrium implies that

$$\frac{P_c}{\tilde{\pi}_c} - \frac{P_{nc}}{\tilde{\pi}_{nc}} = (\tilde{\pi}_c - \tilde{\pi}_{nc})D_{nc},$$

where $D = D_c + D_{nc} < 1$ denotes the total demand. Therefore, inequality (B.3) holds as long as (B.4) is correct. Sine we have shown that $\pi_{nc} = 0 < \pi_c$ holds, our guesses are correct.

B.3 Proof of Lemma 6 and Corollary 1

Proof of Lemma 6 Point (iii) in Lemma 6 is shown in the next paragraph. Suppose that we have $\beta_L > 0$. From Appendix 1, u solves $\Psi(u) = 0$. Note that Ψ is monotonically increasing in $u(\geq 0)$, and $\beta_L > 0$ is identical to $u < \theta$ due to the definitions of β_L and u. Thus, $\beta_L > 0$ if and only if $\Psi(\theta) > 0$, which is the same as the following condition regarding θ:

$$\psi(\theta) \equiv \theta^2(1-\pi) - \theta + \pi(1-\phi) < 0.$$

Since $\psi(0) > 0$ and $\psi(1) < 0$, the smaller solution of $\psi(\theta) = 0$ lies in $[0,1]$, while the larger solution is $\theta > 1$. We set the smaller one as θ_0, meaning that $\beta_L > 0$ if and only if $\theta_0 < \theta$.

Next, suppose that $P_{nc} - (1-\theta)P_c \leq 0$. This induces $\beta_L = 0$ by definition (8). In this case, Appendix 1 implies that $u = \frac{\pi(1-\phi)}{\pi+(1-\pi)(1-\theta)}$. Since u is monotonically increasing in θ, the condition $P_{nc} - (1-\theta)P_c \leq 0$ is identical to $\theta < u$, which is equivalent to $\psi(\theta) \geq 0$. Therefore, the condition is $\theta \leq \theta_0$, and we have established that the equilibrium is continuous at $\theta = \theta_0$.

Proof of Corollary 1 When $\theta < \theta_0$, we have

$$P_c = \phi\left[\phi\pi + (1-\pi)(1-\theta)\right]^{-1}\left[\frac{\pi + (1-\pi)(1-\theta)}{1+\pi+(1-\pi)(1-\theta)}\right],$$
$$\pi_c = \frac{\pi P_c}{S_c} = \phi\left[\phi\pi + (1-\pi)(1-\theta)\right]^{-1}.$$

Thus, the positive reaction of P_c and π_c to θ are easily confirmed by taking derivative of equations above. Also, with $\bar{\theta} \equiv (1-\pi)(1-\theta)$, we have

$$V_c = \left(\frac{\pi+\bar{\theta}}{1+\pi+\bar{\theta}}\right)^2 \frac{\phi}{\phi\pi+\bar{\theta}}.$$

Then

$$\frac{dV_c}{d\bar{\theta}} \propto -\theta^2(1-\pi) + \theta - \frac{1+2\pi(1-\phi)}{1-\pi} < 0, \tag{B.5}$$

where the last inequality comes from $\theta \leq \theta_0$. Since $\bar{\theta}$ is decreasing in θ, (B.5) implies that V_c is increasing in θ.

Regarding point (iii) in Lemma 6, P_{nc} is given by

$$P_{nc} = \frac{\phi}{2-\theta(1-\pi)},$$

which is obviously increasing in θ.

B.4 Proof of Lemma 5 and Proposition 2

Proof of Lemma 5 Note that we focus on $\theta \geq \theta_0$. First, let

$$P^* = \frac{\phi}{2-\pi(1-\phi)}. \tag{B.6}$$

Then, we have $P_c \gtrless P_{nc} \Leftrightarrow P_c \gtrless P^*$. Also, let $g \equiv \frac{1-\theta}{\theta}$ and $\eta \equiv 1 + \frac{\phi\pi}{2-\pi}$. By the market clearing condition for certified assets,

$$D_c = P_c\left[\pi + \frac{(1-\pi)}{\phi}g\eta\right] - \frac{1-\pi}{2-\pi}g,$$
$$S_c = \frac{(1-\phi)\pi P_c}{((1-\phi)\pi+\eta)P_c - \frac{\phi}{2-\pi}}. \tag{B.7}$$

By rearranging $D_c = S_c$ and using $y \equiv P_c^{-1}$, we obtain

$$H(y,g) \equiv \left(\pi + \frac{1-\pi}{\phi}g\eta\right) - \frac{\pi(1-\phi)y}{((1-\phi)\pi+\eta) - \frac{\phi}{2-\pi}y} - \frac{1-\pi}{2-\pi}gy = 0. \tag{B.8}$$

For this function, we have

$$\frac{\partial H}{\partial g} = \frac{1-\pi}{\phi(2-\pi)}(2-\pi(1-\phi)-\phi y) > 0, \tag{B.9}$$
$$\frac{\partial H}{\partial y} = -\frac{\pi(1-\phi)((1-\phi)\pi+\eta)}{[((1-\phi)\pi+\eta)-\frac{\phi}{2-\pi}y]^2} - \frac{1-\pi}{2-\pi}g < 0, \tag{B.10}$$

where both inequalities come from $P_c > P_{nc}$ (or, equivalently, $P_c > P^*$). By the implicit function theorem, $dP_c/d\theta > 0$.

Also, π_c is rewritten as

$$\pi_c = \frac{\pi}{\pi + \frac{1-\pi}{\phi}g(1-\frac{P_{nc}}{P_c})},$$

which implies that

$$\mathrm{sgn}\left(\frac{d\pi_c}{d\theta}\right) = -\mathrm{sgn}\left(\frac{d\pi_c}{dg}\right) = \mathrm{sgn}\left(\frac{d}{dg}\left[g(1-\frac{P_{nc}}{P_c})\right]\right). \tag{B.11}$$

By using (B.2), we can rewrite

$$1 - \frac{P_{nc}}{P_c} = 1 - \frac{\frac{\phi}{2-\pi}(1-\pi P_c)}{P_c} = B\frac{2-\pi(1-\phi)-\phi y}{2-\pi}$$

where B is a constant independent of θ. Hence, the last term of (B.11) becomes

$$\frac{d}{dg}\left[g\left(2-\pi(1-\phi)-\phi y\right)\right] = 2-\pi(1-\phi)-\phi y + g\phi\frac{\partial H/\partial g}{\partial H/\partial y}$$
$$= \frac{2-\pi(1-\phi)-\phi y}{-\partial H/\partial y}\frac{\pi(1-\phi)((1-\phi)\pi+\eta)}{[((1-\phi)\pi+\eta)-\frac{\phi}{2-\pi}y]^2} > 0.$$

The second line comes from the implicit function theorem, and the third and last lines are due to (B.9), (B.10), and $P_c > P^*$. Thus, we established that $\frac{d\pi_c}{d\theta} > 0$. As well, Vol_c is decreasing in θ, which is immediate from (B.7).

Finally, as for point (iii), we have $\Delta P/\Delta\tilde{\pi} = 1 - Vol_c$ from the market clearing conditions. Since we have

$$\frac{d}{d\theta}\left(\frac{\Delta P}{\Delta\pi}\right) = \frac{\Delta\pi\frac{d\Delta P}{d\theta} - \Delta P\frac{d\Delta\pi}{d\theta}}{(\Delta\pi)^2}$$
$$= \frac{\Delta P}{\Delta\pi}\left(\frac{d\log\Delta P}{d\theta} - \frac{d\log\Delta\pi}{d\theta}\right),$$

we can be easily check that $\frac{d\log\Delta P}{d\theta} - \frac{d\log\Delta\pi}{d\theta} \sim -\frac{dVol_c}{d\theta} < 0$.

Proof of Proposition 2 By (B.7), the transaction value of certified assets becomes

$$V_c = \frac{(1-\phi)\pi P_c^2}{((1-\phi)\pi+\eta)P_c - \frac{\phi}{2-\pi}}.$$

Since the RHS does not directly depend on θ, we have

$$\frac{dV_c}{d\theta} = \frac{dP_c}{d\theta}\frac{dV_c}{dP_c} \propto (\eta+(1-\phi)\pi)P_c - \frac{2\phi}{2-\pi}.$$

Therefore, there is a tipping point:

$$P^{**} = \frac{2\phi}{(\eta+(1-\phi)\pi)(2-\pi)},$$

such that

$$\frac{dV_c}{d\theta} \gtrless 0 \Leftrightarrow P_c \gtrless P^{**}. \tag{B.12}$$

Now, by using $H(P_c^{-1}, g) = 0$ in (B.8) and by the fact that $P_c H(P_c^{-1}, g)$ is monotonically increasing in P_c, the condition (B.12) is identical to

$$A(\theta) \equiv g(1-\pi)\,(2\eta-h) + 2\pi[\phi-(1-\phi)(2-\pi)] \lessgtr 0,$$

where $h \equiv \eta+\pi(1-\phi)$. Since $P_c > P^*$, A is monotonically decreasing in θ. By considering $\theta \in [\theta_0, 1]$, we have the following results.

1. If $\phi > (2-\pi)/(3-\pi)$, then $A(\theta) > 0$ for all $\theta \in [\theta_0, 1]$, which implies that $P_c > P^{**}$ always holds in the equilibrium, leading to a monotonically decreasing V_c.

2. If $\phi \leq (2-\pi)/(3-\pi)$, then $A(1) < 0$. Thus, V_c is decreasing in high-θ regions. To understand more global behavior, we need to check if $A(\theta_0) \gtrless 0$. By seeing A as a function of g, we can define g^* that makes $A(g) = 0$:

$$g^*(\phi) = \frac{2\pi(2-\pi-\phi(3-\pi))}{(1-\pi)(1-\pi(1-\phi)+\frac{\phi\pi}{2-\pi})}.$$

Since $A(g)$ is increasing in ϕ, we have $dg^*/d\phi < 0$. Note that we are focusing on $\theta > \theta_0$, which means

$$g < g_0(\phi) \equiv \frac{1-\theta_0(\phi)}{\theta_0(\phi)}.$$

From the definition of θ_0, θ_0 is decreasing in ϕ, while g_0 is increasing in ϕ. We also have $\lim_{\phi\to 0} g^*(\phi) > 0$ and $\lim_{\phi\to 0} g_0(\phi) = \mathbb{I}_{\{\pi<1/2\}}\pi^{-1}$ because $\theta_0 \to \mathbb{I}_{\{\pi\geq 1/2\}} + \mathbb{I}_{\{\pi<1/2\}}\frac{\pi}{1-\pi}$. Thus, we have following two possibilities:

(a) If $\pi \geq 1/2$, there is a unique $\phi = \phi_0$ that solves

$$g^*(\phi) = g_0(\phi). \tag{B.13}$$

ϕ_0 is uniquely determined from the discussion above. In this case, if $\phi < \phi_0$, then $A(g) < 0$ for all $g < g_0$, meaning that V_c is monotonically increasing in θ. If $\phi_0 < \phi < \phi_1$, then $A(g) \gtrless 0 \Leftrightarrow g \gtrless g^*$. Thus, we can define $\theta^* = 1/(1+g^*) \in (\theta_0, 1]$, such that V_c is increasing when $\theta > \theta^*$ and decreasing when $\theta < \theta^*$.

(b) If $\pi < 1/2$, we have a unique $\pi^* \in (0, 1/2)$ that solves

$$g^*(0) = \frac{2\pi(2-\pi)}{(1-\pi)^2} = \frac{1}{\pi} = g_0(0),$$

or equivalently

$$2\pi^3 - 3\pi^2 - 2\pi + 1 = 0.$$

If $\pi^* \leq \pi < 1/2$, then $g^*(0) > g_0(0)$. This implies that we always have θ^* defined by $\theta^* = 1/(1+g^*) \in (\theta_0, 1]$, and V_c is increasing in θ when $\theta > \theta^*$, while it is decreasing in θ when $\theta < \theta^*$. On the other hand, if $0 \leq \pi \leq \pi^*$, we go back to case **(ii-a)** above, and the same results hold.

B.5 Proof of Lemma 10

$$\begin{aligned} &V_c^{tr}(1) > V_c^{tr}(\theta_0) \\ &\Leftrightarrow \pi(1-\phi)\left(1 + \frac{\phi\pi}{2-\pi}\right) + \theta_0\left[1 + \frac{\phi\pi}{2-\pi} - \pi(1-\phi)\right] - \theta_0^2 > [\pi(1-\phi) + u_1]\left[1 + \frac{\phi\pi}{2-\pi} - u_1\right], \end{aligned}$$

with $u_1 = u(\theta = 1)$. Note that u_1 is the positive solution of

$$0 = \pi[1 + (1-\pi)(1-\phi)]u - \pi(1-\phi)(2-\pi)$$

so that

$$u_1 = \frac{(1-\phi)(2-\pi)}{1 + (1-\pi)(1-\phi)}.$$

Also, θ_0 is the solution of $\theta_0^2(1-\pi) - \theta_0 + \pi(1-\phi) = 0$. Thus, the condition is rewritten as

$$V_c^{tr}(1) > V_c^{tr}(\theta_0) \Leftrightarrow \frac{1}{1-\pi}\left(\frac{1}{2} - \sqrt{\frac{1}{4} - (1-\pi)\pi(1-\phi)}\right) < \kappa$$

with

$$\kappa = \frac{-\frac{\phi(1-\phi)}{2-\pi}\left(\frac{2+\pi(1-\pi)(1-\phi)}{1+(1-\pi)(1-\phi)}\right)^2 + \frac{\pi(1-\phi)}{2-\pi}\frac{(2-\pi)^2+\phi\pi(1-\pi)}{1-\pi}}{\pi\frac{1+(1-\pi)(1-\phi)+(1-\phi)(1-\pi)(2-\pi)}{(1-\pi)(2-\pi)}}.$$

Simplifying κ yields the condition in the lemma.

C Welfare and sellers' fee

C.1 Consumer welfare

The consumers (buyers) obtain the following aggregate trading surplus.

$$\begin{aligned}W &= \int_{\alpha^*}(\Delta\tilde{\pi}\alpha - \Delta P)d\alpha + \int_{P_{nc}/\phi}(\phi\alpha - P_{nc})d\alpha \\ &= \frac{\Delta\tilde{\pi}}{2}(1-\alpha^*)^2 + \frac{\phi}{2}\left(1-\frac{P_{nc}}{\phi}\right)^2 \\ &= \frac{1}{2}\left[\pi(1-\phi)V_c + \frac{\phi}{(2-\pi)^2}(1-\pi+\pi P_c)^2\right],\end{aligned} \tag{C.1}$$

where the second term comes from $\alpha^* = \Delta P/\Delta\tilde{\pi}$, and the last term comes from (B.2), $S_j = D_j$, and the definition of π_c that yield $\Delta\tilde{\pi} = (1-\phi)\frac{\pi P_c}{K_c}$. The property of the first term is given by Proposition 2, while the second term is monotonically increasing in θ since so is P_c. Note that this confirms that (i) the welfare gain term ΔW is

$$\Delta W = \frac{1}{2}\pi(1-\phi)V_c,$$

and (ii) the reservation welfare is given by

$$W_{res} = \frac{\phi}{2(2-\pi)^2}(1-\pi+\pi P_c)^2.$$

As P_c is increasing in θ, so is W_{res}. Thus, this completes the proof of Lemma 7 and points (i) and (ii) in Proposition 3.

Now, we investigate the behavior of welfare W. By using (B.7), we have

$$2W = (1-\phi)^2\pi^2\frac{P_c^2}{P_c[\eta+\pi(1-\phi)] - \frac{\phi}{2-\pi}} + \frac{\phi}{(2-\pi)^2}(1-\pi+\pi P_c)^2.$$

Note that θ does not directly affect W in this expression. By letting $h \equiv \eta + \pi(1-\phi)$, we have

$$2\frac{dW}{dP_c} \equiv W_P = (1-\phi)^2\pi^2 P_c\frac{hP_c - 2\frac{\phi}{2-\pi}}{\left(hP_c - \frac{\phi}{2-\pi}\right)^2} + 2\phi\pi\frac{1-\pi+\pi P_c}{(2-\pi)^2}.$$

The second order derivative yields

$$\begin{aligned}\frac{dW_P}{dP_c} \equiv W_{PP} &= \frac{2((1-\phi)\pi)^2}{(hP_c - \frac{\phi}{2-\pi})^3}\left[\left(hP_c - \frac{\phi}{2-\pi}\right)^2 - hP_c\left(hP_c - \frac{2\phi}{2-\pi}\right)\right] + \frac{2\phi\pi^2}{(2-\pi)^2} \\ &= \frac{2((1-\phi)\pi)^2}{(hP_c - \frac{\phi}{2-\pi})^3}\frac{\phi^2}{(2-\pi)^2} + \frac{2\phi\pi^2}{(2-\pi)^2} > 0.\end{aligned}$$

We also have $P_c|_{\theta=1} \equiv P_{c,1} = \frac{1}{h}\left(1-\phi+\frac{\phi}{2-\pi}\right)$ and $W_P(P_{c,1}) > 0$. Thus, if $\lim_{\theta\to\theta_0} W_P < 0$, there is a unique θ^* such that $W_P \gtrless 0 \Leftrightarrow \theta \gtrless \theta^*$, while if $\lim_{\theta\to\theta_0} W_P > 0$, then $W_P > 0$ for all θ.

The following formulas at $\theta = \theta_0$ simplify the analyses. Because the economy is continuous at $\theta = \theta_0$, by letting $\theta \searrow \theta_0$, we have

$$P_{nc,0} \equiv P_{nc}(\theta = \theta_0) = \frac{\phi}{2-\pi}[1-\pi P_c(\theta_0)] = (1-\theta_0)P_c(\theta_0), \tag{C.2}$$

$$\therefore P_{c,0} \equiv P_c(\theta_0) \equiv \frac{\phi}{\pi\phi + (1-\theta_0)(2-\pi)}. \tag{C.3}$$

Moreover, at $\theta = \theta_0$, we have $\beta_L = 0$ by definition. Since the markets have to clear, we have

$$\begin{aligned}
\lim_{\theta \searrow \theta_0} D_c &= \lim_{\theta \searrow \theta_0} \left(1 - \frac{P_c - P_{nc}}{\pi_c(1-\phi)}\right) = \lim_{\theta \searrow \theta_0} \left(1 - D_{nc} - \frac{P_{nc}}{\phi}\right) \\
&= \lim_{\theta \searrow \theta_0} \left(1 - (1-\pi)\beta_L - \frac{P_{nc}}{\phi}\right) \\
&= 1 - \frac{1-\theta_0}{\phi} P_{c,0} = \frac{1 - \pi + \pi P_{c,0}}{2-\pi}
\end{aligned} \tag{C.4}$$

The first line is the definition, the second line comes from the definition of D_{nc}, the third line is from the market clearing condition for uncertified assets, and the fourth and fifth lines are from the definition of θ_0 that gives $\beta_L = 0$ and (C.2). The last line exploits the other expression from (C.2). Also, from (B.7),

$$\lim_{\theta \searrow \theta_0} Vol_c = \frac{(1-\phi)\pi P_{c,0}}{\left[(1-\phi)\pi + \eta\right] P_{c,0} - \frac{\phi}{2-\pi}}. \tag{C.5}$$

By the market clearing conditions, all of these expressions, i.e., (C.4) and (C.5), have to be identical. That is

$$\frac{(1-\phi)\pi P_{c,0}}{h P_{c,0} - \frac{\phi}{2-\pi}} = 1 - \frac{1-\theta_0}{\phi} P_{c,0} = \frac{1 - \pi + \pi P_{c,0}}{2-\pi}. \tag{C.6}$$

Let $W_{P,0} \equiv \lim_{\theta \searrow \theta_0} W_P$. By using the first equality in (C.6),

$$W_{P,0} \propto (1-\phi)\pi \left(1 - \frac{\frac{\phi}{2-\pi}}{h P_{c,0} - \frac{\phi}{2-\pi}}\right) + \frac{2\phi\pi}{2-\pi}.$$

By using (C.6) once again, we also have $h P_{c,0} - \frac{\phi}{2-\pi} = \frac{(1-\phi)\pi P_{c,0}}{1 - \frac{1-\theta_0}{\phi} P_{,c0}}$. Thus,

$$\begin{aligned}
W_{P,0} &\propto (1-\phi)\pi \left(1 - \frac{\phi}{2-\pi} \frac{1 - \frac{1-\theta_0}{\phi} P_{c,0}}{(1-\phi)\pi P_{c,0}}\right) + \frac{2\phi\pi}{2-\pi} \\
&\propto 1 + (1-\pi)(\theta_0 - 2\phi).
\end{aligned}$$

Note that θ_0 is a decreasing function of ϕ, and $\lim_{\phi \to 1} \theta_0 = 0$. Then, $\min_\phi W_{P,0} = 2\pi - 1$. Therefore, if $\pi < \frac{1}{2}$, we can define a unique $\phi = \phi_2$ that solves

$$1 + (1-\pi)(\theta_0 - 2\phi) = 0.$$

If $\phi \leq \phi_2$ or $\pi > 1/2$, on the other hand, $W_P > 0$ for all $\theta \in (\theta_0, 1]$. Thus, W is monotonically increasing in θ. Finally, if $\pi \leq 1/2$ and $\phi > \phi_2$, then there is a unique θ^{**} such that $W_P \gtrless 0 \Leftrightarrow \theta \gtrless \theta^{**}$, meaning that W is U-shaped. Note that this completes the proof of point (iii) in Proposition 3.

C.2 Producer welfare

The welfare of producers (sellers) hinges on the quality of assets endowment that they are allocated upon their arrival at the economy. The aggregate welfare of H- and L-type sellers are defined as

$$
\begin{aligned}
W_H &= \int_{P_c} \beta d\beta + \int^{P_c} P_c d\beta, \\
W_L &= \int_{\frac{P_c}{\phi}} \phi\beta d\beta + \int_{\beta_L}^{\frac{P_c}{\phi}} ((1-\theta)P_c + \theta\phi\beta) d\beta + \int^{\beta_L} P_{nc} d\beta.
\end{aligned}
$$

In both expressions, the first term is the welfare of sellers who voluntarily consume their own assets, while the second term is the welfare of sellers who sell their assets with certifications. The last term of W_L comes from the L-type sellers who do not attempt to obtain certification.

It is easy to check the following proposition:

Corollary 5. *Welfare of H-type sellers W_H is monotonically increasing in θ.*

Higher reliability always benefits sellers of high-quality assets because they can sell at a higher price P_c for sure. On the other hand, we obtain the following local result for L-type sellers:

Corollary 6. *The perfect quality certification cannot achieve the maximum welfare for L-type sellers, i.e.,* $\left.\frac{dW_L}{d\theta}\right|_{\theta=1} < 0$.

Proof. See Appendix C.2. □

Together with Corollary 5, this implies that welfare of L-type sellers cannot agree with H-type sellers regarding the optimal reliability θ.

Welfare gain and reservation welfare As in the case of consumer welfare, we can rewrite producer welfare by the reservation welfare and the welfare gain terms. If a seller has no access to certification, she expects to have the following *ex-ante* utility (i.e., before her endowment is realized):

$$
W_{sell,res} = \pi W_{H,res} + (1-\pi) W_{L,res}
$$

where $W_{i,res}$ represents the reservation welfare of i-type sellers with $i \in \{L, H\}$. Specifically,

$$
W_{i,res} = \begin{cases} \int_0^{P_{nc}} P_{nc} d\beta + \int_{P_{nc}}^1 \beta d\beta & \text{for } i = H \\ \int_0^{\frac{P_{nc}}{\phi}} P_{nc} d\beta + \int_{\frac{P_{nc}}{\phi}}^1 \phi\beta d\beta & \text{for } i = L. \end{cases}
$$

Note that $W_{i,res}$ represents the expected trading surplus that a seller would obtain if she does not have access to the certified assets.

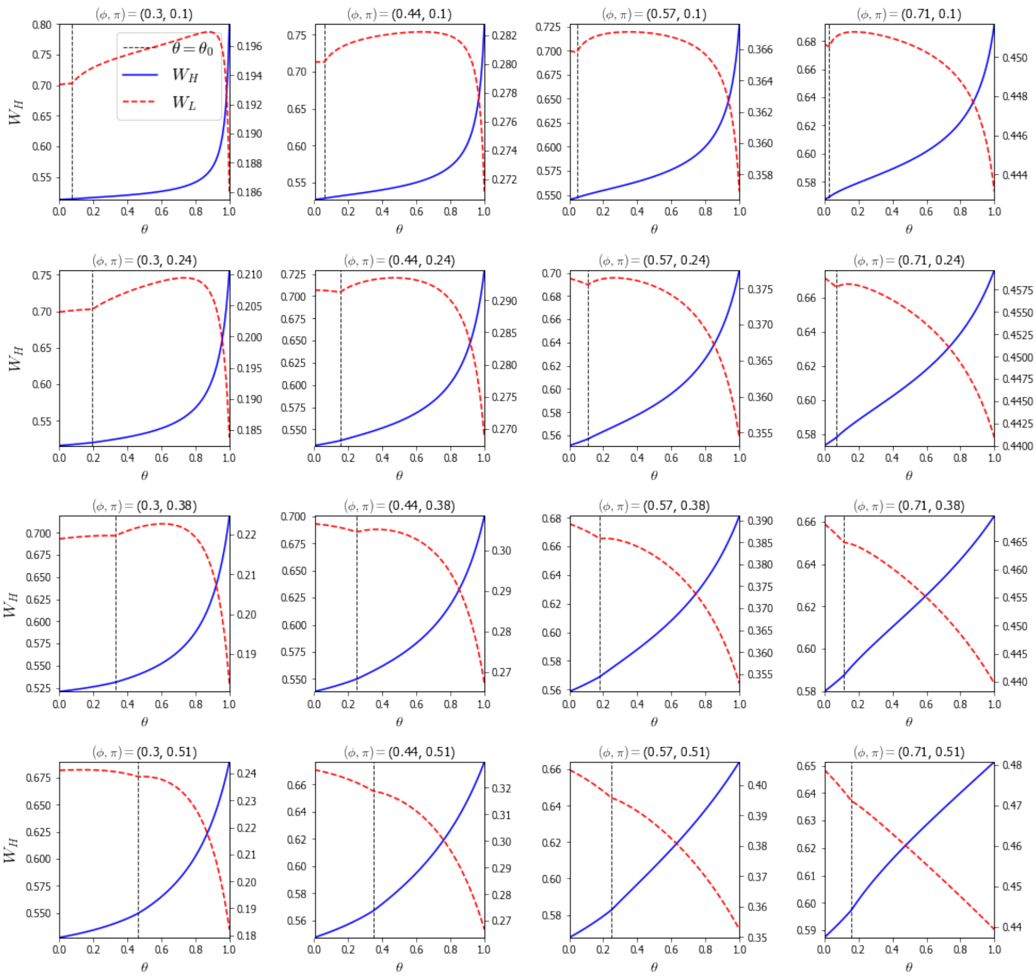
Also, the expected welfare gain from having access to the quality certification is given by

$$
\begin{aligned}
\Delta W_{sell} &= W_{sell} - W_{sell,res} \\
&= \pi \Delta W_H + (1-\pi) \Delta W_L.
\end{aligned} \tag{C.7}
$$

By applying the uniform assumption, we obtain the following simple formulae:

$$
\Delta W_i = \begin{cases} \frac{1}{2}(P_c^2 - P_{nc}^2) & \text{for } j = H \\ (1-\theta)\frac{\Delta P^2}{2\phi\theta} & \text{for } j = L \text{ and } \theta \geq \theta_0, \\ \frac{1-\theta}{2\phi}\Delta P^2 + \frac{\theta}{2\phi} P_{nc}^2 & \text{for } j = L \text{ and } \theta < \theta_0. \end{cases} \tag{C.8}
$$

Figure VI: Producer welfare after asset endowment



ΔW_H is monotonically increasing in θ due to the positive reaction of P_c.

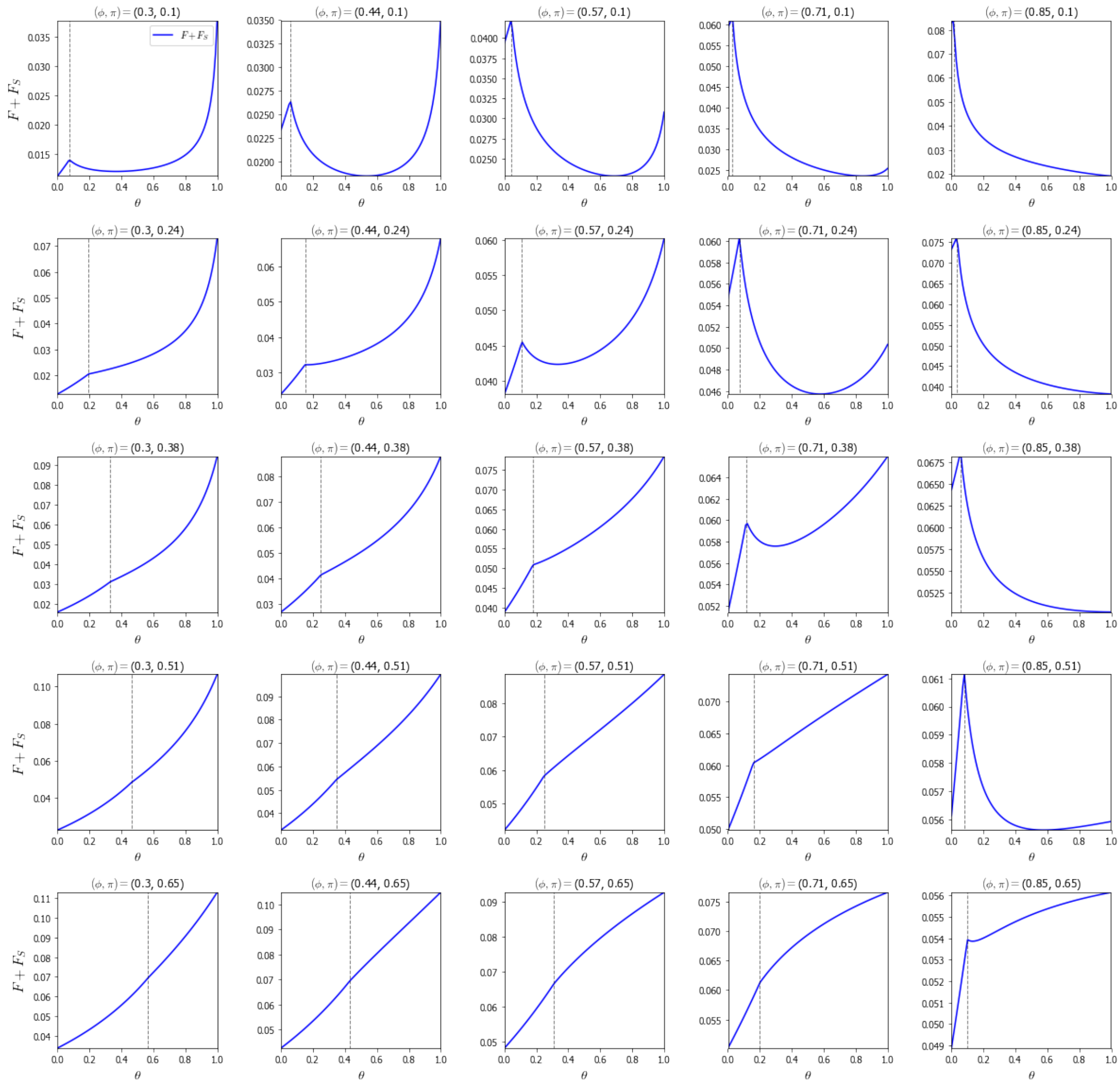
Since the behavior of other variables are hard to analyze, we provide numerical illustrations in Figure VI.[26] It shows that W_H is monotonically increasing in θ, while W_L can be hump-shaped. This is due to the two competing effect of θ on W_L. Firstly, it increases the price of certified assets P_c, which has a positive impact on W_L. However, a higher θ renders it more difficult for L-type sellers to obtain quality certification, thereby reducing W_L. As Figure VI shows, W_L tends to have an upward-sloping region when parameters (π, ϕ) are small. When π is small, a marginal increase in θ has a large negative impact on the composition of the certified assets and causes a substantial increase in the price P_c. As well, a small ϕ makes consumers less likely to switch from certified asset to uncertified asset, helping P_c with increasing. Thus, both of small ϕ and π tend to make the positive impact of θ dominant and leads to an upward-sloping W_L.

Sellers' fee and robustness of main model Suppose that the sellers also must pay the *ex-ante* fee F_S to obtain access to quality certification. By the same logic as the buyers' fee, the equilibrium sellers' fee is

$$F_S = \pi \Delta W_H + (1 - \pi)\Delta W_L.$$

[26] Parameter values (π, ϕ) are truncated for the figures in this appendix but extending them to the entire support $[0, 1] \times [0, 1]$ does not change the results.

Figure VII: Total fee: $F + F_S$



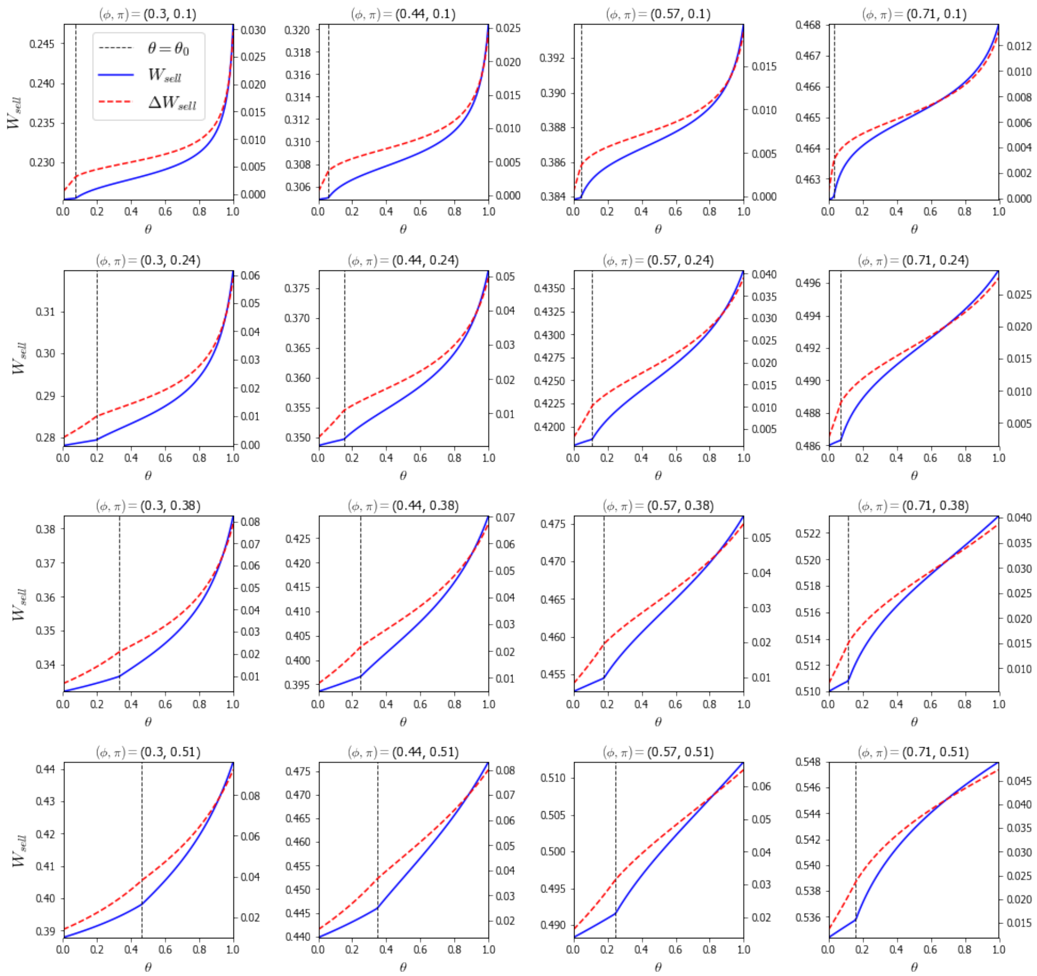
Therefore, F_S represents the additional trading surplus generated by the introduction of quality certification.

To check the robustness of our main results, Figure VII shows the behavior of the total fee $f = F + F_S$. As shown in the main model, the total fee f can be monotonically increasing when (π, ϕ) are small, N-shaped when they are intermediate, and hump-shaped when they are large. This result comes from the non-monotonic behavior of F, and the general equilibrium θ^*, as well as the CRK's optimal θ^*_C, behaves in the same manner as in the main model. Finally, Figure VIII checks that the aggregate producer welfare W_{sell} is monotonically increasing in θ, making the main model's discussions on the welfare robust to inclusion of the welfare of producers.

D Uniqueness of the general equilibrium

Figure IX illustrates the parameter regions in which the fixed point problem $V_c^{tr}(\theta) = V_c^{rc}(\theta)$ has a unique stable solution. The black region in each panel represents parameters (π, ϕ, τ, ρ) that violate the non-negativity constraint in the equilibrium monitoring intensity ($\lambda^* > 0$). The shaded

Figure VIII: Ex-ante producer welfare and welfare gain



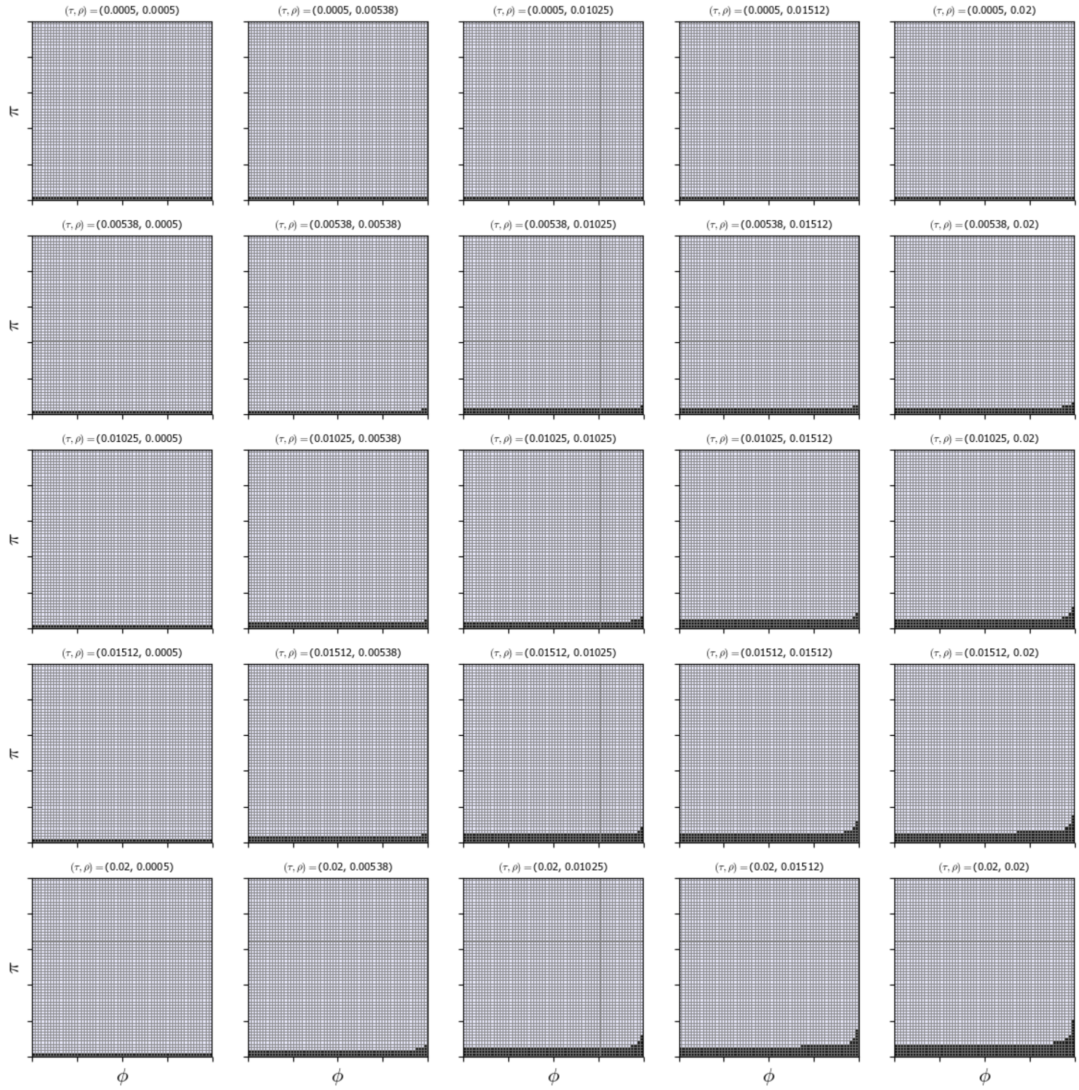
regions represent the parameter regions in which the fixed point problem has a unique solution.

In this figure, (i) we search for the possible solutions by exploiting the grid-search method. We first search for it by ascending θ from $\theta = 0$, while the second search descend θ from $\theta = 1$. We make it cover all $\theta \in [0, 1]$. Then, (ii) we define the absolute difference between possible solutions. If the difference is smaller than a certain criteria, which we set 10^{-6}, we define the solution is unique.

E Decentralized versus centralized monitoring: comprehensive analysis

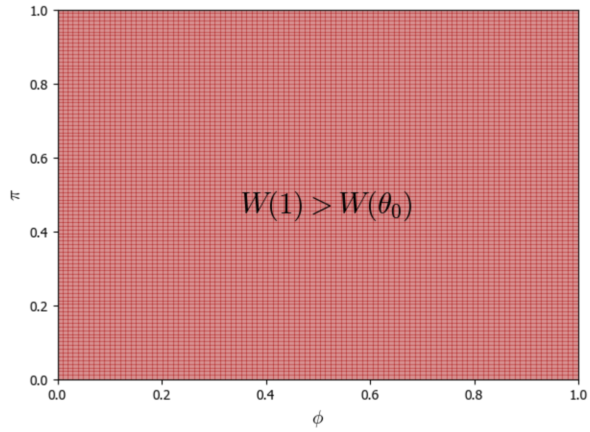
Figures XI and XII show the results for $V(\theta_C^*) \gtrless V(\theta^*)$ and $W(\theta_C^*) \gtrless W(\theta^*)$ with different values of τ. We set $\rho = 0.05$ for the figures but it does not affect the results because only $\rho\tau$ matters for the equilibrium. The white region in Figure XII represents the parameters that makes $(\pi, \phi) \notin \mathcal{P}$ and $W(\theta_C^*) > W(\theta^*)$, and the black region represents the "no-solution" regions that violate the non-negativity constraint on λ^*.

Figure IX: Uniqueness of the solution



Note: This figure shows the results of numerical experiments that test the uniqueness of the fixed-point solution. Parameters (ϕ, π) covers $[0,1] \times [0,1]$ with the grid interval = $1/1000$. Parameters (τ, ρ) fluctuate in $[0.0005, 0.02] \times [0.0005, 0.02]$ woth the grid interval = 0.2.

Figure X: Parameter values for $W(1) > W(\theta_0)$



Note: The shaded area implies $W(1) > W(\theta_0)$.

Figure XI: $V(\theta^*) \gtrless V(\theta^*_C)$ with $\tau > 0$

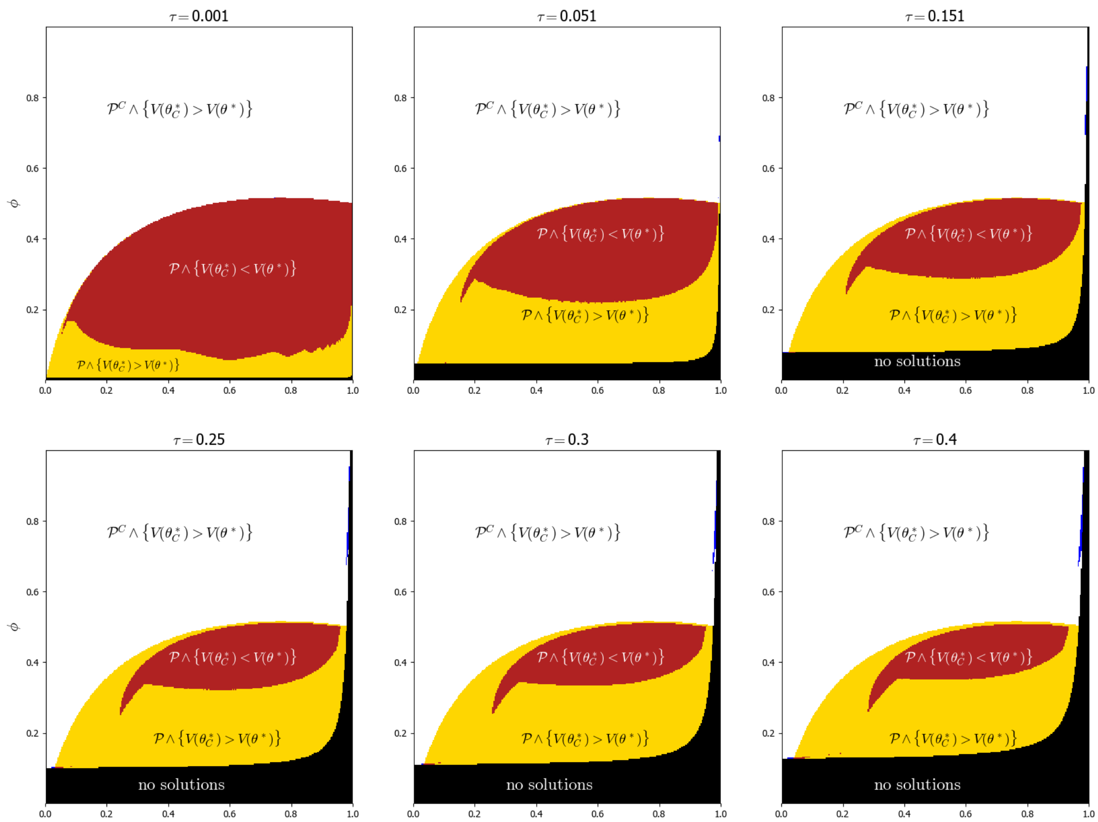


Figure XII: $W(\theta^*) \gtrless W(\theta^*_C)$ with $\tau > 0$