Economic Implications of Blockchain Platforms

Jun Aoyagi* Daisuke Adachi†

March 1, 2019

Abstract

The blockchain protocol mitigates information friction in transactions. As a new trading platform, the blockchain triggers the differentiation of traders, reconfigures the asymmetric information, and generates spreads in asset price and quality between itself and traditional platform. We show that a more efficient blockchain has non-monotonic effects on the trading value in the blockchain platform, the price of cryptocurrency, and consumers' welfare due to general equilibrium effects. Moreover, a platform proposer has an incentive to set blockchain parameters lower than the first best when the underlying information asymmetry is not severe, leading to welfare loss for consumers.

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

Keywords: blockchain, smart contract, cryptocurrency, asymmetric information, FinTech, market structure, two-sided markets.

*Corresponding author. University of California at Berkeley, Department of Economics. E-mail: jun.aoyagi@berkeley.edu, tel: (510) 541-3046. 610 Evans Hall, Berkeley, CA 94720.

†Yale University, Department of Economics. E-mail: daisuke.adachi@yale.edu. 28 Hillhouse Avenue, New Haven, CT 06511.

This paper was initially circulated under the title "Fundamental Values of Cryptocurrencies and Blockchain Technology." We gratefully acknowledge that Christine Parlour gave us invaluable guidance. We also appreciate the constructive comments from Kosuke Aoki, Gadi Barlevy, Will Cong, Shin-ichi Fukuda, Wei Jiang, Xuelin Li (discussant), Giuseppe Perrone, Fahad Saleh, Susumu Sato, Yoko Shibuya, Katrin Tinn (discussant), Harald Uhlig, Noriyuki Yanagawa, and Yingge Yan, and from the seminar participants at the GSU/RFS Fin- Tech Conference, SWET, UC Berkeley, the University of Tokyo, and the Wharton School; we are grateful to Claire Valgardson for copy editing. We also thank Hideaki Kajiura and EY Advisory & Consulting for sharing their data and experience from their wine blockchain project. This research was financially supported by the Berkeley Blockchain Initiative Fund by Ripple.

1 Introduction

> "The technology best known as the record-keeping system behind cryptocurrencies seems poised to play a broader role in business, where it could change how supply chains work."—*Wall Street Journal*, February 6, 2018.

The blockchain can significantly improve the efficiency of transactions because of its decentralized, immutable public information management system and a protocol to implement *a smart contract*—one that is executed automatically based on specified conditions without any centralized authorizations (Szabo, 1997).

Behind the recent hype about the blockchain is the increasing demand of consumers to know more about what they purchase (i.e., its origin and history) because the value and quality of an item cannot be separated from its provenance. For example, in a traditional food supply chain, the record-keeping processes are centralized and involve massive amounts of manual paperwork, making it difficult to keep track of information on products and encouraging counterfeiting. As a result, there is a high risk of asymmetric information, and *centralized* third parties, such as banks, professional quality certifiers, insurance providers, and central securities depositories, work as intermediaries to offload the risks. As we show in Section 2.2, the blockchain can be seen as a new form of quality certification that is more efficient and reliable than the traditional one due to its *decentralized* nature. To exploit these features, a growing number of institutions have adopted the blockchain protocol to facilitate the exchange of assets, products, and information, leading to the coexistence of blockchain-based transactions with traditional centralized ones.[1]

The purpose of this paper is to investigate the *general equilibrium effects* of the blockchain adoption. We consider a simple exchange economy with asymmetric information on assets quality. Trade can be executed by the blockchain or the traditional cash-based platform, and

[1]For example, many blockchain-based trading platforms have been launched, such as those for foods (EY Advisory & Consulting, Walmart), jewelry (HyperLedger), arts and photography (Kodac), security (tZero), and cryptocurrency (Waves, IDEX, Steller, Oasis, OKEx, Cashaa, and more).

this coexistence of platforms triggers differentiation (c.f., Tirole, 1988) because competitive sellers and buyers decide what type of transaction protocol (or platform) to use to exchange assets. If trade occurs on the blockchain (the B-market), buyers receive a signal on the quality of assets, which is more reliable than the one in the traditional platform (the C-market) due to the decentralized nature of the blockchain.[2]

Our main results are as follows. First, a more reliable signal in the B-market is amplified by a general equilibrium effect: the signal quality affects the incentive of sellers to participate in the B-market and endogenously improves the average assets quality. Second, we show that the dollar value of trade in the B-market is non-monotonic in the B-market's signal quality. Also, this value corresponds to the consumer surplus generated by the blockchain and the price of cryptocurrency. This link arises because the endogenous choice of trading platforms by the continuously heterogeneous consumers ensures that only a subset of them, who can make positive surplus, participate in the B-market.

The non-monotonicity is important because it implies that consumer welfare and the price of cryptocurrency may decrease when the blockchain becomes marginally more efficient and provides a higher quality signal. This comes from two competing effects in the general equilibrium: the more efficient quality certification by the blockchain leads to a higher price and quality of assets, but it reduces the trading volume. If the latter outweighs the increase in the price, the negative results arise.

The B-market's trading volume falls due to the general equilibrium effect. A more efficient quality certification is achieved by rejecting a larger number of low-quality assets, and so it reduces the supply amount in the B-market (*the supply-side effect*). This quality improvement, however, makes buyers more willing to participate in the B-market and increases the demand (*the demand-side effect*). To clear the B-market, the price must increase substantially: not only does it push the enhanced demand back to the original level by killing the demand-side effect, but it also dampens demand even more to offset the supply-side effect. Thus, the

[2]In the following, we use terms "reliability," "quality of signal," and "efficiency of the blockchain" interchangeably.

increase in the price outweighs the quality improvement, and buyers—facing a price-quality tradeoff—migrate out of the B-market to the C-market, thereby reducing the equilibrium B-market's trading volume. We show that this negative reaction is strong when the primitive asymmetric information is *not* severe, because switching to the C-market becomes less costly and it enhances migration. This implies that the consumers' trading surplus is more likely to shrink due to a more efficient blockchain when information friction is not severe.

Importantly, the non-monotonic reaction arises due to the coexistence of the blockchain protocol with the traditional one. Without the C-market, the B-market consumers' alternative option would be to refrain from trading. The traditional protocol serves as a buffer and generates strong incentives for B-market consumers to migrate to the C-market, thereby creating a negative reaction of the trading value in the B-market.

In light of the possible negative welfare consequence of increasing the efficiency of the blockchain, we also consider an *ex-ante* platform fee and how much consumers would pay to obtain access to the B-market. Access to the blockchain platform generates a strictly positive extra gain for consumers, which makes them willing to pay the fee. This can be seen as the equilibrium vale added of blockchain technology. This fee has the same implications as the trading value in the B-market and, due to its non-monotonicity, a more efficient blockchain can reduce the technology's value as a trading platform. In this situation, we show that a "proposer" of the blockchain parameters, introduced by Abadi and Brunnermeier (2018), has an incentive to keep the efficiency level of the blockchain lower than the first-best level for consumers because of the non-monotonic value effect.[3]

While our paper is theoretical, we propose several testable implications. First, the non-monotonic effect of the blockchain's efficiency predicts the consequences of a "fork" in the blockchain. In practice, a fluctuation of the efficiency level of the blockchain stems from a change in the rule of consensus formation (e.g., openness of the blockchain, the size of a block, the difficulty target, and so on), and it typically involves a fork. That is, given the nature of a

[3]This is consistent with the literature on strategic management (Teece, 1986; Brandenburger and Stuart Jr, 1996) arguing that a firm may not adopt innovation even though it improves consumers' welfare.

fork—an upgrade or downgrade of the efficiency—we can predict its impact on the subsequent transaction activity and the cryptocurrency price, which depends on the severity of asymmetric information. Moreover, our model suggests that a proposer is more likely to keep the efficiency level lower than the consumers' first best when asymmetric information is not severe. This implies that some government policies that promote the blockchain innovation can effectively enhance consumers' surplus.

After reviewing the related literature, Section 2 provides an overview of the blockchain technology and develop a microfoundation of the "efficiency" and signal of the blockchain. Section 3 introduces the general equilibrium model, while Section 4 analyzes comparative statics to understand the effect of higher efficiency in the blockchain technology. In Section 5, we propose our empirical hypotheses and policy implications, and Section 6 concludes the discussion.

1.1 Literature Review

The research on blockchain technology and cryptocurrencies (or FinTech, in general) is expanding (see Harvey, 2016 for a comprehensive review). First, viewing the blockchain protocol as a new trading platform is widely accepted. Bartoletti and Pompianu (2017) provide empirical evidence for the usage of the blockchain and the smart contract as a platform. Chiu and Koeppl (2017, 2018) analyze the optimal design of the blockchain to guarantee "Delivery vs. Payment" by considering an economy with an intertemporal risk of settlement. Cong, Li and Wang (2018a) develop a model in which the demand and price dynamics of tokens (cryptocurrency) are driven by the size of the blockchain as a platform and its trading needs.[4] Abadi and Brunnermeier (2018) consider the platform selection of blockchain users and record keepers with network externality.

The blockchain can affect consumers' welfare through many channels. According to Cong and He (2018), its reduction of asymmetric information promotes the entrance of firms and

[4]Other papers that investigate the price of cryptocurrency by focusing on the unique features of the supply side and network effect include Pagnotta and Buraschi (2018) and Schilling and Uhlig (2018).

improves consumers' welfare at the risk of collusion. Malinova and Park (2017) are concerned about the risk of front-running and compare the possible degrees of transparency of the private blockchain.[5] Khapko and Zoican (2016) focus on the optimal duration of the transactions under counterparty risk and search friction. Tinn (2018) specifies the optimal contract when it can be dynamically adjusted contingent on a sequence of time-stamped cash flow based on the smart contract.[6]

Our model agrees with these studies that the blockchain essentially reduces the transaction cost by mitigating informational problems. However, our economy, in which buyers face *ex-ante* quality uncertainty, highlights how the blockchain endogenously reconfigures information asymmetry via quality differentiation and platform segmentation—both of which are not analyzed in the literature—and how it affects the value of the blockchain platform and consumers' welfare through the general equilibrium effect. Specifically, the non-monotonic effect of the blockchain efficiency, driven by the coexisting protocols, is novel: for example, Cong and He (2018) show that it is monotonic in a single-market environment.

The second strand of the literature, which emerged from Akerlof (1970), examines adverse selection. Authors such as Kim (2012), Guerrieri and Shimer (2014), and Chang (2017) show that market segmentation leads to quality differences across markets.[7] We see the blockchain as a new platform for trade, which exists alongside the traditional cash market, and analyze the effect of segmentation in the context of FinTech. Unlike the literature, in which the markets are homogeneous *per se*, our analyses propose that the different structure of one market (e.g., the degree of efficiency) affects the entire economy. Also, we do not rely on the strategic motive (e.g., signaling effect) of traders, as we focus on an economy with fully atomistic agents (as in

[5] Users of blockchains can make the network private and limit information transactions within a firm or a group of firms. This category of platforms is called a "closed-type" or "permissioned" blockchain. The public blockchain, in contrast, is called "open-type" or "permissionless."

[6] The feasibility of implementing the blockchain is another hot topic. For example, Biais et al. (2018) consider "the folk theorem" of the blockchain as a coordination game, and Aune, O'Hara and Slama (2017) propose the hash-based protocol to address the issue that stems from miners' incentive to delay the publication of the block.

[7] Another dimension of segmentation is time, i.e., participants can decide when to trade, as analyzed by Fuchs, Green and Papanikolaou (2016), Asriyan, Fuchs and Green (2017), and Fuchs and Skrzypacz (2017).

Kurlat, 2013), and show that non-monotonic results arise even in the competitive environment.[8]

Our paper is also related to the literature in IO that explores endogenous market structures and platform competition with two-sided markets. These topics have been analyzed by Foucault and Parlour (2004), Rochet and Tirole (2006), Damiano and Hao (2008), Ambrus and Argenziano (2009), and Gabszewicz and Wauthy (2014), although they do not study asymmetric information in the form of asset quality uncertainty. Yanelle (1997) and Halaburda and Yehezkel (2013) consider competing platforms under asymmetric information, though they focus on the information asymmetry *between the platform and agents*. In line with these works, our new platform can control the asymmetric information *among agents*, while she does not incorporate some types of externality due to the general equilibrium effects.[9]

Finally, the idea of the blockchain as a record-keeping method that competes with cash is reminiscent of the concept of "money as memory." How money and credit can substitute for each other or coexist has been explored by Kocherlakota (1998), Kocherlakota and Wallace (1998), Lagos and Wright (2005), Rocheteau and Wright (2005), Camera and Li (2008), and Gu, Mattesini and Wright (2014). However, credit as an alternative payment method does not affect the quality of the assets traded because it remains a record of a debtor, not of an asset's quality. Thus, the market segmentation in the literature is intertemporal (e.g., day and night).[10] As some evidence in Section 5.2 suggests, however, the blockchain platform triggers market segmentation even in a static environment. At the same time, its the decentralized record-keeping system is the critical factor that differentiates the blockchain from the traditional centralized system (see the next section).

[8]See Voorneveld and Weibull (2011) for a model with bilateral strategic trading and two-sided uncertainty in a single market environment.

[9]More broadly, a different efficiency level of the blockchain θ in a market with asymmetric information can be interpreted as government intervention, such as the purchase of assets on OTC after the recent financial crisis. Most models of government intervention do not consider the interaction of segmented markets. See, for example, Philippon and Skreta (2012), Tirole (2012), and Chiu and Koeppl (2016).

[10]A decentralized market comes first to make some credit, and a centralized one comes afterwards to settle repayment.

2 The Blockchain as Quality Certification

In general, the value and quality of assets significantly depend on their provenance and transaction histories. However, information above is hard to track, exposing consumers to quality uncertainty.

In the following, we provide a detailed example to specify the problem and how a blockchain may solve it. We choose this example because it fits the model in Subsection 2.2, and the blockchain-based transactions in this field have been already adopted in practice. Other real-world examples can be applied by modifying our microfoundation model.

2.1 Wine Supply Chain

In the wine industry, counterfeiting accounts for roughly 5% of the current secondary market, which amounts to $15 billion worldwide.[11] One of the most prevalent types of fraud is the relabeling of cheaper wines as expensive and high-quality ones. Provenance can be opaque, as the wine supply chain involves many steps: it starts from a vineyard and goes through wine producers, distributers, transit cellars, fillers/packers, wholesalers, and retailers. The quality of wine is affected by conditions in each step, such as storage temperature and time lapse. Throughout the process, data is retrieved manually, and recorded in a centralized database. Record keeping is difficult and costly since data can easily be forged and reproduced. See Biswas et al. (2017) for details.

Many technologies have been adopted to enhance traceability and automate the process: Barcode Radio Frequency Identification (RFID), Quick Response (QR) codes, Electronic Product Codes (EPCs), and so on. They can be analyzed in the same context of the blockchain innovation in our main model, but all of these technologies are adopted in a *centralized* manner, so that the record is easily reproduced.

[11] *Sour Grapes* (2016) is a non-fiction American film about wine fraudster Rudy Kurniawan. He was known as a discerning Burgundy collector and sold countless bottles of fake wine.

2.2 Overview of the Blockchain Technology

The blockchain can be seen as a novel way of managing and tracking transaction information. In the traditional world, we typically maintain a ledger that records participants' state information in a centralized manner, e.g., a bank acts as an intermediary. Bilateral transactions with no intermediation by a credible third party incur the risk of adverse selection due to asymmetric information or settlement risk.

In contrast, on the blockchain platform, 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* requires the information about the state of the economy to be a consensus among all participants. A consensus mechanism determines what data should be recorded as true and what should be rejected as fraudulent. This highlights its first difference from traditional transactions, in which only a centralized authority keeps track of the state information.

Moreover, Ethereum allows complex scripts to be written to describe the conditions under which the information is verified and recorded, which implies that a transaction takes place only if the conditions in the code are fulfilled (i.e., it is state contingent). This is the crucial aspect that differentiates the blockchain from the credit system (or credit cards) as a record-keeping method, since the latter is not responsible for the actual transfer and quality of goods, while both of them are automatically guaranteed on Ethereum.[12]

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 add a new block to the chain. Therefore, if a malicious agent attempts to add fraudulent information to the

[12] A warranty is an example of a similar system to the blockchain. Even though warranties guarantee the quality of products, they have two main differences. First, warranties are provided and executed only if the product is transferred and the *ex-post* quality is verified, while the smart contract transfers the product only if the quality is guaranteed. Second, the execution of warranties comes at a significant cost for consumers, while the smart contract never requires consumers to take the cost because making a transaction serves as a quality certification. See, for example Lehmann and Ostlund (1974) and Palfrey and Romer (1983).

transaction history, she must outpace all miners in the network, which requires prohibitively high computing power.[13]

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.[14] 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 details on Bitcoin and blockchain implementation.

2.2.1 Oracle Problem

Note that the two main factors that determine the traceability (or final quality) of goods are (i) the external data-generating process and (ii) the internal flow of information. For example, suppose that a wine producer and a grape firm agree on a smart contract that states, "The producer purchases raw material if and only if the grape is of grade X." To generate a transaction, data regarding grape quality (say, random $\tilde{X}$) must be observed and brought into the blockchain network. This process is point (i) and may involve the certification of the realized value of $\tilde{X}$. On top of that, after the transaction is executed, it is possible that the wine producer deliberately forges the document and claims that the ingredient is of grade Y. This manipulation refers to point (ii).

The decentralized nature of the blockchain makes it extremely difficult to rewrite X as Y on the blockchain after X is recorded. However, data from outside the blockchain network can be doubtful because the blockchain takes it as given. Namely, the grape firm can misreport that

[13] There are several ways to reach a consensus, and different blockchains adopt different processes. Chiu and Koeppl (2017) provide a theoretical comparison of the efficiency of these methods.

[14] For example, if the state of the transactions up to t is denoted by $s^t = (s_{t-1}, \cdots, s_0)$, a block at t records the information of the transactions at t and the encrypted historical states, $S_t = (s_t, h(s^t))$, where h is a hash function. Now, the next block at $t+1$ records $S_{t+1} = (s_{t+1}, h(S_t))$, etc. If an agent wants to rewrite the past state s_k to s'_k, then she must change all the blocks $S_k, S_{k+1}, \cdots, S_t$ because this attempt induces a change in S_k, which triggers a change in S_{k+1} because $h(S_k)$ with s_k is not identical to that with s'_k, and so on.

its grape is of grade X even though the true grade is $\tilde{X} = Z$. This is called the "oracle problem," and is related to the credibility of the traditional quality certification technologies. We abstract away from it in our main model to focus on the effect of efficiency brought by the blockchain technology.

2.3 Microfoundation of the Blockchain Efficiency

A parameter $\theta \in (0, 1]$ is used to describe how the blockchain is more efficient than the traditional protocol in mitigating asymmetric information. We can think of the following discussion as the microfoundation of θ in our main model in Section 3. We borrow and modify the trade-finance example that Cong and He (2018) propose.

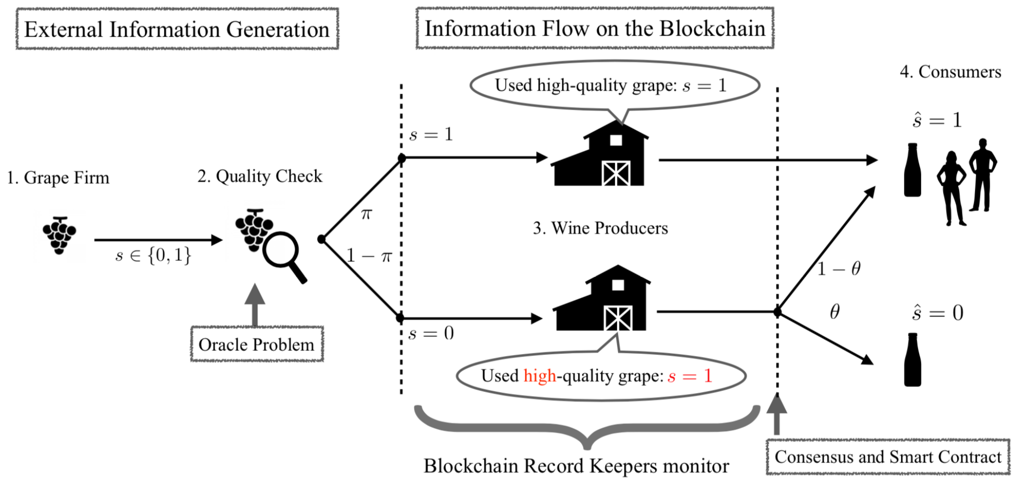
As Cong and He (2018) suggest, the consensus formation is decentralized, as none of the participants in the blockchain has complete control over it. On the other hand, once we introduce an agent who proposes a rule of the blockchain platform, each participant's incentive to participate and tell the truth is affected because the cost of participation (e.g., required computing power and difficulty target), the number of participants who are contacted (e.g., the openness of the chain), and the fraction of supply-chain intermediations that go through the blockchain. Following Abadi and Brunnermeier (2018), we call this agent a "proposer."

2.3.1 Environment

There are sellers (producers) and buyers that trade a good, for example, a bottle of wine. For simplicity, we consider only a couple of intermediation steps and suppose that the quality of the wine is summarized by a stochastic state s, which is determined by the nature (a grape firm), as described by step1 of Figure I. The quality of the grape is identified by a certifier and turns out to be either high ($s = 1$) or low ($s = 0$) with $\Pr(s = 1) = \pi$ (step2 in Figure I). For simplicity, assume that each seller is randomly assigned grapes and obtains utility U_S if the bottle is sold to customers (U_S is endogenized in the main model in Section 3). Figure I describes the entire process.

Note that an imperfect certification may occur in the real world due to the "oracle problem,"

Figure I: The Winne Supply Chain



Note: This figure shows the flow of wine and the possibility of counterfeiting. Before the wine flows from (1) a grape firm to (3) a producer, the quality of the grape must be identified (step 2). Since this certification is done outside the blockchain, it incurs the "oracle problem." Given the identified quality, a flow between (1) and (3) is recorded in the blockchain. Even though a producer with low-quality grapes tries to forge the document (claims $\hat{s} = 1$), this fraudulant information cannot be a consensus and rejected by the smart contract with probability θ.

as mentioned in Subsection 2.2.1. In this model, this corresponds to the credibility of π, i.e., a certifier of grapes may misreport s. In the following, we take π as given and abstract away from the oracle problem to focus on the efficiency of the blockchain achieved by the decentralized monitoring of the information flow.

There are $i \in \{1, \cdots N\}$ potential participants in the blockchain network, i.e., record keepers. They monitor the input s and the transaction between the grape firm and producer (step3 in Figure I). Each record keeper reports $\hat{s}_i \in \{0, 1\}$ to indicate the quality of the ingredients a producer uses.

As in Cong and He (2018), we assume that the blockchain generates a consensus $\hat{s}$ by aggregating $\{\hat{s}_i\}_{i=1}^N$ by the following protocol.[15]

$$\hat{s} = \begin{cases} 1 & \text{with probability } \frac{1}{N}\sum_{i=1}^N \hat{s}_i \\ 0 & \text{otherwise.} \end{cases}$$

Moreover, record keepers have an incentive to misreport. This is because a record keeper may share the utility with a wine supplier, or a seller may participate in the blockchain network as a record keeper to affect the consensus. In fact, we can observe an overlapping community of users of the blockchain and record keepers in practice.[16] Since a seller who purchases low-quality grapes from a producer has an incentive to relabel them as high quality, she will participate as a record keeper and misreport to make the consensus "high." This is represented by the lower producer in step3 of Figure I.

To describe this, let a record keeper obtains some positive revenue R if the bottle is sold.[17] In this case, to obtain R, she is motivated to report $\hat{s}_i = 1$ even though $s = 0$. We assume that she is risk neutral and enjoys the following utility by submitting $\hat{s}_i$:

$$\max_{\hat{s}_i \in \{0,1\}} U(\hat{s}_i, s) = E\left[R\mathbb{I}_{\{\hat{s}=1\}} - c_i|\hat{s}_i - s|\right]. \tag{1}$$

The first component is the utility from reaching $\hat{s} = 1$ and successfully selling the bottle, whereas the second is the cost of misreporting with a stochastic coefficient c_i.[18] We assume that she is not concerned about the other participants' behavior since N is sufficiently large.[19]

[15]This specification of $\hat{s}$ is not essential to our result. We obtain the same implication as long as (i) an agent's "high" (resp. "low") report increases probability that $\hat{s}$ becomes "high" (resp. "low"), and (ii) the influence of her report on $\hat{s}$ diminishes as N increases.

[16]See, for example, Cong and He (2018). Policy discussion regarding the separation of blockchain users from record keepers is provided in Subsection 5.1.

[17]For example, we can set $R = (1-h)U_S$, where $h \in (0,1)$ represents the share of profit that a wine producer grasps.

[18]We can think of this cost as an expense of computing power to perform PoW in the Bitcoin network.

[19]Strategic behavior is an important force that distinguishes the blockchain from the centralized mechanism. We abstract away from it because the focus of our main model from Section 3 onward is not on how θ is affected by the micro-motived behavior, but on how the different θ affects the general equilibrium. See Biais et al. (2018) for the

Finally, buyers write a code on Ethereum to exploit the smart contract. That is, the blockchain makes the transaction contingent on $\hat{s}$ and accepts the bottle only if $\hat{s} = 1$, i.e., the exchange of wine for money happens if, and only if, the consensus states that $\hat{s} = 1$.

2.3.2 Ex-Post Asymmetric Information

Now, we can derive how the blockchain and the smart contract alter the *ex-ante* quality distribution π. Since $E[\mathbb{I}_{\{\hat{s}=1\}}] = \sum_{i=1}^{N} \frac{\hat{s}_i}{N}$, the optimal behavior of each record keeper is as follows. If $s = 1$, then $\hat{s}_i = 1$ is the optimal report, while if $s = 0$,

$$\hat{s}_i = \begin{cases} 1 & \text{if } RN^{-1} \geq c_i \\ 0 & \text{otherwise.} \end{cases} \tag{2}$$

We denote the probability of misreporting as $\psi_{i,N} \equiv \Pr(c_i \leq RN^{-1})$.

Because a buyer with the smart contract stipulates, "Execute my transaction if, and only if, the consensus is high," even though she does not detect the quality by reading the label on the bottle, the fact that the transaction takes place conveys a signal that the bottle she obtains is of high quality with an updated probability $\pi_N(> \pi)$. Given that the smart contract sends the bottle only with $\hat{s} = 1$, the buyer infers that

$$\begin{aligned} \pi_N &\equiv \Pr(s = 1|\hat{s} = 1) \\ &= \frac{\Pr(s = 1)\Pr(\hat{s} = 1|s = 1)}{\Pr(s = 1)\Pr(\hat{s} = 1|s = 1) + \Pr(s = 0)\Pr(\hat{s} = 1|s = 0)} \\ &= \frac{\pi}{\pi + (1 - \pi)\sum_{i=1}^{N} \frac{\psi_{i,N}}{N}} > \pi. \end{aligned} \tag{3}$$

We denote our key parameter as

$$\theta \equiv 1 - \sum_{i=1}^{N} \frac{\psi_{i,N}}{N},$$

so that $\pi_N = \frac{\pi}{\pi + (1-\pi)(1-\theta)}$. Note that θ represents how efficiently the blockchain with the smart contract can reject the low quality wine, i.e., given that the bottle is vetted by the smart contract,

strategic decisions of miners (record keepers).

the buyer knows that a bad product is precluded with probability θ. Also, we can think of $\hat{s}$ as a signal of the blockchain and θ as the quality of it. We use these interpretations interchangeably.

The efficiency level θ is increasing in N and c_i.[20] First, as the number of participants (N) increases, the individual probability of misreporting, $\psi_{i,N}$, declines because the effect of each report diminishes and overturning the consensus becomes difficult. The cost of misreporting, c_i, has the same effect.

In the traditional centralized protocol, we have $N = 1$. Since the centralized agent knows that she can control $\hat{s}$, she has a strong incentive to misreport when $s = 0$. On the other hand, if the consensus aggregates a larger number of reports, it becomes less profitable to submit a wrong report. Therefore, decentralized information management by the blockchain precludes low-quality goods more efficiently than the traditional centralized system: $\theta_{N=1} < \theta_{N=M}$ for $M > 1$. Note that we can normalize $\theta_{N=1} = 0$ without loss of generality.[21]

Finally, we introduce a proposer who *indirectly* controls θ, as in Abadi and Brunnermeier (2018). She is not a centralized authority who generates a consensus, but she can affect its quality by changing the "rule" of a platform. Alternatively, we can consider a group of blockchain participants (record keepers) who intend to make a fork. For example, the Bitcoin blockchain sets the difficulty of its cryptographic problems so that blocks are created by miners every 10 minutes based on its specific hashing algorithm, that is PoW with SHA256. These parameters of Bitcoin blockchain—10 minutes difficulty target, PoW, and SHA256—affect the miners' cost of participation or misreporting since they need sufficient computing power to perform PoW under the given setting. In 2011, Litecoin, proposed by Google computer scientist Charlie Lee, branched off from Bitcoin. It aims to reduce the difficulty target to 2.5 minutes, increase the maximum coin supply, and use a different hashing algorithm (called *script* PoW). This change in the rule of consensus formation can be seen as a fluctuation in θ generated by changes in

[20] As for the effect of N, we suppose that the distribution of c_i is identical for all i, so that $\psi_{i,N}$ does not depend on i.

[21] The range of θ that the blockchain can achieve in our model is given by the limit of N and the distribution of c. For example, $\lim_{N\to\infty} \Pr(c_i \leq RN^{-1}) = 0$ and $\max_N \theta_N = 1$. Also, as $N \to 1$, we have $\theta_1 = 1 - \Pr(c_1 \leq R)$. By controlling the distribution of c, it can achieve $\theta_1 = 0$.

N and c_i. Also, in the case of the wine blockchain, proposers like EY can decide how many intermediation steps are monitored by the blockchain, as well as how many record keepers are contacted to generate a consensus (i.e., openness of a chain). Appendix C provides more real-world examples of blockchains forks that achieve different parameter settings.

In the following sections, we propose our main model to analyze the effect of an improvement in θ on the general equilibrium economy and show that the effect is non-monotonic. Specifically, π_N in (3) is modified once we endogenize the behavior of sellers by letting them incorporate θ.

3 General Equilibrium Model

Consider an economy with two periods ($t = 0, 1$) and segmented markets. There is a continuum of risk-neutral buyers (consumers) and sellers (producers), both characterized by the private value $\alpha \in [0, 1]$. α has a cumulative measure F, which is assumed to be uniform.[22] At date $t = 0$, each buyer is endowed with a certain amount of cash w, draws α, and partakes in the markets to buy an asset.

On the sell side, each seller is endowed with a unit asset with a stochastic quality s, which is either high, $s = 1$, or low, $s = 0$, with $\Pr(s = 1) = \pi \in (0, 1)$ and independent of α. By the law of large numbers, the economy-wide fraction of high-quality assets is π. Also, risk-free saving with a zero interest return is available.

For both sellers and buyers with a private value α, the asset yields the following (per capita) utility at date $t = 1$:

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

$\phi \in (0, 1)$ is the primitive quality difference. If the asset is low-quality, agents obtain only ϕ fraction of the utility.[23] Following the literature on market microstructure (such as Glosten and

[22]Imposing the same F on both sellers' and buyers' α is for tractability and is not essential in our analyses.

[23]Note that the use of the terms "private value" and "quality difference" for (α, ϕ) does not restrict the implications of our model. We can think of s as the quality of a shipping company, so that ϕ can be a time-discount factor due

Milgrom, 1985), agents can trade and hold, at most, one unit of the asset and cannot short-sale.

3.1 Market Structure

There are two trading platforms with different mediums of exchange. One is the blockchain with cryptocurrency (called the B-market) and the other is the traditional market with cash (called the C-market). We give transactions via the blockchain platform an index $j = B$ (blockchain) and those with the traditional one an index $j = C$ ("cash" or centralized protocol). We do not restrict agents' venue choice, while Appendix E shows that our results are robust even if access to the B-market is limited for some agents.

The Blockchain and Smart Contract

To distinguish transactions via the blockchain from those through the traditional market, we assume that information in the blockchain is maintained by N record keepers, while the C-market has $N = 1$ (i.e., it has centralized record-keeping system). According to Section 2.2, we characterize the B-market by the following definition.

Definition 1. θ fraction of low-quality assets that sellers intend to sell in the B-market are detected and rejected by the blockchain mechanism.

The parameter $\theta \in (0, 1]$ is called the "efficiency level."[24] This is motivated by the microfoundation in Section 2.2, in which we derived the rejection probability θ from the decentralized consensus and the smart contract. Appendix A discusses in detail how to bridge the gap between the microfoundation model in Section 2.2 and the main model (or Definition 1). At

to the delay in delivery. Also, α can be idiosyncratic productivity, and assets can be seen as capital that produces consumption goods. In general, s can be any characteristics that consumers care about, and α represents how serious they are.

[24] The economy is not continuous at $\theta = 0$. When we make $\theta \searrow 0$, it converges to an equilibrium with two homogeneous markets, which is different from an economy with only one (the C-market). For this reason, we do not compare the single-market economy with the segmented economy. Rather, we focus on the comparative statics with $\theta > 0$.

first, we take this value as given for participants in the market. Later, in Subsection 4.2.2 and onward, we study a case wherein a proposer of the blockchain can affect this efficiency level.

Moreover, to motivate agents to hold cryptocurrency, we introduce the following restriction:

Assumption 1. To buy k_B amount of assets at price P_B (in terms of cash) in the B-market, a buyer must hold $P_B k_B / Q$ of cryptocurrency, where Q is the price of cryptocurrency in terms of cash (see budget constraint [4]).

This assumption comes from the fact that the endowment is given by cash. We call it the "cryptocurrency in advance" (CIA) constraint in our model, and Schilling and Uhlig (2018) consider a similar formulation. Importantly, Assumption 1 is innocuous and does not change our results regarding blockchain activity.[25] Indeed, it will be clear that the demand and pricing for cryptocurrency are determined outside the asset trading markets because of monetary-neutrality arguments.

3.2 Optimal Behavior of Buyers

A buyer with type α maximizes her expected consumption at $t = 1$, $V(\alpha) = E[c|\alpha]$, under the following budget constraints:

$$w \geq P_C k_C + Qb + a,\ \frac{Q}{P_B} b \geq k_B, \tag{4}$$

$$c = y_C(\alpha) k_C + y_B(\alpha) k_B + a.$$

k_j and P_j represent the demand and price of the asset at market j, Q is the price of cryptocurrency, and b is the demand (quantity) for cryptocurrency. All prices are valued in terms of cash. Thus, the price of assets traded in the B-market in terms of cryptocurrency is P_B/Q.[26] A risk-free

[25] By removing Assumption 1 and imposing it on sellers' behavior, we can analyze the other class of cryptocurrency platforms, such as a part of Ethereum, in which the sellers must have cryptocurrency to verify their authenticity. Also, some blockchains do not involve circulation of tokens, and we can analyze those cases just by ignoring the CIA constraint.

[26] Value transfer by means of Bitcoin can also be analyzed. For example, a grad student in California wants to transfer \$10,000 worth of JPY from his bank account in Japan. He can ask his bank for the remittance, in which case

saving option is denoted by $a \geq 0$. The definition of $y_j(\alpha)$ is given by (5) below.

The constraints in the first line imply that the buyer allocates her cash endowment to the purchase of the asset in the C-market and to cryptocurrency, and the latter is used to buy the asset in the B-market. The purchase amount in the B-market is limited by her holdings of cryptocurrency, as Assumption 1 suggests. As well, the agent can stay inactive to get zero utility from her assets. The second line shows the consumption level, in which, for $j \in \{B, C\}$,

$$y_j(\alpha) \equiv \tilde{\pi}_j \alpha \equiv [\pi_j + (1 - \pi_j)\phi]\alpha, \tag{5}$$

$$\pi_j \equiv \Pr(s = 1 \text{ in market-}j).$$

Hence, y_j represents the expected private return adjusted for the risk of lemons in each market, $1 - \pi_j$. Note that π_j is endogenous.

Because of the risk neutrality and linearity of y, splitting order into two markets is not optimal.[27] Thus, the demand always hits its upper or lower limit ($k_j = 0, 1$), and the CIA constraint is binding, thereby making itself innocuous to our main results.

The expected return from purchasing assets in each market (V_B, V_C) and that from staying inactive (V_0) are given by

$$V_j(\alpha) = \begin{cases} \tilde{\pi}_j \alpha - P_j & \text{for } j \in \{B, C\} \\ 0 & \text{for } j = 0. \end{cases}$$

We subtract w from the equations above because it does not affect the equilibrium behavior.

he purchases dollar (k_C) by paying yen (w) at an exchange rate P_C. Alternatively, he can convert his JPY to Bitcoin at price Q (so that $b = k_B$ of BTC is stored in his wallet on the Bitcoin blockchain). This Bitcoin can be exchanged for USD at the rate Q/P_B, thereby leaving him with Qb value of USD.

[27] Only the buyers on the threshold (defined below) can split the order, but we simplify our discussion by assuming a tie-breaking rule that indifferent agents trade in the B-market.

To solve the venue-choice problem, we guess the following[28]:

$$\frac{P_B}{\tilde{\pi}_B} > \frac{P_C}{\tilde{\pi}_C}, \pi_B > \pi_C, \tag{6}$$

which will be shown to be a unique equilibrium. Intuitively, $P_j/\tilde{\pi}_j$ is a normalized price and represents the cutoff of α that generates indifference between buying in the j-market and staying inactive.[29] It indicates a positive measure of traders with relatively high (resp. low) α who wish to go to the B-market (resp. C-market). Indeed, under (6), the optimal behavior of buyers with type α is determined by the cutoff α^* such that

$$\alpha^* \equiv \frac{P_B - P_C}{\tilde{\pi}_B - \tilde{\pi}_C}.$$

Figure II plots returns, V_i, against α and shows the cutoffs for the optimal behavior. Namely, it is optimal for type α buyers to (i) purchase one unit of the asset in the B-market if $\alpha \geq \alpha^*$, (ii) in the C-market if $\alpha \in [\frac{P_C}{\tilde{\pi}_C}, \alpha^*)$, and (iii) stay inactive otherwise.

Intuitively, each buyer faces a price-quality tradeoff, i.e., the B-market provides higher quality and expected returns, but charges a higher price. Note that the gain from a higher π_j is multiplied by α, while the cost is constantly P_j. Hence, the B-market looks more attractive for high-α buyers.

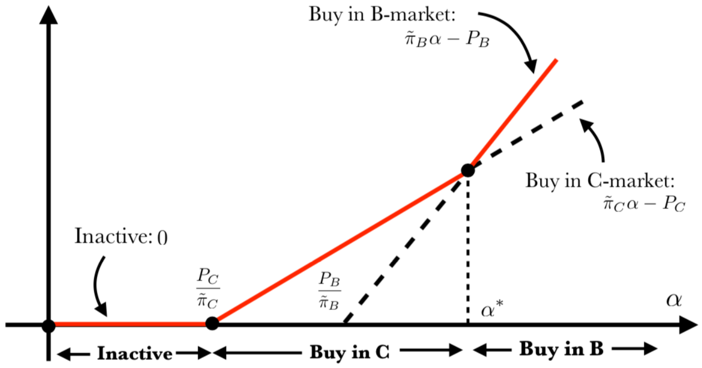
By aggregating along α, the total demand in each market is

$$K_j^D = \begin{cases} 1 - F(\alpha^*) & \text{for } j = B, \\ F(\alpha^*) - F\left(\frac{P_C}{\tilde{\pi}_C}\right) & \text{for } j = C. \end{cases} \tag{7}$$

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

[29]Buyers' behavior can be seen as the model of vertical differentiation, such as the one provided in Chapter 2 of Tirole (1988).

Figure II: Returns for Buyers



The uniform F allows us to derive inverse demand functions:[30]

$$P_j = \begin{cases} \left(\frac{1}{\tilde{\pi}_C} + \frac{1}{\Delta\tilde{\pi}}\right)^{-1}\left(\frac{P_B}{\Delta\tilde{\pi}} - K_C^D\right) & \text{for } j = C \\ P_C + \Delta\tilde{\pi}(1 - K_B^D) & \text{for } j = B, \end{cases} \tag{8}$$

with $\Delta\tilde{\pi} \equiv \tilde{\pi}_B - \tilde{\pi}_C$. Note that plugging in the aggregate supply K_j^S—which will be derived in the next section—yields the equilibrium prices.

From the second equation, the price spread, $\Delta P \equiv P_B - P_C$, stems from the quality difference. This can be seen as a premium: the asset in the B-market obtains a higher valuation than the one in the C-market through its higher quality, $\Delta\tilde{\pi}$. We derive the quality difference from supply-side behavior in the next subsection.

3.3 Optimal Behavior of Sellers: Endogenous Quality

As the literature on adverse selection assumes, each seller knows the quality of her asset (Appendix D generalizes this by assuming that only λ fraction of sellers are informed of the

[30] As for the form of F, the uniform assumption is restrictive in this model. The equilibrium is driven by the migration behavior of agents. For example, if we make F bimodal, or if we only have two types of α, in the extremum case, the effect through the migration is muted. By assuming uniformity, the fundamental effect of the blockchain platform and market structure are not altered by this slope effect (or drastic change in the extensive margin). This is the problem that commonly arises in the model of segmented markets wherein heterogeneous traders decide in which one to participate. See, for example, Zhu (2014) for a similar discussion.

quality). Also, note that each seller does not engage in strategic trading: the signaling effect of venue choice is shunted aside because each trader is non-atomic. Instead, the sell-side selection (screening) occurs due to $\theta > 0$, even in the competitive equilibrium.[31]

3.3.1 Low-Quality Sellers

First, we consider the optimal strategy of sellers with low-quality assets (L-type sellers). If a trader sells the asset in the B-market, she anticipates that it may get low consensus ($\hat{s} = 0$) and be rejected by the smart contract. Thus, the expected return is

$$W_B^L = (1 - \theta)P_B + \theta\phi\alpha. \tag{9}$$

The first term represents the case where her asset gets a high consensus in the blockchain and avoids rejection, while in the second, the asset is rejected by the blockchain since fraudulent reports could not be a consensus.[32] In the latter case, the trader must use the asset to get $\phi\alpha$.[33]

On the other hand, if she sells it in the C-market, the return is $W_C^L = P_C$, while the return from staying inactive is $W_0^L = \phi\alpha$. See the left-hand panel of Figure III for a diagram of these value functions.

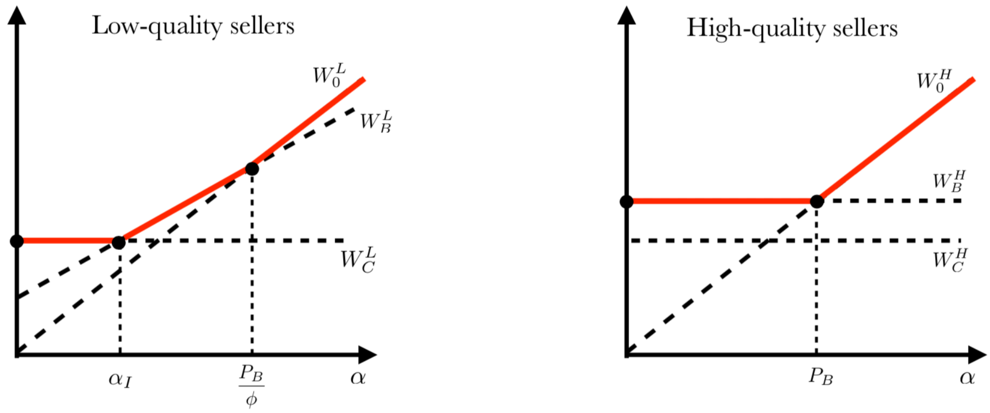
By comparing these three returns as functions of α under (6), we see that the optimal

[31]Notice that, by setting the model in this way, we implicitly exclude the possibility of collusion by sellers as in Cong and He (2018). Since sellers are non-atomic, they expect that their behavior does not affect the market prices, quantity, or quality.

[32]More precisely, a seller in the B-market obtains P_B/Q of cryptocurrency, which amounts to P_B in terms of cash value. We implicitly assume that sellers have access to a dynamic market for cryptocurrency, in which they can trade it for cash at the same exchange rate Q over time. This assumption is motivated by the overlapping generations of traders. The structure of these generations is identical over time, and buyers in their young period arrive at the markets and demand cryptocurrency as a means of exchange. Conversely, old sellers are ready to trade their cryptocurrency for cash.

[33]The alternative assumption is allowing rejected traders to conduct "order routing." A trader can first try to sell in the B-market and, if rejected, can submit a sell order in the C-market. We can show that this alternative assumption does not change our main results, including propositions 1, 2, and 3, though the equilibrium conditions are slightly modified. The results are available upon request.

Figure III: Returns for Sellers



Note: The left (resp. right) panel describes the returns comparison of sellers with low-quality (resp. high-quality) assets.

strategy is to (i) stay inactive if $\alpha > \frac{P_B}{\phi}$, (ii) sell in the B-market if $\alpha \in (\alpha_I, \frac{P_B}{\phi}]$, and (iii) sell in the C-market if $\alpha \leq \alpha_I$, where

$$\alpha_I = \max\left\{\frac{P_C - (1-\theta)P_B}{\phi\theta}, 0\right\} \tag{10}$$

is the cutoff that separates sellers into the B- and C-markets.

When it is strictly positive, the cutoff α_I is increasing in θ, decreasing in ϕ, and increasing in the expected price difference (numerator of α_I). Given the prices, an increase in θ makes sellers who traded in the B-market migrate to the C-market because a higher rejection probability lowers their expected profit. On the other hand, a higher ϕ increases the continuation value and the profit from selling in the B-market, causing marginal sellers to switch to this platform. Finally, a larger difference in the expected prices makes the C-market more attractive.

High-α sellers are more likely to trade lemons in the B-market, while low-α sellers tend to prefer the C-market due to the price-liquidity tradeoff, i.e., the B-market provides a higher selling price, but at the risk of rejection. High-α sellers do not care about the lower execution probability in the B-market because they can obtain a high value of $\phi\alpha$ even if the selling order is rejected, while the opposite is true for their low-α counterparts.

3.3.2 High-Quality Sellers

For a seller with a high-quality asset (H-type seller), the return from trading in the C-market, B-market, and not trading are given by

$$W_j^H = \begin{cases} P_j & \text{for } j = B, C, \\ \alpha & \text{if } j = 0. \end{cases}$$

Under guess (6), the optimal behavior is to (i) stay inactive if $\alpha > P_B$ and (ii) sell in the B-market if $\alpha \leq P_B$. The right-hand panel of Figure III shows this comparison.

3.3.3 Aggregate Supply and Quality

By integrating along α, the aggregate amount of assets that sellers *intend* to sell in each market is

$$S_B = \pi F(P_B) + (1-\pi)\left[F\left(\frac{P_B}{\phi}\right) - F(\alpha_I)\right], \tag{11}$$

$$S_C = (1-\pi)F(\alpha_I). \tag{12}$$

In (11), the first term is the supply from H-type sellers, and the second is that from L-type sellers. (12) only consists of L-type selling behavior. As suggested by the literature on adverse selection with segmented markets (Chen, 2012; Kim, 2012; Guerrieri and Shimer, 2014), a market with a low (high) price and deeper (shallower) liquidity tends to attract low-quality (high-quality) assets because the different prices and liquidity can work as a screening device.

Since the blockchain technology weeds out θ fraction of the lemons from the B-market, the supply functions are given by

$$K_B^S = \pi F(P_B) + (1-\pi)(1-\theta)\left[F\left(\frac{P_B}{\phi}\right) - F(\alpha_I)\right], \tag{13}$$

whereas, in the C-market, all of the selling attempts are accomplished, $K_C^S = S_C$. As a result, the average quality in each market is derived as follows:

Lemma 1. *Endogenous market qualities are given by*

$$\pi_j = \begin{cases} \frac{\pi F(P_B)}{\pi F(P_B)+(1-\pi)(1-\theta)\left[F\left(\frac{P_B}{\phi}\right)-F(\alpha_I)\right]} & \text{if } j = B \\ 0 & \text{if } j = C. \end{cases} \tag{14}$$

Note that this corresponds to π_N in (3), while (14) incorporates the sellers' optimal venue-choice problem. Also, all the assets traded in the C-market are of low quality. This arises from the information structure of sellers (i.e., they all know the quality of their assets) and full access to both markets. In the real economy, it is stretched to claim that $\pi_C = 0$. Thus, Appendices D and E provide more general models to show that our main results are robust with $0 < \pi_C < \pi_B < 1$.

3.4 General Equilibrium

We can define the general equilibrium as follows:

Definition 2. The general equilibrium is defined by the price, quality, and quantity, $(Q, \{P_j, \pi_j, K_j\}_{j\in\{C,B\}})$, that clear the markets ($K_j^S = K_j^D$) with the following equations (under the normalization of cryptocurrency supply to 1):

$$\begin{aligned} &K_C^S = (1-\pi)\alpha_I, K_B^S = \pi P_B + (1-\pi)(1-\theta)\left(\frac{P_B}{\phi} - \alpha_I\right), \\ &K_C^D = \frac{P_B - P_C}{\tilde{\pi}_B - \phi} - \frac{P_C}{\phi}, K_B^D = 1 - \frac{P_B - P_C}{\tilde{\pi}_B - \phi}, \\ &\pi_B = \frac{\pi P_B}{K_B}, Q = P_B K_B^i. \end{aligned} \tag{15}$$

It is worth noting that the economy is characterized by the Walrasian-type equilibrium, and each market has a unique price that equates the aggregate demand to the aggregate supply. The other possible characterization is to describe bilateral trading (e.g., over-the-counter markets) with a more complex smart contract which may be contingent on α and other characteristics of assets, resulting in different prices for different trade. However, in practice, it can be difficult and costly to describe contingent contracts based on a large dimension of quality attributes or preference, which is continuous in our model. Thus, we believe that our model fits an economy in which blockchain users prefer to keep the contract simple to minimize costs of specifying (α, s) and writing a complex contract.[34]

3.4.1 Equilibrium Spreads

We can quantify the spreads in the price and quality between the two markets (see Appendix F.1 for the proofs).

Proposition 1. *The blockchain market achieves a higher quality than the cash market, i.e.,* $\pi_B > \pi_C$.

Proposition 1 has direct implications for the prices. That is, the positive spread in the quality, $\Delta\pi > 0$, results in a higher price in the B-market as well.

Proposition 2. *The price of assets traded in the B-market is higher than that in the traditional C-market, that is,* $P_B > P_C$.

Note that a higher θ affects π_B via two channels. First, it exogenously precludes θ fraction of the lemons, as the second term of K_B^S in (13) suggests. Second, it generates the endogenous sorting of low-quality assets, which manifests in a change in the cutoff α_I caused by the fluctuation of P_j. This happens even if the sellers do not trade strategically. Rather, the sell-side selection is a consequence of the purely competitive tradeoff between the higher equilibrium price in the B-market and detection risk. Due to its higher continuation values, high-quality assets tend to cluster in the B-market, while low-quality assets cluster in the C-market to avoid being rejected. This mechanism generates a higher quality and price in the B-market (spreads), which are self-sustaining in the equilibrium.

4 Comparative Statics: The Effect of Efficiency Improvement

We first investigate how P_B, π_B, and K_B are differently affected by θ.

[34] See, for example, Tinn (2017) for the discussions on how the blockchain can change the landscape of the optimal contracts.

Proposition 3. *The economy admits a unique solution in which (i)* $\frac{dP_B}{d\theta} > 0$, $\frac{d\pi_B}{d\theta} > 0$. *Moreover, (ii) the price spread is more responsive than the quality spread*, i.e., $\frac{d \log \Delta P}{d\theta} > \frac{d \log \Delta \pi}{d\theta} > 0$.

Proof. See Appendix F.3. □

Consider an increase in θ. With a fixed P_B, it reduces K_B^S by detecting and sweeping out low-quality assets (*the supply-side effect*). However, this improves the B-market's quality and makes consumers more willing to buy in the B-market (*the demand-side effect*). Thus, the supply declines while the demand increases, meaning P_B must shoot up to clear the market.

Importantly, P_B increases more than π_B, as the point (ii) suggests. This is because the increase in P_B not only pushes the enhanced demand back to the original level, but it also dampens it even more to make it equal to the reduced supply level. Put differently, an increase in P_B must kill both of the demand-side effect associated with the quality improvement and the supply-side effect.

This argument leads to the negative reaction of the B-market trading volume:

Proposition 4. *The B-market's trading volume is decreasing in* θ, *i.e.*, $\frac{dK_B}{d\theta} < 0$.

This is intuitive not only from the sell-side's perspective but also from the buyers' point of view. Namely, buyers face the price-quality tradeoff, and the price increases more than the quality does (statement [ii] in Proposition 3), so that the B-market consumers want to switch to the C-market. As we see later in subsection 4.3, the decreasing K_B and increasing P_B generate ambiguous and non-monotonic reaction of the trading value $(P_B K_B)$.

Note that, as long as the C-market exists, the opposite argument applies to the reaction of P_C and π_C: the price declines more than the quality does. This gives the result for the *spreads* as the statement (ii) suggests. The reaction of the C-market makes the difference $\frac{d \log \Delta P}{d\theta} - \frac{d \log \Delta \pi}{d\theta}$ wider and strengthens the decline in K_B. This implies that the coexistence of the C-market matters to determine the results.

Specifically, we can separate $\theta \in (0, 1]$ into two regions by the following cutoff, θ_0, that determines the coexistence.

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

Lemma 2. *(i) $\alpha_I > 0$ and $K_C > 0$ if and only if $\theta > \theta_0$. (ii) θ_0 is decreasing in ϕ and π. (iii) $\frac{dP_C}{d\theta} < 0$ when $\theta > \theta_0$.*

Proof. See Appendix F.2 for the statement (i). (ii) follows immediately from the definition of θ_0. □

Recall that α_I is the cutoff for L-type sellers in the B-market ($\alpha \geq \alpha_I$) or in the C-market ($\alpha < \alpha_I$). Therefore, Lemma 2 and (15) imply that the C-market shuts down, $K_C = 0$, when θ is smaller than θ_0. This happens because all of low-type sellers intend to sell in the B-market when θ is sufficiently small. In other words, the coexistence of the traditional system and the blockchain-based settlement is sustained only if θ is sufficiently high. In the real world, most of the blockchains, such as Bitcoin, Ethereum, Ripple, and Symbiont, distribute information to sufficiently large number of record keepers (i.e., N is high), thereby keeping θ high enough and making the coexistence sustainable.

In the following, Subsection 4.1 states the results regarding the trading value ($P_B K_B$) and Q by focusing on $\theta \geq \theta_0$. Before we explain the intuitions and mechanism behind the results in Subsection 4.3, Subsection 4.2 defines the value added of the blockchain and consumers' welfare to show that all of these are driven by the trading value in the B-market. Finally, Subsection 4.4 analyzes the case with a single market, $\theta < \theta_0$, to highlight the importance of the coexistence.[35]

4.1 Non-Monotonic Effects of the Blockchain Efficiency

4.1.1 Trading Value and the Price of Cryptocurrency

Suppose that $\theta \geq \theta_0$. The market clearing condition gives $Q = P_B \int k_B^D dF(\alpha) = P_B K_B$ (with cryptocurrency supply normalized to 1). Let $\phi_1 = \frac{2-\pi}{3-\pi}$, and $\phi_0 (< \phi_1)$ be the unique solution of

[35] In Appendix B, we discuss why the C-market breaks down when θ is small.

(41) in Appendix F.3.

Proposition 5. *(i) If $\phi < \phi_0$, Q and $P_B K_B$ are monotonically increasing in θ.*

(ii) If $\phi_0 \le \phi < \phi_1$, Q and $P_B K_B$ are U-shaped, and there is θ^* s.t.,

$$\frac{dQ}{d\theta} = \frac{dP_B K_B}{d\theta} \lesseqgtr 0 \Leftrightarrow \theta \lesseqgtr \theta^*.$$

(iii) If $\phi_1 \le \phi \le 1$, Q and $P_B K_B$ are monotonically decreasing in θ.

Proof. See Appendix F.3. □

Corollary 1. *In case (ii), θ^* is increasing function of ϕ and π.*

The proposition indicates that the trading value and the price of cryptocurrency exhibit a non-monotonic reaction to the sophistication of the blockchain technology. As shown by Proposition 3, a higher θ increases P_B and decreases K_B, i.e., the B-market becomes a high-quality but exclusive market. Proposition 5 implies that whether the decline in K_B dominates the increase in P_B depends on ϕ and θ. Moreover, Corollary 1 implies that, in case (ii), $P_B K_B$ is more likely to decline when information asymmetry measured by (ϕ, π) is *not* severe. We discuss the intuitions and mechanism in detail in Subsection 4.3.

This finding differentiates our theory from the literature on money versus credit, in which the increase in record-keeping ability monotonically makes cash inessential. This also differs from the result by Cong and He (2018) since they claim that an increase in θ has monotone impacts. As we will see in Subsection 4.3, endogenous price and quality spreads due to the coexisting two platforms, which are absent in the literature, are the key factors that prompt this result.

4.2 The Value of the Blockchain and Welfare Impact

In this subsection, we calculate the aggregate welfare of buyers (consumers), as well as the welfare gain from access to the blockchain platform (see Appendix G.3 for sellers' welfare).

Keep in mind that the market has $\theta \geq \theta_0$.[36]

4.2.1 Buyers' Welfare

We define the aggregate welfare of buyers by integrating their trading surplus (we ignore the common constant endowment w):

$$v_B = \int_{\alpha^*} (\tilde{\pi}_B \alpha - P_B) dF + \int_{P_C/\phi}^{\alpha^*} (\phi\alpha - P_C) dF \tag{16}$$

$$= \underbrace{\int_{\alpha^*} (\Delta\tilde{\pi}\alpha - \Delta P) dF}_{\propto P_B K_B = Q} + \int_{P_C/\phi} (\phi\alpha - P_C) dF \tag{17}$$

In equation (16), the first term is the welfare of buyers who purchase in the B-market, and the second encompasses those who purchase in the C-market. This can be rewritten by using "welfare gain" and "reservation welfare" as in (17). The second term of (17) represents the welfare of all the active buyers from purchasing in the C-market, i.e., the reservation welfare. The first term of (17) is the extra value that stems from changing the trading platform from C to B, which only $\alpha \geq \alpha^*$ agents attempt to do.

Interestingly, the welfare gain is co-linear with the trading value in the B-market (see Appendix G.1 for the proof). If the blockchain platform has cryptocurrency, it further implies that the welfare gain is measured by the price of cryptocurrency, Q. This is natural because $P_B K_B$ represents the extra trading activity generated by the B-market and should reflect the extra trading surplus. The effect of θ on v_B is analyzed later.

4.2.2 Platform Fee and the Value of Blockchain

The first term of equation (17) shows that access to the blockchain technology attains a positive fundamental price. To see this, we consider an *ex-ante* platform usage fee. Specifically, we dis-

[36]Technically, as the CIA constraint always binds, the welfare comparison does not hinge on the existence of cryptocurrency. More generally, the equilibrium variables with and without the CIA constraint are identical except for the formula for Q because of the "monetary neutrality" of cryptocurrency.

cuss the buy-side problem by assuming that consumers must pay a fee to use the blockchain.[37] This is natural because, in practice, users of the blockchain pay some fee to miners (record keepers) for recording users' transaction in a block.[38]

Let us introduce a pre-trade period, $t = -1$, and suppose that a buyer decides whether to pay a fee f_B for access to the B-market before the type α is drawn.[39] We can think of it as a take-or-leave-it offer from the platform. Note that the behavior of this particular agent does not affect the expected market result because her measure is zero.

If the buyer declines the offer, her expected welfare stays at the reservation level in (17), which we denote as

$$v_0 = \int_{\frac{P_C}{\phi}} (\phi\alpha - P_C) dF, \tag{18}$$

while access to the blockchain platform provides a welfare (after the fee) of $v_B - f_B$. Thus, the amount of the fee that makes her indifferent is[40]

$$f_B = \Delta v_B \equiv v_B - v_0 = \int_{\alpha^*} (\Delta\tilde{\pi}\alpha - \Delta P) dF. \tag{19}$$

In other words, the blockchain platform can charge a fee up to the amount of the welfare gain given by (19). We can see this amount as the "price" of the blockchain technology or platform, since traders are willing to "buy" the right to participate in the B-market at the price of f_B. Moreover, we have the following intuitive result.

Proposition 6. *The fundamental price of the blockchain is perfectly correlated with the trading value*

[37] We discuss on the fee imposed on the sell side in Appendix H.1.

[38] For example, if a buyer purchase a cup of coffee from a seller by Bitcoin, some extra bitcoins are deducted from the buyer's digital wallet and they are collected by miners as a transaction fee. See Antonopoulos (2014) for more details.

[39] Another way to think about it is to conceptualize f_B as contingent on the usage of the B-market. In this case, the profit of buying in the B-market is shifted down by f_B only if a trader decides to participate. This formulation, however, generates complicated equilibrium conditions because it changes the cutoff of each trader. To avoid complications, we focus on a setting with the *ex-ante* contract.

[40] We assume the tie-breaking rule so that an agent accepts the offer if she is indifferent.

in the B-market and the price of cryptocurrency Q if the CIA constraint is assumed:

$$f_B = \frac{\pi(1-\phi)}{2} K_B P_B = \frac{\pi(1-\phi)}{2} Q. \tag{20}$$

Proof. See equation (42) in Appendix G.1. □

Corollary 2. *The efficiency of the blockchain technology has the same impact on f_B as proposed by Proposition 5.*

This proposition suggests that, if the blockchain uses cryptocurrency, the fundamental value of the technology is perfectly reflected by the price of cryptocurrency. In other words, the price of both cryptocurrency and the blockchain entirely depends on how active the transactions in the B-market are, which is measured by the trading value.[41]

4.3 Intuitions and Mechanism

The intuition behind the non-monotonic reaction of $Q = P_B K_B \propto f_B$ put forward by Proposition 5 and Corollary 2 is given by the competing behavior of P_B and K_B, which are driven by the migration of buyers.

First, when θ increases, it widens both price and quality spreads, ΔP and $\Delta\pi$. The former reduces the demand in the B-market, while the latter increases it, i.e., the B-market guarantees a higher quality but becomes exclusive. Second, the formula $Q = P_B K_B \propto f_B$ implies that Q and f_B rise when P_B increases more than K_B declines.

Rewriting the derivative of Q by using elasticity makes this clearer. Since K_B can be expressed as a function of P_B (without θ), and P_B is monotonic regarding θ, we have

$$\frac{df_B}{d\theta} \propto \frac{dQ}{d\theta} = (1-\varepsilon_{PK}) K_B \frac{dP_B}{d\theta}$$

[41] The coefficient $\pi(1-\phi)/2$ is the multiplier of $\Delta\tilde{\pi}$: when the quality difference is large, the gain from trading in the B-market rather than the C-market is high. When asymmetric information is not severe (ϕ is high) or the economy-wide share of low-quality assets is large (π is small), the price of cryptocurrency magnifies the fundamental value of the blockchain technology or the welfare gain for buyers (and vice versa).

with

$$\varepsilon_{PK} \equiv -\frac{dK_B/dP_B}{K_B/P_B}.$$

ε_{PK} is the price elasticity of the B-market transaction volume. Thus, if the price elasticity of demand is high, a decline in K_B dominates the increase in P_B, leading to a smaller Q and f_B. To understand the determinants of ε_{PK}, recall that the buyers' venue choice is driven by how easily they can migrate to the C-market to save the price difference.

When ϕ is sufficiently large, asymmetric information is not severe because the difference between the two asset types is small. Then, buyers are not eager to have H-type assets and are not attracted to a high π_B in the B-market. Thus, a marginal increase in P_B leads to a larger decline in K_B, and the transaction activity in the B-market, measured by $P_B K_B$, diminishes. Hence, the price of the blockchain platform and cryptocurrency drops. If ϕ is small, the low-quality assets are significantly bad compared to the high-quality assets. Consumers are eager to avoid the low-quality, and it becomes difficult for them to migrate away to the C-market even if P_B increases. This leads to an increase in $P_B K_B$, Q, and f_B.

If ϕ is intermediate, the level of θ matters because it determines the quality difference between the two markets, $\Delta\pi$ (Proposition 3). If θ is small, so is $\Delta\pi$: the difference in buying in the B-market and C-markets is not large in terms of the probability of purchasing low-quality assets. This facilitates migration to the C-market, since this market provides a lower price, while the difference in quality is negligible. Thus, K_B declines more than an increase in P_B, lowering Q and f_B. If θ is large, the B-market provides a markedly higher average quality, i.e., the quality spread is large, and Q and f_B increase with θ.

The bottom line is that, depending on the underlying information asymmetry, the change in the market structure has a different impact on the market activity. Specifically, even if the blockchain technology could reduce asymmetric information more efficiently, it does not always make this market attractive for consumers and may even dampen its trading value. This finding is a stark difference from the existing models because the negative welfare impact of the blockchain mostly comes from an exogenous cost of decentralized consensus mechanism, i.e., wasteful computing power (Abadi and Brunnermeier, 2018; Cong et al., 2018b; Saleh, 2018), or imperfect competition (Cong and He, 2018). We show that additional innovation can be harmful for consumers even in a perfectly competitive environment without socially wasteful costs.

4.4 The Blockchain Dominance

This subsection analyzes how the absence of the C-market alters the behavior of main variables by focusing on $\theta < \theta_0$.

Corollary 3. *When $\theta < \theta_0$, P_B, P_C, π_B, $P_B K_B$, and v_B are monotonically increasing in θ, while K_B is decreasing in θ.*

Proof. See Appendix F.2 □

This result highlights the importance of the C-market to generate the decreasing $P_B K_B$. As we have discussed, the existence of the C-market strengthens the statement (ii) in Proposition 3, and consumers are more willing to migrate. Once the C-market stops operating, this effect disappears, weakening the negative effect of θ on K_B.

Intuitively, if a consumer decides not to buy in the B-market, she does not have an alternative platform to purchase and must stay inactive. As a result, consumers tend to stick to the B-market, K_B only slightly declines, and an increase in P_B dominates it. Hence, the innovation of the blockchain always improves the market activity in the B-market and consumers' welfare, which is consistent with the monotonic results in Cong and He (2018).

4.5 Optimal θ and Welfare Distortion by the Platform

Now, we seek to determine the optimal level of θ from the perspective of traders' welfare and the blockchain platform. To make our discussion clearer, we follow Abadi and Brunnermeier (2018) and introduce a *blockchain proposer* who tries to maximize the fee revenue by proposing different parameters of the blockchain protocol, such as the difficulty target, the size of a block, and the hashing algorithm, to change the level of θ. The existence of this type of agent is realistic: even though the distributed ledger is managed by the participants of the network, there is an agent who determines the rule to generate a consensus (see Section 2.2 and Appendix C). We can also think of her as a group of record keepers.[42]

First, when $\theta \geq \theta_0$, a marginal increase in θ has the following impact on the consumers' welfare (see Corollary 3 for the results in $\theta < \theta_0$). The threshold ϕ_2 is defined in Appendix G.1.

Proposition 7. *(i) The reservation welfare is monotonically increasing in θ: $\frac{dv_0}{d\theta} > 0$.*

(ii-1) If $\pi > 1/2$, the total welfare is monotonically increasing in θ: $\frac{dv_B}{d\theta} > 0$.

(ii-2) If $\pi \leq 1/2$ and $\phi < \phi_2$, then the total welfare is monotonically increasing: $\frac{dv_B}{d\theta} > 0$.

(ii-3) Otherwise, v_B is U-shaped: there is a unique $\theta^{**} \in (\theta_0, 1]$ such that

$$\frac{dv_B}{d\theta} \gtrless 0 \Leftrightarrow \theta \gtrless \theta^{**}.$$

Proof. See Appendix G.1. □

Together with Q and f_B, buyers' welfare also has a U-shaped trajectory for a certain set of parameters. Interestingly, the reservation welfare is monotonically increasing in θ. This is because a higher θ lowers P_C more than it decreases π_C due to the same mechanism as in Proposition 3-(ii). That is to say, a more efficient blockchain technology not only generates positive extra value ($P_B K_B$) in the B-market, but it also has a positive impact in the traditional market.

The remaining part of v_B, which perfectly correlates with $P_B K_B$, generates non-monotonicity in v_B by the same mechanism as mentioned in Subsection 4.3.

Moreover, the result depends on π. When π is relatively high, the marginal increase in the fraction of assets rejected by the blockchain, $(1 - \pi)\theta$, is small. That is, innovation does not cause a large quality improvement or a huge reduction of K_B^S since the economy has only a few low-quality assets to begin with. The increment in P_B caused by the higher θ is not significant

[42] The assumption that the blockchain platform is a monopolist is also realistic at this point, provided that we have a limited number of blockchain platforms for each product. For example, as of February 2018, HyperLedger is the single leading firm that provides a platform for security trading by using the blockchain. Also Cong and He (2018) point out that the network externality will keep it away from being fully competitive in the long run.

enough to confound the demand in the B-market, and the welfare gain represented by the first term in (17) stays high.

4.5.1 Optimal θ for the Blockchain Proposer

By looking at (17) and (19), we notice that the objective functions of the blockchain proposer and the social planner are different, as the proposer does not care about the reservation welfare, v_0, which is monotonically increasing in θ. Thus, she *undervalues* the marginal benefit of increasing θ compared to the social planner.

Formally, let

$$\theta_f^* = \arg\max_{\theta\in[\theta_0,1]} f_B(\theta)$$
$$\theta_v^* = \arg\max_{\theta\in[\theta_0,1]} v_B(\theta).$$

$\theta_k^*, k \in \{f, v\}$, represents the level of θ that maximizes the fee and buyers' welfare, respectively. Corollary 3 shows that taking $\theta < \theta_0$ is not optimal because both objective functions are monotonically increasing in θ in this region. This is because, when the C-market is shut down, the B-market acquires all the trading share, and the source of the discrepancy between f_B and v_B disappears.

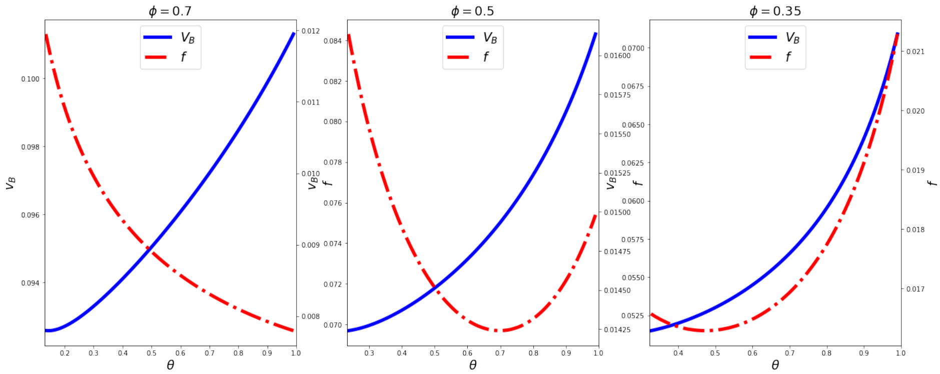
Once the C-market obtains positive trading volume (i.e., $\theta \geq \theta_0$), our non-monotonic results generate welfare distortion. Even though it is difficult to analytically determine $v_B(1) \gtreqless v_B(\theta_0)$, it is obvious that $\theta_f^* \neq \theta_v^*$ when f_B is monotonically decreasing and v_B is monotonically increasing.

Proposition 8. *(i) If $\{\pi > \frac{1}{2}$ and $\phi \in [\phi_1, 1]\}$ or $\{\pi \leq \frac{1}{2}$ and $\phi \in [\phi_1, \phi_2]\}$, the proposer keeps θ lower than the optimal level for consumers, i.e., $\theta_0 = \theta_f^* < \theta_v^* = 1$.*
(ii) If $\{\phi < \phi_0$ and $\pi > \frac{1}{2}\}$ or $\{\pi \leq \frac{1}{2}$ and $\phi < \phi_2\}$, the proposer achieves the maximum consumers' welfare, i.e., $\theta_f^* = \theta_v^* = 1$.

Proposition 8 tells us that, depending on the parameters, welfare loss arises from the conflicting objectives of the proposer and the government. The numerical results are shown in

Figure IV when f_B or v_B has a U-shaped curve.

Figure IV: Fee Revenue and Buyers' Welfare



Note: In each panel, v_B is plotted against the left y-axis, and f_B is against the right y-axis. The range of θ is truncated by $\theta \geq \theta_0$.

This highlights an interesting implication. If the underlying asymmetric information is mild (ϕ is high), as in the left and middle panels, the marginal increase in θ tends to dampen the activity in the B-market. This results in a lower welfare gain in the B-market and reduces the fee revenue for the proposer. Thus, she prefers to keep θ low ($\theta = \theta_0$). The social planner, however, knows that a higher θ boosts the reservation welfare too, and this increment can compensate for losses in the B-market. The level of θ that maximizes buyers' welfare is therefore $\theta = 1$. Thus, the blockchain's parameters and the "rule" for the consensus formation set by the proposer are not enough to achieve θ_v^* and the maximum v_B.

On the other hand, when asymmetric information is relatively severe, as in the right panel, a higher θ facilitates activity in the B-market because P_B increases more than K_B declines. In this case, the fee revenue positively responds to a higher θ, and so does v_B. Therefore, the blockchain environment proposed by the proposer can maximize buyers' welfare.

This is reminiscent of the literature on strategic management, such as Teece (1986) and Brandenburger and Stuart Jr (1996). They suggest that a firm does not fully adopt innovation, even if it creates value for consumers. This is because a firm cannot extract full welfare gain of consumers generated by innovation. We show that this issue arises in the blockchain technology as well. The blockchain innovation generates extra value for consumers both in the

B-market ($P_B K_B > 0$) and C-market ($\frac{dv_0}{d\theta} > 0$). However, since a proposer (or a group of record keepers) cannot extract the extra value in the traditional C-market created by the blockchain technology, she does not adopt the innovation fully.

5 Discussions

5.1 Policy Implications

The preceding discussion indicates that a blockchain proposer values an increment in θ as highly as the social planner only if the price elasticity of the demand is small. This coincidence tends to occur when the underlying information problem is severe because it imposes a higher cost on the migration of buyers. If the market is closer to complete in terms of ϕ or $\Delta\pi$, in contrast, the proposer prefers a lower θ than the socially optimal level since she dislikes a decline in the B-market activity.

This implies that the government should intervene in the intermediation chain to facilitate transactions through the blockchain and to increase θ when the traded goods suffer from non-severe asymmetric information. In contrast, it should remain neutral when the information problem is severe since a proposer voluntarily maximizes consumers' welfare. This runs counter to the traditional views on government intervention in markets with adverse selection (e.g., OTC markets after the recent financial crisis), which believe the government should meddle when adverse selection is severe.

Our conclusion is driven by the fact that asymmetric information arises among agents, while a platform designer, who has a tool to mitigate the problem, is interested only in the fee revenue from a certain part of the market. It fits well if the government does not have a superior tool to detect the lemons and must rely on the technological innovation.

Moreover, one of the ongoing debates on the blockchain management is the separation of record keepers and users of blockchain (Chapman et al., 2017; Cong and He, 2018). It is clear from the model in Section 2.2 that the overlapping communities of record keepers and users keep the consensus from achieving $\theta = 1$ by providing positive R. Separation of users and record keepers can be remedy against this issue and improve the efficiency level. Our model predicts that, however, this type of market structure does not necessarily improve consumers' surplus gain and the blockchain's value since the blockchain transaction can be less attractive for consumers. Once again, it would be critical for a platform proposer or even for the government to know the degree of asymmetric information because it determines whether the policy is effective or harmful for consumers.

5.2 Empirical Implications

We can derive several empirical inferences from our theoretical results. The positive price spread between an asset that is tracked by the blockchain and the one with no blockchains (Proposition 2), as well as the determination of the cryptocurrency price can be easily tested if we have a dataset that contains the transaction price in a market with the blockchain technology, smart contracts, and cryptocurrency.

Information on the wine blockchain is kindly shared by EY Japan. It reveals the financial results of two clients (wine brands) in 2018. One client's retail price per bottle increased from 7.00 to 9.20 Euros, whereas other's increased from 7.00 to 7.46 Euros. Under the assumption that the underlying trend of wine prices is constant, this finding is consistent with the model.

More interestingly, the effect of a marginal increase in the efficiency level of the blockchain is non-monotonic. We have discussed that a change in θ can stem from fluctuations in the record keepers' participation cost (e.g., mining power and difficulty target) and the privacy of the blockchain (i.e., permissioned or permissionless), both controlled by a platform proposer or a group of record keepers. In the real world, this type of change in the rule of consensus formation can involve a "fork" of the blockchain (Abadi and Brunnermeier, 2018; Biais et al., 2018; also, see Appendix C). Our model suggests that, given the nature of a fork (i.e., if it upgrades or downgrades the efficiency), we can predict the consequences for the trading activity, price and quality spreads, a chargeable fee, and the price of digital token if any.

We have established that the result depends on the severity of the informational problem, π and ϕ, as well as the level of efficiency θ. Even if a fork aims to improve the efficiency, it can crimp consumers' surplus and weaken activity on the blockchain by taking a sizable amount of consumers' demand away from it. This negative result is more likely to happen if information asymmetry is not severe or if the traded goods are not that ambiguous regarding quality (high ϕ) but the efficiency level of the chain is questionable (low θ), thereby making consumers anticipate that the blockchain can offer only slightly better quality than the traditional platform.

Furthermore, this mechanism proposes a new factor that alters mining behavior of record keepers (miners). In general, a blockchain platform provides miners with cryptocurrency (token) as the reward of PoW and PoS. Hence, fluctuations in the price of cryptocurrency directly affect the mining behavior. In the existing works that analyze mining incentive (Sapirshtein et al., 2016; Biais et al., 2018; Cong et al., 2018b; Eyal and Sirer, 2018; Saleh, 2018), the reward for mining is determined mostly by how many blocks a miner has mined or whether a chain becomes the longest, but the price of token is not taken into account. Our theory proposes a novel channel through which the behavior of record keepers, the efficiency level θ, and the price of cryptocurrency, Q, interact each other via the secondary market activity.

Also, by the reverse argument, our results can be used as a measure of information asymmetry (π) and quality difference (ϕ). Of course we can infer these parameters in some cases: for example, in the wine market, counterfeits amount to $15 billion (or 5%) per year, and this can be a proxy for $1 - \pi$. In general, however, it depends on in what markets and goods we are interested, and the probability of taking a good-quality product (π) differs depending on the definition of the "quality" which is very subjective. Our model suggests that, given the data on the pre-fork transaction activity and its consequences, we can infer severity of the informational problem for consumers. If an increase in θ results in more (resp. less) activity in the blockchain platform, it indicates that the traded asset suffers from severe (resp. non-severe) informational problems.[43]

[43] This argument can be achieved if we could quantify the quality ϕ which is written in Ethereum as a part of the smart contract.

6 Conclusion

We develop a simple model to analyze some economic implications of the blockchain technology as a new transaction platform. Following the notion of the smart contract, we consider the blockchain protocol as a way to mitigate asymmetric information and investigate the general equilibrium effect of technological innovation on the economy.

Firstly, the blockchain as a platform causes the segmentation of the trading venues and the differentiation of both sides of the markets (buyers and sellers). We consider asymmetric information among the agents and show that the segmentation and differentiation endogenously generate spreads in the price and quality of the assets traded in segmented markets.

We find that the efficiency level of the blockchain has non-monotonic effects on the trading value in the blockchain, the fundamental value of the platform, the price of cryptocurrency, and consumers' welfare. That is, innovation does not necessarily increase the value of the blockchain and consumers' welfare. This is because a more efficient blockchain attracts high-quality assets and boosts their price. Since the price increases more than the quality, the blockchain platform becomes "an exclusive market." When the underlying asymmetric information is not severe, innovation makes a large number of consumers migrate away from the blockchain platform to the traditional one, because they are willing to accept lower-quality assets to save a price cost.

The non-monotonicity leads to a welfare loss when a blockchain proposer, who competes with the traditional market, controls the level of the efficiency by setting the parameters of the blockchain. Since a very efficient blockchain platform is not attractive for most consumers, the platform cannot charge a high access fee. Thus, the proposer has an incentive to keep the efficiency level lower than the first best.

This paper proposes the first theoretical framework to study the measurable outcomes of new digital innovations. The model is simple and general enough to investigate the equilibrium effect of broad types of quality certification, while we take the blockchain as the leading example.

In addition, one possible future project is the extension of this framework into a dynamic setup with more detailed supply mechanisms of cryptocurrency. Our model can be seen as a secondary market of digital tokens, while the supply function of cryptocurrency, driven by miners' behavior, is another salient difference of the blockchain from traditional cash, as Cong et al. (2018b), Pagnotta and Buraschi (2018), Schilling and Uhlig (2018), and other papers in the literature point out. Thus, incorporating both of these factors provides a more comprehensive pricing theory for cryptocurrency.

Also, depending on assets, the smart contract in practice can be more complicated than the one we described in our model. Even though our model can be seen as a deep and competitive market (i.e., Walrasian equilibrium), we can extend it to have a bilateral over-the-counter (OTC) markets based on α-contingent contracts. Besides the property of the optimal contract, it will generate interesting insight for the blockchain-based bilateral trading, such as a tradeoff between search friction (à la Duffie et al., 2005) and better quality, since it has been believed that OTC markets are typically opaque, while the blockchain innovation can make it transparent.

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 being 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.

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.

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.

Asriyan, Vladimir, William Fuchs, and Brett S Green, "Information aggregation in dynamic markets with adverse selection," 2017.

Aune, Rune, Maureen O'Hara, and Ouziel Slama, "Footprints on the Blockchain: Information Leakage in Distributed Ledgers," 2017.

Bartoletti, Massimo and Livio Pompianu, "An empirical analysis of smart contracts: platforms, applications, and design patterns," in "International Conference on Financial Cryptography and Data Security" Springer 2017, pp. 494–509.

Biais, Bruno, Christophe Bisiere, Matthieu Bouvard, and Catherine Casamatta, "The blockchain folk theorem," 2018.

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

Brandenburger, Adam M and Harborne W Stuart Jr, "Value-based business strategy," *Journal of economics & management strategy*, 1996, *5* (1), 5–24.

Camera, Gabriele and Yiting Li, "Another Example of a Credit System that Co-Exists with Money," *Journal of Money, Credit and Banking*, 2008, *40* (6), 1295–1308.

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

Chapman, James, Rodney Garratt, Scott Hendry, Andrew McCormack, and Wade McMahon, "Project Jasper: are distributed wholesale payment systems feasible yet?," *Financial System*, 2017, p. 59.

Chen, Xiaoping, "Market Segmentation, Sorting with Multiple Dimensions of Asymmetric Information," Technical Report, Working Paper 2012.

Chiu, Jonathan and Thorsten V Koeppl, "Trading dynamics with adverse selection and search: Market freeze, intervention and recovery," *The Review of Economic Studies*, 2016, *83* (3), 969–1000.

_ and _ , "The economics of cryptocurrencies–bitcoin and beyond," 2017.

_ and _ , "Blockchain-based Settlement for Asset Trading," 2018.

Cong, Lin William and Zhiguo He, "Blockchain Disruption and Smart Contracts," 2018.

_ , Ye Li, and Neng Wang, "Tokenomics: Dynamic adoption and valuation," 2018.

_ , Zhiguo He, and Jiasun Li, "Decentralized mining in centralized pools," 2018.

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

Duffie, Darrell, Nicolae Gârleanu, and Lasse Heje Pedersen, "Over-the-counter markets," *Econometrica*, 2005, *73* (6), 1815–1847.

Eyal, Ittay and Emin Gün Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Communications of the ACM*, 2018, *61* (7), 95–102.

Foucault, Thierry and Christine A Parlour, "Competition for listings," *Rand Journal of Economics*, 2004, pp. 329–355.

Fuchs, William and Andrzej Skrzypacz, "Costs and Benefits of Dynamic Trading in a Lemons Market," *Working Paper*, 2017.

— **, Brett Green, and Dimitris Papanikolaou**, "Adverse selection, slow-moving capital, and misallocation," *Journal of Financial Economics*, 2016, *120* (2), 286–308.

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.

Gu, Chao, Fabrizio Mattesini, and Randall Wright, "Money and credit redux," *Econometrica, forthcoming*, 2014.

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," 2016.

Khapko, Mariana and Marius A Zoican, "'Smart'Settlement," 2016.

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

Kocherlakota, Narayana and Neil Wallace, "Incomplete record-keeping and optimal payment arrangements," *Journal of Economic Theory*, 1998, *81* (2), 272–289.

Kocherlakota, Narayana R, "Money is Memory," *Journal of Economic Theory*, 1998, *81* (2), 232–251.

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

Lagos, Ricardo and Randall Wright, "A unified framework for monetary theory and policy analysis," *Journal of political Economy*, 2005, *113* (3), 463–484.

Lehmann, Donald R and Lyman E Ostlund, "Consumer perceptions of product warranties: an exploratory study," *ACR North American Advances*, 1974.

Malinova, Katya and Andreas Park, "Market Design with Blockchain Technology," 2017.

Pagnotta, Emiliano and Andrea Buraschi, "An equilibrium valuation of bitcoin and decentralized network assets," 2018.

Palfrey, Thomas and Thomas Romer, "Warranties, performance, and the resolution of buyer-seller disputes," *The Bell Journal of Economics*, 1983, pp. 97–117.

Philippon, Thomas and Vasiliki Skreta, "Optimal interventions in markets with adverse selection," *American Economic Review*, 2012, *102* (1), 1–28.

Rochet, Jean-Charles and Jean Tirole, "Two-sided markets: a progress report," *The RAND journal of economics*, 2006, *37* (3), 645–667.

Rocheteau, Guillaume and Randall Wright, "Money in search equilibrium, in competitive equilibrium, and in competitive search equilibrium," *Econometrica*, 2005, *73* (1), 175–202.

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

Sapirshtein, Ayelet, Yonatan Sompolinsky, and Aviv Zohar, "Optimal selfish mining strategies in bitcoin," in "International Conference on Financial Cryptography and Data Security" Springer 2016, pp. 515–532.

Schilling, Linda and Harald Uhlig, "Some Simple Bitcoin Economics," *NBER Working Paper*, 2018, *No. 24483.*

Szabo, Nick, "Formalizing and securing relationships on public networks," *First Monday*, 1997, *2* (9).

Teece, David J, "Profiting from technological innovation: Implications for integration, collaboration, licensing and public policy," *Research policy*, 1986, *15* (6), 285–305.

Tinn, Katrin, "Blockchain and the Future of Optimal Financing Contracts," 2017.

_ , "'Smart'Contracts and External Financing," *Available at SSRN 3072854*, 2018.

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

_ , "Overcoming adverse selection: How public intervention can restore market functioning," *American Economic Review*, 2012, *102* (1), 29–59.

Voorneveld, Mark and Jörgen W Weibull, "A Scent of Lemon—Seller Meets Buyer with a Noisy Quality Observation," *Games*, 2011, *2* (1), 163–186.

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.

A Appendix: From the Microfoundation to the Main Model

This section explains how to embed the preliminary model in Section 2.2 in our main model in Section 3. First, we use $s \in \{0, 1\}$ to denote the true state with $\Pr(s = 1) = \pi$. Also, a seller's utility, U_S, is now replaced by $\{W_j\}_{j\in\{0,B,C\}}$ in the main model. For notational convenience, we use α to indicate each seller with type α (e.g., s_α represents s of a type-α seller). The consensus generating mechanism is the same as (2).

Consider $k = 1, 2 \cdots, N$ record keepers who monitor the states of all the sellers. As in Section 2.2, a record keeper k obtains the following utility by reporting $\hat{s}^k \equiv (\hat{s}_{k,\alpha})_{\alpha\in[0,1]}$, where $\hat{s}_{k,\alpha}$ denotes the report for s_α.

$$\max_{\hat{s}^k} U^k_{RK} = \int_{\alpha\in\mathcal{B}} E\left[R\mathbb{I}_{\{\hat{s}_\alpha=1\}} - c_k|\hat{s}_{k,\alpha} - s_\alpha|\right] dF. \tag{21}$$

$\mathcal{B}$ denotes the set of sellers who try to sell in the B-market. Thus, (21) is an aggregated (1). We assume that N is sufficiently large so that each record keeper does not behave strategically.

Note that the optimal reporting profile is determined by maximizing the utility for each α, i.e., $\hat{s}_{k,\alpha}$ maximizes (1). Therefore, the optimal reporting strategy is

$$\hat{s}_{k,\alpha} = \begin{cases} 1 & \text{if } s_\alpha = 1 \\ 1 & \text{if } s_\alpha = 0 \text{ and } RN^{-1} > c_k \\ 0 & \text{otherwise.} \end{cases}$$

This implies that, if a type-α seller is of high quality, all the record keepers report the true state. On the other hand, if a seller is of low type, the discussion in Section 2.2 implies that each record keeper tries to manipulate it only if $RN^{-1} > c_k$.

As a result, the consensus that each seller expects to obtain is as follows: if she is H-type, a seller always obtains $\hat{s}_\alpha = 1$ and gets to sell her bottle. If a seller is L-type,

$$\hat{s}_\alpha = \begin{cases} 1 & \text{w.p. } \sum_{i=1}^{N} \frac{\psi_{i,N}}{N} \\ 0 & \text{otherwise.} \end{cases}$$

Thus, for L-type sellers, her product will get the high consensus and be sold only with probability $1 - \theta \equiv \sum_{i=1}^{N} \frac{\psi_{i,N}}{N}$. With the complement probability, the blockchain rejects the fraudulent report, and she has to consume her bottle by her own. This defines the trading benefit of sellers $\{W_j^L, W_j^H\}_{j \in \{0,B,C\}}$ in the main model. The structure of the buy-side market stays the same as in the main model.

Importantly, knowing that a low-quality bottle can get bad consensus and be rejected with probability $\theta = 1 - \sum_{i=1}^{N} \frac{\psi_{i,N}}{N}$, each low-type seller's behavior changes, and the set $\mathcal{B}$ variates. The assumption that each record keeper does not reckon with the effect of her report on $\mathcal{B}$ is justified by two ways. First possibility is that N is sufficiently large as mentioned earlier. The second possibility is that a record keeper understands that her report may change the behavior of individual type-α seller, but this seller is atomistic and does not have any impact on the equilibrium condition.

B Appendix: Cash-Market Breakdown

The result with $\theta \leq \theta_0$ seems rather drastic: the existence of the blockchain platform can completely destroy the activity of the cash market when the efficiency level θ is sufficiently *low*. This is a consequence of θ being too low to sustain $\alpha_I = P_C - (1-\theta)P_B > 0$. We denote the region $\Theta_{NC} \equiv (0, \theta_0]$ as the *no C-market* region.

The result comes from the supply-side behavior. Remember that only L-type sellers trade their assets in the C-market. They wish to sell the asset at a higher price P_B, but they fear rejection. $\theta \leq \theta_0$ makes the rejection risk sufficiently small so that the price improvement in the B-market becomes dominant. As a result, all the sellers migrate out of the C-market and try to sell in the B-market.

Of course, this increases P_C because the supply shrinks to zero, but the price is bounded and cannot explode due to the existence of outside options for buyers (buying in the B-market or staying inactive). Also, the higher share of high-quality assets in the B-market always makes $P_B > P_C$ even at the limit of $K_C^S = 0$, making the shutdown of the C-market an equilibrium outcome.

We can characterize Θ_{NC} as follows:

Corollary 4. *A smaller ϕ and π make the cash-market breakdown more likely, i.e., they make Θ_{NC} larger.*

Proof. Immediate from Lemma 2. □

This result should also be intuitive if we recall that the critical θ is expressed as $\theta_0 = \frac{P_B - P_C}{P_B}$. The lower ϕ and π mean that the underlying asymmetric information is severe, and both make buyers more eager to trade in the B-market, leading to a larger spread, $P_B - P_C$, sustainable. Then, sellers of low-quality assets are more willing to sell in the B-market and are likely to abandon the traditional cash market.[44]

C Examples of Forks and Changes in Parameters

Since Bitcoin was launched in 2009, many other cryptocurrencies with different environments of the consensus formation have been developed. A part of these alternatives are implemented "from scratch," meaning that they are not using Bitcoin source code (not forked from Bitcoin blockchain), while others are derived from the source code and involve a fork. As a reference, Bitcoin's parameters for the consensus formation is as follows: a difficulty target is to generate block every 10 minutes, the total supply of coin is 21 million coins, it uses SHA256 hashing algorithm, and PoW is the rule of consensus formation.

Litecoin It is released on October 7, 2011 by Charlie Lee, a Google employee. The difficulty target is reduced to 2.5 minutes, which makes the total supply of coin fixed at 84 million by 2140. The consensus generating algorithm is script PoW—an algorithm originally designed for password stretching (brute-force resistance).

Dogecoin Dogecoin was created by programmer Billy Markus from Portland, Oregon, and released in December 2013 as a fork of Litecoin. Its difficulty target is 60 seconds and use script PoW.

Blackcoin It is forked in February 2014 by the developer called Rat4. Its difficulty target is 1 minute and does not have total currency supply cap. Notably, it adopts Proof-of-Stakes (PoS) consensus formation.

Bitcoin Cash It is proposed by Bitcoin community including Roger Ver and forked by mining pools, such as ViaBTC. It expanded transaction capacity of Bitcoin to 8MB and removed Segregated Witness code optimization.

NXT It is an example of "from-scratch" implementation of an alternative protocol. It uses PoS as consensus generation, enables name registry, a de-centralized asset exchange, de-centralized messaging, and stake delegation (delegated PoS).

These are the just the tip of the iceberg, and many other examples can be found at forkdrop.io.

[44] Technically, we can avoid this by considering the general model with $\lambda < 1$, by restricting our focus on $\theta \geq \theta_0$, and by modifying the model according to the discussion in note 33.

Online Appendix

D Online Appendix: Generalized Model with Uninformed Sellers

Consider the same structure as in the main model. In addition, assume that a seller is informed with probability λ and uninformed with probability $1-\lambda$. If one is informed, she knows a specific characteristic of high-quality assets and can distinguish the lemons, while uninformed agents cannot tell the difference.[45] The optimal behavior of informed sellers is same as the main model.

D.1 Optimal Behavior of Uninformed Sellers

Behavior of an uninformed seller is determined by comparing the following returns:

$$\begin{aligned} W_0^U &= (\pi + \phi(1-\pi))\alpha, \\ W_C^U &= P_C, \\ W_B^U &= (\pi + (1-\pi)(1-\theta))P_B + (1-\pi)\theta\phi\alpha. \end{aligned} \tag{22}$$

The first one is the return from consuming her own asset, the second one is the return from selling in the C-market, and the last one is the return from selling in the B-market. In the last case, she obtains P_B if the transaction is completed, while she ends up consuming her asset if her order is rejected. The two coefficients in (22) represent the probability of successful trade and rejection. Let

$$\tilde{\pi} \equiv \pi + \phi(1-\pi), \pi_0 \equiv \pi + (1-\pi)(1-\theta)$$

and define a parameter

$$\xi \equiv \frac{\pi + (1-\pi)(1-\theta)}{\pi + \phi(1-\pi)(1-\theta)}\tilde{\pi}.$$

The behavior of uninformed sellers is similar to those of informed sellers with low-quality assets since both of them fear the risk of detection. As we can see from (22), however, the return from selling in the B-market, W_B^U, is lower than that of informed sellers, W_B^L in (9), because the return is discounted by the probability that her asset is of low-quality. On the other hand, the return from selling in the C-market is not affected by this.

Sufficiently low price in the B-market

If the price in B-market is sufficiently low ($\xi P_B \leq P_C$), trading in the B-market is not optimal: they try to sell in the C-market or stay inactive. Hence, there is a unique threshold

$$\alpha^U = \frac{P_c}{\tilde{\pi}}.$$

[45] In this case, assume, for simplicity, that the realization of α is independent of the realization of being informed or uninformed.

This separates uninformed sellers who go to the C-market and stay inactive. The amount of sell orders from *uninformed* sellers is

$$S_B^U = 0,$$
$$S_C^U = (1-\lambda)F\left(\frac{P_C}{\tilde{\pi}}\right),$$

and they directly corresponds to the supply amounts: $K_j^U = S_j^U$.

Sufficiently high price in the B-market

On the other hand, if the price in the B-market is sufficiently high, $\xi P_B > P_C$, the uninformed sellers use both of the two markets because the higher price in the B-market strictly outweighs the risk of holding lemons for high-α sellers. That is, there are two thresholds,

$$\alpha_0^U = \frac{P_C - \pi_0 P_B}{\phi\theta(1-\pi)}, \alpha_1^U = \frac{\pi_0}{\pi + \phi(1-\pi)(1-\theta)} P_B,$$

which separate uninformed sellers into three groups. As in the case of informed sellers of low-quality assets, uninformed sellers (i) sell in the C-market if $\alpha \leq \alpha_0^U$, (ii) in the B-market if $\alpha \in (\alpha_0^U, \alpha_1^U]$, and (iii) stay inactive otherwise. Hence, the amount of sell orders from uninformed traders is

$$S_B^U = (1-\lambda)[F(\alpha_1^U) - F(\alpha_0^U)],$$
$$S_C^U = (1-\lambda)F(\alpha_0^U),$$

and the supply after the screening by the blockchain is

$$K_B^U = (1-\lambda)\pi_0[F(\alpha_1^U) - F(\alpha_0^U)],$$
$$K_C^U = (1-\lambda)F(\alpha_0^U).$$

D.2 Aggregate Supply and Market Quality

Let χ be an indicator function for $\xi P_B > P_C$, i.e., $\chi = \mathbb{I}_{\{\xi P_B > P_C\}}$. The aggregate supply sums up the supply from both types of sellers:

$$K_C^S = \lambda(1-\pi)F(\alpha_I) + (1-\lambda)\left[\chi F(\alpha_0^U) + (1-\chi)F\left(\frac{P_C}{\tilde{\pi}}\right)\right] \tag{23}$$

$$K_B^S = \lambda\left\{\pi F(P_B) + (1-\pi)(1-\theta)\left[F\left(\frac{P_B}{\phi}\right) - F(\alpha_I)\right]\right\} \tag{24}$$
$$+ (1-\lambda)\pi_0\chi[F(\alpha_1^U) - F(\alpha_0^U)].$$

By using these equations, we can derive the average quality in both markets:

$$\pi_C = \frac{(1-\lambda)\pi\left[\chi F(\alpha_0^U) + (1-\chi)F\left(\frac{P_C}{\tilde{\pi}}\right)\right]}{K_C^S} \tag{25}$$

$$\pi_B = \frac{\lambda\pi F(P_B) + (1-\lambda)\pi\chi[F(\alpha_1^U) - F(\alpha_0^U)]}{K_B^S}. \tag{26}$$

The determination of Q is the same as before.

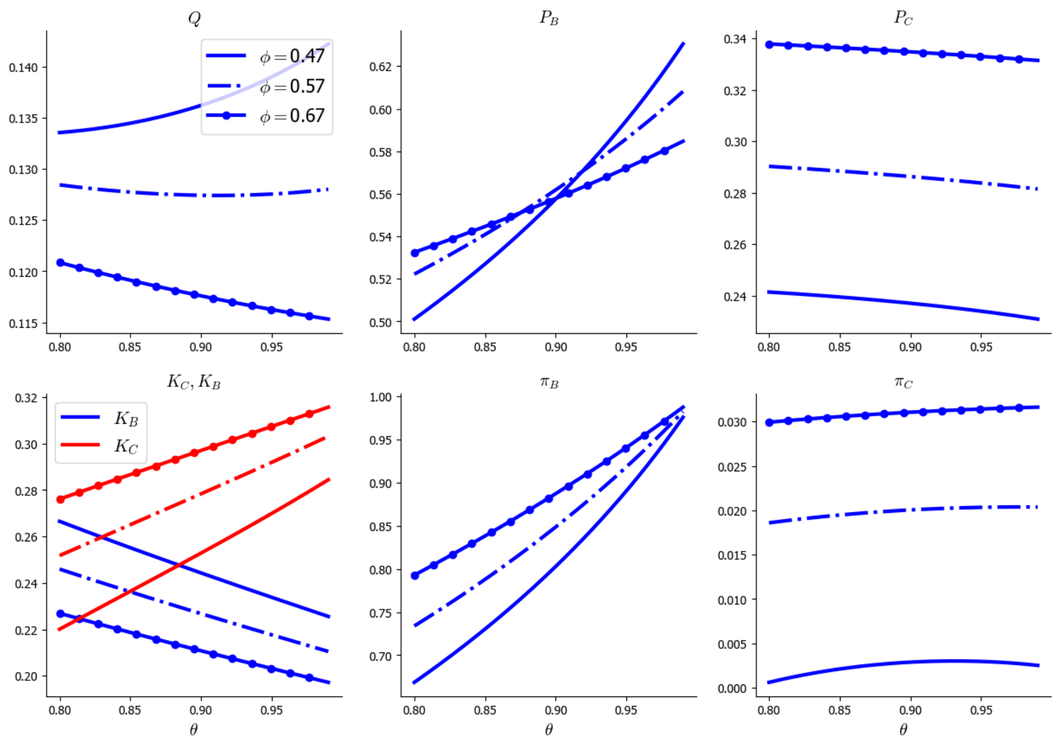
D.3 Numerical Examples for the General Model

The generalized model cannot be characterized analytically. Thus, we conduct numerical simulations. Figure V plots the effect of θ on the economic variables with different values of ϕ.

First, the solid lines represent our results when asymmetric information is relatively severe ($\phi = 0.47$).[46] We obtain a monotonically increasing $Q = K_B P_B$, P_B, K_C, and π_B, while P_C and K_B is decreasing. These results are consistent with those in the benchmark model. Namely, a severe informational problem makes it costly for the B-market consumers to switch to the C-market, thereby minimizing a decline in K_B compared to an increase in P_B. This leads to the increasing trading activity in the B-market.

As asymmetric information becomes less severe ($\phi = 0.57$), the non-monotonicity in Q arises. This is given by the dashed lines in the figure. If it becomes even less severe ($\phi = 0.67$), migration motivation becomes stronger because purchasing in the C-market and consuming low-quality assets do not harm utility much. As a result, Q becomes monotonically increasing in θ. These results show that our arguments in the benchmark model are robust even if we consider a more general information structure.

Figure V: Effect of θ with uninformed sellers



[46] Other parameter values for the numerical examples are given by $\lambda = 0.9$ and $\pi = 0.45$.

E Online Appendix: Generalized Model with Limited Blockchain Access

This section provides a model in which only a certain fraction of agents have access to the B-market. Suppose that with probability $\gamma_B, \gamma_S \in (0,1)$, buyers and sellers can participate in the B-market. Otherwise, the behavior of agents is restricted to participating in the C-market or staying inactive. By the law of large numbers, γ_j represents the fraction of buyers and sellers who can participate in the B-market. Given the price and quality, behavior of these agents is same as the benchmark model. In the following discussion, we call buyers and sellers with no access to the B-market the "*restricted* agents."

A restricted buyer compares $V_C = \tilde{\pi}_C \alpha - P_C$ to $V_0 = 0$. Thus, restricted buyers with $\alpha \geq \frac{P_C}{\tilde{\pi}_C}$ purchase assets in the C-market, while other agents stay inactive. Then, the total demand is given by

$$K_j^D = \begin{cases} \gamma_B(1 - F(\alpha^*)) & \text{for } j = B \\ \gamma_B\left[F(\alpha^*) - F\left(\frac{P_C}{\tilde{\pi}_C}\right)\right] + (1-\gamma_B)\left[1 - F\left(\frac{P_C}{\tilde{\pi}_C}\right)\right] & \text{for } j = C. \end{cases}$$

If a restricted seller has a low-quality asset, she compares $W_C^L = P_C$ to $W_0^L = \phi\alpha$. Thus, the set of low-type restricted sellers who supply in the C-market is $\alpha \in [0, \frac{P_C}{\phi}]$. The same argument derives the set of high-type restricted seller to the C-market if $\alpha \in [0, P_C]$. As a result, the total selling *attempt* is given by

$$\begin{aligned} S_B &= \gamma_S\left[\pi F(P_B) + (1-\pi)\left(F\left(\frac{P_B}{\phi}\right) - F(\alpha_I)\right)\right] \\ S_C &= \pi(1-\gamma_S)F(P_C) + (1-\pi)\left[\gamma F(\alpha_I) + (1-\gamma_S)F\left(\frac{P_C}{\phi}\right)\right], \end{aligned}$$

which results in the following supply function:

$$K_j^S = \begin{cases} \gamma_S\left[\pi F(P_B) + (1-\pi)(1-\theta)\left(F\left(\frac{P_B}{\phi}\right) - F(\alpha_I)\right)\right] & \text{for } j = B \\ S_C & \text{for } j = C. \end{cases}$$

Note that this modification does not change the properties of the B-market: it scales the activity in the B-market down (or up) by γ_B/γ_S. However, this modification affects the C-market. Specifically, as in Appendix D, we have $\pi_C > 0$ since a certain fraction of agents must be stuck at the C-market. By following the same procedure as in Appendix F, we can show that $\pi_B > \pi_C$ and $P_B > P_C$ as long as $\theta > 0$.

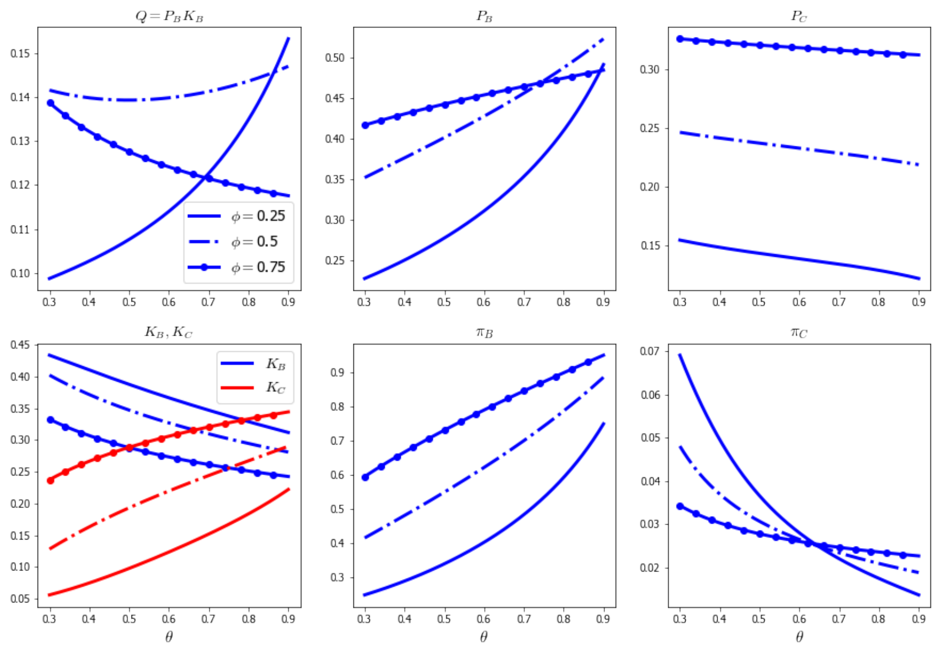
We solve this model numerically. Figure VI shows the behavior of main variables with different values of ϕ.[47] We can confirm that our result in the main model is robust, and our intuitions can be applied.

The definition of (*ex-ante*) consumers' welfare is slightly modified. Let v_B^γ be the aggregate welfare of consumers when they face the access restriction with γ_B:

$$\begin{aligned} v_B^\gamma &\equiv \gamma_B\left[\int_{\alpha^*}(\alpha\tilde{\pi}_B - P_B)dF(\alpha) + \int_{\frac{P_C}{\tilde{\pi}_C}}^{\alpha^*}(\alpha\tilde{\pi}_C - P_C)dF(\alpha)\right] + (1-\gamma_B)\int_{\frac{P_C}{\tilde{\pi}_C}}(\alpha\tilde{\pi}_C - P_C)dF(\alpha) \\ &= \gamma_B v_B^0 + (1-\gamma_B)v_0 \\ &= \gamma_B\Delta v + v_0. \end{aligned}$$

[47]The other parameters are set to $(\pi, \gamma_B, \gamma_C) = (0.5, 0.9, 0.9)$.

Figure VI: Effect of θ with restricted participation



In the equations above, v_B^0 is the welfare of those who have blockchain access and defined by (16). $\Delta v = v_B^0 - v_0$ is the welfare gain, and v_0 is the reservation welfare, both defined by (17). From this equation, the maximum fee that the blockchain platform can charge is modified as

$$f^{\gamma} = \gamma_B \Delta v.$$

From these equations and the results in Figure VI, it is obvious that the behavior of welfare-related variables, including f^{γ}, have the same implications as the main model. The only difference is that the welfare gain due to the B-market, as well as the fee revenue of the platform, is discounted by γ_B since only γ_B fraction of consumers can exploit the new platform.

F Online Appendix : Proof

F.1 Proof for Proposition 1 and 2

The following argument proves the claim under the generalized model with $\lambda \in [0, 1]$ whose equilibrium conditions are provided in Appendix D. Making $\lambda = 1$ proves the proposition for the benchmark model.

Our arguments start from two conditions. In the buyers' problem, our guesses are

$$P_B \tilde{\pi}_C > P_C \tilde{\pi}_B \tag{27}$$

and

$$\pi_B > \pi_C. \tag{28}$$

Given these, the buyers' partial equilibrium implies that

$$\frac{P_B}{\tilde{\pi}_B} - \frac{P_C}{\tilde{\pi}_C} = (1 - K) + (\tilde{\pi}_B - \tilde{\pi}_C)K_C - (1 - K) > 0,$$

where $K = K_B + K_C$. Therefore, we have shown that the inequality (27) holds in the equilibrium as long as the guess (28) is correct (note that (28) and $\tilde{\pi}_B > \tilde{\pi}_C$ are equivalent).

As the next step, we obtain π_B and π_C in the general equilibrium under the guess (28) (and (27)). By letting $\Delta\pi \equiv \pi_B - \pi_C$ and F be uniform, we have

$$\Delta\pi = \frac{\pi}{K_B K_C}\left[L - \lambda(1-\lambda)(1-\pi)(1-\theta)\beta_0^U \frac{\Delta P}{\phi\theta}\right] \tag{29}$$

where $\Delta P = P_B - P_C$ and

$$L = \lambda(1-\pi)\alpha_I(P_B + \beta_1^U) + (1-\lambda)\beta_0^U(\lambda(1-\pi)P_B + (1-\lambda)(1-\pi_0)\beta_1^U),$$

$$\beta_0^U = \frac{P_C}{\tilde{\pi}} + \chi\left(\alpha_0^U - \frac{P_C}{\tilde{\pi}}\right), \beta_1^U = \chi(\alpha_1^U - \alpha_0^U).$$

Since both of $\alpha_0^U - P_C/\tilde{\pi}$ and $\alpha_1^U - \alpha_0^U$ are (positively) proportional to $\xi P_B - P_C$, we have $\beta_0^U > 0$ and $\beta_1^U \geq 0$. Therefore, $L > 0$. Moreover, from (8), the difference in prices is

$$\Delta P = (\tilde{\pi}_B - \tilde{\pi}_C)(1 - K_B) = (1 - K_B)(1-\phi)\Delta\pi, \tag{30}$$

where we obviously have $K_B < 1$. By plugging this into (29), we obtain

$$\Delta\pi = \frac{\pi}{K_B K_C}\left[L - \lambda(1-\lambda)(1-\pi)(1-\theta)\beta_0^U \frac{(1-K_B)(1-\phi)}{\phi\theta}\Delta\pi\right]$$

$$\therefore \Delta\pi = \frac{\frac{\pi}{K_B K_C} L}{1 + \frac{\pi}{K_B K_C}\lambda(1-\lambda)(1-\pi)(1-\theta)\beta_0^U \frac{(1-K_B)(1-\phi)}{\phi\theta}} > 0.$$

Thus, the guess (28) holds in the general equilibrium, and (30) implies $P_B > P_C$.

F.2 Proof for Lemma 2 and Corollary 3

Suppose that we have $\alpha_I > 0$. Then the equilibrium solves

$$\begin{aligned}
K_C^S &= (1-\pi)\frac{P_C - (1-\theta)P_B}{\theta\phi}, K_B^S = \pi P_B + (1-\pi)(1-\theta)\left(\frac{P_B - P_C}{\phi\theta}\right), \\
K_B^D &= 1 - \frac{P_B - P_C}{(1-\phi)\pi_B}, K_C^D = \frac{P_B - P_C}{(1-\phi)\pi_B} - \frac{P_C}{\phi}, \\
\pi_B &= \frac{\pi P_B}{K_B}.
\end{aligned} \tag{31}$$

Let $S = (P_B - P_C)/P_B$ be the normalized spread across markets. Then, rearranging the trading volumes gives

$$K_B^D = 1 - \frac{S}{\pi(1-\phi)} K_B^S, \frac{K_B^S}{P_B} = \pi + (1-\pi)(1-\theta)\frac{S}{\phi\theta},$$

$$K_C^S = \frac{1-\pi}{\phi} P_B\left(1 - \frac{S}{\theta}\right), K_C^D = \frac{S K_B^S}{\pi(1-\phi)} + \frac{P_B S}{\phi} - \frac{P_B}{\phi}.$$

By equating $K_C^S = K_C^D$ and substituting K_B^is, we get a quadratic equation for S. Namely, in the equilibrium, S solves

$$\frac{S}{1-\phi} + \frac{(1-\pi)(1-\theta)}{\phi\pi\theta(1-\phi)}S^2 + \frac{S-1}{\phi} - \frac{1-\pi}{\phi} + \frac{1-\pi}{\theta\phi}S = 0.$$

Note that the LHS is monotonically increasing in $S(\geq 0)$, and the condition $\alpha_I > 0$ is identical to $S < \theta$ by definition (10). Thus, in the equilibrium, $\alpha_I > 0$ if and only if

$$\frac{\theta}{1-\phi} + \frac{(1-\pi)(1-\theta)}{\phi\pi\theta(1-\phi)}\theta^2 + \frac{\theta-1}{\phi} - \frac{1-\pi}{\phi} + \frac{1-\pi}{\theta\phi}\theta > 0,$$

which can be rewritten as

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

Note that if $\theta = 0$ then the LHS of this inequality is positive, while if $\theta = 1$ then it is negative. Thus, the smaller solution of the equation $\theta^2(1-\pi) - \theta + \pi(1-\phi) = 0$ is between 0 and 1. We set this solution as θ_0. Thus, $\alpha_I > 0$ if and only if $\theta_0 < \theta \leq 1$.

Next, suppose that $P_C - (1-\theta)P_B \leq 0$. This induces $\alpha_I = 0$ by definition (10), and the equilibrium solves

$$\begin{aligned}
&K_C^S = 0, K_B^S = \pi P_B + (1-\pi)(1-\theta)\frac{P_B}{\phi}, && (32)\\
&K_B^D = 1 - \frac{P_B - P_C}{\tilde{\pi}_B - \phi}, K_C^D = \frac{P_B - P_C}{\tilde{\pi}_B - \phi} - \frac{P_C}{\phi},\\
&\pi_B = \frac{\pi P_B}{K_B}.
\end{aligned}$$

By using the market clearing in C-market and the definition of π_B, we obtain

$$K_B^D = 1 - \frac{mP_B - \phi}{(1-\phi)\pi P_B}K_B^S, K_B^S = \left(\pi + \frac{(1-\theta)(1-\pi)}{\phi}\right)P_B,$$

with $m = 1 + \pi\phi + (1-\pi)(1-\theta)$. By clearing B-market, we have

$$P_B = \frac{\phi(\pi + (1-\pi)(1-\theta))}{(2-\theta(1-\pi))(\phi\pi + (1-\pi)(1-\theta))}, \tag{33}$$

$$K_B = \frac{\pi + (1-\pi)(1-\theta)}{2-\theta(1-\pi)}. \tag{34}$$

Moreover, we can express the market clearing in B-market by using S:

$$K_B\left(1 + \frac{S}{\pi(1-\phi)}\right) = 1.$$

By plugging the explicit solution of K_B, we have

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

Since S is monotonically increasing in θ, the condition $P_C - (1-\theta)P_B \leq 0$ is identical to $\theta < S$, that is

$$\theta^2(1-\pi) - \theta + \pi(1-\phi) \geq 0.$$

Therefore, the condition is $\theta \leq \theta_0$, and we have established that the equilibrium is continuous at $\theta = \theta_0$.

Proof of Corollary 3

Results for P_B and π_B are obvious from (33) and (32) in Appendix F.2. By using (33) and (34), we have

$$Q = \left(\frac{\pi + s}{1 + \pi + s}\right)^2 \frac{\phi}{\phi\pi + s}, \; s = (1-\pi)(1-\theta).$$

Then

$$\frac{dQ}{ds} \propto 2(\phi\pi + s) - (\pi + s)(1 + \pi + s) \equiv D_Q,$$

and

$$(1-\pi)D_Q = -\theta^2(1-\pi) + \theta - \frac{1 + 2\pi(1-\phi)}{1-\pi} < 0$$

where the last inequality comes from $\theta \leq \theta_0$. With the fact that $ds/d\theta < 0$, we have $dQ/d\theta > 0$. The result for K_B is obvious, and that for P_C is given by solving equilibrium condition. Specifically, it reduces to

$$P_C = \frac{\phi}{2 - \theta(1-\pi)}.$$

F.3 Proof for Proposition 3 and 5

To see the uniqueness, we plot these K_B's against P_B (see Figure VII). Obviously, K_B^S is positive linear function in P_B. We can also check that K_B^D is concave, has only one inflection point in $P_B > 0$, and $\frac{dK_B^D}{dP_B} < 0$ for a sufficiently large P_B. Since $K_B^D = 1 > K_B^S$ at P_B such that $K_B^S = 0$, these two curves cross only once in $P_B > 0$.

First, by $K_B^D + K_C^D = 1 - P_C/\phi$, and equating $K_j^D = K_j^S$, we obtain

$$P_C = \frac{\phi}{2-\pi}(1 - \pi P_B). \tag{35}$$

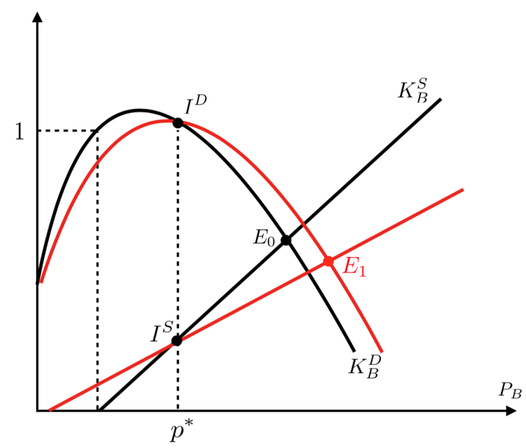
Now, suppose that θ increases. This is represented by the red curves in Figure VII. We have

$$p^* = \frac{\phi}{2 - \pi(1-\phi)} \tag{36}$$

such that $P_B \gtrless P_C \Leftrightarrow P_B \gtrless p^*$. Also, let $g \equiv \frac{1-\theta}{\theta}$, $\eta \equiv 1 + \frac{\phi\pi}{2-\pi}$. In the equilibrium, we have $K_B^S = K_B^D \equiv K_B$, so that they are respectively expressed as

$$K_B = P_B\left[\pi + \frac{(1-\pi)}{\phi} g\eta\right] - \frac{1-\pi}{2-\pi} g,$$
$$K_B = \frac{(1-\phi)\pi P_B}{((1-\phi)\pi + \eta)P_B - \frac{\phi}{2-\pi}}. \tag{37}$$

Figure VII: Effect of θ on B-market



By equating these two equations and rearranging it in terms of $y \equiv P_B^{-1}$, we obtain

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

For this function, we have

$$\frac{\partial H}{\partial g} = \frac{1-\pi}{\phi(2-\pi)}(2 - \pi(1-\phi) - \phi y) > 0, \tag{38}$$

$$\frac{\partial H}{\partial y} = -\frac{\pi(1-\phi)((1-\phi)\pi + \eta)}{[((1-\phi)\pi + \eta) - \frac{\phi}{2-\pi}y]^2} - \frac{1-\pi}{2-\pi} g < 0. \tag{39}$$

Note that both inequality comes from $P_B > P_C$ (equivalently, $P_B > p^*$). These confirm, by the implicit function theorem, $dP_B/d\theta > 0$.

We rearrange the equation for π_B as

$$\pi_B = \frac{\pi}{\pi + \frac{1-\pi}{\phi} g(1 - \frac{P_C}{P_B})},$$

which implies

$$\mathrm{sgn}\left(\frac{d\pi_B}{d\theta}\right) = -\mathrm{sgn}\left(\frac{d\pi_B}{dg}\right) = \mathrm{sgn}\left(\frac{d}{dg}\left[g(1 - \frac{P_C}{P_B})\right]\right).$$

By using (35), we can rewrite the inside of the last brackets:

$$1 - \frac{P_C}{P_B} = 1 - \frac{\frac{\phi}{2-\pi}(1 - \pi P_B)}{P_B} \propto \frac{2 - \pi(1-\phi) - \phi y}{2-\pi}.$$

Hence, the last term can be calculated as follows.

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

where the second line comes from the implicit function theorem, and the third to last lines are due to (38), (39) and $P_B > p^*$. Thus, we established that $\frac{d\pi_B}{d\theta} > 0$. Also, K_B is decreasing in θ, which is immediate from (37). The statement (iii) can be checked by the decreasing K_B and $\Delta P/\Delta\tilde{\pi} = 1-K_B$ in the equilibrium.

As for the price Q, (37) yields

$$QB_S = P_B K_B = \frac{(1-\phi)\pi P_B^2}{((1-\phi)\pi+\eta)P_B - \frac{\phi}{2-\pi}}.$$

Since the right hand side does not contain θ, taking a derivative of the last term is

$$\frac{dQ}{d\theta} = \frac{dP_B}{d\theta}\frac{dQ}{dP_B} \propto (\eta+(1-\phi)\pi)P_B - \frac{2\phi}{2-\pi}.$$

Therefore, there is an inflection point

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

which determines the sign of the effect:

$$\frac{dQ}{d\theta} \gtrless 0 \Leftrightarrow P_B \gtrless p^{**}. \tag{40}$$

Now, by using the implicit formula $H(P_B^{-1}, g) = 0$ and the fact that $P_B H(P_B^{-1}, g)$ is monotonically increasing in P_B, the condition (40) is identical to

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

Note that A is monotonically decreasing in θ (this can be confirmed by using $P_B > p^*$ again). By letting θ fluctuate from θ_0 to 1, we have the following result.

(i) If $\phi > (2-\pi)/(3-\pi)$, then $A(\theta) > 0$ for all $\theta \in [\theta_0, 1]$, which implies that $P_B > p^{**}$ always holds in the equilibrium, leading to a monotonically decreasing Q. (ii) If $\phi \le (2-\pi)/(3-\pi)$, then $A(1) < 0$, so Q is decreasing in high-θ region. 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 $A(g) = 0$ as

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

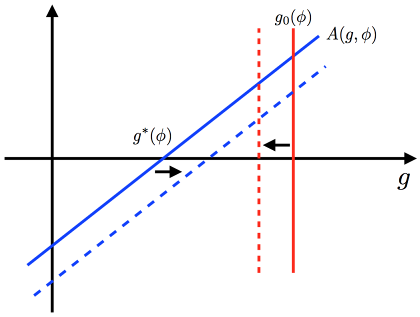
Since $A(g)$ is increasing in ϕ, we have $dg^*/d\phi < 0$. Note that we are focusing on $\theta > \theta_0$, which means

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

From the definition of θ_0, we know θ_0 is decreasing and 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 $\theta_0 \to \mathbb{I}_{\{\pi\geq 1/2\}} + \mathbb{I}_{\{\pi<1/2\}}\frac{\pi}{1-\pi}$. Figure VIII shows the effect of a smaller ϕ on g^* and g_0. We have following two possibilities.

Figure VIII: Behavior of A



(ii-a) Suppose that $\pi \geq 1/2$. Then there is ϕ_0 that solves

$$g^*(\phi) = g_0(\phi). \tag{41}$$

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

(ii-b) Also, consider the case with $\pi < 1/2$. In this case, 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 and Q is increasing when $\theta > \theta^*$ and decreasing when $\theta < \theta^*$. On the other hand, if $0 \leq \pi \leq \pi^*$, then the arguments go back to the case **(ii-a)** and the same results hold.

G Welfare Analyses

G.1 Welfare Analyses for Buyers

The buyers' welfare in aggregate is

$$\begin{aligned} v_B &= \int_{\alpha^*} (\Delta\tilde{\pi}\alpha - \Delta P)dF + \int_{P_C/\phi} (\phi\alpha - P_C)dF \\ &= \frac{\Delta\tilde{\pi}}{2}(1-\alpha^*)^2 + \frac{\phi}{2}(1-\frac{P_C}{\phi})^2 \\ &= \frac{1}{2}\left[\pi(1-\phi)P_B K_B + \frac{\phi}{(2-\pi)^2}(1-\pi+\pi P_B)^2\right], \end{aligned} \tag{42}$$

where the second term comes from $\alpha^* = \Delta P/\Delta\tilde{\pi}$, and the last term comes from (35), (15), $K_j^S = K_j^D$, and the definition of π_B:

$$\Delta\tilde{\pi} = (1-\phi)\frac{\pi P_B}{K_B}.$$

The property of the first term is given by Proposition 5, while the second term is monotonically increasing in θ. Furthermore, by using (37),

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

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

$$\frac{d2v_B}{dP_B} \equiv D_B = ((1-\phi)\pi)^2 \frac{P_B(hP_B - 2\frac{\phi}{2-\pi})}{(hP_B - \frac{\phi}{2-\pi})^2} + \frac{2\phi\pi}{(2-\pi)^2}(1-\pi+\pi P_B).$$

The second order derivative yields

$$\begin{aligned}\frac{dD_B}{dP_B} &= \frac{2((1-\phi)\pi)^2}{(hP_B - \frac{\phi}{2-\pi})^3}\left[\left(hP_B - \frac{\phi}{2-\pi}\right)^2 - hP_B\left(hP_B - \frac{2\phi}{2-\pi}\right)\right] + \frac{2\phi\pi^2}{(2-\pi)^2} \\ &= \frac{2((1-\phi)\pi)^2}{(hP_B - \frac{\phi}{2-\pi})^3}\frac{\phi^2}{(2-\pi)^2} + \frac{2\phi\pi^2}{(2-\pi)^2} > 0.\end{aligned}$$

We also have $P_B(\theta = 1) \equiv \hat{p}_1 = \frac{1-\phi+\frac{\phi}{2-\pi}}{h}$ and can check $D_B(P_B = \hat{p}_1) > 0$. Thus, if $\lim_{\theta\to\theta_0} D_B < 0$, there is a unique θ^* such that $D_B \gtrless 0 \Leftrightarrow \theta \gtrless \theta^*$, while if $\lim_{\theta\to\theta_0} D_B > 0$, then $D_B > 0$ for all θ.

The following formulas at $\theta = \theta_0$ simplify the analyses. First, as $\theta \searrow \theta_0$, we have

$$P_C = \frac{\phi}{2-\pi}(1-\pi P_B) = (1-\theta_0)P_B, \tag{43}$$

$$\therefore P_B = \tilde{p} \equiv \frac{\phi}{\pi\phi + (1-\theta_0)(2-\pi)}. \tag{44}$$

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

$$\begin{aligned}\lim_{\theta\searrow\theta_0} K_B^D &= \lim_{\theta\searrow\theta_0}\left(1 - \frac{P_B - P_C}{\pi_B(1-\phi)}\right) = \lim_{\theta\searrow\theta_0}\left(1 - K_C^D - \frac{P_C}{\phi}\right) \\ &= \lim_{\theta\searrow\theta_0}\left(1 - (1-\pi)\alpha_I - \frac{P_C}{\phi}\right) \\ &= 1 - \frac{1-\theta_0}{\phi}\tilde{p} = \frac{1-\pi+\pi\tilde{p}}{2-\pi}\end{aligned} \tag{45}$$

The first line is the definition, the second line is from the definition of K_C^D, the third line is from the market clearing condition in C-market, and the fourth and fifth lines are from the definition of θ_0 that gives $\alpha_I = 0$ and (43). The last line is the other expression from (43). Also, from (37)

$$\lim_{\theta \searrow \theta_0} K_B = \frac{(1-\phi)\pi\tilde{p}}{((1-\phi)\pi + \eta)\tilde{p} - \frac{\phi}{2-\pi}}. \tag{46}$$

Since markets have to clear, all of these expressions (45, 46) have to be identical. That is

$$\frac{(1-\phi)\pi\tilde{p}}{h\tilde{p} - \frac{\phi}{2-\pi}} = 1 - \frac{1-\theta_0}{\phi}\tilde{p} = \frac{1-\pi+\pi\tilde{p}}{2-\pi}, \tag{47}$$

at (44).

Let $D_{B,0} \equiv \lim_{\theta \searrow \theta_0} D_B$. By using the equality of the first and last term in (47),

$$D_{B,0} \propto (1-\phi)\pi \left(1 - \frac{\frac{\phi}{2-\pi}}{h\tilde{p} - \frac{\phi}{2-\pi}} \right) + \frac{2\phi\pi}{2-\pi}.$$

By using (47) once again, $h\tilde{p} - \frac{\phi}{2-\pi} = \frac{(1-\phi)\pi\tilde{p}}{1-\frac{1-\theta_0}{\phi}\tilde{p}}$. Thus,

$$\begin{aligned} D_{B,0} &\propto (1-\phi)\pi \left(1 - \frac{\phi}{2-\pi} \frac{1-\frac{1-\theta_0}{\phi}\tilde{p}}{(1-\phi)\pi\tilde{p}} \right) + \frac{2\phi\pi}{2-\pi} \\ &\propto [(1-\theta_0) + (2-\pi)(1-\phi)] + 2\pi\phi - \frac{\phi}{\tilde{p}} \\ &= 1 + (1-\pi)(\theta_0 - 2\phi). \end{aligned}$$

Note that θ_0 is decreasing function of ϕ and $\lim_{\phi \to 1} \theta_0 = 0$. Then, $\min_\phi D_{B,0} = \lim_{\phi \to 1} D_{B,0} = 2\pi - 1$. 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 $\pi > 1/2$, then $D_B > 0$ for all $\theta \in (\theta_0, 1]$, and v_B is monotonically increasing. On the other hand, if $\pi \leq 1/2$ and $\phi > \phi_2$, then there is a unique θ^{**} such that $D_B \gtrless 0 \Leftrightarrow \theta \gtrless \theta^{**}$.

G.2 Welfare of Sellers

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

$$\begin{aligned} v_{S,H} &= \int_{P_B} \alpha dF + \int^{P_B} P_B dF, \\ v_{S,L} &= \int_{\frac{P_B}{\phi}} \phi\alpha dF + \int_{\alpha^I}^{\frac{P_B}{\phi}} ((1-\theta)P_B + \theta\phi\alpha) dF + \int^{\alpha^I} P_C dF. \end{aligned}$$

In both expressions, the first term is the welfare of sellers being inactive, while the second term is for selling in the B-market. The last term of $v_{S,L}$ comes from sellers of L-assets in the C-market. It is easy to check the following proposition:

Proposition 9. *The welfare of sellers with high-quality assets, $v_{S,H}$, is monotonically increasing in θ.*

The innovation in the blockchain always benefits sellers of high-quality assets because they can always sell at a higher price P_B. On the other hand, we can obtain the following local result for L-type sellers:

Proposition 10. $\left.\frac{dv_{S,L}}{d\theta}\right|_{\theta=1} < 0$, *that is,* $\theta = 1$ *cannot be the maximizer of* $v_{S,L}$.

Proof. See Appendix G.3. □

Together with Proposition 9, this implies that the ex-post welfare of L-type sellers cannot agree with H-type sellers regarding the optimal θ.

To obtain more intuitions, we can separate $v_{S,L}$ into the "welfare gain" and the "reservation welfare," as in the case of buyers' welfare,

$$v_{S,L} = P_C + \int_{\alpha^I}^{1} ((1-\theta)P_B - P_C + \theta\phi\alpha)dF + \int_{\frac{P_B}{\phi}}^{1} (1-\theta)(\phi\alpha - P_B)dF. \tag{48}$$

First, all the L-type sellers can obtain the reservation welfare of P_C by selling in the C-market (the first term). If $\alpha > \alpha_I$, the sellers switch to either selling in the B-market or keeping it. The second term in (48) represents the welfare gain of sellers who will opt-out from the C-market: all of them ($\alpha > \alpha_I$) can potentially obtain the additional welfare by selling in the B-market. Within this subgroup, agents with relatively high α (such that $\alpha > \frac{P_B}{\phi}$) prefer to keep the asset by giving up the revenue P_B, which yields the further welfare gain exhibited by the last term of $v_{S,L}$.

The first and last terms are monotonically decreasing in θ. That is, the reservation welfare (the first term) and the gain from changing behavior from "selling in the C-market" to "being inactive" decline as the blockchain market becomes more profitable. The impact on the middle term is determined by two competing effects. On one hand, a higher θ boots the revenue by heightening P_B. On the other hand, it reduces the expected revenue by making the rejection risk higher.

G.3 Welfare Gain for Sellers

Hypothetically, suppose that a randomly picked seller is deprived of the access to the B-market. Ex-ante (before she is endowed with an asset), she expects to have $v_S^0 = \pi v_{S,H}^0 + (1-\pi)v_{S,L}^0$, where $v_{S,i}^0$ represents the reservation welfare of the seller when she obtains the asset-i with $i \in \{L, H\}$. Specifically,

$$v_{S,i}^0 = \begin{cases} \int_0^{P_C} P_C dF + \int_{P_C}^1 \alpha dF & \text{for } i = H \\ \int_0^{\frac{P_C}{\phi}} P_C dF + \int_{\frac{P_C}{\phi}}^1 \phi\alpha dF & \text{for } i = L. \end{cases}$$

For this agent, the expected welfare gain from having access to the B-market is given by

$$\begin{aligned} \Delta v_S &= v_S - v_S^0 \\ &= \pi \Delta v_{S,H} + (1-\pi)\Delta v_{S,L}. \end{aligned} \tag{49}$$

By applying uniform assumption, we obtain simple formulae:

$$\Delta v_{S,j} = \begin{cases} \frac{1}{2}(P_B^2 - P_C^2) & \text{if } j = H \\ (1-\theta)\frac{\Delta P^2}{2\phi\theta} & \text{if } j = L. \end{cases} \tag{50}$$

Obviously, $\Delta v_{S,H}$ is monotonically increasing in θ since P_C is monotonically decreasing in θ. Intuitively, the *reservation* welfare for sellers with H-asset is decreasing in θ since the terms of trade in the C-market will deteriorate if the blockchain technology improves. That is, the more secure the blockchain becomes, the larger the gain from having the access to the B-market will be for H-type sellers.

On the other hand, as for $\Delta v_{S,L}$, we have

$$\frac{d\Delta v_{S,L}}{d\theta} = \frac{\Delta P}{2\phi}\left[\Delta P\frac{dg}{d\theta} + 2g\frac{d\Delta P}{d\theta}\right]$$

where $g = (1-\theta)/\theta$. Since, $P_C = \phi(1-\pi P_B)/(2-\pi)$ in the equilibrium, it becomes

$$\frac{d\Delta v_{S,L}}{d\theta} = \frac{\Delta P}{2\phi}\frac{dg}{d\theta}\frac{1}{2-\pi}\left[[2-\pi(1-\phi)]P_B(1-\varepsilon_P)-\phi\right], \; \varepsilon_P \equiv -\frac{dP_B/dg}{P_B/g} > 0. \tag{51}$$

ε_P represents the elasticity of P_B regarding the change in the efficiency θ (since g and θ have negative monotone relationship, we consider it as the effect of θ). When the elasticity is high, i.e., ε_P is large, $\Delta v_{S,L}$ is increasing in θ. Otherwise, it is decreasing in θ.

Since the welfare gain of sellers with L-assets comes only from the transaction through the B-market, a higher θ has two competing effects. First, a higher θ increases the offer price P_B in the B-market, which has a positive impact on the sellers' welfare. This higher P_B proliferates the positive impact on $\Delta v_{S,L}$ by inducing a higher probability of submitting selling order into the B-market. On the other hand, a higher θ means a higher rejection probability. This reduces the gain for sellers with L-assets. The first positive effect dominates the latter effect when the increment of P_B is large, namely, ε_P is high.

When is the elasticity more likely to be high? It can be translated into the market equilibrium: a higher P_B confounds the demand when the cost of migration for the buyers is low. On the other hand, if the cost of migration is high, the higher price can sustain itself, making the elasticity of P_B high. Thus, $\Delta v_{S,L}$ exhibits upward sloping curve when (i) ϕ is low or (ii) $\Delta\pi$ is large.

H Imposing Fee on Sellers

We can fall back on the same logic as the main model to obtain $f_S = \Delta v_S$ with Δv_S in (50). When $\Delta v_{S,L}$ is increasing in θ, the total fee f_S is also increasing, while if $\Delta v_{S,L}$ is decreasing, the form of f_S is ambiguous since it depends on the level of π.

Suppose that the parameter values make $\Delta v_{S,L}$ decreasing in θ. Under this situation, it seems natural to conclude that a lower π makes f_S downward sloping because it puts more weight on $\Delta v_{S,L}$. However, this is not necessarily the case. For example, if we make $\pi \to 0$, we have $d\Delta v_{S,L}/d\theta \to 0$ and $df_S/d\theta \to 0$. This is because of the dominating L-assets in the market. As the level of π diminishes, the share of L-assets increases, and, at the limit, there are only L-assets in both markets. This implies that the access to the B-market does not payout: the welfare gain converges to zero.

H.1 Blockchain Proposer vs. Sellers' Welfare

Next, suppose that the platform makes money by imposing the fee on the sell-side of the market, while the government tries to maximize sellers' welfare. From (49), (50), and (51), we know the followings: the welfare gain of H-assets holders is monotonically increasing, imposing a positive pressure on f_S, while that of L-assets holders has an ambiguous effect. Moreover, Proposition 10 implies that, as long as f_S is monotonically increasing in θ the optimal θ set by the proposer cannot agree with θ that maximizes $v_{S,L}$. Thus, even if the welfare of H-assets holders is maximized, sellers with L-quality assets incur welfare loss: once the type of assets is realized, even the social planner cannot maximize the welfare of both types.

Since we cannot analytically characterize the properties of sellers' welfare further, we rely on the numerical examples. We find the total fee revenue is upward sloping, and the maximizing f_S agrees with maximizing $v_{S,H}$ in most ranges of parameters.

Figures and Tables

Figures IX ~ XV

The following figures provide the numerical examples for the sellers' welfare and fee. Parameters take $\pi \in \{0.01, 0.1, 0.4, 0.7, 0.9\}$, and $\phi \in \{0.35, 0.5, 0.7\}$. The first (second) column shows the total and reservation welfare of H-type (L-type) sellers, as well as the fee imposed by the proposer, f_S. The third column is the plot of the total (*ex-ante*) welfare of sellers and f_S.

As suggested by the theory, v_H is monotonically increasing in θ, while $v_{S,L}$ is either monotonically decreasing or hump-shaped. If f_S can be decreasing in θ, that should occur when θ is relatively high. However, even if we set the share of L-type sellers large ($\pi = 0.01$), the configuration of f_S is upward sloping. This is because the change in θ affects $v_{S,L}$ mostly through the change in $v^0_{S,L}$ when π is small. That is, the welfare gain for L-type sellers, $v_{S,L} - v^0_{S,L}$, is not affected by θ (see the difference between blue and green-dotted lines). Of course, a higher θ increases the welfare gain from trading in the B-market. Meanwhile, it reduces the welfare gain in the C-market, which has a dominating effect on the welfare because only $1 - \theta$ fraction of selling attempts have a benefit of a higher θ.

Figure IX: Welfare of Sellers and Fee: $\pi = 0.01$

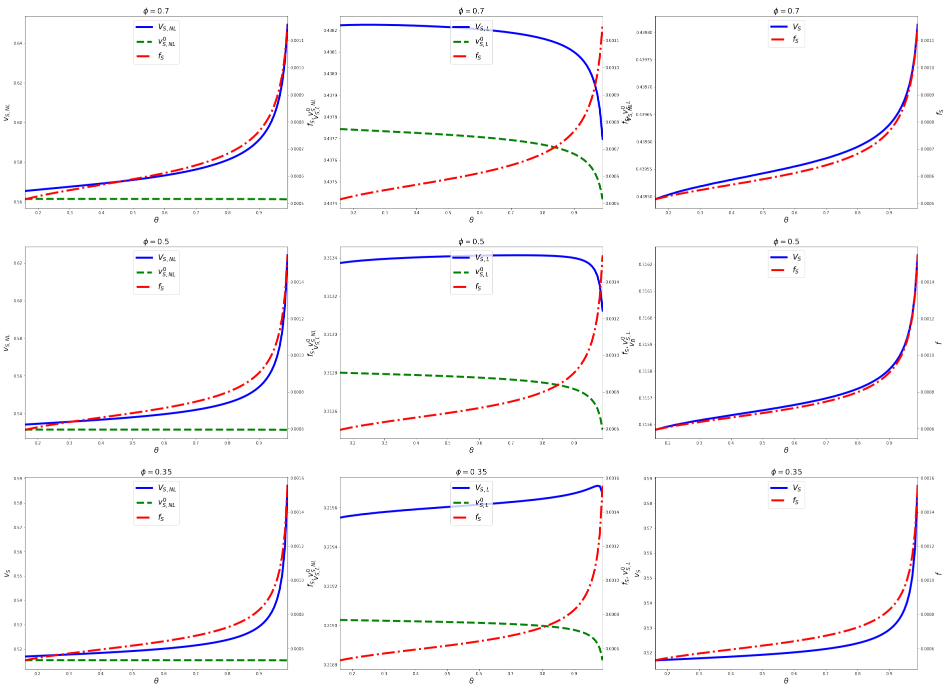


Figure X: Welfare of Sellers and Fee: $\pi = 0.1$

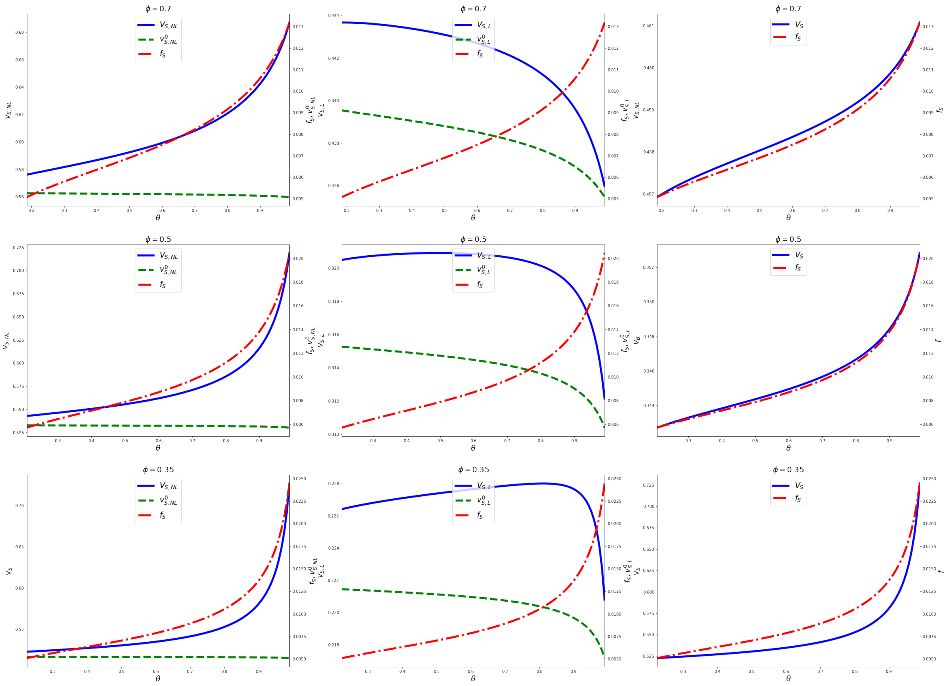


Figure XI: Welfare of Sellers and Fee: $\pi = 0.4$

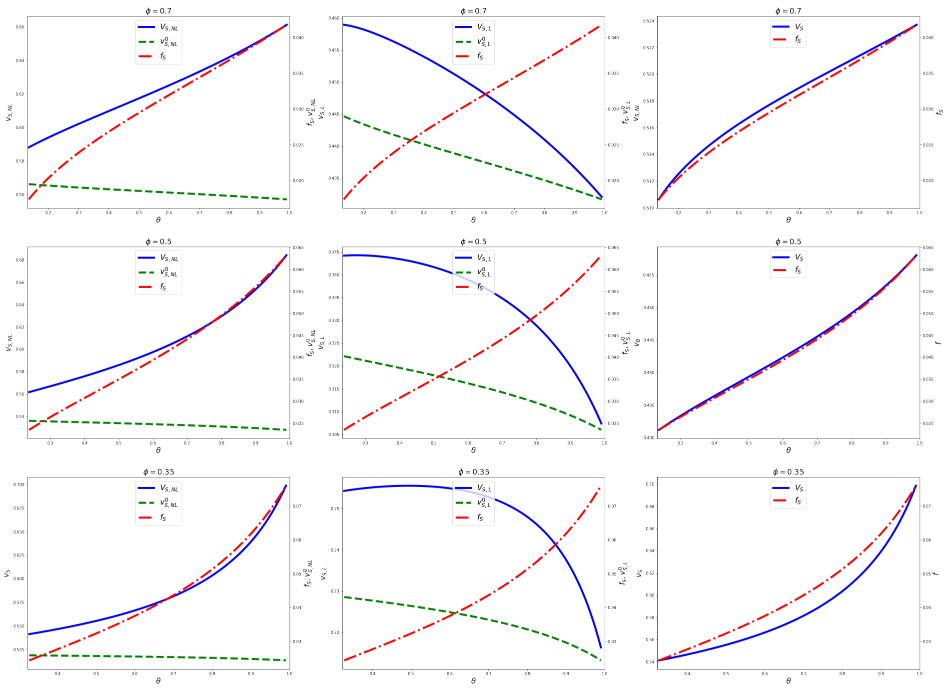


Figure XII: Welfare of Sellers and Fee: $\pi = 0.7$

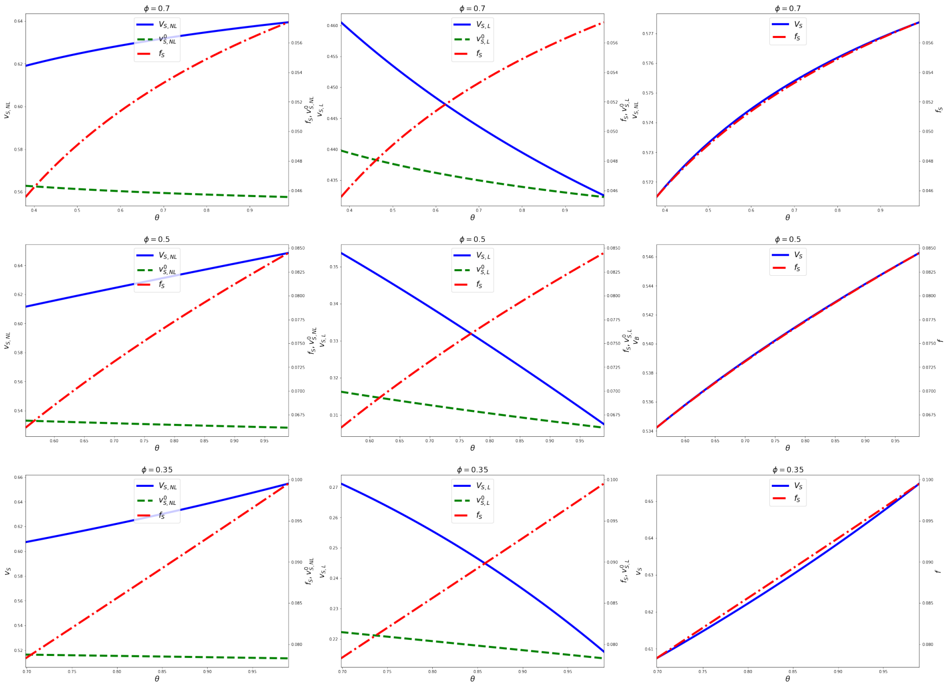


Figure XIII: Welfare of Sellers and Fee: $\pi = 0.9$