Blockchain Disruption and Smart Contracts

Lin William Cong
Booth School of Business, University of Chicago

Zhiguo He
Booth School of Business, University of Chicago Booth School and NBER

Blockchain technology provides decentralized consensus and potentially enlarges the contracting space through smart contracts. Meanwhile, generating decentralized consensus entails distributing information that necessarily alters the informational environment. We analyze how decentralization relates to consensus quality and how the quintessential features of blockchain remold the landscape of competition. Smart contracts can mitigate informational asymmetry and improve welfare and consumer surplus through enhanced entry and competition, yet distributing information during consensus generation may encourage greater collusion. In general, blockchains sustain market equilibria with a wider range of economic outcomes. We further discuss the implications for antitrust policies targeted at blockchain applications. (*JEL* C73, D82, D86, G29, L13, L86)

Received May 31, 2017; editorial decision May 29, 2018 by Editor Itay Goldstein.

Blockchain, a distributed ledger technology typically managed in a decentralized manner, was first popularized as the technology behind the cryptocurrency Bitcoin. It has since emerged in various other forms, often with the ability to store and execute computer programs. This has given rise to applications, such as smart contracts, featuring payments triggered by a tamper-proof consensus of contingent outcomes and financing through initial coin offerings. Many industry practitioners argue that the blockchain technology has the potential to disrupt business and financial services in the way the

The authors thank Matthieu Bouvard, Alex Edmans, Andreas Park, Maureen O'Hara, Edward "Ned" Prescott, and Hongda Zhong and an anonymous referee for insightful discussions of the paper. They also thank Jingtao Zheng for excellent research assistance that helped shape an initial version of the paper. Susan Athey, Tom Ding, Itay Goldstein, Brett Green, Campbell Harvey, Gur Huberman, Wei Jiang, Andrew Karolyi, Jiasun Li, Minyu Peng, Chung-Hua Shen, Dominic Williams, and David Yermack and seminar and conference participants at Chicago Booth, HBS, Notre Dame Mendoza, CUHK Econ, Ant Financial, AEA, NBER Conference on Competition and the Industrial Organization of Securities Markets, RFS FinTech workshop, NYU Stern FinTech Conference, Federal Reserve Bank in Philadelphia FinTech Conference, USC FOM Conference, 25th SFM Conference, CEIBS Behavioral Finance and FinTech Forum, SFS Calvacade Asia-Pacific, AMAC FinTech and Smart Investing Workshop, TAU Finance Conference, and NBER Conference on Financial Market Regulation provided very helpful feedback and comments. This research was partially funded by the National Science Foundation of China [71503183]. Send correspondence to Lin William Cong, Booth School of Business, University of Chicago, 5807 S. Woodlawn Ave., Chicago, IL 60637; telephone: (773)834-1436. E-mail: will.cong@chicagobooth.edu.

doi:10.1093/rfs/hhz007

Internet disrupted off-line commerce. Others remain skeptical of its genuine innovativeness and real-world applicability, not to mention its association with money laundering or drug dealing.[1] Figure 1 displays Google searches showing the rising popularity of the blockchain technology in recent years, as well as the growing number of open-source projects related to blockchain and smart contracts.

In this paper, we argue that despite a plethora of definitions, descriptions, and applications of blockchain and decentralized ledger, the technology and its various incarnations share a core functionality in providing a "decentralized consensus." Decentralized consensus is a description of the state of the world—for example, whether the goods have been delivered or whether a payment has been made—universally accepted and acted on by all agents in the system. Economists have long recognized that consensus enables agents with divergent perspectives and incentives to interact as if it provided the "truth," which has profound implications on the functioning of society, including ethics, contracting, and legal enforcement, among others. What is key for blockchain technology is that such a consensus is generated and maintained in a decentralized manner, which blockchain advocates believe can improve the resilience of the system and reduce the rent extracted by centralized third parties.[2] For example, on the Bitcoin blockchain, given the transaction history, agents can check and verify transaction records digitally to prevent "double spending" the digital currency and freeing everyone from the need of a centralized trustworthy arbitrator or third party.[3]

Public blockchains and many permissioned blockchains interact with dispersed record-keepers to reach decentralized consensus using the latest technologies. Two economic forces naturally arise: programmable decentralized consensus, if achieved, tends to make contracting on contingencies easier, thanks to its temper-proof and automated nature; however, achieving such consensus requires sufficiently distributing information for verification. Consequently, blockchain applications typically feature a fundamental tension between *decentralized consensus* and *information distribution*. The former enhances contractibility and is welfare improving, whereas the latter could be detrimental to the society. This fundamental tension we highlight has been since recognized by governments, media, and industry research. For example,

---

[1] *The Economist* (2015) has argued that "the technology behind bitcoin could change how the economy works." Marc Andreessen, the cocreator of Netscape, even exclaimed "This is the thing! This is the distributed trust network that the Internet always needed and never had" (Fung 2014). On the negative side, see Narayanan and Clark (2017), Jeffries (2018), and Stinchcombe (2017).

[2] This is evident when Satoshi Nakamoto, founder of Bitcoin, remarked, "A lot of people automatically dismiss e-currency as a lost cause because of all the companies that failed since the 1990s. I hope its obvious it was only the centrally controlled nature of those systems that doomed them. I think this is the first time were trying a decentralized, non-trust-based system" (Narayanan et al. 2016).

[3] Double spending is a potential flaw in a digital cash system in which the same digital currency can be spent more than once when a consensus record of transaction histories is lacking. Such a lack can result when digital files are duplicated or falsified.

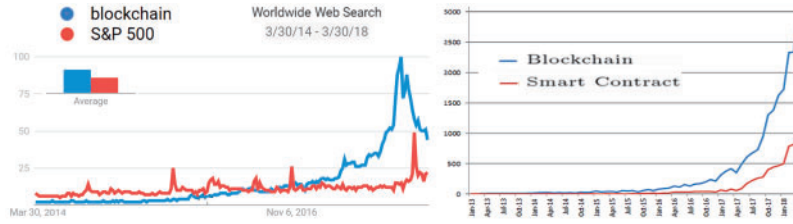

Figure 1
Trends in blockchain and smart contracts
The left panel displays the relative search interest and plots each search term relative to its peak (normalized to 100) for the given region and time. The right panel shows the number of blockchains and smart contract projects hosted on Github, a major open-source development platform for coding programs around the world, from January 2013 to April 2018.

the Jasper Project at the Bank of Canada in 2017 revealed that "More robust data verification requires wider sharing of information. The balance required between transparency and privacy poses a fundamental question to the viability of the system for such uses once its core and defining feature is limited."[4]

Our paper offers the first analysis on this core issue of blockchain. As we discuss in more detail in the literature review, there are two economically relevant areas of research on blockchain: (1) blockchain mechanisms for generating and maintaining decentralized consensus and (2) real-world implications given the functionality blockchain provides. Our paper contributes to both fronts by highlighting a universal trade-off in this technology (as opposed to analyzing the strategic mining games specific to the Bitcoin protocol) and studying the impact of this technology on industrial organization.

We first provide a simple framework to think about the process of reaching decentralized consensus on a blockchain in a trade finance application. Most blockchains have overlapping communities of record-keepers and users. Similar to third-party arbitrators in the real world, they receive signals on the true state of the world and may have incentives to misreport (tamper or manipulate). With the help of fast-developing real-time communication technologies among decentralized record-keepers, a carefully designed protocol on blockchains can reduce individual's incentive to manipulate and misreport, allowing more efficient information aggregation. Compared to traditional contracting, blockchains have the potential to produce a consensus that better reflects the "truth" of contingencies that are highly relevant for business operations, thereby enhancing contracting on these contingencies. Nevertheless, generating a more effective consensus (i.e., a consensus closer to truth) is predicated on decentralized record-keepers' observing and receiving

[4] See Gillis and Trusca (2017) and Chapman et al. (2017). de Vilaca Burgos et al. (2017) emphasize the same point.

greater amount of information.[5] The key insight is that the information distribution process changes the informational environment and, hence, the economic behaviors of blockchain participants.

Armed with this insight, we then analyze the impact of blockchain technology on competition and industrial organization. Specifically, our model features two incumbent sellers known to be authentic, and an entrant who only has some probability of being authentic. Authentic sellers always deliver the goods while the fraudulent ones cannot. In each period, buyers as a group show up with a constant probability (reflecting the aggregate business condition), shop the sellers based on price quotes, and then exit the economy. Each seller observes her own customers but does not observe the other sellers' prices or customers. We call this economic environment the "traditional world," in which it is infeasible to communicate information across agents, in the spirit of Green and Porter (1984).

In this traditional world, because of contract incompleteness, sellers cannot offer prices contingent on the success of delivering the goods. The lemons problem thus precludes entry. On the other hand, two incumbents might engage in collusion in equilibrium. However, because incumbent sellers cannot differentiate the event of no buyers showing up from the event of the other seller stealing her market share, aggressive price wars occur too often, making it relatively difficult to sustain collusion among incumbent sellers.

In contrast, blockchains, via decentralized consensus, enable agents to contract on delivery outcomes and automate contingent transfers. Hence, the authentic entrant is now able to signal her authenticity fully. This eliminates information asymmetry as a barrier for entry and greater competition, enhancing welfare and consumer surplus in this "blockchain world." Beyond authenticity and delivery, we further show that in an extension with privately observed seller qualities, blockchain consensus can also mitigate informational asymmetry over service qualities, thereby improving consumer surplus and welfare.

However, as mentioned before, generating decentralized consensus also inevitably leads to greater knowledge of aggregate business condition on the blockchain, which we show can foster tacit collusion among sellers. In contrast to the traditional world where sellers do not observe one another's business activities, in the blockchain world they at least can infer the aggregate business condition on the blockchain—by serving as record-keepers—and hence are able to detect deviations in any collusive equilibrium. Consistent with this intuition, we show that with blockchains in which only incumbents can participate, there are always weakly more collusion equilibria than those sustainable in the traditional world.

Our model thus features the trade-off between potentially enhanced competition and aggravated collusion, both arising from the blockchain

[5] Some of the information can be encrypted. In the case of public blockchains (e.g., Bitcoins), the consensus is typically generated by all users.

technology. More generally, with blockchain (accessible to both incumbents and entrants) and smart contracts, the set of possible dynamic equilibria expands, leading to social welfare and consumer surplus that could be higher or lower than in a traditional world.

Our findings relate to the widespread concern that blockchains may jeopardize market competitiveness in a serious way. This becomes especially relevant for permissioned blockchains with powerful financial institutions as exclusive members (Kaminska 2015). Our paper highlights one salient economic mechanism through which blockchain facilitates collusion, and we explore policy implications of our model. For instance, an oft-neglected regulatory solution is to separate usage and consensus generation on blockchains, so that sellers cannot use the consensus-generating information for the purpose of sustaining collusion. By providing a conceptual description of blockchain and smart contracts from an economic perspective, our analysis aims to demonstrate that blockchains are not merely database technologies that reduce the cost of storing or sharing data. Rather, the design of the blockchain can have profound economic implications on consensus generation, industrial organization, smart contract design, and antitrust policy. Overall, we provide a cautionary tale that blockchain technology, while holding great potential in mitigating information asymmetry and encouraging entry, can also lead to greater collusive behavior.

Our paper adds to the emerging literature on blockchains, which thus far has mainly come from computer scientists. Two areas of research on blockchain are economically relevant: (1) blockchain mechanisms for generating and maintaining decentralized consensus, and (2) real-world implications, given the functionality blockchain provides. The first category can be further divided into those studies analyzing the general process of consensus generation for most blockchains, emphasizing the trade-offs in decentralization, and those studies exploring the game theoretical topics, including incentive provisions and market microstructure, taking as given a particular blockchain protocol, such as the mining protocols in Bitcoin. While most of existing literatures focus on the latter subcategory, our paper adds to the former, and links the analysis directly to the technology's impact on the real economy.

Among studies on the application and economic impact of the technology, Harvey (2016) surveys the mechanics and applications of crypto-finance.[6] Yermack (2017) evaluates the potential impacts of the technology on corporate governance. Complementary to our discussion on smart contracts, Bartoletti and Pompianu (2017) empirically document how smart contracts are interpreted and programmed on various blockchain platforms. We add by examining arguably the most defining features of blockchain, and how they interact

[6] Other papers on various blockchain application include Malinova and Park (2018) on trading, Tinn (2018) on time-stamping and contracting, Cao et al. (2018) on auditing, Chiu and Koeppl (2019) and Khapko and Zoican (2018) on settlement, and Cong et al. (2018b,c) on crypto-token valuation and platform development.

with information asymmetry and affect market competition, both of which are important, general issues in economics.

Related to our analysis on the underlying mechanism for generating decentralized consensus are studies on Bitcoin mining games. Kroll et al. (2013) note that miners' following the "longest chain rule" should be a Nash equilibrium. Biais et al. (2019) formalize the mining game and discuss multiple equilibria.[7] Instead of taking as given specific blockchain protocols, such as that of Bitcoin, and analyzing strategic behaviors of miners or market microstructure, we take a holistic approach to examine universal features of blockchains, with a direct focus on how the information distribution that comes with decentralization interacts with the quality of consensus generation. Relatedly, Abadi and Brunnermeier (2018) show that entry competition in many blockchains promotes fork competition that benefits users. Importantly, the technology's core concept of decentralization has both pros and cons. Concerns for information distribution constitute a natural force to make a supposedly decentralized system centralized. We focus on the information channel in this paper while Cong et al. (2018a) explore a risk-sharing channel.

Our analysis on collusion adds to the large literature on industrial organization and repeated games with monitoring (Tirole 1988). Our model ingredients partially derive from Porter (1983) and Green and Porter (1984), who study collusion in a Cournot setting with imperfect public monitoring. A recent empirical study by Bourveau et al. (2017) shows how collusion relates to firms' financial disclosure strategies (information distribution in our language). We instead examine Bertrand competition and link the additional observable or contractible information to the type of monitoring in repeated games under the technological innovation.[8]

1. Blockchain as a Decentralized Consensus

It is commonly recognized that blockchains provide many functions, such as distributed data storage, anonymity, data obfuscation, shared ledgers, and so on. Because solutions to these problems are well known outside of the blockchain space, the impact of blockchain along these dimensions, though material, is somewhat incidental. We therefore focus on their core functionality of providing decentralized consensus. Consequently, our model would not apply to a subset of permissioned or private blockchains that generate consensus

[7] Eyal and Sirer (2014) and Nayak et al. (2016) study "selfish mining" and the related "stubborn mining" in which miners launch block-withholding attacks. Easley et al. (2017) and Huberman et al. (2017) analyze Bitcoin transaction fees and discuss the inefficiencies and congestion in mining and transactions. Cong et al. (2018a) study how mining pools aggravate the mining arms race and energy consumption, and the associated industrial organization.

[8] Our analysis of sustainable equilibria is related to Fudenberg and Maskin (1986); our discussion on the application of blockchain and smart contract in financial services and transactions is broadly linked to optimal contracting, especially concerning information asymmetry and contract incompleteness (e.g., Baron and Myerson 1982; Hart and Moore 1988; Tirole 1999).

in the traditional, centralized manner. In other words, rather than analyzing the technical details of various protocols or additional benefits the technology brings about, this paper underscores the economic implications of decentralized consensus, and the natural process that accompanies it, that is, information distribution due to decentralization.

In this section, we first provide an overview of the blockchain technology, highlighting decentralized consensus as its core feature and the trade-offs therein. We then model the generation of decentralized consensus and information distribution, before discussing various real-world business applications in the financial industry.

1.1 Blockchains and smart contracts

The work on blockchains dates to 1990s (Haber and Stornetta 1990). However, it was not until 2008 that blockchains were popularized by Satoshi Nakamoto through the cryptocurrency Bitcoin (Nakamoto 2008).[9] Its simplest form entails a distributed database that autonomously maintains a continuously growing list of public transaction records in units of "blocks," secured from tampering and revision. Each block contains a time stamp and a link to a previous block. Other forms of blockchains have emerged subsequently with different designs on exclusivity, transparency, and maintenance of the records. Yermack (2017) summarizes how blockchains work.

All blockchains—to varying degrees—aim to create a database system in which decentralized agents or institutions can jointly record information and maintain it, with no individual party exercising persistent market power or control. One defining feature of blockchain architectures is thus their ability to maintain, in a relatively more effective way, a uniform view on the state of things and the order of events – a consensus.

As consensus is essential to many economic and social functions, the benefits and empowerment for everyone sharing and trusting the same ledger are clear. Settlements in some cases no longer take days, lemons problems and frauds can be mitigated, and the list continues. These outcomes will likely affect the agents' ex ante incentives in the economy. Traditionally, courts, governments, notary agencies, etc., provide such consensus, but in a way that was sometimes thought to be labor intensive, time consuming, and prone to tampering and monopoly power. In this regard, many advocates of the technology believe that blockchains hold the promise of disrupting many industries by providing consensus in a more decentralized manner, albeit still potentially costly in ways of energy consumption as well as informational concerns that we focus on in this paper.

[9] Böhme et al. (2015) surveys Bitcoin's design principles and properties, risks, and regulation. Narayanan et al. (2016) provides an in-depth introduction to the technical details of Bitcoin blockchain. True to the Stigler's law of eponymy, the ingredients and principles for Bitcoin were introduced much earlier, and Nakamoto's innovation truly lies in putting it altogether. See Narayanan and Clark (2017) for further details.

1.1.1 Decentralized consensus. To produce and maintain a *decentralized* consensus without a centralized authority, blockchain protocols have to incentivize responsible and accurate record-keeping by a community of dispersed "record-keepers," typically in a competitive manner, while reducing manipulation and tampering. In a sense, all decentralized consensus must come to some form of "majority" vote, though the algorithms may significantly vary across projects and applications.

Two widely discussed designs for maintaining decentralized consensus are proof-of-work (PoW) and proof-of-stake (PoS). PoW rewards record-keepers who solve complicated cryptographical puzzles in order to validate transactions and create new blocks (i.e., mining). It prevents attacks, such as a denial-of-service (DoS) attack, and ensures that once one observes a valid state of the ledger, transactions of a certain age cannot be negated, because doing so requires the malicious entity to have computing power that can compete with the entire network. Consequently, the blockchain achieves a tamper-proof consensus of the validity of these transactions. Unlike PoW, in PoS the creator of the next block is chosen based on his/her holding of the native cryptocurrency (i.e., the stake). Other prominent designs include practical byzantine fault tolerance algorithm (PBFT) and the delegated proof-of-stake algorithm (DPoS).[10] Instead of comparing specific designs, we will model decentralized consensus algorithm in abstraction in order to shed light on most extant designs.

Many algorithm designs in their current forms are imperfect, but they have improved quickly and substantially. For instance, several hacking incidents have occurred on blockchains and Bitcoin has been criticized for wasting electricity, but multiple proposals to address these issues by improving the protocol design and furthering decentralization have been made.[11] Practitioners are actively researching another problem: the lack of consensus when modifying blockchain protocols, which generally leads to forking and temporary confusion about which blockchain users should follow.

1.1.2 Smart contracts. Szabo envisioned in 1994 (e.g., Tapscott and Tapscott 2016) the concept of smart contracts. Although a universally accepted definition (no pun intended) for smart contracts has yet to be reached, their core functionality is clear: transfer at little cost or even automate value transfers based on a decentralized consensus record of the states of the world. This leads to a natural functional definition: smart contracts are digital contracts allowing

[10] DPoS works along the same lines as the PoS system, except that individuals vote for an overarching entity who represents their portion of stake in the system (hence the word delegation). PBFT deals with robust synchronous agreement in the presence of malicious fault nodes.

[11] Lightning, which builds on the Bitcoin blockchain, reduces the amount of information that has to be recorded on the blockchain to increase processing power; Dfinity incubated by String Lab builds on Ethereum to ensure higher security and execution speed; and startup firms, such as BOINC, channel mining computation to solve scientific problems.

terms contingent on decentralized consensus that are tamper-proof and typically self-enforcing through automated execution.

Our definition is consistent with and nests the definitions commonly seen among legal scholars (Lauslahti et al. 2016; Szabo 1997, 1998). It is important to note that smart contracts are neither merely digital contracts (many of which rely on trusted authority for reaching consensus and execution) nor are they entailing artificial intelligence (on the contrary they are rather robotic).

Without decentralized consensus, the party providing centralized consensus often enjoys huge market power (e.g., a third party with data monopoly). And traditional resolutions by third parties, such as courts or arbitrators, involve high degrees of human intervention that are less algorithmic, potentially leading to greater uncertainty and cost. Smart contracts can increase contractibility and facilitate exchanging money, property, shares, service, or anything of value in an algorithmically automated and conflict-free way.[12]

Concerning contracting theory, the decentralized consensus reached by blockchain technology has the potential to greatly reduce the scope of noncontractible contingencies, the underpinning of the incomplete contract literature (e.g., Hart 1995). In particular, smart contracts can augment contractibility and enforceability on certain contingencies, be it the lock-in requirement for fund withdrawal or the automated payment upon an importer's successfully receiving the goods. That said, the improved contractibility requires greater information distribution, and the overall impact on the economy is far from obvious.

1.1.3 Information distribution. Achieving decentralized consensus requires distributing information to some participants in the system. The economic trade-offs involved in information distribution necessary for generating a decentralized consensus are highly relevant from the practical or regulatory perspective. With Bitcoin, the consensus is reached and maintained through distributing all transaction information (with public-key-encrypted owner addresses) to the entire population on the blockchain, so all transaction details (except for identities) recorded on the consensus are public information. One obvious issue that arises when pushing for real-world blockchain applications is business privacy. For instance, financial institutions are typically sensitive to reveal the details of the transaction to unrelated parties. For example, traders may want to hide their identities to prevent front-running (Malinova and Park 2018), and greater information distribution may also affect industrial organization and competition, as this paper shows.

Facing this fundamental trade-off, many proposals for better encryption effectively mask sensitive information in the process of consensus generation.

[12] Although a weaker definition of smart contracting requires execution be conducted by centralized parties, having a consensus record still significantly reduces contracting and execution frictions, as seen in recent applications in the land registry in Georgia (Weiss and Corsi 2017).

Another straightforward compromise is to reach a decentralized consensus for only a subset of important states of world or to request verification from fewer nodes (record-keepers) in the blockchain network.[13] In what ways does information distribution matter beyond privacy concerns? Will it affect the effectiveness of blockchain consensus? Extant theory tells us very little.

1.2 A model of decentralized consensus and information

We build a simple economic model of the mechanism of consensus generation, highlighting the role of record-keepers and the inevitable nature of information distribution. Our model setup is motivated by the application of trade finance, which has been proposed and widely explored by industry practitioners.

1.2.1 Trade finance example. Consider the following scenario many industry pioneers discuss: there are multiple potentially international exporters (sellers) of certain goods which require shipping with proper care (say, wine, so the temperature is critical for good condition). The success of selling these goods to importers (customers) require various other parties, such as logistics providers, international ports and customs (for the flow of goods), notaries, and financing intermediaries (for the flow of payments).

Say a seller is shipping the goods to a customer; we focus on the information flow in generating the consensus on delivering the goods, a contingency represented by $\tilde{\omega}$ in Figure 2. The participants, necessarily including the seller and buyer, can monitor the physical conditions (e.g., location and temperature) of the goods via the end-to-end information collection, enabled by sensors, smart input mechanisms, and real-time data processing, or more broadly, Internet-of-Things (IoT). For better monitoring and more transparency, these IoT sensors could be installed on other relevant parties that handle logistics. The seller-buyer pair receives this information (including notification of final delivery) along the way.

Other parties on the blockchain may receive relevant information that can help monitor the process. For instance, the other sellers may also have installed IoT sensors able to detect the goods' delivery. Even without the help of IoT, other customers who happen to collect other goods at the same port may observe relevant information on this particular delivery. At this stage, these signals are not yet recorded on blockchain.

One crucial step on blockchain is to generate a decentralized consensus on "whether the goods has been successfully delivered," so that information from many relevant parties can be aggregated to something that is accepted by the community—and recorded to the blockchain. This is done by contacting

[13] For example, Aune et al. (2017) discuss the use of first-stage hashing to secure time priority without revealing detailed information and revealing information later, in order to prevent front-running a transaction before it is recorded on a block on distributed ledgers. Directly related are the so-called "zero knowledge protocols" in computer science that allow participants to agree about certain facts without revealing detailed information.

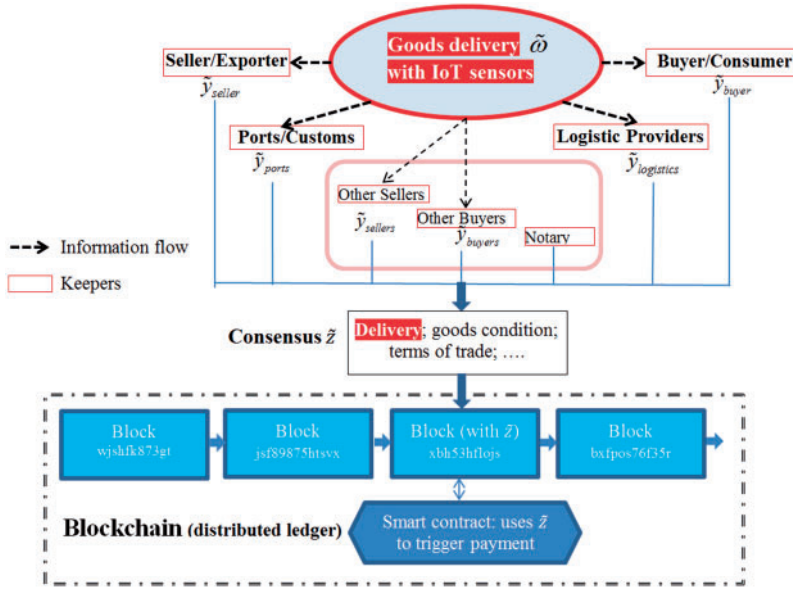

Figure 2
A diagram of the trade finance example of a blockchain
A seller delivers goods to a buyer, with $\tilde{\omega}$ denoting the contingency of successful delivery. Record-keepers, potentially with real-time IoT sensors, monitor the delivery and submit their reports, $\tilde{y}_k$'s. The protocol of blockchain aggregates these reports to form a decentralized consensus, $\tilde{z}$. This consensus, together with the smart contract, is stored in the block and then added to the blockchain.

verifiers on the blockchain. In our trade finance example, the seller-buyer pair, logistic providers, and ports must be contacted. Likely, other sellers with IoTs are contacted as well, because they have the expertise to verify the "success" of the delivery in case of disputes. In blockchain applications, they are what we call "record-keepers." Contacted agents might not truthfully report their signals—a possibility that is allowed by our model. Finally, other customers are contacted as well, perhaps serving the purpose of "consistency check. "

Contacted parties then submit their reports $\widetilde{y}_k$ to the blockchain. Then the blockchain protocol generates the decentralized consensus $\widetilde{z}$ regarding the contingency in question based the reports $\{\widetilde{y}_k\}$. A newly created block is added to the entire chain, as shown at the bottom of Figure 2. This newly created block must pass certain consistency checks with respect to the history of the existing blockchain (which can be thought of incorporating past reports as an input for generating current consensus) before more blocks are added to it.[14]

In this example, sellers beyond the seller-buyer pair may receive information via two sources on blockchain: one via the terminals connected to the

[14] This thematic treatment covers the case in which the added block still requires further verification like in the case of Bitcoin, so "added" corresponds more to "finalized" or "confirmed."

IoT sensors and the other via being contacted to verify the transaction. In our perspective, they are playing different roles, but the second—as the essential step in generating the consensus—is more crucial for the blockchain technology. Putting the concern of collusion aside, the more information these industry experts have, the better the chance of forming a higher quality consensus in this process. There is also a lower bound on information distribution: Even if the transaction to be verified is encrypted, the mere fact of being contacted actually reveals information (this point will be highlighted in our model).

1.2.2 Model setup. To illustrate how decentralization makes the consensus more effective at the expense of greater information distribution, we now formalize the above trade finance example. Our analysis applies to both public and permissioned blockchains.

Suppose a smart contract references a contingent outcome $\widetilde{\omega}$, which we refer to as the "delivery" of service or goods, in the context of our main model in Section 3. The random variable $\tilde{\omega}$ takes the value of one if the delivery is successful and zero otherwise, and denote the decentralized consensus on $\widetilde{\omega}$ on a blockchain by $\widetilde{z}$, which takes value in $\{0, 1\}$ as well.

As illustrated by the trade finance example, participants on the blockchain receive various signals with the aid of real-time IoT technologies.[15] For simplicity we assume all agents observe $\tilde{\omega}$ perfectly. Although we could model the information environment as agents receiving signals that might be different from the true contingency $\tilde{\omega}$, this complication is unnecessary given the misreporting incentives introduced later. In fact, Appendix A considers this possibility under a more general formulation and repeats the analysis for a large class of linear models to demonstrate the robustness of the trade-off that we highlight.

In practice, to reach a decentralized consensus, blockchains contact a set of record-keepers, who are typically dispersed blockchain participants (hence the name "decentralized").[16] Cryptocurrency mining to maintain consensus record is a prominent feature for the likes of Bitcoin and Ethereum. Ripple and R3 CEV use their own consensus process but also rely on a community of record-keepers. The process typically entails both competition and assignment for record-keeping as well as post-block validations and is an interesting industry on its own.

To model this, suppose that the blockchain protocol contacts a set of K potential record-keepers. Record-keepers in the set $\mathbb{K} \equiv \{1, 2, \cdots, K\}$ are homogeneous, and for simplicity we model the effectiveness of the consensus

[15] Clearly, the technology is not applicable for verifying subjective experience.

[16] Table 1 in Zurrer (2017) contains a detailed list of further examples of record-keepers.

for contracting (and potentially other purposes) by $-Var(\widetilde{\omega}-\widetilde{z})$.[17] An effective consensus is the cornerstone for the trust that many Fintech firms purport.

Upon contact, each record-keeper $k \in \mathbb{K}$ submits $\widetilde{y}_k$ taking values in $\{0,1\}$, yielding a collection of reports $\mathbf{y} \equiv \{\widetilde{y}_k\}_{k\in\mathbb{K}}$. As we will elaborate later, record-keepers might misreport, that is, $\widetilde{y}_k \neq \widetilde{\omega}$. For illustration, we examine the case in which the consensus is given by

$$\widetilde{z}(\mathbf{y}) = \begin{cases} 1 & \textit{with probability} \quad \sum_k w_k \widetilde{y}_k, \\ 0 & \textit{otherwise}, \end{cases}$$

where the weights of the validating notes, w_k, are nonnegative and sum to unity. We also assume that $w_k \to 0$ as $K \to \infty$, which captures the key concept of decentralization. The consensus function implies that if record-keepers report more successful delivery, then the consensus is more likely to be successful delivery. We focus on how the metric of decentralization K affects the quality of decentralized consensus and the system-wide information distribution.[18]

1.2.3 Record-keepers' information and misreporting. Suppose each record-keeper on the blockchain observes the realization of $\tilde{\omega}$, the delivery status. While payment verifications on Bitcoin mostly concerns double-spending issues and require limited information distribution (e.g., the real identities of transaction parties are masked), the validations of general economic activities are typically more complicated, potentially requiring more nuanced information. For example, many trade finance blockchains use information from local ships, ports, banks, and border customs to track delivery status, potential aided by sensors and IoT devices with details not fully publicly available (e.g., Corda or some Hyperlydger blockchains).[19] In addition, record-keepers may also receive extra information about the transaction upon contact. For example, IBM currently works on trade finance blockchains that provide record-keepers additional information about shipment status, since to generate consensus on delivery requires off-chain collaborations and cross-validations with shipping companies and import-export controls.

Record-keepers may have incentives to misreport. For example, in trade finance applications record-keepers are also parties involved in the transaction;

[17] In reality, effectiveness depends on the purpose and use of consensus on each specific blockchain. Our specification qualitatively captures the universal feature that a consensus is not effective even when it is unbiased if it is uncertain to always reflect truth accurately. Our results are robust to introducing penalty terms for bias and high moments of $-Var(\widetilde{\omega}-\widetilde{z})$.

[18] Our results hold for a general $\widetilde{z}(\mathbf{y}) = \tilde{Z}\left(\sum_k w_k \widetilde{y}_k\right)$, where $\tilde{Z}$ is a function that takes the values of $\{0,1\}$ and satisfies that $\mathbb{E}[\tilde{Z}]$ is differentiable and increasing in the argument, and takes the value of 0 or 1 when the argument is 0 or 1. This implies that if the reports are all accurate, the consensus reflects the true state of the world. These requirements are broadly consistent with extant blockchain protocols.

[19] For more complicated business situations, the record-keepers likely only observe a noisy signal of the true state, and public information disclosure policy on any blockchain likely affects the record-keeper's signal quality, thereby affecting the quality of decentralized consensus. We discuss these issues in Appendix A when we introduce the general linear model.

Bitcoin miners may hide report through "selfish-mining" or double spend certain coins.[20] Such incentives also exist in traditional economies: business arbitrators may favor a client, and double spending was the issue in traditional online payments that originally inspired the creation of Bitcoin. In fact, media reports and practitioners' discussions have largely centered on how blockchain helps reduce tampering, manipulation, and hacking.

In our reduced-form model, we assume that each risk-neutral record-keeper k submits a report of y_k to maximize his normalized utility $U(y_k;\mathbf{y})$. In particular, he solves

$$\max_{y_k\in\{0,1\}} U(y_k;\mathbf{y}) = b_k\cdot|\widetilde{z}(\mathbf{y})-\widetilde{\omega}| - h_k|y_k-\widetilde{\omega}|, \tag{1}$$

where b_k and h_k are positive, uniformly bounded above and below from zero for all k. The first coefficient b_k is record-keeper k's benefit when the wrong consensus is reached (forming $1-\tilde{\omega}$ when the true state is $\tilde{\omega}$). In the second term, h_k captures the cost of misreporting. Depending on the protocol design in specific trade finance applications, h_k could correspond to reputation cost in a blockchain alliance, or it could be the cost of counterfeiting signals in IoT sensors. In the case of Bitcoin, inaccurate records take longer to be confirmed and have a higher probability to be reversed, not to mention the extremely large computation power required in PoW systems.

1.2.4 Information distribution and quality of consensus. Each contacted record-keeper chooses y_k to optimize U in (1), which gives

$$\widetilde{y}_k^* = \begin{cases} \widetilde{\omega} & if \quad b_k w_k \le h_k, \\ 1-\widetilde{\omega} & otherwise. \end{cases} \tag{2}$$

The benefit of misreporting is $b_k w_k$ because it shifts the consensus by w_k given other people's equilibrium strategies, whereas the cost is h_k. The equilibrium consensus then is

$$\widetilde{z} = \begin{cases} \widetilde{\omega} & w.p. \quad \sum_{k\in\mathbb{K}^*} w_k, \\ 1-\widetilde{\omega} & otherwise. \end{cases} \tag{3}$$

where $\mathbb{K}^* \equiv \{k\in\mathbb{K}: b_k w_k < h_k\}$ is the set of truth-telling record-keepers. The resultant quality of the decentralized consensus is

$$-Var(\widetilde{\omega}-\widetilde{z}) = -Var(2\tilde{\omega}-1)\left(1-\sum_{k\in\mathbb{K}^*}\omega_k\right)^2, \quad where \quad \mathbb{K}^* \equiv \{k\in\mathbb{K}: b_k w_k < h_k\}. \tag{4}$$

[20] In our model, misreporting represents noise, but it can also result from record-keepers being hacked.

Notice that $Var(2\tilde{\omega}-1)$ is independent of K. Therefore, the greater the set $\mathbb{K}^*$, the higher the quality of the decentralized consensus. The benefit of decentralization manifests in how the size of contact K improves the quality of consensus, by diminishing each record-keeper's manipulation incentives and edging the set with truthful report $\mathbb{K}^*$ closer to the full set $\mathbb{K}$. For illustration, consider the case with homogeneous symmetric record-keepers with $b_k = b > 0$, $h_k = k > 0$, and $w_k = 1/K$, where the consensus quality is proportional to $-\mathbb{I}_{\{K \leq \frac{b}{h}\}}$ which is increasing in K.

For more general b_k and h_k satisfying conditions given below Equation (1), the consensus becomes perfect, that is, $\widetilde{z} = \widetilde{\omega}$ as $K \to \infty$; we focus on this case in Section 2, and show how decentralized consensus improves the contractibility and enhances entry (hence competition). We discuss imperfect consensus in Section 3.

1.2.5 Relating to the literature on information economics. It is important to highlight the difference between our analysis and the extant literature applying information economics to finance and trading. The key difference hinges on the unique functionality provided by blockchain, that is, the generation of decentralized consensus through information distribution among the set of record-keepers. This is the first stage involving "decentralization": in our trade finance example illustrated by Figure 2, the system contacts record-keepers like trading partners, ports, and other sellers/customers and they contribute to form the consensus that is accepted by the community. Then the consensus can be—and often is—further distributed to all agents on the blockchain—this is the second stage of information distribution.

Earlier literature in financial economics often studies distribution of available information, which can be thought of the second stage described above. The leading examples are studies on information disclosure that typically concern transparency, for example, the TRACE reporting system on the corporate bond market.[21] Although transparency affects traders' incentives and the effectiveness of market function, it is arguably true that trading and aggregation can still take place, even without pre- and post- transparency requirements on TRACE. In other words, in traditional settings, when greater public information is detrimental, regulators or agents can opt to distribute less information.

In contrast, our paper emphasizes the first stage: the distribution of information during consensus generation serves the core function of blockchain in providing decentralized consensus and tamper-proofness. The greater the degree of information distribution, the higher the quality of decentralized consensus. This point shares the same spirit as Chapman et al. (2017), who find that attempts of restricting decentralization in order to reduce information

[21] See, for example Goldstein et al. (2006) and Bessembinder and Maxwell (2008). In particular, Bloomfield and O'Hara (1999) also find that market makers can use trade information to maintain collusive behavior.

distribution often reduce the operational resilience that is supposedly the technology's advantage over centralized systems.

In general, the quality of consensus, and the amount of information distribution on blockchains depend on their specific protocols. Detailing the various consensus mechanisms or deriving the "optimal" blockchain design is beyond the scope of this paper. Nevertheless, we provide a brief description of blockchain applications in the financial industry and the concerns practitioners share about the informational issue we highlight.

1.3 Blockchain applications in the financial industry

With the core functioning of blockchain in mind, we now discuss various blockchain projects in real-world. The applications of blockchain technology and smart contracts are broad, sometimes even beyond the Fintech industry; and the applications discussed here are not merely proofs of concept.[22] Readers familiar with the institutional background may skip this subsection and go to Section 1.4 directly.

1.3.1 Trade and trade finance. Recall our motivating example in Section 1.2 that involves international trade and its associated financing activities. International trade easily accounts for more than USD 10 trillion annually according to recent World Trade Organization (WTO) report.[23] Despite technological advances in many areas of financial services, trade finance remains a largely paper-based, manual process, involving multiple participants in various jurisdictions around the world, and prone to human error and delays along the supply chain.[24] An importer may fail to strike a deal because the bank offering the letter of credit is not well known in the exporter's country. An exporter may fail to get advanced financing because the bank worries whether the goods can be successfully and timely delivered and whether payments from the importer can be secured.

Blockchain technology can help alleviate the aforementioned frictions in trade. As mentioned, there are two classes of solutions that the blockchain technology can offer. One concerns the flow of goods, as a decentralized ledger can better track goods during the process in which goods are shipped, stored, and delivered (e.g., physical locations and movements or whether goods are kept with the right temperature), with the help of modern communication

[22] Bartoletti and Pompianu (2017) analyze 834 smart contracts from Bitcoin and Ethereum with 1,673,271 transactions. They find five main usage scenarios (financial, notary, games, wallet, and library), three of which are related to monetary transfers and transactions, and the remaining two are related to recording consensus information. More than two-thirds of the uses are on managing, gathering, or distributing money.

[23] For example, World Trade Statistical Review 2017 available at https://www.wto.org/english/res_e/statis_e/wts2017_e/wts17_toc_e.htm.

[24] Small suppliers wait as long as 60 to 90 days to be paid for delivered goods. Slow payment hinders their access to working capital.

technology, such as the Internet of Things (IoT) and "oracles," which are feeders of information from the offline world. The second solution concerns the flow of money associated with trade (e.g., letter of credit and trade finance; this is related to the previously discussed trusted payments). Currently, both solutions are being developed in isolation, but the industry envisions a fully integrated system in the future, with a network of shippers, freight forwarders, ocean carriers, ports and customs authorities, and banks interacting on a blockchain in real time.

In 2016, Barclays and Fintech start-up Wave claim to have become the first organizations to complete a global trade transaction using the new Wave blockchain platform (Taylor 2016). IBM also has been spearheading the application of blockchain and smart contracts to trade finance (Haswell 2018). In March 2017, IBM and Maersk, cooperating with Hyperledger Fabric, announced the completion of an end-to-end digitalized supply chain pilot using blockchain technology, which involves trading parties and various ports and custom authorities (Allison 2017).[25] In early 2017, IBM has ventured further by rolling out the Yijian Blockchain Technology Application System for the Chinese pharmaceutical sector. It has also collaborated with a group companies to develop a blockchain-based crude oil trade finance platform (Higgins 2017a).[26]

Some progress has been made in applying blockchain technology to the freight and logistics industry. In September 2017, Maersk partnered with EY, Microsoft, Willis Towers Watson, and several insurance companies to securely share shipping data on KSI, a blockchain developed by Guardtime (Hackett 2017). In November 2017, it was reported that the association Blockchain in Transport Alliance (BITA; https://bita.studio/), whose members include start-up blockchain companies like ShipChain, had attracted global giants like SAP and UPS in the traditional sector (BlockchainNews 2017).

1.3.2 Trusted payments. Payments across long distance or among unknown parties are difficult due to the lack of trust. The Society for Worldwide Interbank Financial Telecommunications (SWIFT) mitigates the problem, but often entails ineffective coordination across multiple institutions and hefty fees. This concern becomes further exacerbated with digital payments, which are plagued by "double-spending" issues.

Bitcoin was first offered as a solution, and it enables anonymous peer-to-peer transactions recorded on the Bitcoin blockchain that is secure and time stamped

[25] This pilot was a consignment of goods from Schneider Electric from Lyon to Newark, which involved the Port of Rotterdam, the Port of Newark, the Customs Administration of the Netherlands, the U.S. Department of Homeland Security Science and Technology Directorate, and U.S. Customs and Border Protection (Allison 2017).

[26] Other blockchain-based platforms that support lending, issuing letters of credit, export credit, and insurance include HK Blockchain for trade finance, TradeSafe, and Digital Trade Chain (DTC). Recently, blockchain startup R3, a trade finance tech provider TradeIX, and a group of major banks have moved their Marco Polo trade finance platform to the pilot stage (Palmer 2018).

to make it tamper-proof (Nakamoto 2008).[27] More importantly, by broadcasting all candidate transactions publicly and having "miners" constantly competing for the recording right of new blocks to earn Bitcoins, its distributed ledger provides a decentralized consensus on whether a transaction has taken place.

By design, maintaining the decentralized consensus record on Bitcoin blockchain requires the miners to solve NP-complete computational problems (i.e., mining, a form of PoW) whose difficulty level increases with computation power by design, making it unsuitable for large volumes of financial transactions. Subsequent platforms, such as Lightning (built on the Bitcoin blockchain) and Stellar (a separate blockchain), have helped improve the processing capacity through local channels and multisignature accounts so that unnecessary information does not have to be part of the decentralized consensus.[28]

That said, these blockchains' scripting language is limited. Ethereum, the second largest blockchain platform by market capitalization after the Bitcoin blockchain, allows the use of Turing-complete language and permits more complex contingent operations (Turing 1937), providing the archetypal implementation of smart contracts (Buterin 2014). All valid updates to the contract states are recorded and automatically executed. A group of voluntary participants (Ether miners) maintain a decentralized consensus recording of the states, and other interacting parties utilize the consensus information to automate executions of contract terms. Additional applications, such as Monax and Phi (String Lab), build on Ethereum to enrich and optimize their smart contract functionalities and processing power, similar to how Web sites build on the Internet protocol.

Traditional players in the financial industry have started the process of accommodating the blockchain technology to address the payment problem. Originally known as Ripple Labs, Ripple was founded in 2012 to provide global financial transactions and real-time cross-border payments and has since been increasingly adopted by major banks and payment networks. A (typically large) set of validating nodes achieve decentralized consensus using the Ripple transaction protocol RTXP—an iterative consensus process as an alternative to PoW, in which transactions are broadcasted repeatedly across the network of validating nodes until an agreement is reached. Digital transfers are then automated by connecting electronically to bank accounts or using the native crypto-token Ripples (XRP).

1.3.3 Other applications. In addition to applications in payments and trade finance, blockchain and smart contracts also can be used in exchanges and

[27] Many retailers in Japan already accept Bitcoins (e.g., *The Economist* 2017).

[28] Counterparty also builds on the Bitcoin blockchain, but allows for more flexible smart contracts and maintains consensus through "proof-of-burn"; that is, fees paid in cryptocurrency paid by clients are destroyed, and nodes are rewarded for validation from the appreciation of the currency.

trading, voting, and even syndicated loans. To that end, in 2015, Nasdaq Inc. launched the Linq Platform for managing and exchanging pre-IPO shares, and, in early 2017, they successfully completed a test using blockchain technology to run proxy voting on Estonian Tallinn Stock Exchange (Shin 2017). Smart contracts can enforce a standard transactional rule set for derivatives (a security with an asset-dependent price) to streamline over-the-counter (OTC) financial agreements. Symbiont offers product with a simple interface for specifying the terms and conditions when issuing smart securities, as well as integration with market data feeds.[29]

Furthermore, Credit Suisse and 12 other banks, together with Symbiont, lead the application of the blockchain technology to syndicated loans (Terekhova 2017). Finally, Walmart recently partnered with IBM and JD.com for a blockchain tracking food production, safety, and distribution (Higgins 2017b).

1.4 Verification and informational concerns in practice

Our theory highlights the potential downside of information distribution during the process of decentralized consensus. The concern about information distribution and privacy is voiced by practitioners, among which R3 CEV, an active blockchain consortium, has been outspoken. R3's Corda system sets out to tackle the challenge that the only parties who should have access to the details of a financial transaction are those parties themselves and others with a legitimate need to know. Even with that, the request, itself a form of information, for proving transaction uniqueness is distributed to some independent observers, changing the information environment of this economy at least partially.

While these measures potentially ensure confidentiality, two important economic insights are missing from current discussions. First, contacting fewer record-keepers may reduce the effectiveness of the consensus; second, encrypting data means some contingencies cannot be validated and thus cannot be used in smart contracts. Moreover, even encrypted data are still data, as the mere act of verification request is still informative to record-keepers, an insight to be highlighted in our model. As de Vilaca Burgos et al. (2017) point out in a report for the central bank of Brazil, simply encrypting sensitive data is not a viable solution because smart contracts then cannot decide whether a transaction is valid.

These observations imply that restricting information distribution often comes at the expense of compromising the consensus effectiveness. For instance, R3's Corda's validating model restricts information distribution only to the notaries.[30] As pointed out in the Bank of Canada report mentioned earlier,

[29] Symbiont is a member of the Hyperledger project, a cross-industry, open-source, collaborative project led by the nonprofit Linux Foundation to advance blockchain technology by coming up with common standards.

[30] This restriction is to prevent denial-of-service (DoS) attacks; that is, a node knowingly builds an invalid transaction consuming some set of existing states and sends it to the notary, causing the states to be marked as consumed.

Chapman et al. (2017), Corda's model requires data replication from the notaries to ensure business continuity rather than each node providing resilience to the system, like in the case with many public blockchains. This makes the so-called "single point of failure" (SPOF) more likely because the system is once again centralized. In fact, in phase 2 of Project Jasper, the role of notary in Corda is performed by the Bank of Canada, so an outage at the Bank would prevent the processing of any payments.

Our model underscores this tension: contacting fewer record-keepers reduces the information distribution, but at the expense of compromising the quality of consensus. We now go one step further to analyze the consequence of distributing information on industrial organization and competition in Section 2.

2. Blockchain Disruption and Industrial Organization

To understand blockchain's impact on the real economy, we now cast our model of decentralized-consensus generation in a standard dynamic industrial organization setting similar to Green and Porter (1984). We show that smart contracts on decentralized consensus help entry which promotes competition, but greater information distribution may foster collusion which hurts competition.

2.1 Model setup

Consider a risk-neutral world in which time is infinite and discrete and is indexed by t, $t=0,1,2,\ldots$. Every agent has a discount factor $\delta \in (0,1)$. In every period $t \geq 0$, with probability λ a unit measure of buyers show up, each demanding a unit of goods. They shop sellers and choose the most attractive offer. We use $\mathbb{I}_t$ to denote this aggregate business condition whether buyers show up in period t. Throughout, we use "buyers," "consumers," and "customers" interchangeably.

The goods delivery between the seller and the buyer is modeled like in Section 1.2. It should be clear that, although we are building our model in the context of trade finance, goods can be interpreted as a service, such as a fund transfer, a loan origination, or trade financing. Buyers (if present) only live for one period and then exit the economy.

Three long-lived sellers, who are either authentic or fraudulent, are present. A fraudulent seller is unable to deliver the good, whereas an authentic seller always delivers the good to the consumer. The consumer obtains an expected utility q_i from seller i. In particular, with probability q_i, the consumer obtains a utility of one, and, with probability $1-q_i$, they obtain zero.

At the start of the game $t=0$, two of the sellers, A and B, are incumbents known to be authentic (who have already established a good reputation). A new entrant C privately knows her authenticity, but others only have the common prior belief that C is authentic with probability π, later referred to as C's reputation.

In every period $t \geq 0$, each seller receives an i.i.d. draw of q_i, $i \in \{A, B, C\}$. The quality profile $\mathbf{q}=(q_A, q_B, q_C)$ is publicly observable, capturing temporal differences among sellers. We discuss the case when quality is the seller's privately information in Section 3.3. Denote the elements in $\mathbf{q}$ in decreasing order by $q^{(1)}$, $q^{(2)}$, and $q^{(3)}$ respectively; this implies that even buyers' choice of incumbent sellers has welfare consequences. We denote the cumulative distribution function and probability density function of quality distribution by $\phi(\cdot)$ and $\Phi(\cdot)$, and its support by $[\underline{q}, \bar{q}]$. It costs a seller μ to produce the goods, where $\mu < \underline{q}$ to reflect that the transaction with an authentic seller is welfare-improving.

Seller C can potentially enter by paying an arbitrarily small cost of $\epsilon > 0$; hence C enters only if she can ever make strictly positive profit in this market after entry.[31] This allows us to focus on information asymmetry of seller authenticity as the relevant entry barrier. We further assume that before obtaining customers, the entrant has no loss-absorbing capacity.[32]

2.2 Traditional world

We analyze the model in the traditional world, starting with the key assumption on contracting space and information environment there.

2.2.1 Contracting space and information.

Assumption 1. In traditional world, no payment can be contingent on whether or not service delivery occurs. Each seller can only observe her own buyers and associated transaction information.

The first part of Assumption 1 reflects certain real-life contract incompleteness that either limits the effectiveness of consensus or makes contracting on it too costly; for a good reference on the costs of writing and enforcing complete contracts, see Hart (1995) and Tirole (1999). In our context, this implies that the sellers can only quote a noncontingent price $p_i(\mathbf{q})$ privately to buyers.[33] The second part of Assumption 1 implies that in the traditional world sellers do not observe others' price quotes, and can be interpreted as seller's quoting customized or "bespoke" prices based on their proprietary

[31] Whether or not the entry decision is made before the quality q_C realization is immaterial, given the arbitrary small entry cost.

[32] This can be microfounded by some borrowing capacity, so that potential entrants cannot implement aggressive penetration pricing schemes. It is a sufficient condition to rule out aggressive penetration pricing (in which entrants suffer huge losses in order to enter). This is realistic because without accumulation of service profit over time, the entrant typically does not have large initial capital (deep pocket) to undercut price aggressively. In fact, all we need is that C's tolerance for loss, L, is no more than $[\underline{q} - \pi\bar{q}]^+$.

[33] That sellers make offers is realistic in many applications where the customers or buyers are short-lived and dispersed. For example, banks typically quote the fee for making an international transfer, and customers can decide which bank to go to. Our main results are robust to this particular trading protocol.

data and private interaction with buyers. In other words, it is infeasible to communicate information across agents beyond transactions. This assumption plays a role when we solve for the sellers' collusion equilibrium and is similar to the assumption in Green and Porter (1984) and Porter (1983).

2.2.2 Bertrand competition and entry. First, we consider a competitive equilibrium, in which sellers lower their offered prices until their competitors quit. Suppose that an authentic C enters. If $\pi q_C < \max\{q_A, q_B\}$, any incumbent will compete to lower the price to μ, to entice the customer this period and prevent the enhanced future competition they would have faced had C entered in this period. Without a reputation for being authentic, an authentic C only stands the chance of enticing a customer if $\pi q_C \geq \max\{q_A, q_B\}$.[34] Basically, entrants can entice customers only when their perceived quality is higher than that of the incumbents. The next proposition follows.

Proposition 2.1. In a competitive equilibrium, the first time an authentic C can serve customers is in period $\tau \equiv \min\{t \geq 0 | \pi q_{C,t} \mathbb{I}_t \geq \max\{q_{A,t}, q_{B,t}\}\}$ or later. Consequently, C never enters if $\pi \overline{q} < \underline{q}$.

In the remainder of the paper, we focus on the case $\underline{q} > \pi \overline{q}$; in other words, the entrant C's reputation is sufficiently low that no entry ever occurs in the traditional world. The expected future consumer (buyer) surplus and social welfare at any time s are, respectively,

$$\Pi_{buyer} = \mathbb{E}_s \left[\sum_{t=s+1}^{\infty} \delta^{t-s} \mathbb{I}_t \left(\min\{q_{A_t}, q_{B_t}\} - \mu \right) \right] = \frac{\delta \lambda}{1-\delta} \mathbb{E}[\min\{q_A, q_B\} - \mu] \quad (5)$$

and

$$\Pi_{total} = \mathbb{E}_s \left[\sum_{t=s+1}^{\infty} \delta^{t-s} \mathbb{I}_t (\max\{q_{A_t}, q_{B_t}\} - \mu) \right] = \frac{\delta \lambda}{1-\delta} \mathbb{E}[\max\{q_A, q_B\} - \mu]. \quad (6)$$

The presence of fraudulent sellers causes no-entrance of a high quality C, a standard lemons problem. We show later that this problem can be better or even fully resolved by smart contracts with blockchain technology offering decentralized consensus.

2.2.3 Collusive equilibria. Besides the competitive equilibrium derived, there may exist collusive equilibria in this economy. Given no-entrance of seller C, we only need to examine potential tacit collusion among the incumbents.

[34] Even so, C may not entice the customer if their incumbents use predatory pricing. Note that when $\pi \overline{q} < \underline{q}$, no matter what $\mathbf{q}$ is, C cannot enter even with penetration pricing because the maximum loss C can afford is less than $\underline{q} - \pi \overline{q}$.

We restrict each seller's strategy to the standard supergame strategies discussed in, for example, Green and Porter (1984). Specifically, consider the following strategy, indexed by $\{T, f\}$, for A and B to collude. There are two phases:

1. *Collusion phase*: Every period, after the realization of types, A charges price q_A and B charges price q_B. A and B entice $\mathbb{I}_t f(q_A, q_B)$ and $f(q_B, q_A) = \mathbb{I}_t(1 - f(q_A, q_B))$ fractions of buyers, respectively.[35] Here, $f(x, y) \in (0, 1)$ is the proposed anonymous allocation function, potentially as a function of realized types (e.g., via setting quotas). This allocation function f includes the case in which sellers always equally split buyers and the case in which buyers all go to the better seller.
2. *Punishment phase*: The punishment phase is triggered once one of the sellers does not have any buyers. More specifically, the punishment phase can be triggered either by (1) buyers not showing up this period or (2) one of the sellers deviating by quoting a cheaper price to entice all the buyers. Once triggered, A and B are engaged in Bertrand competition for a fixed T period.

Recall that the sellers do not observe other sellers' price quotes, and only observes their own customers. However, this repeated game with private monitoring is essentially a game with imperfect public monitoring, because sellers can use the private observation to infer whether there is aggregate activity (customers arriving). It is imperfect in the sense that punishment could be triggered even when no one deviates. The equilibrium notion corresponding to the above strategies is thus akin to public perfect equilibrium.

A standard result in the literature of dynamic repeated games is that sustainable equilibria crucially depend on the discount factor δ, with the Folk theorem as the best-known example. We therefore proceed to derive the lower bound of discount factor, denoted by $\delta_{(T,f)}$, above which an equilibrium with a specified T and $f(x, y)$ exists.

Lemma 2.2. Define $f(q_i) \equiv \mathbb{E}_{q_j}[f(q_i, q_j)]$ to be the expected fraction of buyers a seller of type q_i entices. A collusion strategy with (T, f) as described above is an equilibrium, if

$$(M_1 - M_2)\lambda\delta\left(1 - \delta^T\right) \geq M_3(1 - \lambda\delta - (1 - \lambda)\delta^{T+1}), \tag{7}$$

where $M_1 \equiv \mathbb{E}[f(q_i)(q_i - \mu)]$, $M_2 \equiv \mathbb{E}[(q_i - q_j)^+]$, $M_3 \equiv \max_{\{q_i \in [\underline{q}, \overline{q}]\}}[(1 - f(q_i))\,(q_i - \mu)]$.

Here, M_1 is a seller's expected payoff in the "stage game" in each period during the collusion phase, M_2 is that during the punishment phase, and M_3 is

[35] Our analysis is robust to sellers charging a lower colluding price (less than q_i).

the maximum gain from deviating. When the discount factor δ is sufficiently low (impatient), the payoff from deviation is relatively large compared with the punishment going forward, so no collusion equilibria can be sustained.

Proposition 2.3. When the discount factor $\delta < \delta_o^{Traditional} \equiv inf_f \delta_{(T,f)}^{Traditional} = \inf_f \frac{1}{\lambda} \frac{M_3}{M_1+M_3-M_2}$, no collusion equilibrium exists for any (T, f).

The welfare under (T, f) collusion is determined by f, and consumer surplus is determined by both (T, f) and the colluding price. The consumer surplus depends on the length of punishment period T because buyers earn positive surplus only when the punishment phase is triggered because of an absence of buyers in the economy (which occurs with probability $1-\lambda$ in each period).

2.3 Blockchain world

The blockchain technology enables the consensus recording of goods-delivery status by recordkeepers' verifications. As detailed earlier in Section 1.2, this verification typically involves distributing information.

To highlight the economic force, we examine the case of perfect consensus, that is, when $K \to \infty$ so that $\widetilde{z}=\widetilde{\omega}$, and smart contracts on the blockchain can trigger payment based on this consensus. This case captures many extant blockchains, such as Bitcoin, Ripple, and Symbiont, where either the verification request or transaction information is distributed to sufficiently large numbers of parties including major institutional participants. Note, this does not imply record-keepers are the entire population of the blockchain. Moreover, as we discuss in Section 3.2, the basic trade-off under imperfect consensus is qualitatively the same.

Assumption 2. The blockchain contacts infinite participants (including the sellers and a continuum of consumers) to generate an effective decentralized consensus. More specifically, the blockchain consensus $\widetilde{z}=\widetilde{\omega}$, and a seller knows the aggregate business condition either by observing the presence of her own customers or by inferring the presence of customers upon being contacted.

Recall $\widetilde{\omega}$ is the delivery outcome (whether or not successful). This assumption implies that (1) self-executed smart contracts can be perfectly contingent on delivery outcome consensus and (2) the sellers observe the aggregate business condition. These are in sharp contrast to Assumption 1. We also note that the blockchain system may have richer information and the results can be extended to the cases wherein this information is used. But our arguments require weaker conditions, and it suffices that they observe the aggregate activity.

In the rest of this section, we demonstrate how blockchain and smart contracts can enhance entry and competition, show that the same technology can lead to greater collusive behavior, and discuss regulatory implications.

2.3.1 Smart contracts and enhanced entry. With blockchain, the entrant now can offer a price contingent on the success of delivery so that $\mathbb{P}=(p^s, p^f)$, with p^s and p^f being prices charged upon success and failure. An authentic entrant C can separate from her fraudulent peer by offering $(p^s,0)$. The fraudulent type gains nothing from mimicking: she knows that she will fail to deliver and hence never receive the payment. As a result, the authentic seller C enters for sure. We have the following proposition for the competitive equilibrium without potential collusion.

Proposition 2.4. In the competitive equilibrium in the blockchain world, the authentic entrant C enters almost surely, and first entices customers in period $\tau=\min\{t\geq 0|q_{C,t}\mathbb{I}_t\geq\max\{q_{A,t},q_{B,t}\}\}$ or earlier.

In the world with blockchain, the expected future consumer surplus and total welfare at $t=s$ under a competitive equilibrium are, respectively,

$$\Pi_{buyer}=\mathbb{E}_s\left[\sum_{t=s+1}^{\infty}\delta^{t-s}\mathbb{I}_t\left(q^{(2)}-\mu\right)\right]=\frac{\delta\lambda}{1-\delta}\mathbb{E}\left[q^{(2)}-\mu\right] \tag{8}$$

and

$$\Pi_{total}=\mathbb{E}_s\left[\sum_{t=s+1}^{\infty}\delta^{t-s}\mathbb{I}_t(q^{(1)}-\mu)\right]=\frac{\delta\lambda}{1-\delta}\mathbb{E}\left[q^{(1)}-\mu\right]. \tag{9}$$

Compared with Equations (5) and (6), we see that with smart contracts that facilitate entry and hence competition, the economy becomes more efficient, as both consumer surplus (linear in the second-order statistic) and welfare (linear in the first-order statistic) improve.

2.3.2 Enhanced collusion under permissioned blockchain. While blockchain and smart contracts can improve both consumer surplus and welfare by encouraging entry and competition, a dark side of blockchain may result in dynamic equilibria with lower welfare or consumer surplus than in the traditional world. To highlight the collusion-enhancing effect of blockchain, we first focus on permissioned blockchain for the incumbents which C cannot use (hence no entry), before discussing blockchains that C can utilize.

2.3.2.1 Collusion using smart contracts. With blockchain and smart contracts, sellers can use the enlarged contingencies and hence side payment to facilitate collusion, as illustrated by the following example. All sellers collude to charge the highest amount they can charge upon delivery, that is, q_i, effectively extracting full rents from buyers. The sellers reach an agreement that only the best-quality seller in each period takes all consumers, and if a seller who does not have the best quality takes any consumer, a smart contract can

take all its profit automatically and transfer it to other sellers.[36] By imposing automatic punishment on deviation, the smart contract can potentially support any collusion, regardless of the discount factor.

Such explicit form of collusion using smart contracts is easy to detect and can be forbidden by antitrust law (Section 3.1.2). The more relevant and interesting phenomenon is that even without explicit side payment, the blockchain still can facilitate greater collusion, which we discuss next.

2.3.2.2 Tacit collusion with a permissioned blockchain. In the case of tacit collusion, we consider the same collusion and punishment phases, as well as the allocation rule f, like in the traditional world. The catch is that, instead of triggering punishment upon deviating or receiving no buyers, punishment in the blockchain world can be further conditioned on whether buyers show up. This is because participants upon being contacted for verification at least know that service requests are made; this does not even require installment of IoT sensors on participants. However, being contacted for verification reveals the aggregate state of the presence of buyers, which allows the sellers to perfectly monitor deviation behavior by a colluding fellow.[37]

In other words, the repeated game with traditionally imperfect public monitoring now achieves perfect public monitoring as deviations can be accurately detected on blockchain during the consensus generation process. Collusive equilibria hence become easier to sustain (without punishment along the equilibrium path).

Proposition 2.5. For given (T, f), denote the threshold discount factor above which collusion is sustained with permissioned blockchain by $\delta_{(T,f)}^{Blockchain2}$, and recall $\delta_{(T,f)}^{Traditional}$ and $\delta_{o}^{Traditional}$ are defined in Proposition 2.3.

1. For any (T, f), we have $\delta_{(T,f)}^{Blockchain2} < \delta_{(T,f)}^{Traditional}$.
2. When $\delta \in \left[\inf_f\{\delta_{(\infty,f)}^{Blockchain2}\}, \delta_{o}^{Traditional}\right)$, there cannot be collusion without blockchain, but there could be with blockchain.

In case 2), the consumer welfare under collusion with blockchain is lower than that under competitive equilibrium but without blockchain.

---

[36] For smart contracts to work, decentralized consensus on delivery contingency of the seller identity is needed so that the blockchain system has to recognize whether the best-quality seller is serving all consumers. In general, depending on specific collusive equilibria, one may penalize deviating contingencies using smart contracts, even without information on sellers identity/characteristic.

[37] The deviating seller might potentially choose to conduct his/her transaction off-chain to avoid triggering the price war, and this is relevant given our simplified assumption of incumbents being established authentic ones. However, in general, the augmented contractibility of smart contracts benefits all participants, and off-chain stealing can be quite ineffective even for incumbents. Besides, the flexibility of sellers switching between on-chain and off-chain businesses is also questionable, given the context of our trade finance applications.

2.4 Blockchain disruption

Suppose now that there is a (potentially public) blockchain that all three firms (incumbents A, B, and new entrant C) have access to. Would the benefit of entry to consumer outweigh the cost of potential greater collusion?

2.4.1 Consumer surplus under a public blockchain. Recall that Section 2.3.1 has solved the competitive equilibrium. To characterize other collusive equilibria in this economy, consider the following collusion strategy:

1. *Collusion phase*: Every period, after the realization of types, each seller i charges q_i contingent on success. Let $\hat{f}(q_i, q_j, q_k) \in (0,1)$ be the fraction of the buyers that go to the seller with quality q_i when the other two sellers have qualities q_j and q_k.
2. *Punishment phase*: The punishment phase is triggered if one of the sellers does not have any buyers *and* there are buyers showing up in this period. In other words, the punishment phase is triggered only if there is some seller deviates. Once triggered, all sellers are involved in Bertrand competition for T periods.

Lemma 2.6. Define $\hat{f}(q_i) \equiv \mathbb{E}_{q_{-i}}[\hat{f}(q_i, q_{-i})]$ to be the expected fraction of buyers a seller of type q_i entices. With blockchain, the above strategy is an equilibrium if the parameters satisfy

$$\delta\lambda\left(1-\delta^T\right)(\hat{M}_1 - \hat{M}_2) \geq (1-\delta)\hat{M}_3 \tag{10}$$

where $\hat{M}_1 \equiv E[\hat{f}(q_i)(q_i - \mu)]$, $\hat{M}_2 \equiv E[(q_i - \max_{j \neq i} q_j)^+]$, and $\hat{M}_3 \equiv \max_{\{q_i \in [\underline{q}, \overline{q}]\}}[(1 - \hat{f}(q_i))(q_i - \mu)]$.

The $\hat{M}$s can be interpreted similar to that in Lemma 2.2, but for three sellers, not two. The left-hand side of Equation (10) is also modified because with perfect public monitoring, the punishment is more accurately targeted.

2.4.2 Dynamic equilibria under blockchain disruption. More generally, in terms of welfare and consumer surplus, the set of equilibrium outcomes with blockchain disruption is a nontrivial superset of those in equilibria in the traditional world. Denote by *Blockchain3* the public blockchain with all three sellers.

Theorem 2.7. The threshold of discount factor $\delta_a^{Blockchain3} \equiv \sup_{\hat{f}}\{\delta_{(\infty,\hat{f})}^{Blockchain3}\}$ is well defined and satisfies $\delta_a^{Blockchain3} < 1$. For all $\delta > \delta_a^{Blockchain3}$, any consumer surplus and welfare attainable in the traditional world can be attained with blockchain, and some additional equilibria with higher or lower consumer surplus or welfare also can be sustained.

In this theorem, the subscript a in $\delta_a^{Blockchain3}$ stands for "all," indicating that *all* collusion equilibria can be sustained if the discount factor is above $\delta_a^{Blockchain3}$. We can similarly define threshold $\delta_o^{Blockchain3} \equiv \inf_{\hat{f}}\{\delta_{(\infty,\hat{f})}^{Blockchain3}\}$. Then an even weaker condition for blockchain to potentially hurt consumers is $\delta > \delta_o^{Blockchain3}$.

It is also worth remarking that with blockchain the total welfare can be reduced, because it is now possible to sustain an equilibrium in which firms collude so that in any given period all sales go to the seller with the lowest q_i, which is lower than that with only incumbents.

Our findings are robust qualitatively to having more incumbents and entrants, and the next corollary illustrates how consumer surplus could be lower with blockchain in this more general case.

Corollary 2.8. For $m \geq n \geq 2$, if $\lambda < \frac{n-1}{n}$, then $\delta_o^{Traditional,n} > \delta_o^{Blockchain,m}$, where m and n indicate the number of colluding sellers with and without blockchain respectively. Consequently for all $\delta \in [\delta_o^{Blockchain,m}, 1]$, there is no collusion in the traditional world with n incumbents, while blockchain can lower consumer surplus (with m sellers including new entrants).

3. Discussions and Extensions

This section provides discussions from a regulatory angle and considers several extensions of our model.

3.1 Measures to reduce collusion on blockchains

Our concern that blockchains can jeopardize market competitiveness is also shared by other market observers. The concern becomes especially acute for permissioned blockchains like R3 whose members are powerful financial institutions. As described by Kaminska 2015, what "… the technology really facilitates is *cartel management* for groups that don't trust each other but which still need to work together if they are the value and stability of the markets they serve." Our paper highlights one particular economic mechanism through which blockchains could hinder competition, and provides a rigorous analysis on why and how collusion could occur. In fact, empirical evidence suggests that greater information sharing indeed facilitates collusion (Bourveau et al. 2017). We now explore regulatory and market solutions to curb collusive behaviors in our framework.

3.1.1 Blockchain competition versus firm competition. Although we focus on the case of a single blockchain on which multiple sellers compete, in practice there are likely to be multiple blockchains which both sellers and buyers can choose. The competition among blockchains naturally goes against the collusive behaviors of sellers on one blockchain, as buyers can always pick the blockchain which offers the best price-adjusted service. Although blockchain

competition may mitigate collusive behaviors on specific blockchains, in the long run if a single blockchain becomes dominant due to a network effect, regulators still have to step in to prevent collusion by breaking up blockchain platforms. While this approach of "breaking up big players works for traditional industrial firms as well, this point is especially relevant for blockchain. This is because coordination is integral to the ecosystem of blockchain, and likely interferes with its operation. For a new blockchain platform to be used and competition-enhancing, different institutional and retail users have to coordinate on adoption. Coordination issues have already manifested themselves in the dominance of early movers, such as Bitcoin and Ethereum in the cryptocurrency markets.[38]

Of course, the above discussion raises other questions: Why is it more difficult for blockchains to collude, at least relative to sellers on the same blockchain? What can governments do to facilitate coordinated adoption of better designed blockchain platforms? These are all interesting questions for future research.

3.1.2 Regulatory nodes and design. In the traditional world, in general it helps for regulatory agency to observe and collect more information about the market in order to better detect collusive behaviors. Similarly, adding a regulatory node in the blockchain, especially for private permissioned chains that do not automatically include regulators as part of the business ecosystem, can help regulator monitor the economic behaviors of market participants and reduce tacit collusion. However, in this regard, blockchain is no different from traditional world: The government who has the authority to investigate and penalize firms can reach the same outcome in both scenarios. For instance, within our model, the regulator can detect and hence deter collusion by monitoring whether buyers (if present) are purchasing goods with the highest quality.

In this regard, blockchain may offer a significant advantage relative to the traditional world thanks to real-time and tamper-proof records. As a result, regulators do not have to worry about misreporting and time-delays, enabling the detection and containment of collusion and market malfunctions at relatively high frequency. Moreover, retrospective auditing is no longer prone to manipulation. The hyperledger fabric example in Section 2.3 illustrates these effects.

Regulators can also potentially participate in the protocol design. For example, the government can reserve access to certain encrypted information that is broadcasted to blockchain participants or record-keepers. This direct access not only enables the elimination of collusions using smart contracts

[38] We thank the editor, Itay Goldstein, for pointing this out to us.

(see Section 2.3.2) but also allows for the detection of tacit collusion based on statistical analysis of transaction and pricing behaviors.[39]

3.1.3 Separation of usage and consensus generation. In the model, sellers can use the information on the blockchain to punish deviations from collusion in a more accurate way. They observe the information because the information is distributed and recorded on the blockchain during the process of consensus generation. From this perspective, one obvious potential solution is to separate the players who help generate the decentralized consensus, from the users of that consensus. For example, in our model if sellers can only use the blockchain for signing smart contracts with buyers but are excluded from record-keeping activities, they no longer have access to the aggregate-activity information that fosters collusion.

As discussed in the trade finance example in Section 1.2, excluding sellers from record-keeping activities might be challenging. This is because, naturally, the parties that we should exclude from being contacted for record-keeping are also likely the ones who are the most qualified to validate a record (e.g., the experienced sellers with great expertise within the same industry). Most extant public blockchains do not separate the two groups. On some blockchains, such as Symbiont, record-keepers tend to be a rather separate group from the end users, though this resolution has not been sufficiently explored.

The separation of usage and consensus generation is new in the discussion among blockchain practitioners. It reflects yet another economic trade-off between decentralization (a resilient system needs a wider range of participants) and centralization (but only a small set of agents with expertise are able to provide high-quality inputs), and constitutes a direction for future policy discussions concerning blockchain applications.[40]

3.2 Imperfect consensus

In Section 2 we have assumed that an infinite number of blockchain participants are contacted as record-keepers ($K \to \infty$), rendering perfect consensus. Suppose a finite number of blockchain participants serve as record-keepers, so that $|\mathbb{K}| = K < \infty$. Then the resultant imperfect consensus has probability ψ to correctly record the delivery status, where $\psi = \sum_{k \in \mathbb{K}^*} w_k \leq 1$ and $\mathbb{K}^* = \{k \in \mathbb{K} : b_k w_k < h_k\}$ as derived in Equation (3).

---

[39] Regulation also touches another important concern when the blockchain storages and processes data on a large scale. In trade finance applications, it is most likely that at a significant portion of the data are personal data and hence is subject to regulations, such as the General Data Protection Regulation (GDPR), which was enacted on May 25, 2018, and is directly applicable to blockchain-based platforms in all EU member states. As such, a public and permissionless blockchain would not work. It needs to be a private and permissioned blockchain that is operated by one or more entities who set up the terms of use, and these entities serve as controllers who are responsible and liable for the lawful processing of personal data in compiling with the regulation.

[40] According to Chapman et al. (2017), sufficient decentralization among the record-keepers who are not users may still preserve the blockchain advantage of resilient and effective consensus.

The precision ψ essentially captures in reduced form the quality of consensus when consensus generation is imperfect, and is consistent with many alternative protocols.[41] In words, a successful (failed) delivery might be recorded as a successful delivery with probability ψ $(1-\psi)$. Given the imperfect consensus, can the authentic type still enter the market with the help of blockchain with smart contract (p^s, p^f) and separate from (instead of pool with) the fraudulent type?

We introduce the entrants capacity to bear its initial loss $L \geq 0$; this loss capacity helps authentic entrants separate from fraudulent ones, and is a relaxation of the condition to exclude aggressive pricing strategy in footnote 33 in Section 2. The authentic seller in the separating equilibrium of stage game solves the following:

$$\max_{(p^s,p^f)} \quad \psi p^s + (1-\psi)p^f$$

$$s.t. \quad \psi p^s + (1-\psi)p^f \geq \mu, \quad -p^f \leq L, \quad and \quad (1-\psi)p^s + \psi p^f < 0,$$

where the inequalities are the authentic types participation constraint, limited loss capacity, and the fraudulent types no-mimicking constraint, respectively. For instance, in the last inequality, the fraudulent entrant who never delivers the good has probability $1-\psi$ of being recorded as having a successful delivery and paid by p^s, and with probability ψ of being recorded as failed, receiving p^f. The above program admits a solution when $\psi > \frac{\mu+L}{\mu+2L}$, which allows the authentic type enter for some positive profit without imitation by the fraudulent type, yielding the following proposition.

Proposition 3.1. The use of smart contract on blockchain facilitates entry of the authentic type if the consensus quality is sufficiently high, that is, $\psi > \frac{\mu+L}{\mu+2L}$.

In the limit of $\mu = 0$, we find that smart contracting facilitates entry as long as the consensus is slightly informative of the true state ($\psi > \frac{1}{2}$).

In our model, there is a continuum of consumers upon arrival, which implies that there is a continuum of transactions to be verified. If each verification process draws record-keepers in some independent way, then the law of large numbers across transactions reveals the aggregate state of customer arrival, even under imperfect consensus. Therefore, imperfect consensus does not affect the collusive equilibria supported. Overall, it weakly reduces entry and competition, and it is in this sense weakly welfare improving to have perfect consensus.

[41] Consider the situation with noisy observation of the true state $\tilde{\omega}$, but no misreporting (say the misreporting benefit b is small). Suppose that all symmetric record-keepers correctly observe the delivery outcome with probability $\theta > \frac{1}{2}$. If the consensus on successful delivery is based on unanimity rule, then $\psi = \theta^K$. Similarly, the majority rule says $\psi = \sum_{k=\lceil \frac{K}{2} \rceil}^{K} \binom{K}{k} \theta^k (1-\theta)^{K-k}$.

As we mentioned, the key to reducing collusion is to separate sellers from record-keepers and directly reduce contacting the former. To model this exclusion of sellers, we suppose that, for each delivery, a seller is contacted with probability $\hat{\zeta}$; then the probability that a seller is completely unaware of the aggregate service activity conditional on consumers arriving is $1-\zeta \equiv (1-\hat{\zeta})^n$, where n is the number of transactions. In the collusion-phase a deviation is detected with probability of ζ instead of with probability one, triggering less punishment and making the collusion equilibrium more difficult to sustain. That said, if the number of transactions is large, the equilibrium approaches the one with perfect public monitoring unless the sellers are strictly prohibited from acting as record-keepers ($\hat{\zeta}=0$).

3.3 Information asymmetry and private qualities

In our analysis so far, the seller quality is publicly known. In this section we allow for privately observed qualities. Collusion with private information in general is complex (Athey and Bagwell 2001; Miller 2011); therefore, our focus is on the competitive equilibrium (and competitive stage games in the punishment phase of a collusion.) We characterize how smart contracts can help mitigate allocative inefficiency beyond entry and derive the equilibrium form of smart contracts under market equilibrium.

In particular, we have shown that smart contracts that are contingent on delivery success or failure can separate fraudulent sellers from authentic ones. More generally, the blockchain can also provide consensus on the quality of service q. We model such functionality by assuming that a noisy signal of quality is contractible using decentralized consensus on the blockchain. This hardly matters when quality is public, but can help mitigate information asymmetry when quality is private.

Specifically, we assume that when the service quality is q, the goods are defective (yielding zero utility to the buyers) with probability $1-q$ and are satisfactory otherwise (yielding unit utility to the buyers). The blockchain provides consensus on whether the goods are defective, which can be used in smart contracts. Here "defection;; or "satisfaction" should be something that people can potentially agree about (i.e., not subjective feelings about the experience).

Under this extension smart contracts now have three contingencies: successfully delivered and satisfactory (s), successfully delivered but defective (sd), and failure to deliver (f). The corresponding price offers are denoted by (p^s, p^{sd}, p^f).

3.3.1 Allocative inefficiency in the traditional world. Without smart contracts, the entrant would always claim it is authentic and has high quality (cheap talk). Similarly, incumbents cannot separate themselves either. Following the same logic as before, the lemons problem prevents entry and

separation cannot occur even among incumbents with different qualities. We have

Lemma 3.2. In the traditional world, sellers post the same price $p_i = \mu$, and each buyer selects (randomly) one of them. Each period the buyers surplus and social welfare is $\mathbb{E}[q_i] - \mu$.

3.3.2 World with blockchain and equilibrium smart contracts. Smart contracts enlarge the space of price quotes that sellers can use. An authentic entrant would always offer $p^f = 0$ to separate from fraudulent entrants who have no incentive to mimic. Meanwhile, the choice of p^f is immaterial for incumbents because they always deliver and p^f is made with zero probability. We further impose that $p^{sd} \leq p^s$ so that payment to the seller is lower upon having a defective good—a standard monotonicity assumption in the security design literature.[42]. Then upon enticing customers, seller i with quality $q_i = q$ earns $S_q(\mathbb{P}) = qp^s + (1-q)p^{sd} - \mu$, and the buyer obtains a utility $B_q(\mathbb{P}) = q(1-p^s) + (1-q)(-p^{sd})$, where $1 - p^s$ is the utility from the good/service less the payment.

Sellers may offer a large variety of smart contracts; but only one particular class of contracts emerges in equilibrium, as shown by the following proposition (recall that Φ is the cdf of q).

Proposition 3.3. There is a competitive equilibrium for each stage game that is essentially unique in terms of equilibrium payoffs. In this equilibrium, sellers offer contracts of the form $\mathbb{P}^* = (p, p-1, 0)$. A seller of quality $q_i = q$ offers $(p_q, p_q - 1, 0)$ with

$$p_q = 1 - q + \mu + \int_{\underline{q}}^{q} \left[\frac{\Phi(q)}{\Phi(q)} \right]^2 dq, \tag{11}$$

which is decreasing in q. Buyers go to the highest-quality seller.

Note that a higher-quality seller is willing to offer a greater warranty on the product. The expected payoff of the seller is still increasing in her quality even though a higher-quality seller charges a lower price, because her probability of buyer satisfaction is higher.

Under the equilibrium contract $(p_q, p_q - 1, 0)$, buyers obtain utility $1 - p_q$ regardless of the satisfaction outcome. The competitive equilibrium essentially is a cash auction in which a bidder with quality $q_i = q$ has a private valuation of

[42] See, for example, Innes (1990), Hart and Moore (1995), and DeMarzo and Duffie (1999). Under a market mechanism by which buyers shop sellers and choose the most favorable one, our setup has a natural reinterpretation under informal first-price auctions with security bids (e.g., DeMarzo et al. 2005; Cong 2017).

his/her service opportunity $q-\mu$, and bids p_q.[43] In equilibrium, buyers choose the highest quality seller, who obtains the second-highest valuation $\mathbb{E}[q^{(2)}-\mu]$ in each period with customer arrival (the revenue equivalence theorem), and the economic outcomes are the same as those in the case in which **q** is publicly known (Equations ((8) and (9))).

Corollary 3.4. Smart contracts fully resolve informational asymmetry in a competitive equilibrium, and welfare and consumer surplus are independent of whether or not seller qualities are private.

That said, one can show that restricting the form of smart contracts can potentially increase the consumer surplus in a way similar to how security design affects issuers payoffs. For regulators concerned with consumer surplus, collusion and smart contract forms should be jointly considered. This joint consideration is a topic for future studies.

4. Conclusion

In this paper we argue that decentralized ledger technologies, such as blockchains, feature decentralized consensus and tamper-proof algorithmic executions and, consequently, enlarge the contracting space and facilitate the creation of smart contracts. However, the process of reaching decentralized consensus changes the information environment on the blockchain, potentially engendering welfare-destroying consequences by promoting collusion.

We analyze how this fundamental tension can reshape industry organization and the landscape of competition; it can deliver higher social welfare and consumer surplus through enhanced entry and competition, yet it may also lead to greater collusion. In general, blockchain and smart contracts can sustain market equilibria with a larger range of economic outcomes. We discuss regulatory and market solutions to further improve consumer surplus, such as separating agents generating consensus from end users.

We have modeled the universal feature of blockchains and the key trade-offs of consensus generation and information distribution in reduced form. Although beyond the scope of this paper, designing a robust consensus protocol and providing the right incentives for maintaining consensus on specific blockchains would be an interesting next step and would likely require the joint effort of computer scientists and economists.

[43] This mirrors the well-known result in the literature of security design that the sellers would offer the least information-sensitive security ("flattest security in the language of security-bid auctions, e.g., DeMarzo et al. 2005).

Appendix A. Consensus Generation: Alternative Specifications

We still denote the decentralized consensus on $\widetilde{\omega}$ on a blockchain by $\widetilde{z}$, except that they can take on a continuum rather than binary values. The set of record-keepers and the effectiveness measure are as previously specified. Upon contact, each record-keeper $k \in \mathbb{K}$ submits $\widetilde{y}_k$, taking a continuum of values and yielding a collection of reports $\mathbf{y} \equiv \{\widetilde{y}_k\}_{k\in\mathbb{K}}$.

Depending on the specific blockchain protocol, the consensus $\widetilde{z}(\mathbf{y})$ is then a transformation of inputs collected from these contacted record-keepers. Again, we can write it as

$$\widetilde{z}(\mathbf{y}) = \tilde{Z}\left(\sum_k \widetilde{w}_k \widetilde{y}_k\right), \tag{A1}$$

which includes many well-known blockchains, such as Bitcoin, in which the miner who solves a hard NP complete problem first (which is completely random if miners have homogeneous computation power) makes the record block. In the language of our model, the blockchain protocol randomly chooses one report from all contacted record-keepers (all miners).

For simplicity, we examine a large class of linear model typically used in continuum-signal space.

$$\widetilde{z}(\mathbf{y}) = \frac{1}{K}\sum_k \widetilde{y}_k, \tag{A2}$$

Here, the decentralized consensus is a simple average of all selected reports. It is easy to show that our results are robust to heterogeneous and stochastic weights on signals.

A.1 Information Set of Record-keepers. To incorporate potentially noisy observation, we assume that each record-keeper on the blockchain has a private signal $\widetilde{x}_i = \widetilde{\omega} + \widetilde{\eta}_i$, where for simplicity $\widetilde{\eta}_i$ are i.i.d. with a mean of 0 and a variance of σ_η^2. $\widetilde{\eta}_i$ captures noisy observations of the true state based on public information and off-chain information available on blockchain, as well as additional information record-keepers have when generating consensus.

$\mathbf{1}_k$ denotes the event of record-keeper k being contacted, upon which his or her signal becomes $\widetilde{x}_k = \widetilde{\omega} + \widetilde{\eta}_k$, where $\widetilde{\eta}_k$'s has a mean of 0 and a variance σ_K^2. We have $\sigma_K \leq \sigma_\eta$, thanks to the additional (potentially encrypted) information. In summary, the set of all information on the blockchain can be written as a tuple of $\left\{\mathbb{K}, \{\widetilde{x}_i\}_{i\notin\mathbb{K}}, \{\widetilde{x}_k, \mathbf{1}_k\}_{k\in\mathbb{K}}, \widetilde{z}\right\}$.

A.2 Misreporting and Manipulation. We modify the normalized utility of each risk-neutral record-keeper who submits a report of y_k to

$$U(y_k; \mathbf{y}) = \widetilde{b}_k \cdot (\widetilde{z}(\mathbf{y}) - \widetilde{x}_k) - \frac{1}{2h}(y_k - \widetilde{x}_k)^2, \tag{A3}$$

The first coefficient $\widetilde{b}_k \equiv \widetilde{b} + \widetilde{\varepsilon}_k$ is record-keeper k's bias in misreporting, which is known to the record-keeper k before submitting his/her report. Here, the common bias $\widetilde{b}$ (among contacted record-keepers) has a mean of 0 and a variance σ_b^2, capturing the common bias on the blockchain, which can be interpreted as one institutional transaction party choosing validators within its proprietary network (peer selection on Ripple or notary choice on Corda), an attempt by holders of the crypto-currency to slow down the creation of inflation of the native currency, and/or a system-wide hacking motive. Such common bias is not alien in the traditional economy: arbitrators in business arbitration are only rewarded if they are chosen by their clients and may systematically cater to major clients. The idiosyncratic part $\widetilde{\varepsilon}_k$ is i.i.d., with a mean of 0 and a variance of σ_ε^2.

The second term captures the private cost of manipulation, where h parametrizes how quickly the cost rises with the magnitude of misreporting, which depends on the consensus protocol design.

A.3 Information Distribution and Quality of Consensus. Each contacted record-keeper chooses y_r to maximize U in (A3), which gives

$$\widetilde{y}_k^* = \widetilde{\omega} + \widetilde{\eta}_k + \frac{h}{K}\widetilde{b}_k. \tag{A4}$$

The equilibrium consensus then is (recall $\widetilde{b}_k = \widetilde{b} + \widetilde{\varepsilon}_k$)

$$\widetilde{z} = \frac{1}{K}\sum_k \widetilde{y}_k = \widetilde{\omega} + \frac{1}{K}\sum_k \widetilde{\eta}_k + \frac{h}{K}\left(\widetilde{b} + \frac{1}{K}\sum_k \widetilde{\varepsilon}_k\right), \tag{A5}$$

with the resultant quality of the decentralized consensus:

$$-Var(\widetilde{\omega} - \widetilde{z}) = -\left[\underbrace{\frac{\sigma_K^2}{K}}_{\text{signal quality}} + \underbrace{\frac{h^2}{K^2}\left[\sigma_b^2 + \frac{\sigma_\varepsilon^2}{K}\right]}_{\text{manipulation}}\right]. \tag{A6}$$

The first term directly relates to signal quality. For instance, contacting for verification by sharing some details of the transaction information may reduce σ_K and hence improves quality. Additionally, the first term in (A6) shows that the average over a greater sample size K smooths out the observation noises $\widetilde{\eta}_k$'s and hence leads to a better consensus.

The more novel second channel is rooted in the process of decentralized consensus generation. When the blockchain contacts more and more record-keepers, that is, a greater K, each understands that each individual has less influence on the final consensus outcome. The resultant reduced manipulation in report $\widetilde{y}_k^*$ in (A4) translates to a higher consensus effectiveness. This effect is reflected in the scaling of $1/K^2$ in the "manipulation" terms in (A6). This is the key economic reason blockchain is deemed more secure, in addition to its technical improvements on cybersecurity. Of course, aggregation certainly helps reach a better consensus by reducing the idiosyncratic components of misreporting, as reflected in the denominator of the second term in "manipulation" in (A6).

However, contacting more record-keepers affects the information environment in which the agents reside on the blockchain. First, depending on detailed blockchain protocols, soliciting reports involves transferring certain transaction information to contacted record-keepers, changing σ_K.[44] Second, even with encrypted content information, the act of contacting conveys information (denoted by $\mathbf{1}_k$). In the context of an industrial organization framework analyzed in Section 2, this renders the aggregate economic activities public information if all agents are contacted, which makes collusion easier and jeopardizes competition.

In conclusion, we have demonstrated the robustness in a large set linear models of the trade-off between greater decentralization to improve consensus quality and lesser decentralization to reduce information distribution.

Appendix B. Derivations and Proofs

Proof of Proposition 2.1

Proof. In a competitive equilibrium, each seller lowers his or her price until competitors quit. If $\pi q_C < \max\{q_A, q_B\}$, at least one of the incumbents always competes to lower the price to μ to entice the customer this period and prevent the enhanced future competition had C entered in this period. Without a reputation of being authentic, an authentic C can only entice a customer if buyers show up and $\pi q_C \geq \max\{q_A, q_B\}$.

Because C does not have a capacity to bear loss at the point of entry, C cannot charge a penetration price below production cost μ and entice customers when $\pi q_{C,t}\mathbb{I}_t < \max\{q_{A,t}, q_{B,t}\}$. Even when $\pi q_{C,t}\mathbb{I}_t \geq \max\{q_{A,t}, q_{B,t}\}$, C may not be able to enter if the incumbents have deep pockets and can engage in predatory pricing. ■

[44] Recall the example of Corda's validating model in Section 1.4.

Proof of Lemma 2.2

Proof. We use q_i and q interchangeably in various places in the proof to denote the quality of a generic seller i. Let $V^+(q_i, q_{-i})$ be the present value of payoff to a seller with realized quality q_i in the collusion phase. In the collusion phase, buyers are indifferent between different sellers.

Let V^- be the present value of payoff to a seller before the realization of type in the first period of punishment phase. According to the collusion strategy, the continuation values satisfy

$$V^+(q_i, q_{-i}) = \lambda(f(q_i, q_{-i})(q_i - \mu) + \delta V^+) + (1-\lambda)\delta V^-, \tag{A7}$$

$$V^-(q_i, q_{-i}) = \lambda E[(q_i - \max_{j \neq i} q_j)^+] \frac{1-\delta^T}{1-\delta} + \delta^T V^+. \tag{A8}$$

For the strategy to be an equilibrium, we need to verify, by the one-shot deviation principal, that a seller does not have incentive to unilaterally deviate. This is obvious in the punishment phase, since it is a Bertrand equilibrium. In the collusion phase, to prevent deviation, we need

$$\forall q, V^+(q) \geq \lambda((q-\mu) + \delta V^-) + (1-\lambda)\delta V^-. \tag{A9}$$

Denote $V^+(q_i) = E_{q_{-i}}[V^+(q_i, q_{-i})]$, $f(q_i) = E_{q_{-i}}[f(q_i, q_{-i})]$. Integrating (A7), we have

$$V^+(q) = \lambda(f(q)(q-\mu) + \delta V^+) + (1-\lambda)\delta V^-, \tag{A10}$$

$$V^+ = \lambda(E[f(q)(q-\mu)] + \delta V^+) + (1-\lambda)\delta V^-. \tag{A11}$$

With (A9)–(A11), we have

$$\delta(V^+ - V^-) \geq (1 - f(q))(q-\mu), \forall q \in [\underline{q}, \bar{q}]. \tag{A12}$$

From (A8) to (A11), we solve for $(V^+ - V^-)$. Plugging this into the above equation, we obtain the range of discount factors that support the collusion strategy as an equilibrium:

$$\delta\lambda\left(1-\delta^T\right)(M_1 - M_2) \geq M_3 1 - \lambda\delta - (1-\lambda)\delta^{T+1}, \tag{A13}$$

where M_1, M_2, and M_3 are as defined in the statement of the lemma. ■

Proof of Proposition 2.3

Proof. Since M_1 is the expected stage-game collusion rent to a seller, and M_2 is her payoff in a competitive stage-game equilibrium, we have $M_1 > M_2$. Moreover, $M_1 + M_3 > \mathbb{E}[q] - \mu$, thus $\frac{1}{\lambda}\frac{M_3}{M_1+M_3-M_2} > \frac{1}{\lambda}\frac{\mathbb{E}[q]-\mu-M_1}{\mathbb{E}[q]-\mu-M_2} > 0$. Because the least-upper-bound property (and its implied greatest-lower-bound property) holds, the infimum exists. ■

Proof of Proposition 2.4

Proof. Since the payment can be contingent on completion of service, the authentic type can be separated out from fraudulent type by the following smart contract: The buyer pays the seller p^s conditional on the success of service, otherwise pays zero (or an infinitesimally small negative amount). The fraudulent type cannot afford to imitate the good type, because she can never complete the service and receive the payment. Consequently, she does not enter and never entices customers. The authentic entrant can entice buyers (if present), if $q_C \geq \max\{q_A, q_B\}$. Then she can charge payment $p^s = \frac{\mu + (q_C - \max\{q_A, q_B\})}{q_C}$ contingent on completion of service, and zero upon failure, to break the fraudulent type's indifference, because there is a tiny cost for entry and the fraudulent type would never enter since she will never be paid.

Given the smart contract allows authentic C to costlessly separate. A, B, and C essentially compete based on $\mathbf{q}$. Any predatory behaviors would only incur losses for the current period without improving future continuation value as future $\mathbf{q}$ is i.i.d. Therefore, there would not be any predatory (or penetration) pricing.

Finally, for collusive equilibria, if A and B collude, they must be charging a weakly higher price, which enables C to entice the first customer earlier. ■

Proof of Proposition 2.5

Proof. Again, we use q_i and q interchangeably in various places in the proof to denote the quality of a generic seller i. It is easy to derive

$$V^+(q_i,q_{-i})=\lambda(f(q_i,q_{-i})(q_i-\mu)+\delta V^+)+(1-\lambda)\delta V^+, \tag{A14}$$

$$V^+=\lambda(E[f(q)(q-\mu)]+\delta V^+)+(1-\lambda)\delta V^+, \tag{A15}$$

$$V^-=\lambda E[(q_i-q_{-i})^+]\frac{1-\delta^T}{1-\delta}+\delta^T V^+, \tag{A16}$$

$$\forall q, V^+(q)\geq\lambda((q-\mu)+\delta V^-)+(1-\lambda)\delta V^+. \tag{A17}$$

Collusion can be supported if

$$\delta\lambda(M_1-M_2)\left(1-\delta^T\right)\geq M_3(1-\delta), \tag{A18}$$

where $M_1\equiv\mathbb{E}[f(q_i)(q_i-\mu)]$, $M_2\equiv\mathbb{E}[(q_i-q_{-i})^+]$, $M_3\equiv\max_{\{q_i\in[\underline{q},\overline{q}]\}}[(1-f(q_i))(q_i-\mu)]$, $f(q_i)\equiv\mathbb{E}_{q_{-i}}[f(q_i,q_{-i})]$.

Compared to tacit collusion without blockchain, the only difference in the above recursive equations is that the punishment phase is not trigged if the buyers do not show up; that is, the corresponding part of the continuation value is $(1-\lambda)\delta V^+$ instead of $(1-\lambda)\delta V^-$.

We show that whenever (7) is satisfied, so is (A18). This is equivalent to showing

$$1-\lambda\delta-(1-\lambda)\delta^{T+1}>1-\delta, \tag{A19}$$

which is equivalent to

$$\delta(1-\delta^T)(1-\lambda)>0. \tag{A20}$$

Now for the second part of the proposition: note that collusion being impossible when $\delta<\delta_o^{Traditional}$ is already proven in Proposition 2.3.

To show there could be when $\delta\geq\inf_f\{\delta_{(\infty,f)}^{Blockchain2}\}$, we note again by the least upper bound property, $\inf_f\{\delta_{(\infty,f)}^{Blockchain2}\}$ is well defined and positive. To show one collusion equilibrium exists, we only need to search within the class of f such that $f(q)$ is continuous function; that is, $f\in\mathcal{C}([0,1])$. Because $\mathcal{C}([0,1])$ is a locally convex Hausdorff space that is complete, there exists a sequence of allocation functions that gets infinitely close to the infimum. This means for any $\delta\geq\delta_o^{Blockchain2}$, we can find a (T,f) that can be sustained. This holds true for our later discussions on infimum and supremum as well. ■

Proof of Lemma 2.6

Proof.

$$V^+(q_i,q_{-i})=\lambda(\hat{f}(q_i,q_{-i})(q_i-\mu)+\delta V^+)+(1-\lambda)\delta V^+, \tag{A21}$$

$$V^+=\lambda(E[\hat{f}(q)(q-\mu)]+\delta V^+)+(1-\lambda)\delta V^+, \tag{A22}$$

$$V^-=\lambda E[(q_i-\max_{j\neq i}q_j)^+]\frac{1-\delta^T}{1-\delta}+\delta^T V^+, \tag{A23}$$

$$\forall q, V^+(q)\geq\lambda((q-\mu)+\delta V^-)+(1-\lambda)\delta V^+. \tag{A24}$$

Note $V^+-V^-=\frac{\lambda\left(\hat{M}_1-\hat{M}_2\right)\left(1-\delta^T\right)}{1-\delta}$. ■

Proof of Theorem 2.7 and Discussion

Proof. Again, $\frac{\hat{M}_3}{\hat{M}_3+\lambda(\hat{M}_1-\hat{M}_2)} \in (0,1)$ for all $\hat{f}$. Therefore by the least upper bound property, $\sup_f\{\delta^{Blockchain3}_{(\infty,\hat{f})}\}$ exists and is less than 1. When $\delta > \sup_f\{\delta^{Blockchain3}_{(\infty,\hat{f})}\}$, any $(\infty,\hat{f})$ can be sustained, including the one allocating buyers to the highest quality seller and the one allocating to the lowest-quality seller. Note that for any realization of seller qualities, the best-quality seller with blockchain is better than the best-quality incumbent, we could attain higher or lower welfare; similarly, the worst-quality seller with blockchain and entry is worse than the worst-quality incumbent, so welfare could be lower. Moreover, since competitive stage game is always on the equilibrium path without blockchain, the consumer surplus is positive. With blockchain sellers can extract full rent, so lower consumer surplus is attainable. Moreover, by introducing some punishing on the equilibrium path or lowering the collusion price under blockchain, consumer surplus can be increased to be higher than that in the traditional world (e.g., under perfect competition). Thus, consumer surplus also can be higher with blockchain.

Note for the corollary, the most collusive equilibria maximize welfare, but sellers fully extract all welfare surplus. This equilibrium can be sustained, and the results follow. ■

We note $\hat{M}_2$ is simply the payoff to a seller in a competitive stage game, and is almost surely less than M_1 which is the expected stage game payoff under collusion. Therefore, $\inf_{\hat{f}}\{\delta^{Blockchain3}_{(\infty,\hat{f})}\} = \inf_{\hat{f}} \frac{\hat{M}_3}{\hat{M}_3+\lambda(\hat{M}_1-\hat{M}_2)}$. But $\frac{\hat{M}_3}{\hat{M}_3+\lambda(\hat{M}_1-\hat{M}_2)} \in (0,1)$ for all $\hat{f}$. Again, by the greatest-lower bound property of real-numbered set, the threshold is well defined and smaller than 1.

When $\delta > \delta^{Blockchain3}_{o}$, the blockchain can support at least one collusion equilibrium that fully extracts consumer surplus (with no punishment phase on equilibrium path). This is because, again, there is a sequence of allocation function $\hat{f}$ within in the complete function space $\mathcal{C}[0,1]$ that arbitrarily approaches the infimum. Without blockchain, consumer surplus is never zero as competitive stage game is always on the equilibrium path. Note that even with collusion, there has to be punishment on the equilibrium path. Thus consumer surplus is always positive. The conclusion follows.

Proof of Corollary 2.8

Proof. For $m > 2$ in general, the previous proposition's proof still applies and $\delta^{Blockchain,m}_{o} < 1$. For $n \geq 2$, when $\lambda < \frac{n-1}{n}$, we have $\frac{1}{\lambda}\frac{M_3}{M_1+M_3-M_2} > \frac{1}{\lambda}\frac{\mathbb{E}[q]-\mu-M_1}{\mathbb{E}[q]-\mu-M_2} > \frac{1}{\lambda}\frac{\mathbb{E}[q]-\mu-\frac{1}{n}(\mathbb{E}[q]-\mu)}{\mathbb{E}[q]-\mu} > 1$. Therefore there cannot be collusion with $n \geq 2$ in the traditional world. The corollary follows. ■

Proof of Lemma 3.2

Proof. The information asymmetry here is that the buyer does not know a seller's type. Therefore the buyer makes his decision based on his perception of the type $\hat{q}_i$ and the price charged p_i. To be specific, the buyer maximizes his payoff by choosing the seller who can deliver the highest expected utility:

$$\max_i \hat{q}_i - p_i. \tag{A25}$$

If the payoff by choosing any seller is negative, the buyer will step out of the market.

Suppose there is a separating equilibrium where the pricing schedule is $p(q)$ and the probability for a seller with type q to be chosen is $f(q)$. For a seller with type q, she can pretend to be type $\tilde{q}$ by posting the price $p(\tilde{q})$. The seller's expected payoff by doing so is

$$f(\tilde{q})(p(\tilde{q})-\mu). \tag{A26}$$

Every seller will choose the same $\tilde{q}$ to maximize (A26), which does not depend on q. Therefore, the separating equilibrium does not exist.

Since there is no separating equilibrium, we consider the pooling equilibrium. Without a reputation system, the buyer's perception of each seller's type is the mean $\mathbb{E}[q]$.

This is similar to Bertrand competition. Suppose the lower price of the two firms is higher than μ, say, $p_1 > \mu$. Consider a deviation for the second firm to the price $p_2 = p_1 - \epsilon > \mu$, which increases the profit of the second firm. Therefore, in equilibrium, we must have $p_1 = p_2 = \mu$. Since we always assume the buyer's decision rule is nondiscriminating, the tie is broken randomly. Therefore, the ex ante consumer surplus and social welfare is $\mathbb{E}[q_i u - \mu]$, where the expectation is taken over the realization of q_i. This yields $\mathbb{E}[q] - \mu$. As a remark outside our parameter assumption, if the cost is so high that $\mu > \mathbb{E}[q]$, ex ante utility for the buyer is negative, and the buyer will stay out of the market; that is, the market breaks down. ■

Proof of Proposition 3.3

Proof. We first show that using $\mathbb{P}^*$ is an equilibrium. We then prove that no other equilibrium exists. The proof resembles the argument in DeMarzo et al. (2005) on how the flattest securities are always used in an equilibrium of informal auctions with security bids. However, because the sellers can always offer smart contracts that make the buyers' payoff insensitive to the seller's type, we do not need to worry about equilibrium refinement. Readers who are familiar with DeMarzo et al. (2005) should skip the detailed proof below.

With $\mathbb{P}^*$, buyers obtain utility $1 - p$ regardless of the service outcome. Conversely, any smart contract that makes buyers' payoff insensitive to seller type has to be of the form $\mathbb{P}^*$. Given that the buyer taking an offer $(p, p-1, 0)$ obtains $1 - p$ utility, the setup is equivalent to a first-price auction where the buyers are the auctioneers who allocate the business opportunity, and sellers are bidders who bid cash $1 - p$. The buyers go to the seller with the lowest p. From the auction literature, a unique symmetric equilibrium with cash bids exists. Therefore, there is a unique equilibrium when restricting smart contracts to $\mathbb{P}^*$, implying that there is no profitable deviation using contracts that give buyers payoff insensitive to seller type. The equilibrium offer of type q follows the solution of symmetric equilibrium of first price auctions (Krishna 2009) and is given by the p_q that solves

$$1 - p_q = \mathbb{E}\left[q^{(1),N-1} - \mu | q^{(1),N-1} < q\right] = q - \mu - \int_{\underline{q}}^{q} \left[\frac{\Phi(q')}{\Phi(q)}\right]^{N-1} dq', \tag{A27}$$

where $q^{(1),N-1}$ is the highest realized quality among other $N-1$ sellers. We note the expression is increasing in q, thus buyers all choose the highest-quality seller. Substituting $N = 3$ (one authentic entrant and two incumbents) gives the expression in the proposition.

Now suppose this equilibrium breaks down when we allow for smart contracts beyond $\mathbb{P}^*$, then there must be a profitable deviation by a type q to a quality-sensitive smart contract $\mathbb{P}_q$ such that $Pr(B(\mathbb{P}_q))S_q(\mathbb{P}_q) > Pr(B_q(\mathbb{P}_q^*))S_q(\mathbb{P}_q^*)$, where $Pr(B)$ is the probability of enticing customers when buyers believe that they can obtain utility B, and $B(\mathbb{P}_q)$ is the buyers' perceived value of the deviation contract. Denote the set of types that find it profitable to deviate to $\mathbb{P}_q$ by Q. Then $B(\mathbb{P}_q) \in B(\mathbb{P}_q(Q))$. Therefore, $\exists q' \in Q$ (possibly q) such that $q' - S_{q'}(\mathbb{P}_q) = B(\mathbb{P}_q(q')) > B(\mathbb{P}_q)$. Consider the deviation by type q' to $(p', p'-1, 0)$, where $p' = 1 - q' + S_{q'}(\mathbb{P}_q)$. Then the probability of winning is higher than q' deviating to use $\mathbb{P}_q$, and the payoff conditional on enticing customers are both $S'_q(\mathbb{P}_q)$, implying that if it is profitable for q' to deviate to $\mathbb{P}_q$ (which is true since $q' \in Q$). It is also profitable for q' to deviate to the contract $(p', p'-1, 0)$. However, this contradicts the fact that there is no profitable deviation using contracts that make buyers' payoff insensitive to seller type. Therefore, we conclude that the equilibrium described in the previous paragraph is an equilibrium even when we allow general smart contract forms.

Next, we show that the above equilibrium is essentially unique for the game; that is, all other symmetric equilibria have the same payoffs.

We first argue that if a smart contract $\mathbb{P}$ is offered in an equilibrium and is quality sensitive, then at most one type uses it. Suppose otherwise and more than one type use it. Let the lowest and highest types offering the smart contract be q_L and q_H, then $B(\mathbb{P})=B_{q^*}(\mathbb{P}_{q^*})$ for some $q^*\in(q_L,q_H)$. However, $\mathbb{P}$ is increasing in quality because $p^s > p^{sd}$. Consequently, q_L would find it profitable to deviate to offering $(p, p-1, 0)$ where $p=1-B(\mathbb{P})$, contradicting that in equilibrium both q_L offers $\mathbb{P}$. Therefore, at most one type uses $\mathbb{P}$.

Let the type be q, then $B(\mathbb{P}_q)=B_q(\mathbb{P}_q)$. This implies the allocation and payoffs are unaltered if type q replaces the offer by $(p_q, p_q-1, 0)$ where $p_q=1-B(\mathbb{P}_q)$. This is because, $S_q(\mathbb{P}_q)=q-B_q(\mathbb{P}_q)=q-(1-p_q)$.

Because each type q is solving the same optimization problem used in the case in which we restrict to $\mathbb{P}^*$, we have shown that any unrestricted equilibrium is payoff equivalent to the unique and monotone equilibrium with restriction of smart contracts to $\mathbb{P}^*$.

Next, the smart contract $(p_q^s, p_q^{sd}, 0)$ used by type q in such an essentially unique equilibrium gives type q the same value as $(p_q, p_q-1, 0)$. That is, $qp_q^s+(1-q)p_q^{sd}=qp_q+(1-q)p_q$. Because in the equilibrium with $\mathbb{P}^*$, a seller's expected payoff is differentiable q for all q, by a standard envelope argument, taking derivatives in the unrestricted equilibrium yields $p_q^s-p_q^{sd}=0$. From this we conclude that all possible equilibria are payoff equivalent to the unique equilibrium when restricting smart contracts to $\mathbb{P}^*$ and the smart contracts used are also in $\mathbb{P}^*$. This means that no equilibrium exists other than the one described in the second paragraph of the proof.

Finally, we remark that for incumbents, they can use $p^f\neq 0$ without affecting the payoffs and equilibrium outcomes. That is why we say the equilibrium is only essentially unique. ■

References

Abadi, J., and M. Brunnermeier. 2018. Blockchain economics. Working Paper.

Allison, I. 2017. Maersk and IBM want 10 million shipping containers on the global supply blockchain by year-end. *International Business Times*, March 8. https://www.ibtimes.co.uk/maersk-ibm-aim-get-10-million-shipping-containers-onto-global-supply-blockchain-by-year-end-1609778.

Athey, S., and K. Bagwell. 2001. Optimal collusion with private information. *RAND Journal of Economics* 32:428–65.

Aune, R. T., M. O'Hara, and O. Slama. 2017. Footprints on the Blockchain: Trading and Information Leakage in Distributed Ledgers. *Journal of Trading* 12:5–13.

Baron, D. P., and R. B. Myerson. 1982. Regulating a monopolist with unknown costs. *Econometrica* 50:911–30.

Bartoletti, M., and L. Pompianu. 2017. An empirical analysis of smart contracts: Platforms, applications, and design patterns. In *Financial cryptography and data security*, eds. M. Brenner, K. Rohloff, J. Bonneau, A. Miller, P. Y. Ryan, V. Teague, A. Bracciali, M. Sala, F. Pintore, and M. Jakobsson, 494–509. Cham, UK: Springer International Publishing.

Bessembinder, H., and W. Maxwell. 2008. Markets transparency and the corporate bond market. *Journal of Economic Perspectives* 22:217–34.

Biais, B., C. Bisière, M. Bouvard, and C. Casamatta. 2019. The blockchain folk theorem. *Review of Financial Studies*, 32:1662–715.

BlockchainNews. 2017. UPS-backed blockchain consortium seeks to disrupt the freight and logistics industry. *CCN*, November 17. https://www.ccn.com/bita-looking-disrupt-freight-logistics-industry/.

Bloomfield, R., and M. O'Hara. 1999. Market transparency: who wins and who loses? *Review of Financial Studies* 12:5–35.

Böhme, R., N. Christin, B. Edelman, and T. Moore. 2015. Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives* 29:213–38.

Bourveau, T., G. She, and A. Zaldokas. 2017. Naughty firms, noisy disclosure. Working Paper.

Buterin, V. 2014. Ethereum: A next-generation smart contract and decentralized application platform. White Paper.

Cao, S., L. W. Cong, and B. Yang. 2018. Auditing and blockchains: Pricing, misstatements, and regulation. Working Paper.

Chapman, J., R. Garratt, S. Hendry, A. McCormack, and W. McMahon. 2017. Project Jasper: Are distributed wholesale payment systems feasible yet? Working Paper.

Chiu, J., and T. Koeppl. 2019. Blockchain-based settlement for asset trading. *Review of Financial Studies*, 32:1716–53.

Cong, L. W. 2017. Auctions of real options. Working Paper.

Cong, L. W., Z. He, and J. Li. 2018a. Decentralized mining in centralized pools. Working Paper.

Cong, L. W., Y. Li, and N. Wang. 2018b. Tokenomics: Dynamic adoption and valuation. Working Paper.

Cong, L. W., Y. Li, and N. Wang. 2018c. Token-based corporate finance. Working Paper.

de Vilaca Burgos, A., J. D. de Oliveira Filho, M. V. C. Suares, and R. S. de Almeida. 2017. Distributed ledger technical research in Central Bank of Brazil. Working Paper.

DeMarzo, P., and D. Duffie. 1999. A liquidity-based model of security design. *Econometrica* 67:65–99.

DeMarzo, P., I. Kremer, and A. Skrzypacz. 2005. Bidding with Securities: Auctions and Security Design. *American Economic Review* 95:936–59.

Easley, D., M. O'Hara, and S. Basu. 2017. From mining to markets: The evolution of bitcoin transaction fees. Working Paper.

The Economist. 2015. The trust machine. October 31, https://www.economist.com/leaders/2015/10/31/the-trust-machine.

———. 2017. A yen for plastic. November 4.

Eyal, I., and E. G. Sirer. 2014. Majority is not enough: Bitcoin mining is vulnerable. In *International Conference on Financial Cryptography and Data Security*, 436–54. New York: Springer.

Fudenberg, D., and E. Maskin. 1986. The folk theorem in repeated games with discounting or with incomplete information. *Econometrica* 54:533–54.

Fung, B. 2014. Marc Andreessen: In 20 years, well talk about Bitcoin like we talk about the Internet today. *Washington Post,* May 21. https://www.washingtonpost.com/news/the-switch/wp/2014/05/21/marc-andreessen-in-20-years-well-talk-about-bitcoin-like-we-talk-about-the-internet-today/?noredirectōn&utm_term=.24553687a085.

Gillis, M., and A. Trusca. 2017. 'Not there yet': Bank of Canada experiments with blockchain wholesale payment system. *CyberLex,* June 19. https://www.mccarthy.ca/en/insights/blogs/snipits/not-there-yet-bank-canada-experiments-blockchain-wholesale-payment-system.

Goldstein, M. A., E. S. Hotchkiss, and E. R. Sirri. 2006. Transparency and liquidity: A controlled experiment on corporate bonds. *Review of Financial Studies* 20:235–73.

Green, E. J., and R. H. Porter. 1984. Noncooperative collusion under imperfect price information. *Econometrica* 56:87–100.

Haber, S., and W. S. Stornetta. 1990. How to time-stamp a digital document. In *Conference on the Theory and Application of Cryptography*, 437–55. New York: Springer.

Hackett, R. 2017. Maersk and Microsoft tested a blockchain for shipping insurance. *Fortune Finance,* Sept 5. http://fortune.com/2017/09/05/maersk-blockchain-insurance/.

Hart, O. 1995. *Firms, contracts, and financial structure*. London: Clarendon Press.

Hart, O., and J. Moore. 1988. Incomplete contracts and renegotiation. *Econometrica* 56:755–85.

———. 1995. Debt and seniority: An analysis of the role of hard claims in constraining management. *American Economic Review* 85:567–85.

Harvey, C. R. 2016. Cryptofinance. Working Paper.

Haswell, H. 2018. Maersk and IBM introduce TradeLens blockchain shipping solution. *IBM News Room,* August 9. https://newsroom.ibm.com/2018-08-09-Maersk-and-IBM-Introduce-TradeLens-Blockchain-Shipping-Solution.

Higgins, S. 2017a. IBM unveils blockchain platform for oil trade finance. *Coindesk,* March 28. http://www.coindesk.com/ibm-blockchain-platform-oil-trade-finance/.

———. 2017b. Walmart, JD.com back blockchain food tracking effort in China. *CoinDesk,* December 14. https://www.coindesk.com/walmart-jd-com-back-blockchain-food-tracking-effort-china.

Huberman, G., J. D. Leshno, and C. C. Moallemi. 2017. Monopoly without a monopolist: An economic analysis of the bitcoin payment system. Working Paper.

Innes, R. D. 1990. Limited liability and incentive contracting with ex-ante action choices. *Journal of Economic Theory* 52:45–67.

Jeffries, A. 2018. Blockchain is meaningless. *Verge,* March 7. https://www.theverge.com/2018/3/7/17091766/blockchain-bitcoin-ethereum-cryptocurrency-meaning.

Kaminska, I. 2015. Exposing the 'if we call it a blockchain, perhaps it won't be deemed a cartel?' tactic. *Financial Times,* May 11. https://hackernoon.com/ten-years-in-nobody-has-come-up-with-a-use-case-for-blockchain-ee98c180100.

Khapko, M., and M. Zoican. 2018. How fast should trades settle. Working Paper.

Krishna, V. 2009. *Auction theory*. Hoboken, NJ: Academic Press.

Kroll, J. A., I. C. Davey, and E. W. Felten. 2013. The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In *Proceedings of WEIS*, vol. 2013.

Lauslahti, K., J. Mattila, T. Seppälä, et al. 2016. Smart Contracts–How will blockchain technology affect contractual practices? Technical Report, The Research Institute of the Finnish Economy.

Malinova, K., and A. Park. 2018. Market Design for Trading with Blockchain Technology. Working Paper.

Miller, D. A. 2011. Robust collusion with private information. *Review of Economic Studies* 79:778–811.

Nakamoto, S. 2008. Bitcoin: A peer-to-peer electronic cash system. Working Paper.

Narayanan, A., J. Bonneau, E. Felten, A. Miller, and S. Goldfeder. 2016. *Bitcoin and cryptocurrency technologies*. Princeton, NJ: Princeton University Press.

Narayanan, A., and J. Clark. 2017. Bitcoin's academic pedigree. *Communications of the ACM* 60:36–45.

Nayak, K., S. Kumar, A. Miller, and E. Shi. 2016. Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In *Security and Privacy (EuroS&P), 2016 IEEE European Symposium*, 305–20. Piscataway, NJ: IEEE.

Palmer, D. 2018. R3 pilots blockchain trade finance platform with global banks. *Coindesk,* February 21. https://www.coindesk.com/r3-pilots-blockchain-trade-finance-platform-with-global-banks/.

Porter, R. H. 1983. Optimal cartel trigger price strategies. *Journal of Economic Theory* 29:313–38.

Shin, L. 2017. Why Nasdaq is even more optimistic about blockchain than it was 3 years ago. *Forbes,* Feb 21. https://www.forbes.com/sites/laurashin/2017/02/21/why-nasdaq-is-even-more-optimistic-about-blockchain-than-it-was-3-years-ago/#234a83271a26.

Stinchcombe, K. 2017. Ten years in, nobody has come up with a use for blockchain. *Hackernoon,* December 22. https://hackernoon.com/ten-years-in-nobody-has-come-up-with-a-use-case-for-blockchain-ee98c180100.

Szabo, N. 1997. Formalizing and securing relationships on public networks. *First Monday* 2.

———. 1998. Secure property titles with owner authority. Online at http://szabo.best.vwh.net/securetitle.html.

Tapscott, D., and A. Tapscott. 2016. *Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world*. New York: Penguin.

Taylor, C. 2016. Ornua involved in groundbreaking blockchain transaction. *Irish Times,* September 7. https://www.irishtimes.com/business/technology/ornua-involved-in-groundbreaking-blockchain-transaction-1.2782748.

Terekhova, M. 2017. Credit Suisse-led blockchain solution makes progress. *Business Insider,* August 23. https://www.businessinsider.com/credit-suisse-led-blockchain-solution-makes-progress-2017-8.

Tinn, K. 2018. Blockchain and the future of optimal financing contracts. Working Paper.

Tirole, J. 1988. *The theory of industrial organization*. Cambridge: MIT Press.

———. 1999. Incomplete contracts: Where do we stand? *Econometrica* 67:741–81.

Turing, A. M. 1937. On computable numbers, with an application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society* 2:230–65.

Weiss, M., and E. Corsi. 2017. Bitfury: Blockchain for government. *HBS Case Study* January 12:818–031.

Yermack, D. 2017. Corporate governance and blockchains. *Review of Finance* 21:7–31.

Zurrer, R. 2017. Keepers—Workers that maintain blockchain networks. *Medium,* August 5. https://medium.com/rzurrer/keepers-workers-that-maintain-blockchain-networks-a40182615b66.